

Ein eigener Mailserver zu Hause im LAN

Bernd Strößenreuther
<linux-cafe@stroessenreuther.net>

Linux-Cafe 2026-04-15

Lizenz

Sie dürfen die Text-Inhalte dieses Dokument verwenden unter den Bedingungen der Creative Commons Lizenz:

<http://creativecommons.org/licenses/by-nc-sa/3.0/de/>

Alle nicht separat gekennzeichneten Grafiken und Icons von OpenClipArt.org - "released to the public domain".

Agenda

- **Wie funktioniert eMail eigentlich?**
- **Ein Mailserver zu Hause im LAN: Warum das denn!?**
- **Mögliche Einsatz-Szenarien:**
 - Nur als Mail-Relay – keine Mails speichern
 - Mails im LAN zentral vorhalten
- **Die Komponenten:**
 - Postfix / nullmailer / Dovecot / fetchmail / procmail
- **Worüber wir nicht sprechen werden:**
 - Rspamd / Amavis / vacation / Webmailer / Certbot
- **Eure Fragen**

Wie funktioniert eMail eigentlich?

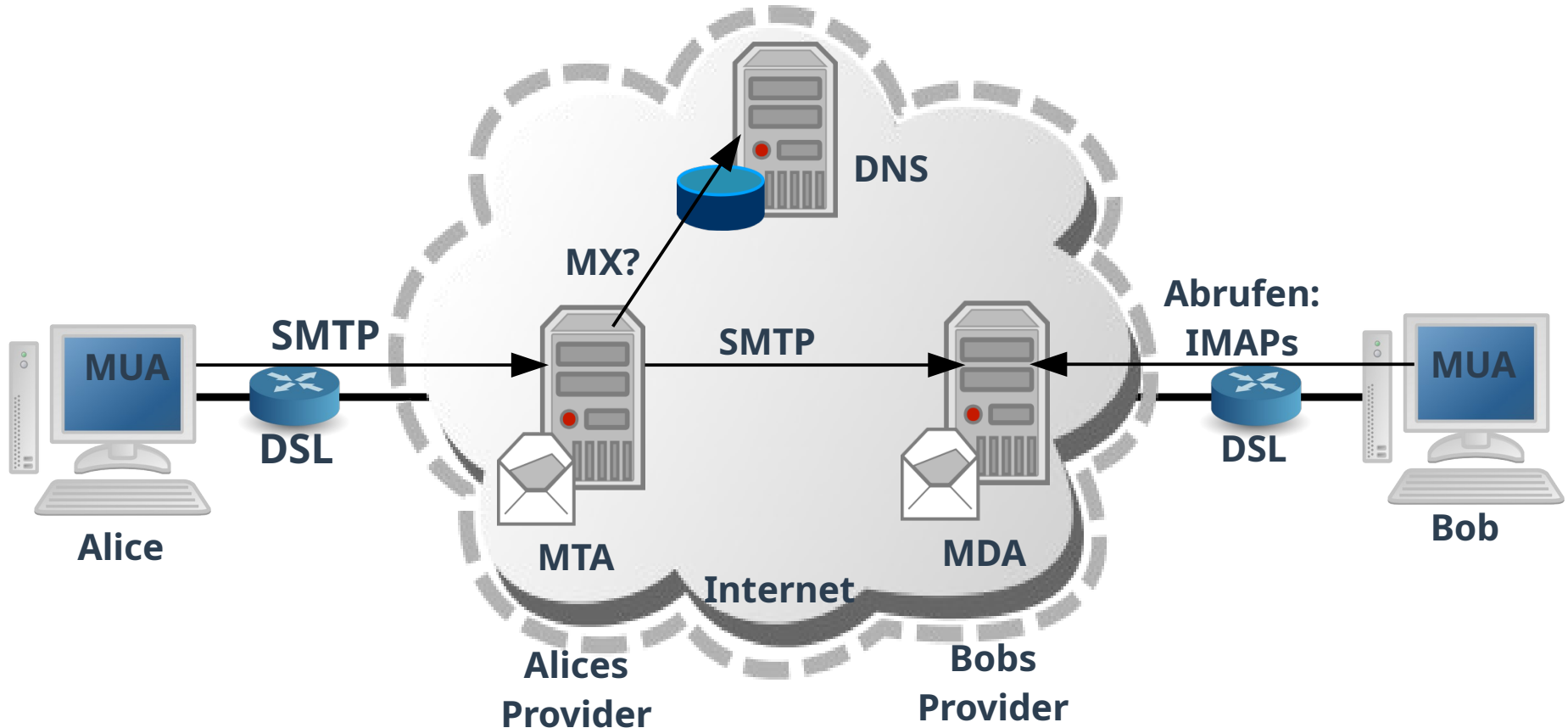
- **Protokolle**

- SMTP
- IMAPs
- (POP3s)

- **Beteiligte Systeme**

- MUA: Mail User Agent (z. B. Thunderbird, KMail, ...)
- MTA: Mail Transfer Agent (z. B. Postfix, Sendmail, ...)
- MDA: Mail Delivery Agent (z. B. maildrop, procmail, ...)

Der "Standard-Weg" beim Heimnutzer



Ein Mailserver zu Hause: Warum das denn!?

Pro

- vereinfachte Konfiguration auf sämtlichen Servern / Serverchen / Diensten im LAN
- mehr Daten-Autonomie
- Zentrale Datensicherung
- Erfahrung sammeln / eigenes Wissen erweitern

Contra

- Lass das doch jemanden machen, der sich damit auskennt!
- Mail-Provider bieten Redundanz
- Gute Mail-Provider bieten ebenfalls:
 - viel Speicherplatz zu fairen Preisen
 - tolle Features
 - DSGVO-konformes Hosting
 - und kümmern sich zeitnah um Security-Fixes

Einsatz-Szenario: Mail-Relay

Mail-Relay

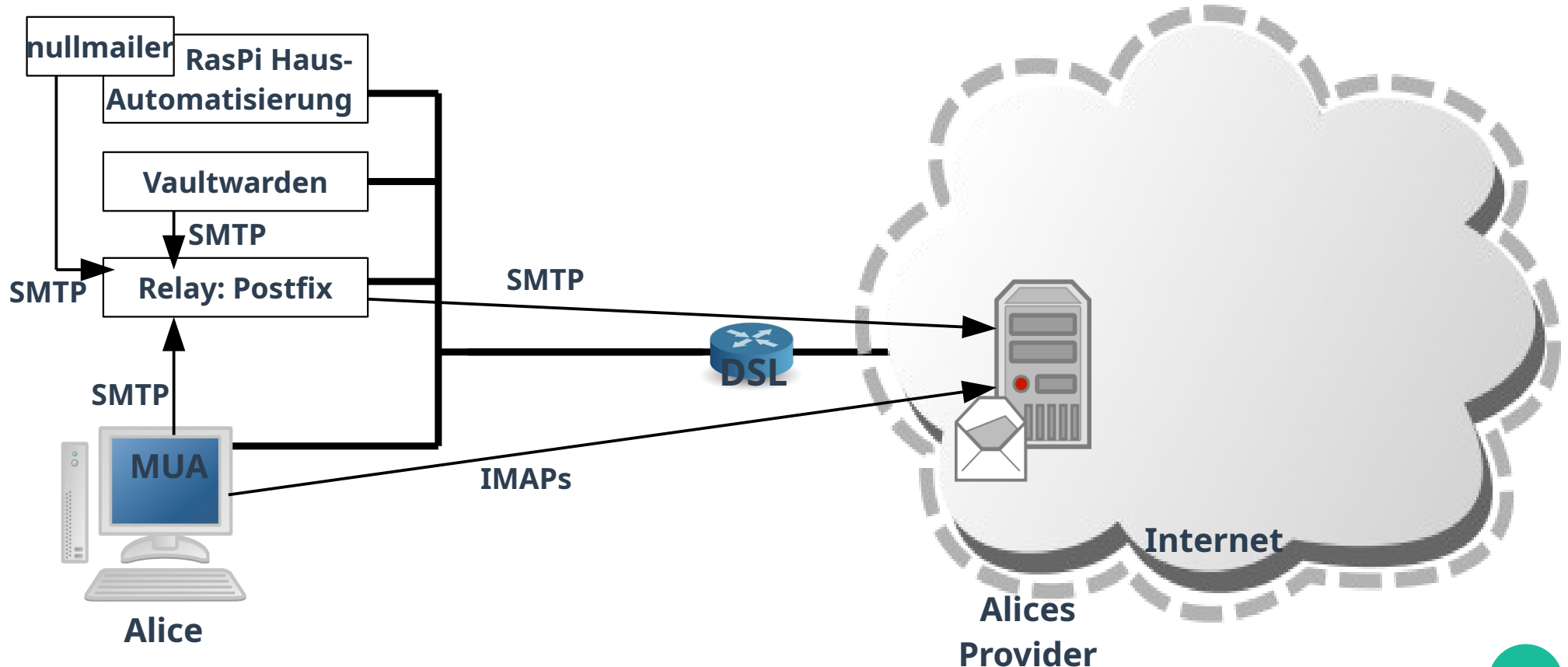
Herausforderung

- Mails der „kleinen Helferlein“
 - Pi-hole / Vaultwarden / Kodi / Fritz!Box / etc. aber auch Cron-Jobs oder eigene Scripte versenden Mails, laufen jedoch sehr verteilt im LAN
 - diese sollen einfach und zuverlässig beim richtigen User ankommen

Idee

- Ein zentrales Mail-Relay im LAN (z. B. Postfix) nimmt diese entgegen und leitet sie TLS-verschlüsselt an den finalen Mailserver weiter
 - alle „Mail-Produzenten“ schicken an das Mail-Relay
 - im OS des Mail-Produzenten ist maximal ein nullmailer oder ssmtp nötig

Alice hat ein Mail-Relay



Postfix zu Hause: Mails im LAN annehmen

- zumindest opportunistic TLS aktivieren (in `/etc/postfix/main.cf`)
`smtpd_tls_security_level = may`
- sofern alle „Mail-Produzenten“ STARTTLS unterstützen
`smtpd_tls_security_level = encrypt`
- Weitere wichtige Direktiven (in `/etc/postfix/main.cf`):
`smtpd_tls_*`
 - Zertifikate setzen
 - alte Ciphers ausschließen
 - Protokolle bis mindestens TLSv1.1 ausschließen

Postfix zu Hause: Wer darf was?

- **Von wem darf ich Mails annehmen?**

```
mynetworks = 192.168.127.0/24, 192.168.128.0/24, 192.168.178.1/32,  
127.0.0.0/8, [::1]/128, [fe80::]/10, [fd17:17:cafe::]/48
```

```
smtpd_recipient_restrictions = permit_mynetworks,reject_unauth_destination
```

Postfix zu Hause: Ausgehende Mails

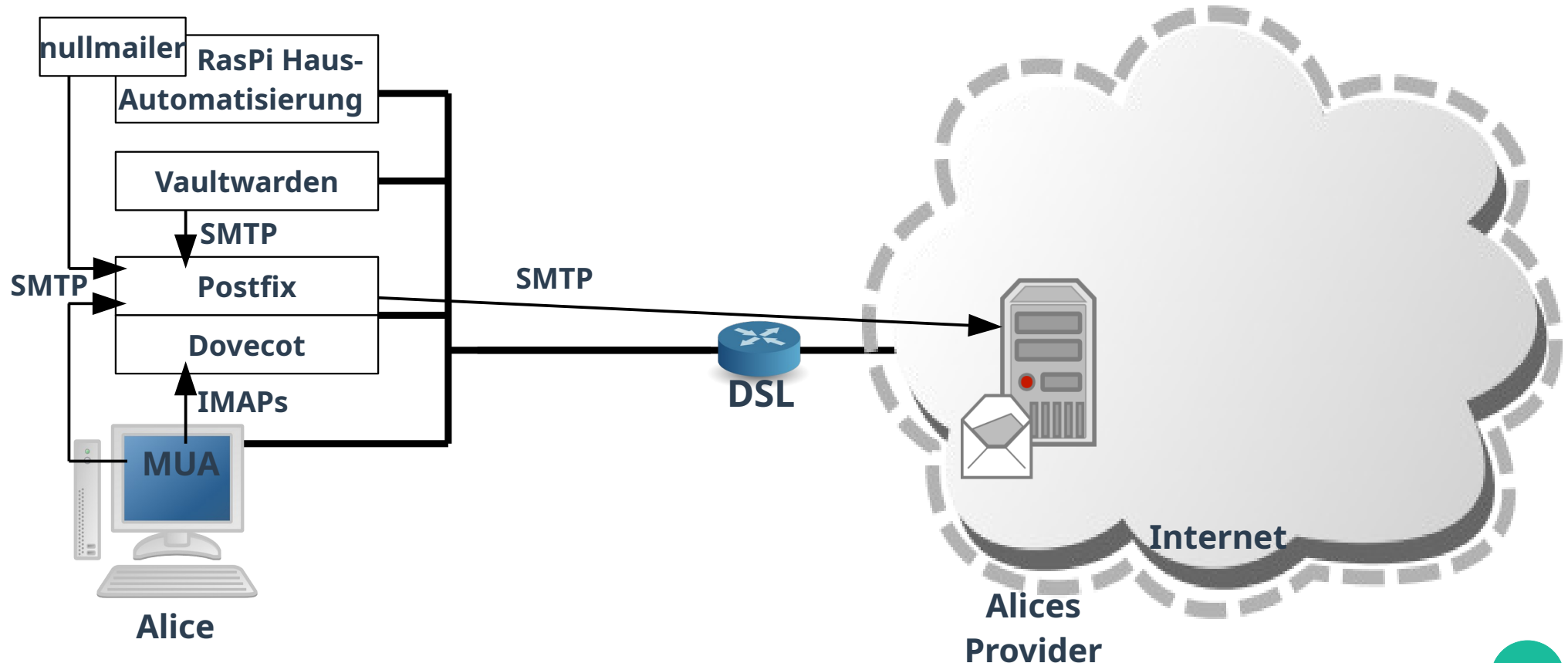
- Direkte Zustellung (laut MX-Record) ist aussichtslos! Ihr kommt aus einem Dialup-Range: Mails werden geblockt oder gefiltert!
- Mails immer beim SMTP-Server Eures Providers einliefern: SMTP-Auth nutzen

- Wichtige Direktiven (in /etc/postfix/main.cf):

```
relayhost = [mail.your-server.de]:587          # Beispiel: Hetzner
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd_upstream
smtp_use_tls = yes
smtp_tls_security_level = encrypt
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, !TLSv1.2
smtp_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1, !TLSv1.2
```

Einsatz-Szenario: Mails im LAN zentral vorhalten

Mails werden im LAN zentral vorgehalten



Domain

- Der Mailserver im LAN braucht eine Domain, für die er sich „zuständig“ fühlt
- Welche Domain soll ich verwenden?
Empfehlung in absteigender Reihenfolge
 - Eine eigene Domain oder eine Third-Level-Domain davon
 - Eine "geliehene" Third-Level-Domain, siehe z. B. <http://freedns.afraid.org/>
 - ggf. auch möglich: Eine Test-Domain nach RFC 2606:
 meinedomain.example
 meinedomain.test
 siehe auch <http://tools.ietf.org/html/rfc2606>
- Direktiven (in /etc/postfix/main.cf):
myhostname = mail.exercise.jumpingcrab.com
mydestination = exercise.jumpingcrab.com, \$myhostname, localhost.localdomain, localhost

Wir brauchen eMail-Postfächer

- Zu Hause wohl am einfachsten:
 - Pro Postfach einen Linux-User anlegen
 - Mails speichern im Home-Verzeichnis
 - Pro Postfach beliebig viele eMail-Adressen (`/etc/aliases`)
- Empfehlung: Im MailDir-Format speichern (vom mbox-Format wird explizit abgeraten!!)
- Wichtige Direktiven (in `/etc/postfix/main.cf`):
home_mailbox = Maildir/
mailbox_size_limit = 0
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = \$mydomain

Aliases

`#/etc/aliases`

```
root:          alice
webmaster:     alice
commander.spock: bob
```

- **anschließend:**
postmap /etc/aliases
- **oder:**
newaliases

Und wir brauchen IMAPs

- `apt install dovecot-imapd`
- `/etc/dovecot/dovecot.conf` für Dovecot 2.3

```
Listen = *, [::]
log_timestamp = "%Y-%m-%d %H:%M:%S "
mail_privileged_group = mail
mail_location = maildir:~/Maildir
passdb {
    driver = pam
}
protocols = imap
ssl_min_protocol = TLSv1.2
ssl_prefer_server_ciphers = yes
service auth {
    user = root
}
ssl_cert = </etc/letsencrypt/live/imap.exercise.jumpingcrab.com/fullchain.pem
ssl_key = </etc/letsencrypt/live/imap.exercise.jumpingcrab.com/privkey.pem
userdb {
    driver = passwd
}
```

Vorsicht bei Dovecot 2.4

- Die Konfiguration von Dovecot 2.4 unterscheidet sich deutlich von 2.3
- <https://dovecot.org/upgrader/> konvertiert diese für Euch

Eingehende eMails aus dem Internet: direkt

Direkte Zustellung zum Mailserver im LAN

- Port 25 nach außen offen
- MX-Record zeigt per Dyn-DNS da hin

Wichtig in diesem Fall:

- tagesaktueller Patch- und Konfigurationsstand
- kein Open Relay betreiben!!
- TLS mandatory
- Rspamd
- System sollte möglichst 24x7 online sein

Eingehende eMails per fetchmail

- Mails werden am Mailserver beim Provider empfangen
- fetchmail holt sie dort regelmäßig (POP3s / IMAPs) ab und stellt sie lokal per SMTP zu
- Um SPAM-Filter kümmert sich der Provider
- Der Provider hat redundante Systeme

```
# fetchmailrc

set postmaster "postmaster"
set bouncemail
set properties ""

poll mail.your-server.de
  proto POP3
  user "webmaster@jumpingcrab.com"
  password "FdspH3XNbo6bKEJgUCLv"
  is alice
  fetchall
  ssl
  sslcertck
  smtp host mail.exercise.jumpingcrab.com
```

Monitoring / Debugging

Nützlich für den angehenden Mailserver-Admin:

- `mailq`
→ **Mail-Queue anzeigen: noch nicht zugestellte Mails**
- `sendmail -q`
→ **neuer Zustellversuch für alle Mails in der Mail-Queue**
- `postsuper -d <queue_id>`
→ **Mail aus der Mail-Queue löschen**
- `/var/log/mail.log`
- `systemctl status dovecot.service`
- `systemctl status postfix.service`

Bonus-Features

Sortierungsregeln für Mails: procmail

```
~/home/alice/.forward
```

```
"| /usr/bin/procmail -t"
```

```
~/home/alice/.procmailrc
```

```
DEFAULT="$HOME/Maildir/"
```

```
LOGABSTRACT=all
```

```
LOGFILE=$HOME/.procmail.log/procmail.log
```

```
:0:
```

```
* ^From: .*fritz.box@
```

```
$HOME/Maildir/.Incoming.System-Meldungen/
```

```
:0:
```

```
* ^X-Spam-Status: Yes
```

```
$HOME/Maildir/.Incoming.Spam/
```

```
:0:
```

```
* ^(To|Cc):.*alice@gluga.de
```

```
$HOME/Maildir/.Incoming.Gluga/
```

Raus und wieder rein vermeiden

- Alice und Bob nutzen beide den Mailserver im LAN
- Alice sendet eine Mail an bob@jumpingcrab.com
- Postfix: nicht in mydestination also ausgehend:
Ab zum Provider
- Zustellung dort ins Postfach von Bob
- fetchmail holt sie von da ab und stellt sie lokal zu

```
#/etc/postfix/main.cf:  
virtual_maps = hash:/etc/postfix/virtual
```

```
#/etc/postfix/virtual  
bob@jumpingcrab.com bob@exercise.jumpingcrab.com
```

anschließend:

```
postmap /etc/postfix/virtual
```



Noch Fragen?