Ein eigener Mailserver

Linux-Cafe - 2014-12-01

Fortsetzung zum Vortrag

”Ein Server für zu Hause”

siehe

http://pub.stroessenreuther.info/Vortrag_Server_fuer_zu_Hause.pdf

Referent: Bernd Strößenreuther

mailto:linux-cafe@stroessenreuther.net

Lizenz

- Sie dürfen dieses Dokument verwenden unter den Bedingungen der Creative Commons Lizenz: http://creativecommons.org/licenses/by-nc-sa/3.0/de/

- Alle Grafiken und Icons von OpenClipArt.org ”released to the public domain”.

Agenda

- Warum ein eigener Mailserver?
- Wie funktioniert eMail eingentlich genau?
  - Exkurs: Das Spam-Problem
- Infrastrukturvarianten
- Setup Teil 1: Der Einstieg
  - Postfix, Dovecot, fetchmail
  - Exkurs: X.509 Zertifikate
- Setup Teil 2: Mehr Möglichkeiten
  - procmail, vacation, Amavis, Webmailer
- Diskussion

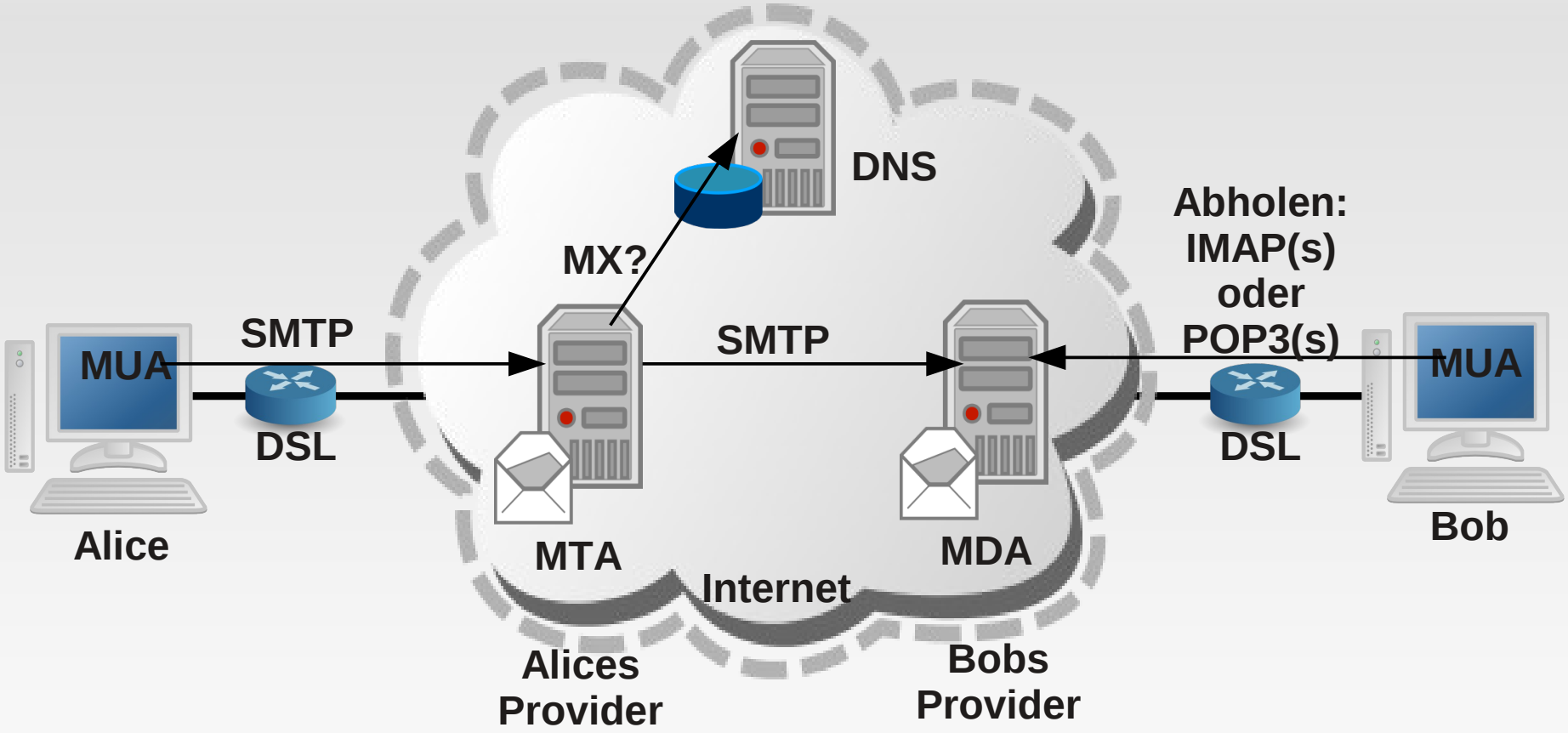
Warum ein eigener Mailserver?

- Verfügungsgewalt über die eigenen Daten
- Besserer Schutz vertraulicher Inhalte
- Nie mehr das POP3-Problem
- Zentrale Regeln zum Sortieren von Mails
- Zentrales Malware-Scanning
- Zentrale Datensicherung
- Beliebig viel Speicherplatz
- Komfort-Funktionen

Wie funktioniert eMail eigentlich genau?

- Protokolle
  - SMTP
  - LMTP
  - IMAP(s)
  - POP3(s)
- Beteiligte Systeme
  - MUA: Mail User Agent (z. B. Thunderbird, KMail, …)
  - MTA: Mail Transfer Agent (z. B. Sendmail, Postfix, ...)
  - MDA: Mail Delivery Agent (z. B. maildrop, procmail, ...)

Der ”Standard-Weg” beim Heimnutzer



MX-Record im DNS

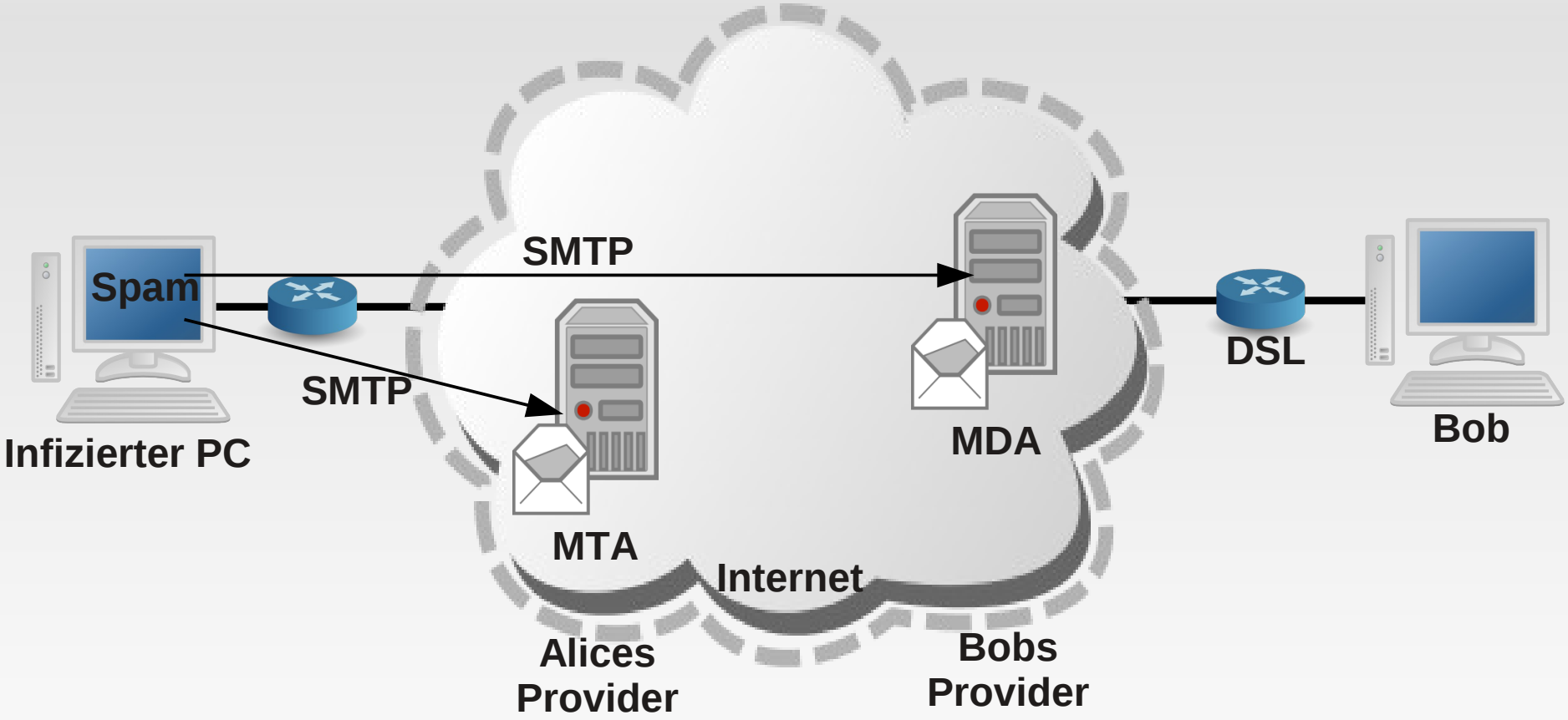
Welche(r) Server ist/sind zuständig für Mails an die Domain example.com?

```
~# dig stroessenreuther.info
[...]
;; QUESTION SECTION:
;stroessenreuther.info.       IN A

;; ANSWER SECTION:
stroessenreuther.info. 7200   IN A  213.239.215.162

~# dig -t MX stroessenreuther.info
[...]
;; ANSWER SECTION:
stroessenreuther.info. 7200   IN MX 10 mail.stroessenreuther.info.

;; ADDITIONAL SECTION:
mail.stroessenreuther.info. 2022 IN A  188.40.2.8
```

Exkurs: Das Spam-Problem

- Filtern / automatisches Verschieben in den Spam-Ordner bringt deutlich mehr Probleme als Nutzen
- Das einzige was wirklich hilft: Spam nicht annehmen!
- Ich darf per SMPT nicht alle Mails annehmen
- Welche Mails will ich annehmen?
  - Mails von meinen legitimen Usern
  - ”echte” Mails an meine User (von beliebigen Absendern)

Spam-Verbreitung



Spam: Gegenmaßnahmen (1)

- Kein offenes Mailrelay betreiben!!
- Am Mailserver des Absenders
  - SMTP-Auth
  - ggf. noch SMTP-after-POP
  - Mail-Relay in einem geschützten Netzwerksegment

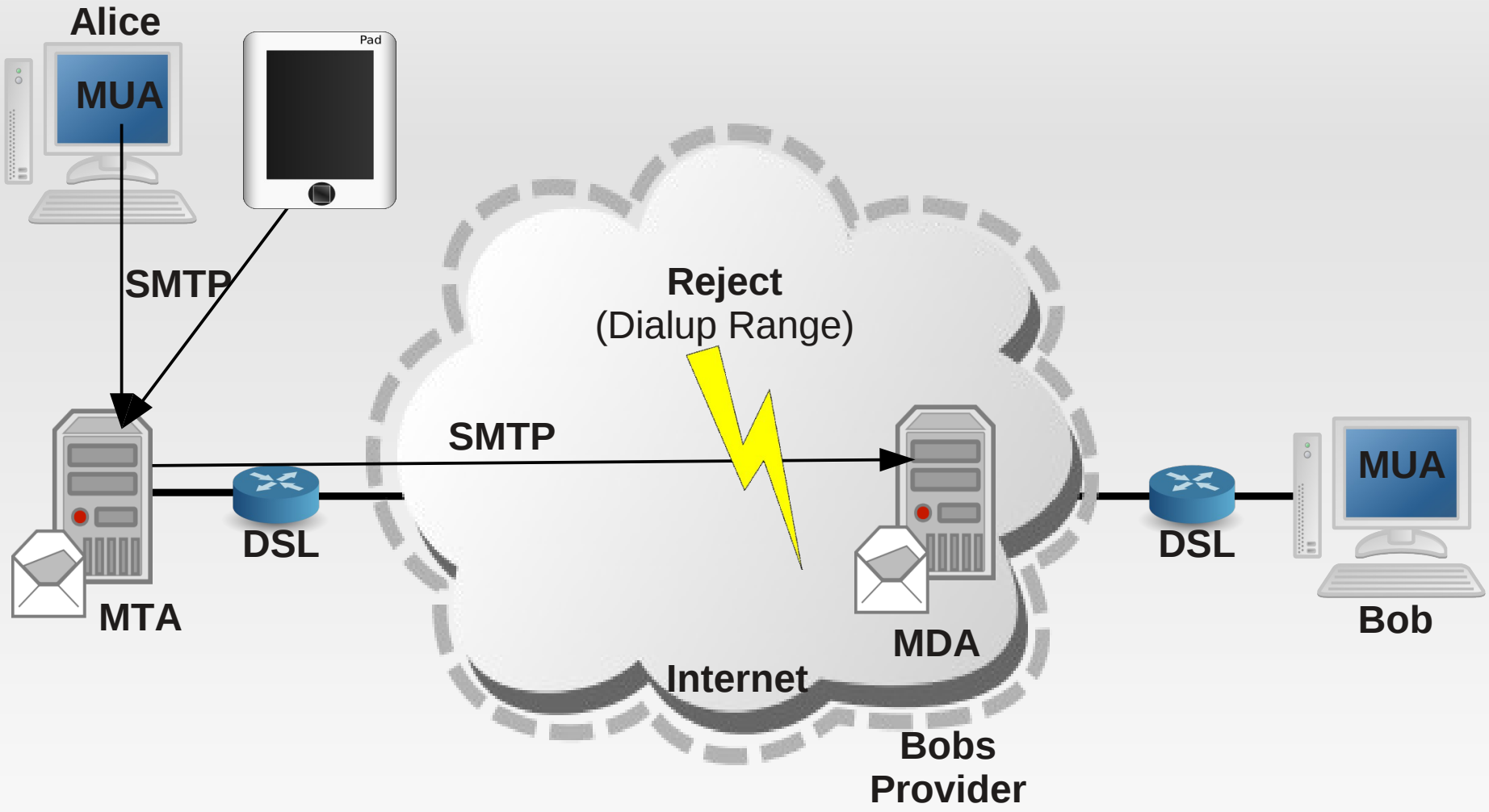
Spam: Gegenmaßnahmen (2)

- Am Mailserver des Empfängers
  - Blacklists: IP-Adressen bekannter Spamschleudern
  - Blacklists: Dialup-Ranges
  - Greylisting
  - ...

Eigener Mailserver: Infrastrukturvarianten

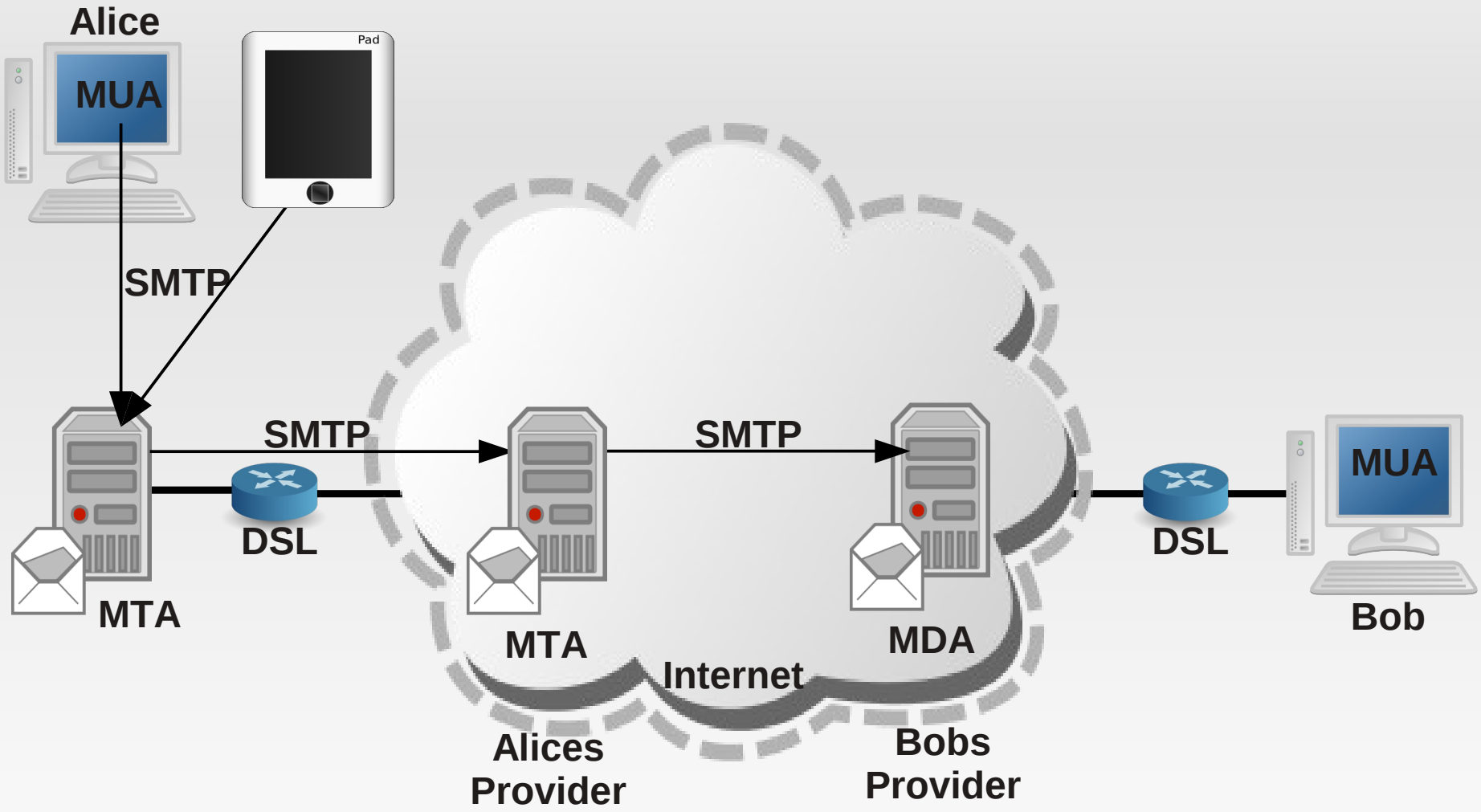
- Ausgehende eMails
- Eingehende eMails

Ausgehende eMails: Szenario 1



Szenario 1: Nicht empfohlen!

Ausgehende eMails: Szenario 2



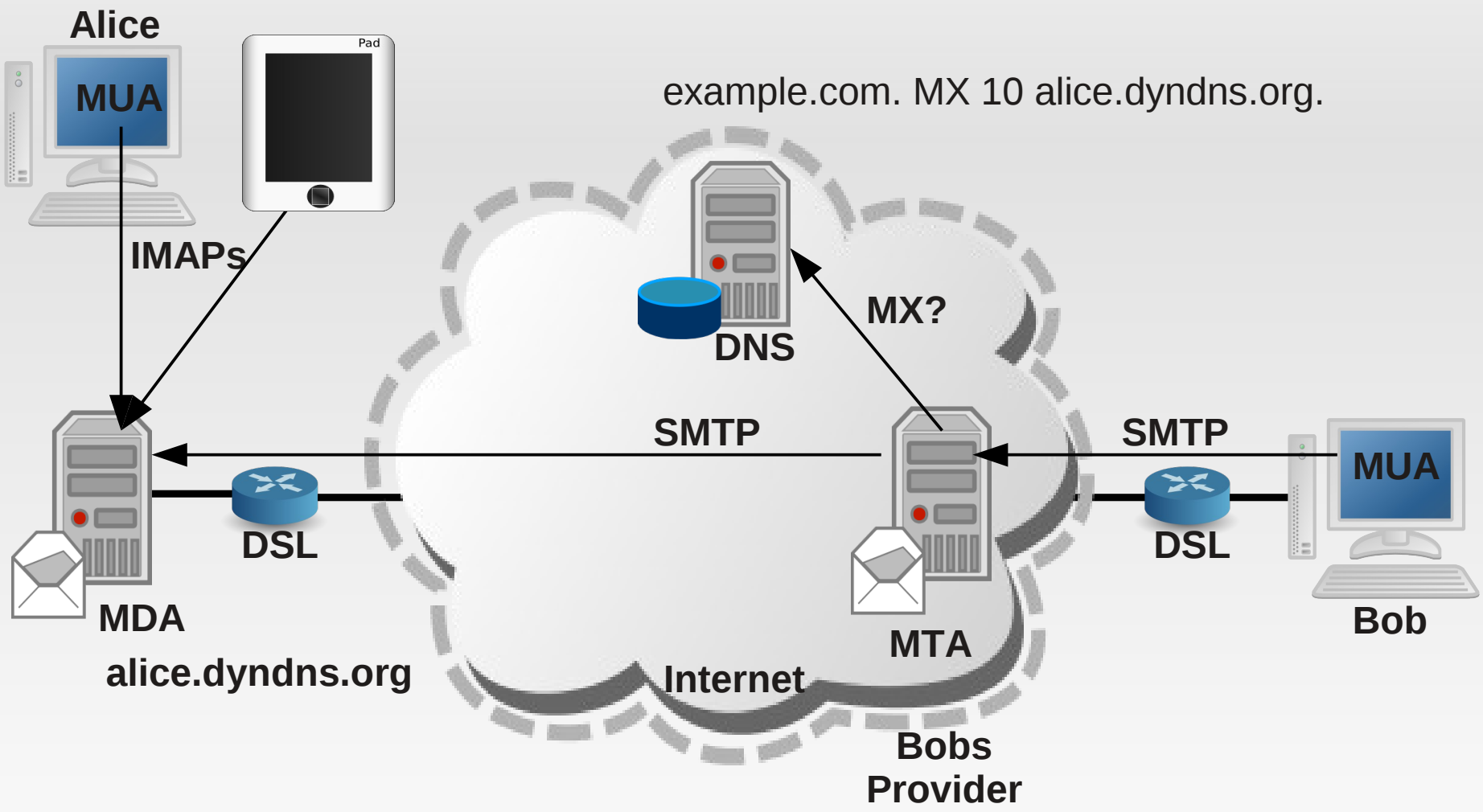
Empfehlung: SMTP-Server beim Provider als Smarthost eintragen!

Smarthost

Beim eigenen Mailserver sollte unbedingt der SMTP-Server beim Provider als Smarthost eingetragen werden:

- SMTP-Auth kann bei Postfix direkt konfiguriert werden
- SMTP-after-POP erfordert Scripting

Eingehende eMails: Szenario 1



Szenario 1: Direkte Zustellung

- Der eigene Server ist per Dynamic DNS unter einem festen Namen von aussen erreichbar
- Portforwarding am DSL-Router (Port 25)
- Der MX-Record für die eigene Domain oder eine beliebige Subdomain (im Beispiel example.com) zeigt direkt auf den DynDNS-Namen.

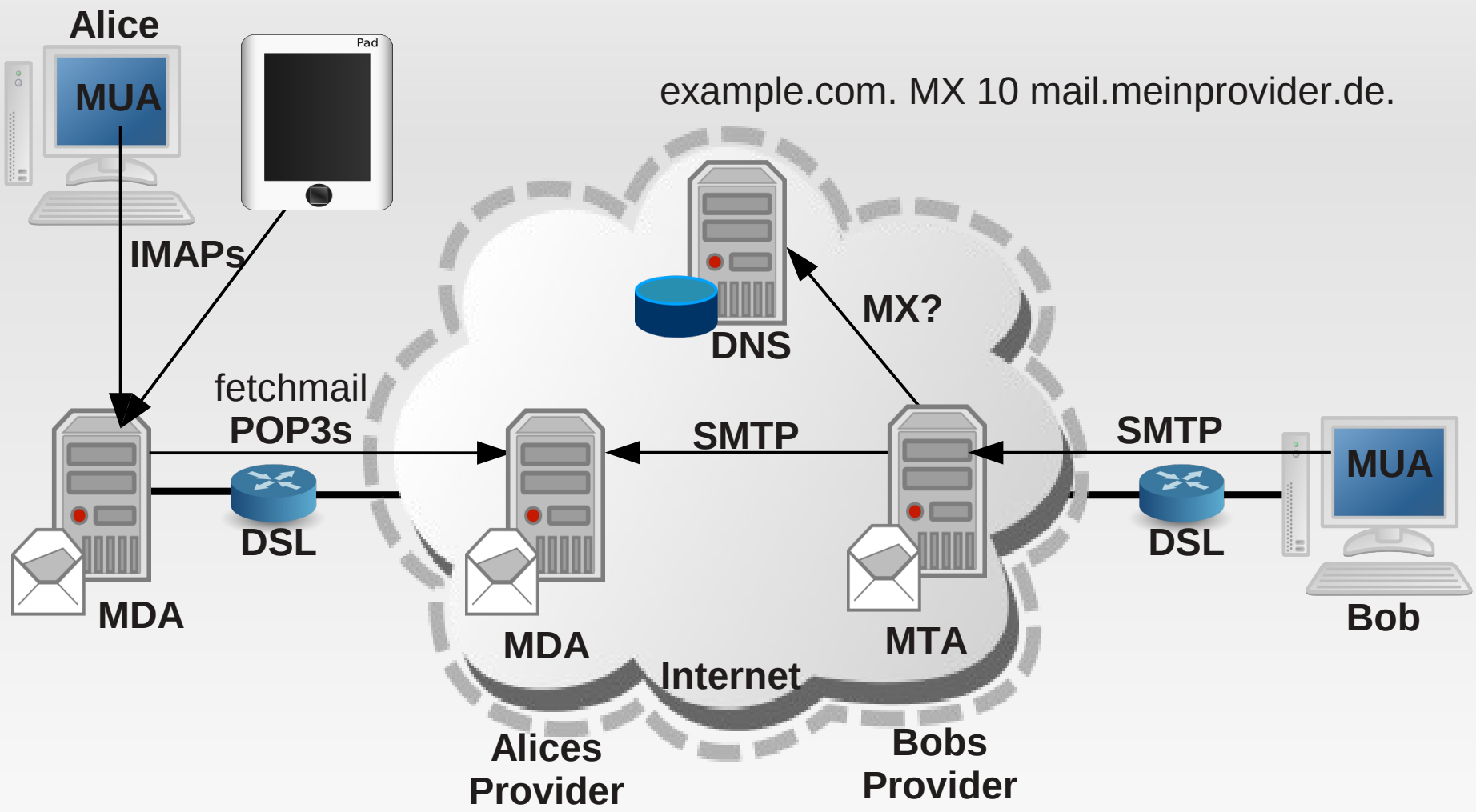
Szenario 1: Vorteile

- Der Mailserver beim Provider ist nicht beteiligt
- Grösstmögliche Autonomie
- Spam-Schutz kann nach den eigenen Vorstellungen vollständig selbst konfiguriert und für die eigenen Bedürfnisse optimiert werden

Szenario 1: Nachteile

- Um Verzögerungen beim Empfang zu vermeiden
  - sollte der Server möglichst immer online sein
  - ist ein Dynamic DNS-Dienst mit sehr kurzen TTLs zu empfehlen
- Spamschutz muss selbst aufgesetzt und laufend gepflegt werden
- Da der Server dann direkt im Internet erreichbar ist
  - stellt er ein potentielles Angriffsziel dar
  - sollte er immer gut gewartet und gepatcht sein
  - der Admin sollte sein Wissen über (neue) Angriffe aktuell halten

Eingehende eMails: Szenario 2



Szenario 2: Vorteile

- Kein Problem, wenn der Heimserver zeitweise ausgeschaltet oder offline ist
- Meist redundanter MX
- Um Spamschutz kümmert sich weiterhin der Provider
- Server muß nicht von aussen erreichbar sein
- Keine potentiellen Angriffe über SMTP-Port

Szenario 2: Nachteile

- Beim Spam-Schutz muß man sich auf die Maßnahmen des Providers verlassen und diese akzeptieren

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/
- Bei Szenario 2 auch möglich:
  Eine Test-Domain nach RFC 2606:

  `meinedomain.example`
  `meinedomain.test`

  siehe auch http://tools.ietf.org/html/rfc2606

Installation / Konfiguration: Teil 1

- Einfaches Setup
  - Postfix: SMTP Server
  - Dovecot: IMAP Server
  - fetchmail: zum Abholen und lokal zustellen

Bei Debian

- Die verwendete Mail-Domain in /etc/mailname eintragen:
  `echo example.com > /etc/mailname`

Postfix (1)

- aptitude install postfix
- Minimalversion von /etc/postfix/main.cf:

```
myorigin = example.com
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
append_dot_mydomain = no
delay_warning_time = 4h
myhostname = mail.gallien.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = gallien.example.com, majestix, majestix.gallien.example.com,
$myhostname, alice.dyndns.org, localhost.$mydomain, localhost.localdomain, localhost
relayhost = [mail.meinprovider.de]
mynetworks = 192.168.56.0/24 [2001:db8::]/32 127.0.0.0/8 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtpd_recipient_restrictions = permit_mynetworks,reject_unauth_destination
home_mailbox = Maildir/
# SMTP-AUTH for relay host (upstream)
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd_upstream
```

Postfix (2)

- In /etc/postfix/sasl_passwd_upstream:

```
mail.meinprovider.de   hanswurst:geheim
```

- Aktivieren:

```
postmap /etc/postfix/sasl_passwd_upstream
/etc/init.d/postfix start
/etc/init.d/postfix status
```

- Testen:

```
echo test | mail -s test1 booboo@gallien.example.com
```

Postfix (3)

- Log prüfen:

```
tail /var/log/mail.log
```

```
Sep 21 19:40:47 dunno postfix/pickup[1723]: 8D31A6041A: uid=0 from=<root>
Sep 21 19:40:47 dunno postfix/cleanup[2268]: 8D31A6041A: message-
id=<20140921174047.8D31A6041A@mail.gallien.example.com>
Sep 21 19:40:47 dunno postfix/qmgr[1724]: 8D31A6041A: from=<root@example.com>,
size=319, nrcpt=1 (queue active)
Sep 21 19:40:47 dunno postfix/local[2271]: 8D31A6041A:
to=<booboo@gallien.example.com>, relay=local, delay=0.11, delays=0.07/0.04/0/0,
dsn=2.0.0, status=sent (delivered to maildir)
Sep 21 19:40:47 dunno postfix/qmgr[1724]: 8D31A6041A: removed
```

Postfix (4)

- Maileingang prüfen:

```
booboo@dunno:~$ cd ~/Maildir/new/
booboo@dunno:~/Maildir/new$ ls
1411321247.Vfc00Ia116dM663503.dunno

booboo@ubu1204prod:~/Maildir/new$ cat 1411321247.Vfc00Ia116dM663503.dunno
Return-Path: <root@example.com>
X-Original-To: booboo@gallien.example.com
Delivered-To: booboo@gallien.example.com
Received: by mail.gallien.example.com (Postfix, from userid 0)
id 8D31A6041A; Sun, 21 Sep 2014 19:40:47 +0200 (CEST)
To: booboo@gallien.example.com
Subject: test1
Message-Id: <20140921174047.8D31A6041A@mail.gallien.example.com>
Date: Sun, 21 Sep 2014 19:40:47 +0200 (CEST)
From: root@example.com (root)

test
```

Postfix (5)

- Test eMail ins Internet:

```
echo test | mail -s test2 linux-cafe@stroessenreuther.net
```

- Log prüfen:

```
tail /var/log/mail.log
```

```
Sep 21 20:09:31 dunno postfix/pickup[2927]: 7789F6041A: uid=1001
from=<booboo>
Sep 21 20:09:31 dunno postfix/cleanup[3049]: 7789F6041A: message-
id=<20140921180931.7789F6041A@mail.gallien.example.com>
Sep 21 20:09:31 dunno postfix/qmgr[2928]: 7789F6041A:
from=<booboo@example.com>, size=303, nrcpt=1 (queue active)
Sep 21 20:09:31 dunno postfix/smtp[3051]: 7789F6041A: to=<linux-
cafe@stroessenreuther.net>,
relay=mail.meinprovider.de[2001:db8::6]:25, delay=0.26,
delays=0.05/0.11/0.01/0.08, dsn=2.0.0, status=sent (250 2.0.0 Ok:
queued as 0DBFD101EB9)
Sep 21 20:09:31 dunno postfix/qmgr[2928]: 7789F6041A: removed
```

Dovecot (1)

- aptitude install dovecot-imapd

Dovecot (2)

- Konfiguration in /etc/dovecot/dovecot.conf (komplett):

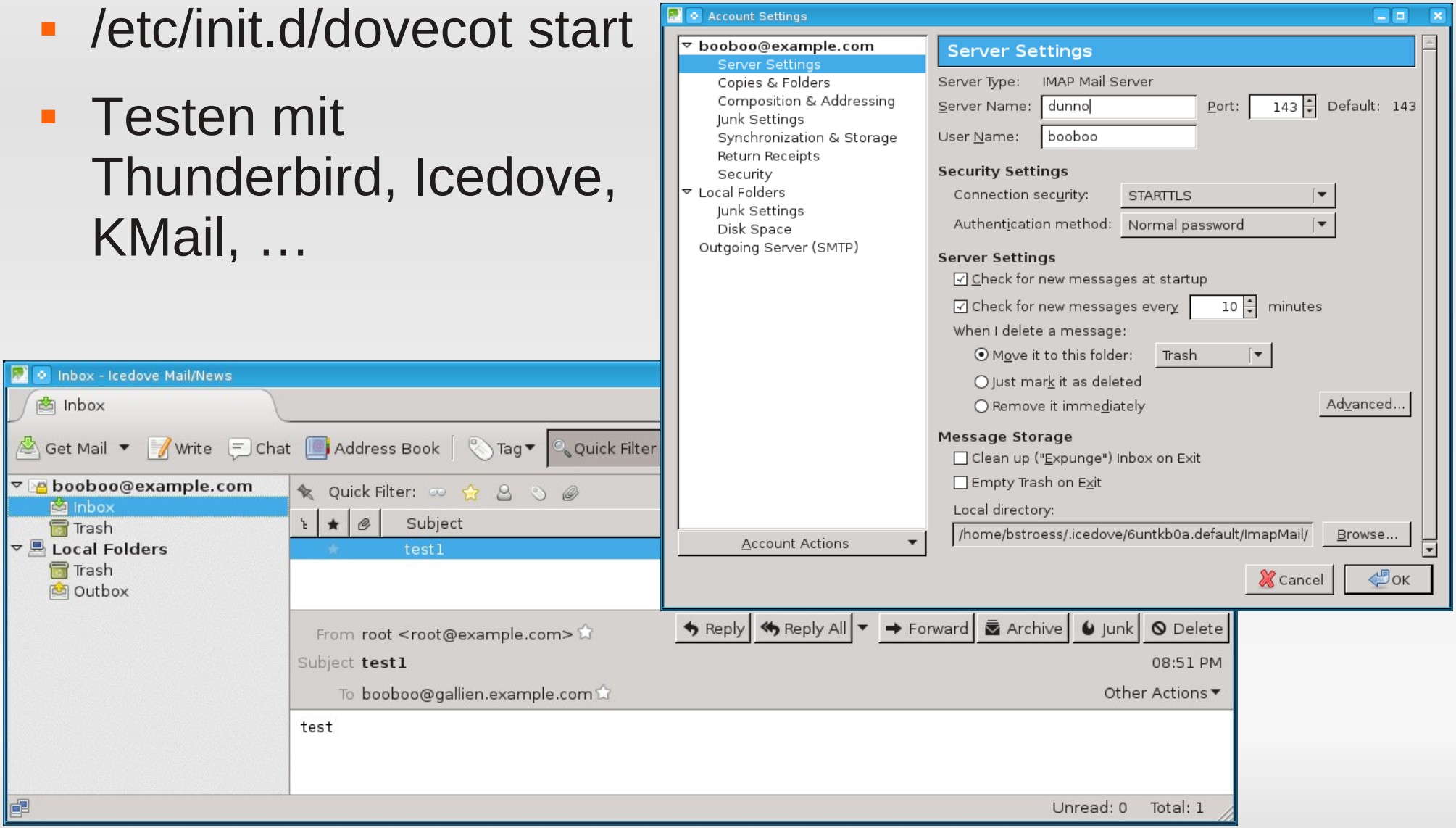
```
listen = *, [::]
log_timestamp = "%Y-%m-%d %H:%M:%S "
mail_privileged_group = mail
passdb {
  driver = pam
}
protocols = imap
service auth {
  user = root
}
ssl_cert = </etc/dovecot/imap.gallien.example.com.crt
ssl_cipher_list = HIGH:!EXP:!SSLv2:!ADH
ssl_key = </etc/dovecot/imap.gallien.example.com.key
# ab Dovecot Version 2.1 aktivieren
# ssl_protocols = !SSLv2 !SSLv3
userdb {
  driver = passwd
}
```

Exkurs: X.509 Zertifikate

```
cd /etc/dovecot

export CERT=imap.gallien.example.com

openssl genrsa -out ${CERT}.key 2048

openssl req -new -key ${CERT}.key -out ${CERT}.csr

openssl x509 -req -days 1000 -in ${CERT}.csr -signkey ${CERT}.key
-out ${CERT}.crt
```

Dovecot (3)

- /etc/init.d/dovecot start
- Testen mit Thunderbird, Icedove, KMail, …



fetchmail

- aptitude install fetchmail fetchmailconf
- /etc/fetchmailrc anlegen und schützen:

```
touch /etc/fetchmailrc
chmod 600 /etc/fetchmailrc
chown root.root /etc/fetchmailrc
```

- Füllen mit Login-Daten, ein solcher Abschnitt je Postfach beim Provider:

```
poll mail.meinprovider.de with proto POP3
    user "hans.wurst" there with password "GehHeim"
    is booboo here options fetchall
```

- /etc/default/fetchmail:

```
START_DAEMON=yes
```

- `/etc/init.d/fetchmail start`

Installation / Konfiguration: Teil 2

- Mehr Möglichkeiten
  - weitere Konfigurationsmöglichkeiten und nützliche Features von Postfix
  - procmail: Sortieren von Mails am Server
  - eMail-Aliases: schönere/mehr eMail-Adressen
  - Vacation: eMails automatisch beantworten
  - Zentrales Malware-Scanning mit Amavis
  - Webmailer

Postfix: Transportverschlüsselung mit TLS

- Siehe auch
  http://postfix.state-of-mind.de/patrick.koetter/smtpauth/postfix_tls_support.html
- /etc/postfix/main.cf

```
smtpd_use_tls = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
smtpd_tls_cert_file=/etc/postfix/mail.gallien.example.com.crt
smtpd_tls_key_file=/etc/postfix/mail.gallien.example.com.key
smtpd_tls_CAfile = /etc/postfix/cacert-root.crt
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache

# turning off ssl and weak ciphers
smtpd_tls_mandatory_ciphers = HIGH
smtpd_tls_mandatory_exclude_ciphers = aNULL, MD5, EXP
smtpd_tls_ciphers = HIGH
smtpd_tls_exclude_ciphers = aNULL, MD5, EXP
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_protocols = !SSLv2, !SSLv3
```

Postfix: TLS mit relayhost

- /etc/postfix/main.cf

```
smtp_use_tls = yes
smtp_sasl_security_options =
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtp_tls_protocols = !SSLv2, !SSLv3
```

Postfix virtual table

- ”Umleitung” für bestimmte Mails
- /etc/postfix/main.cf

```
virtual_maps = hash:/etc/postfix/virtual
```

- /etc/postfix/virtual

```
someone@web.de      someone@galien.example.com
```

- hash-Format erzeugen

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

- Auch nutzbar, wenn nicht alle Adressen der 2nd-Level-Domain lokal zugestellt werden sollen (alice@example.com lokal, bob@example.com remote)

Weitere nützliche Parameter von Postfix (1)

- /etc/postfix/main.cf
  (siehe hierzu auch `man 5 postconf`)

```
# increase log level if required
debug_peer_level = 2
# maybe combine with debug_peer_list

# The maximal amount of original message text that is sent in a
# non-delivery notification. Specify a byte count.
bounce_size_limit = 50000

# The maximal size in bytes of a message, including envelope
# information.
message_size_limit = 102400000

# The maximal size of any local(8) individual mailbox or maildir
# file, or zero (no limit).
mailbox_size_limit = 512000000
```

Weitere nützliche Parameter von Postfix (2)

- /etc/postfix/main.cf

```
# provides the information that is used in "user has moved to
# new_location"  bounce  messages
relocated_maps = hash:/etc/postfix/relocated

# selectively reject or accept mail from or to specific hosts,
# domains, networks, host addresses or  mail addresses.
smtpd_sender_restrictions = hash:/etc/postfix/access

# Optional list of domains whose subdomain structure will be
# stripped off in email addresses.
masquerade_domains = example.com
masquerade_exceptions = root

# IPv6
# see http://www.postfix.org/IPV6_README.html
inet_protocols = ipv4, ipv6
```

Procmail (1)

- aptitude install procmail
- ~/.forward

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

- ~/.procmailrc

```
DEFAULT="$HOME/Maildir/"
LOGABSTRACT=all
LOGFILE=$HOME/log/procmail.log

:0:
* ^To:.gluga@example.com
$HOME/Maildir/.Incoming.Gluga/
```

Procmail (2)

- Mehrere Kriterien (alle müssen zutreffen)

```
:0:
* ^From: hans.wurst@example.org$
* ^To: gluga@example.com$
* ^Subject:.*Katzenbilder
$HOME/Maildir/.Incoming.Unfug/
```

- Regular Expressions nutzen

```
:0:
* ^(To|Cc):.*linux-cafe@.*
$HOME/Maildir/.Incoming.Linux-Cafe/
```

eMail-Aliases

- Standard-Adresse: <username>@<$mydomain>
  z. B. booboo@example.com
- /etc/aliases:
  `bernd.stroessenreuther: booboo`
- Anschliessend hashen mit
  `newaliases`
- Ab sofort auch:
  bernd.stroessenreuther@example.com

Lokale Verteiler

- /etc/aliases
  ```
  alle: hans, hugo, franz
  ```
- hashen nicht vergessen
  ```
  newaliases
  ```
- Ergebnis:
  Mails an alle@example.com werden an alle genannten Postfächer zugestellt
- Mehr zu /etc/aliase:
  ```
  man 5 aliases
  ```

Vacation: Out-Of-Office Mails, ...

- aptitude install vacation
- ~/.vacation.db neu (leer) anlegen mit:
  ```
  vacation -i
  ```
- ~/.vacation.msg
  ```
  Lieber Absender,
  ich bin momentan nicht da und werde Ihre Mail
  erst lesen, wenn ich wieder zurück bin.
  ```
- ~/.forward
  ```
  \booboo, "| /usr/bin/vacation -a ↷
  bernd.stroessenreuther booboo"
  ```
- Anzeigen wer wann vacation-Mails bekommen hat:
  ```
  vacation -l
  ```

Zentrales Malware-Scanning mit Amavis (1)

- Amavis kümmert sich um auspacken und zerlegen der Mails und Reporting.
- Doku unter /usr/share/doc/amavisd-new/ und z. B. http://postfix.state-of-mind.de/patrick.koetter/amavisd-new/
- Bevorzugte(n) Virenscanner installieren
- Falls ClamAV gewünscht ist:

  ```
  aptitude install clamav-daemon
  ```

  User clamav muss Mitglied in der Gruppe amavis sein, um die Dateien lesen zu dürfen, die Amavis ausgepackt hat:

  ```
  usermod -a -G amavis clamav
  /etc/init.d/clamav-daemon start
  ```

Zentrales Malware-Scanning mit Amavis (2)

- Amavis installieren:
  `aptitude install amavisd-new-postfix`
- Virenscanner festlegen in
  `/etc/amavis/conf.d/15-av_scanners`
- Virus-Scanning aktivieren in
  `/etc/amavis/conf.d/15-content_filter_mode`
  mit

```
@bypass_virus_checks_maps = (
   \%bypass_virus_checks,
   \@bypass_virus_checks_acl,
   \$bypass_virus_checks_re);
```

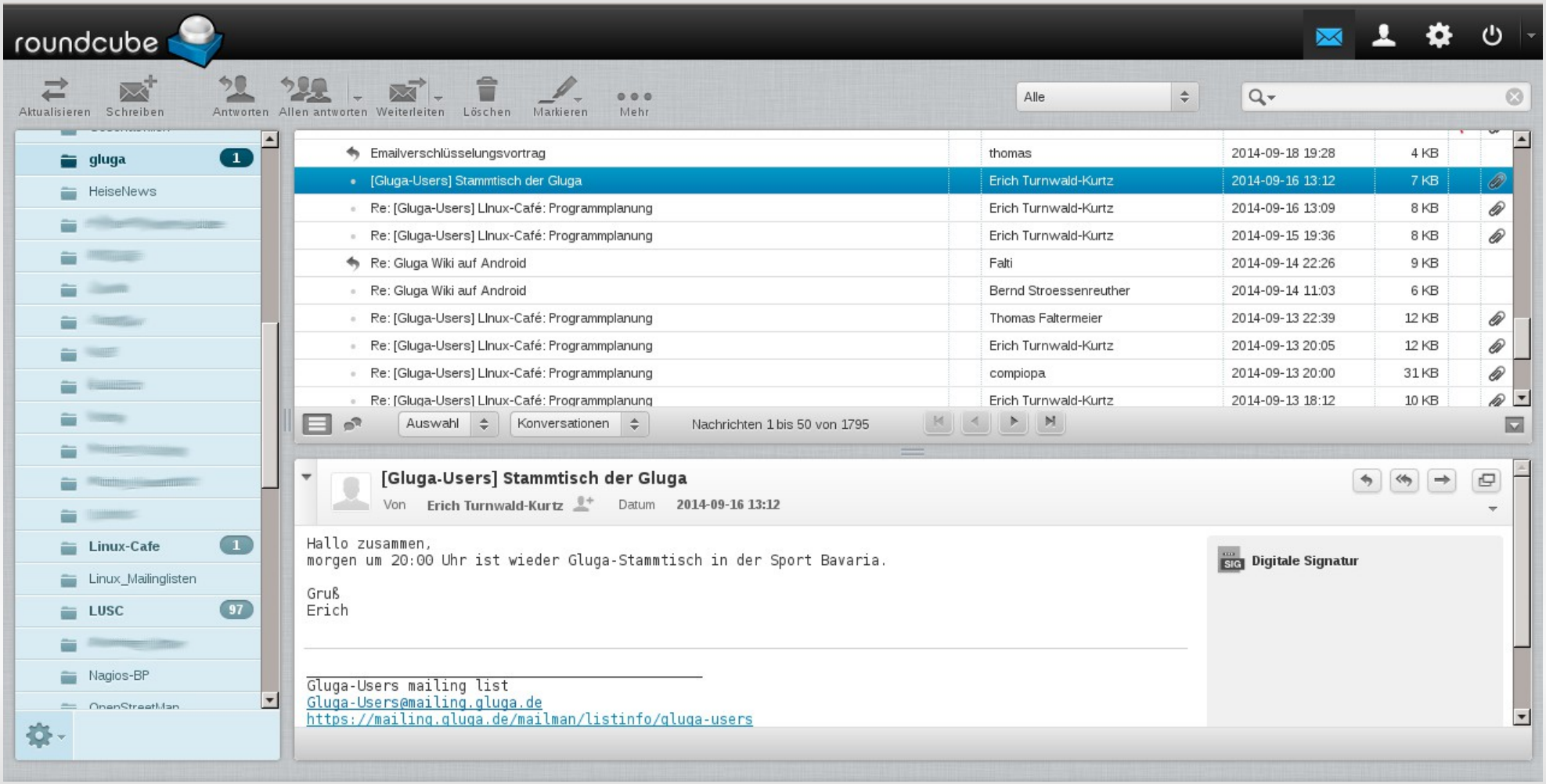
- Ggf. hier auch Spamassassin aktivieren

Zentrales Malware-Scanning mit Amavis (3)

- Amavis starten:
  `/etc/init.d/amavis start`
- Logs prüfen:
  `/var/log/mail.log`
- Postfix muss Mails an Amavis weiterreichen. Dazu in `/etc/postfix/main.cf` einfügen:
  `content_filter=smtp-amavis:[127.0.0.1]:10024`
- Restart von Postfix:
  `/etc/init.d/postfix restart`
- Testen mit testfiles aus Paket clamav-testfiles

Webmailer (1)

- z. B. Roundcube Webmailer http://roundcube.net/



Webmailer (2)

- IMAP-Client
- Kann auch auf dem gleichen Server in einem Apache Webserver mit betrieben werden
- Zusätzliche Authentifizierung mit SSL-Clientzertifikaten möglich, siehe

  http://pub.stroessenreuther.info/Vortrag_Zugriff_ueber_Internet_auf_PC_zu_Hause_OpenVPN_und_Co.pdf

Ausblick: Spamschutz
nur interessant für Szenario 1

- Blacklists (DNSBL, RBL)
  - direkt in Postfix oder integriert in Policyd-weight
- Greylisting
  - z. B. mit postgrey, ggf. kombiniert mit Whitelists
- Domain Key Identified Mail (DKIM), RFC 4871
  - nur ”soft” prüfen
- Ggf. SpamAssassin und/oder Bayes Filter
  - prüft nur ”soft”
- Ggf. Razor/Pyzor/DCC
- Ggf. ”Teergruben” (Tarpits)

Noch Fragen?

- Jetzt und hier
- Im Anschluß beim Bier
- Bei (fast) jedem Linux-Cafe Gluga-Stammtisch, Ubuntuusers-Stammtisch, … (siehe http://termine.gluga.de/)
- Jederzeit auf der Gluga Users Mailingliste, siehe http://mailing.gluga.de/