Mailtransport im Internet

oder warum die Abwehr von Spam nicht so einfach ist

Jörg Kinzebach
<joerg@duck.franken.de>

Spam

Unerwünschte Email:

- Kostet Speicherplatz
- Kostet Transfervolumen
- Kostet CPU
- Kostet Zeit

Motivation für Spam

- Werbung für eigene Website/Linkliste
- Werbung für Firma/Shop
- Werbung für Erwachsenenunterhaltung
- Werbung für böse Web-Seiten
- Überprüfung von Adressen
- Sammeln von Adressen
- Verbreitung von Viren/Würme
- Vergeltung/Joe-Job
- Ego-Spam

Joe-Job

Fingierter Spam, der anscheinend einen offensichtlichen Begünstigten hat

Transport

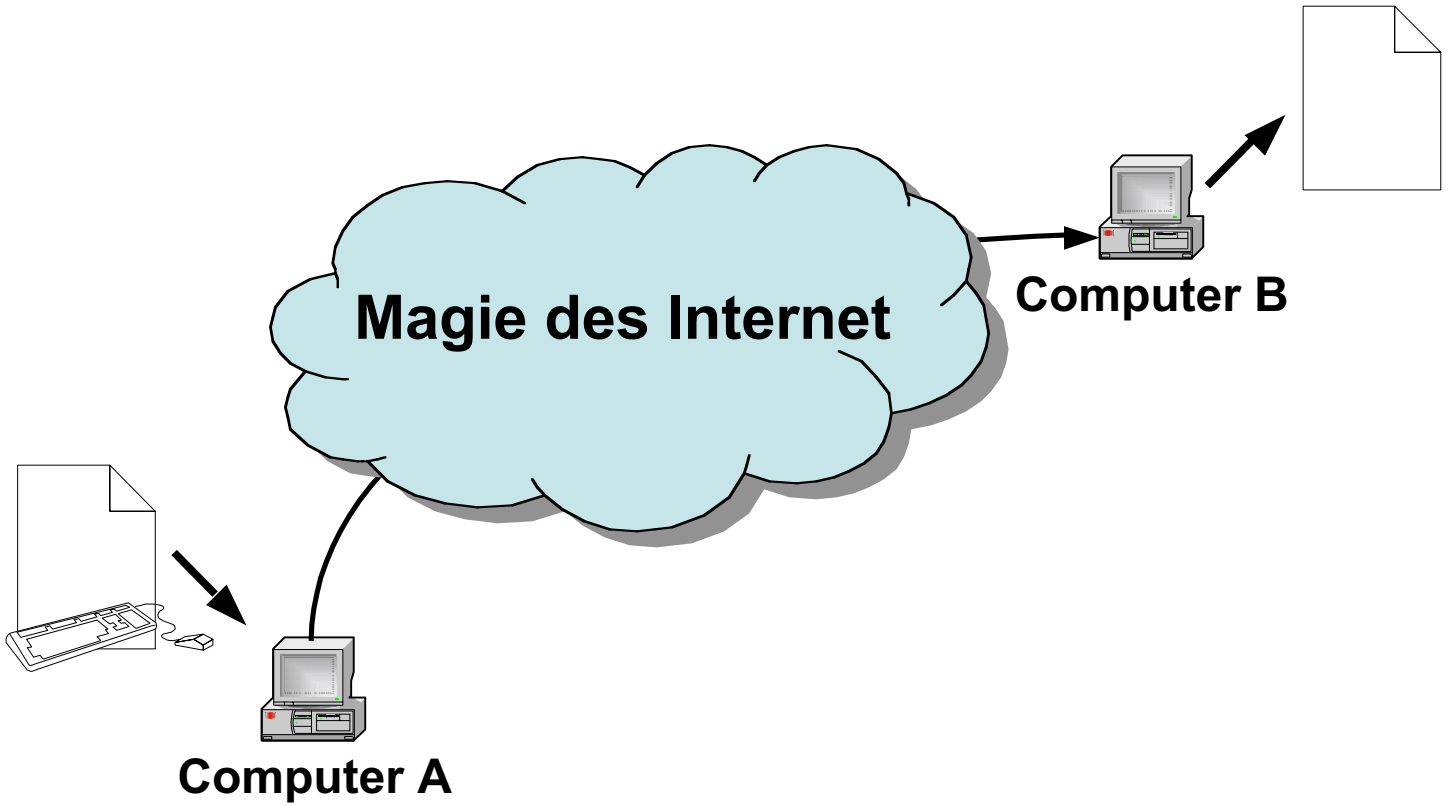
- Verbreitetste Methode um im Internet Mail zu transportieren:

SMTP

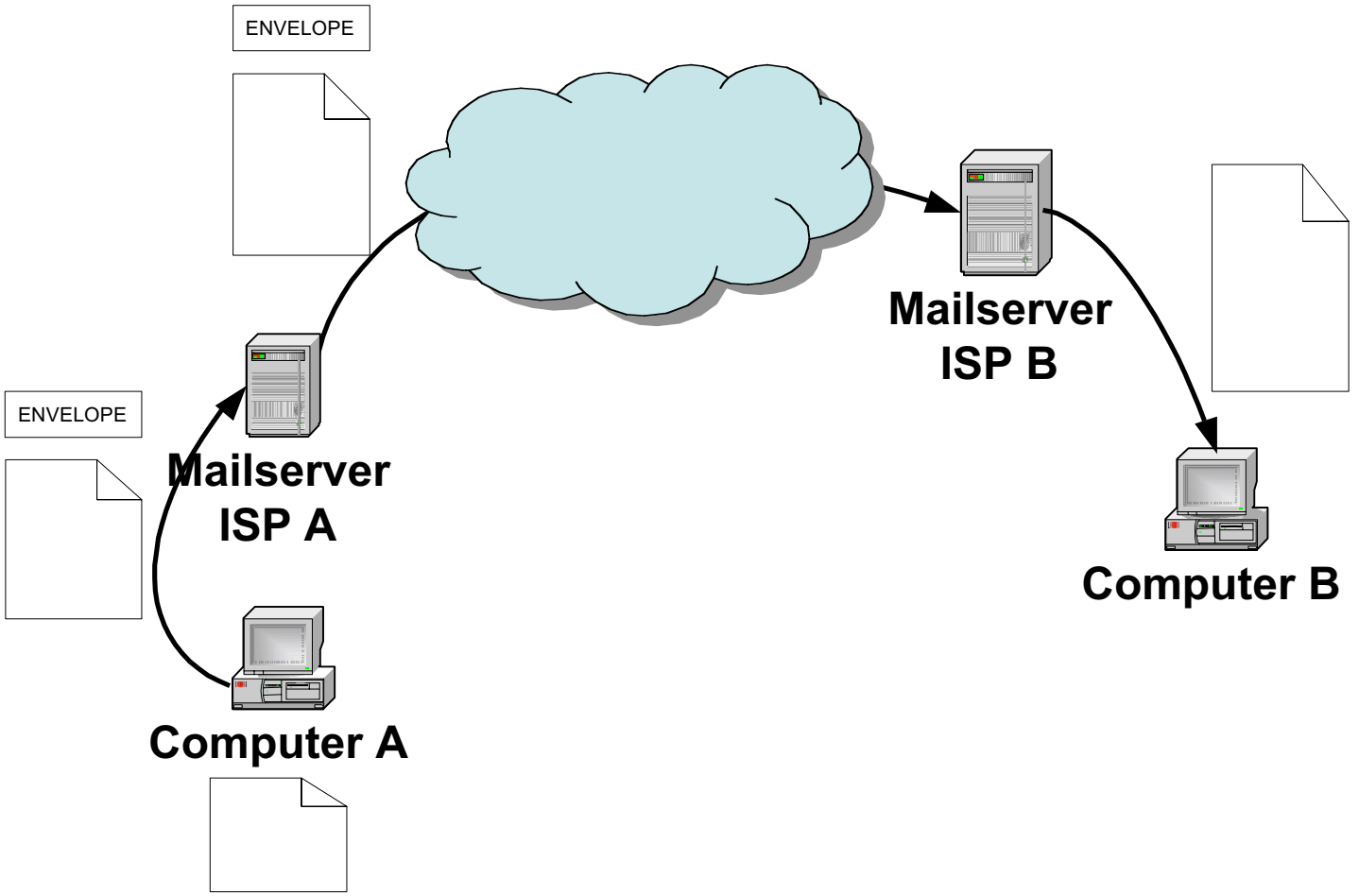
Andere Möglichkeiten:

- UUCP
- POP3
- IMAP

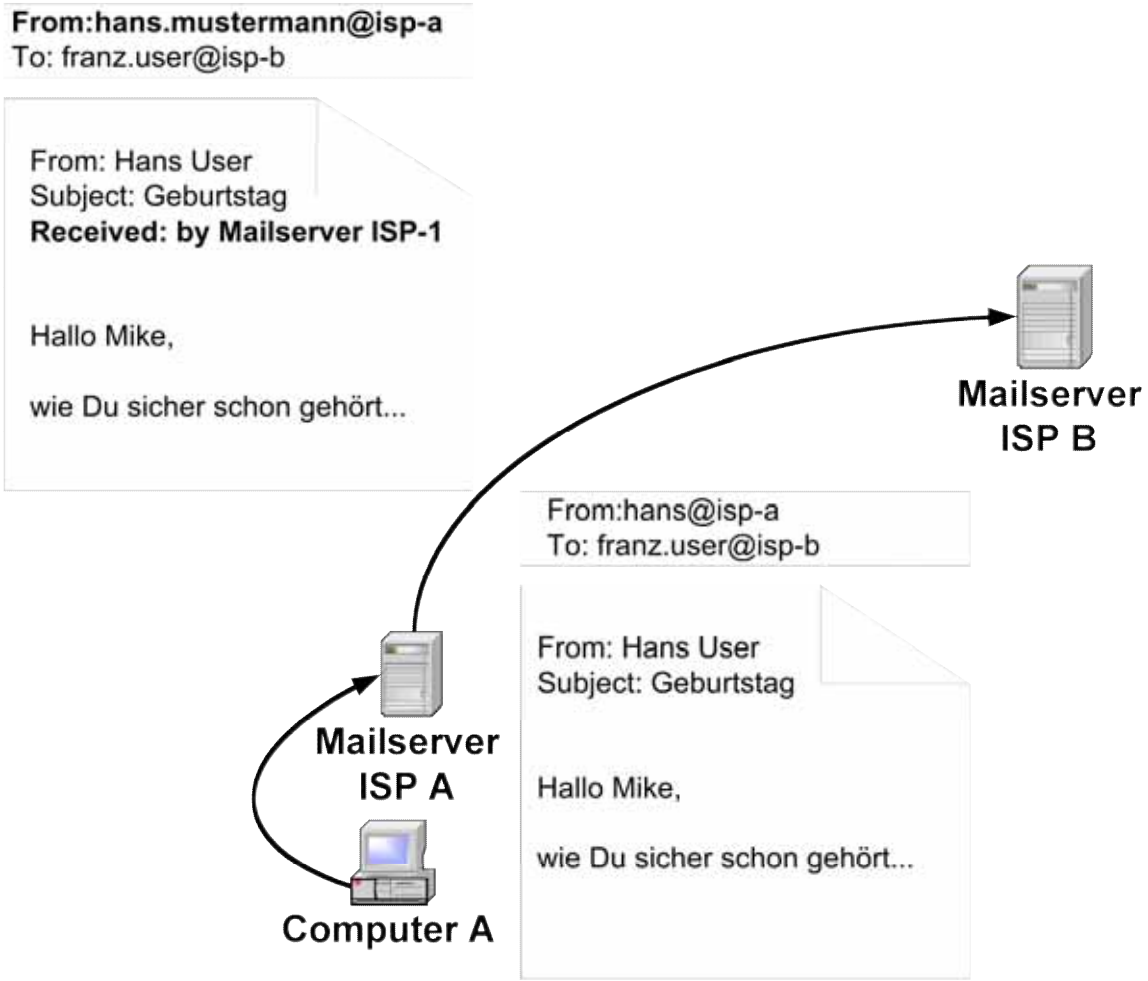
SMTP



SMTP


ENVELOPE
ENVELOPE
Mailserver
ISP A
Mailserver
ISP B
Computer A
Computer B

SMTP


From:hans.mustermann@isp-a
To: franz.user@isp-b
From: Hans User
Subject: Geburtstag
Received: by Mailserver ISP-1
Hallo Mike,
wie Du sicher schon gehört...
Mailserver
ISP B
From:hans@isp-a
To: franz.user@isp-b
From: Hans User
Subject: Geburtstag
Hallo Mike,
wie Du sicher schon gehört...
Mailserver
ISP A
Computer A

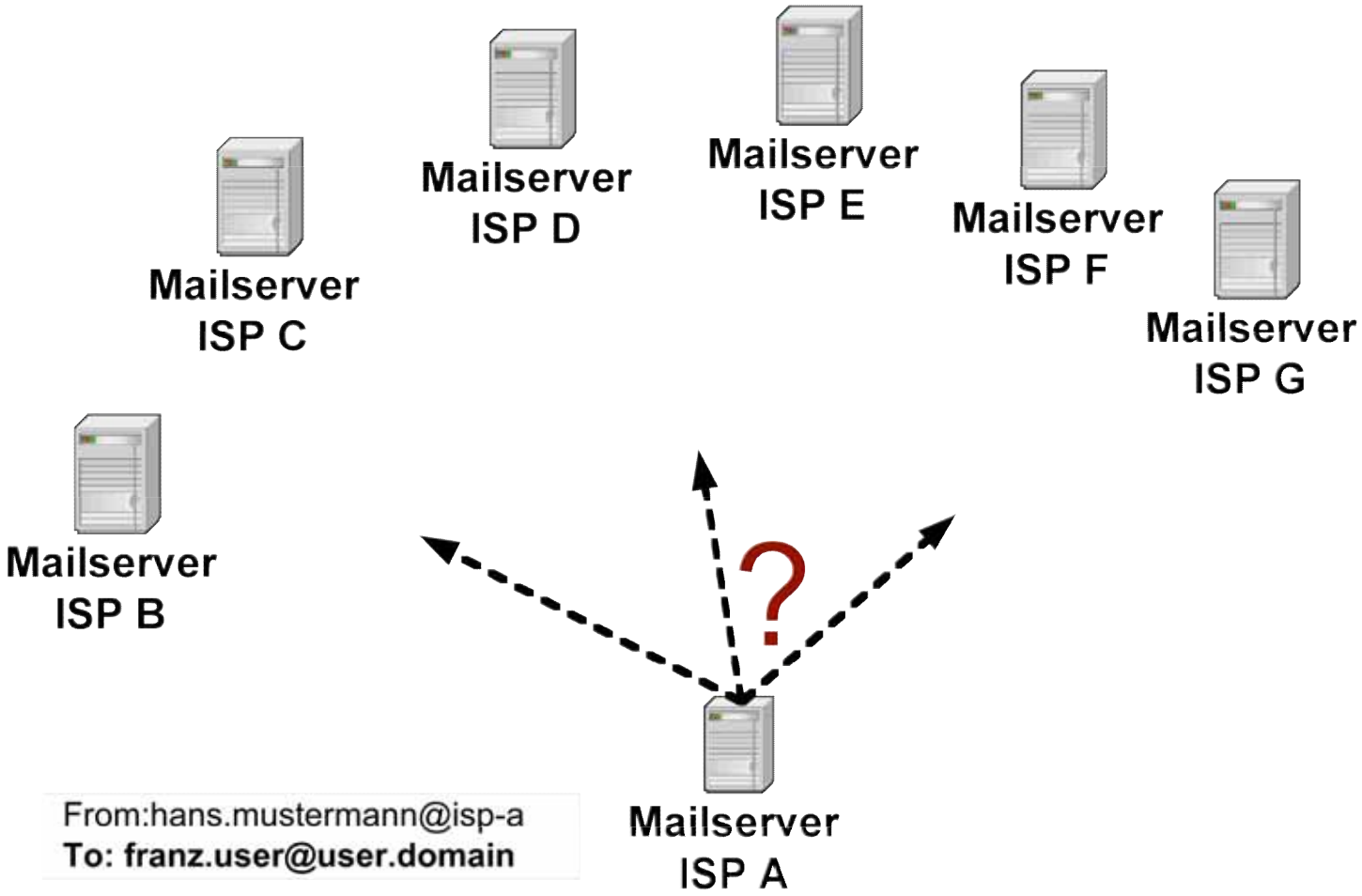
SMTP

helo foo.franken.de
250 mail-n.franken.de
mail from: <joerg@duck.franken.de>
250 Ok
rcpt to: <joerg@sysnet.net>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Test
From: Joerg Kinzebach <joerg@duck.franken.de>
To: sombody <somebody@foo>

Hallo Mike,

.
250 Ok: queued as 70B22245C4

SMTP


Mailserver
ISP C
Mailserver
ISP D
Mailserver
ISP E
Mailserver
ISP F
Mailserver
ISP G
Mailserver
ISP B
?
From:hans.mustermann@isp-a
To: franz.user@user.domain
Mailserver
ISP A

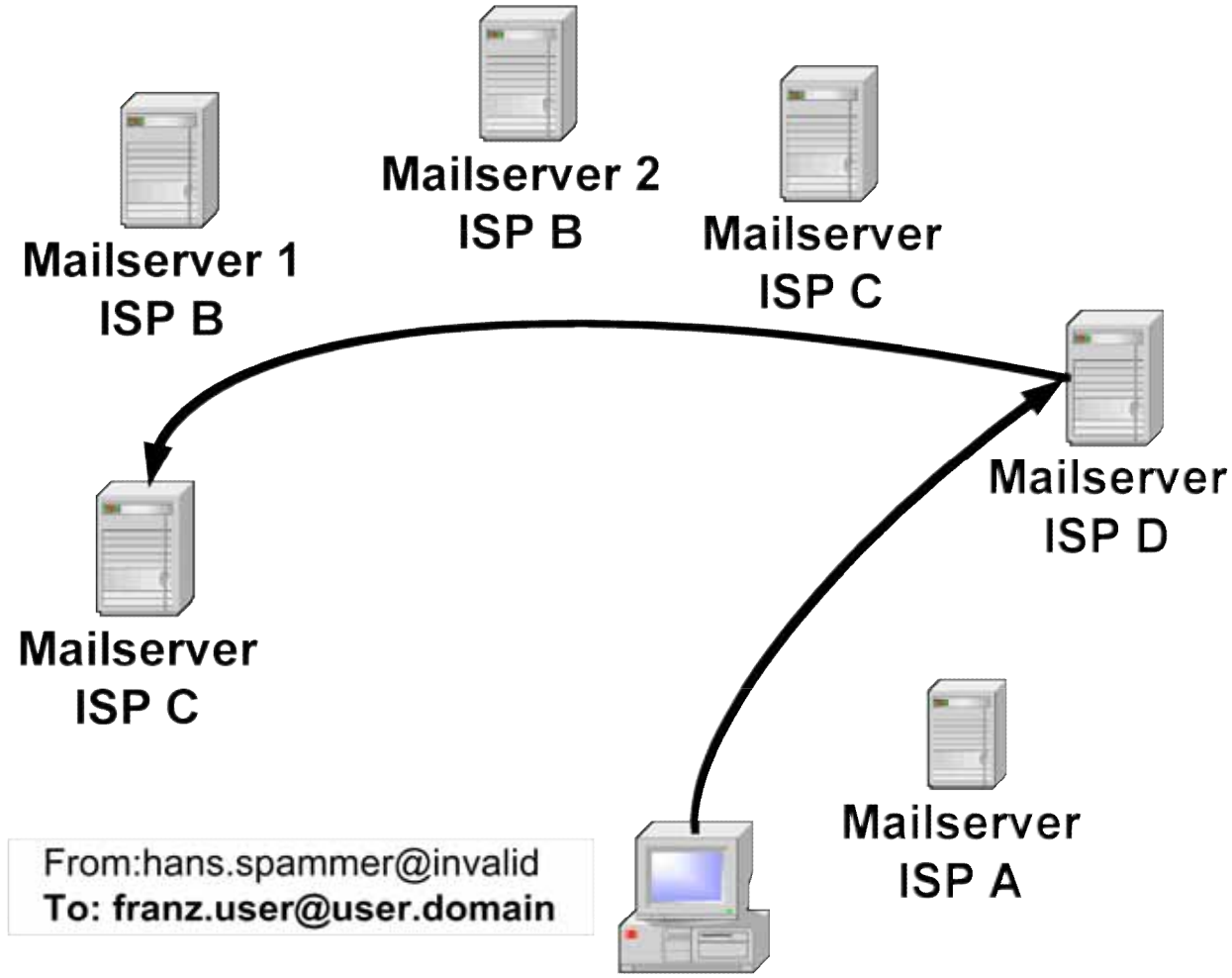
SMTP

- Abfrage der Mailexchangers (MX) der Ziel-Domain
- Versuch der Auslieferung an Mailexchanger der Zieldomain, niedrigste Prioritäts-Kennung zuerst

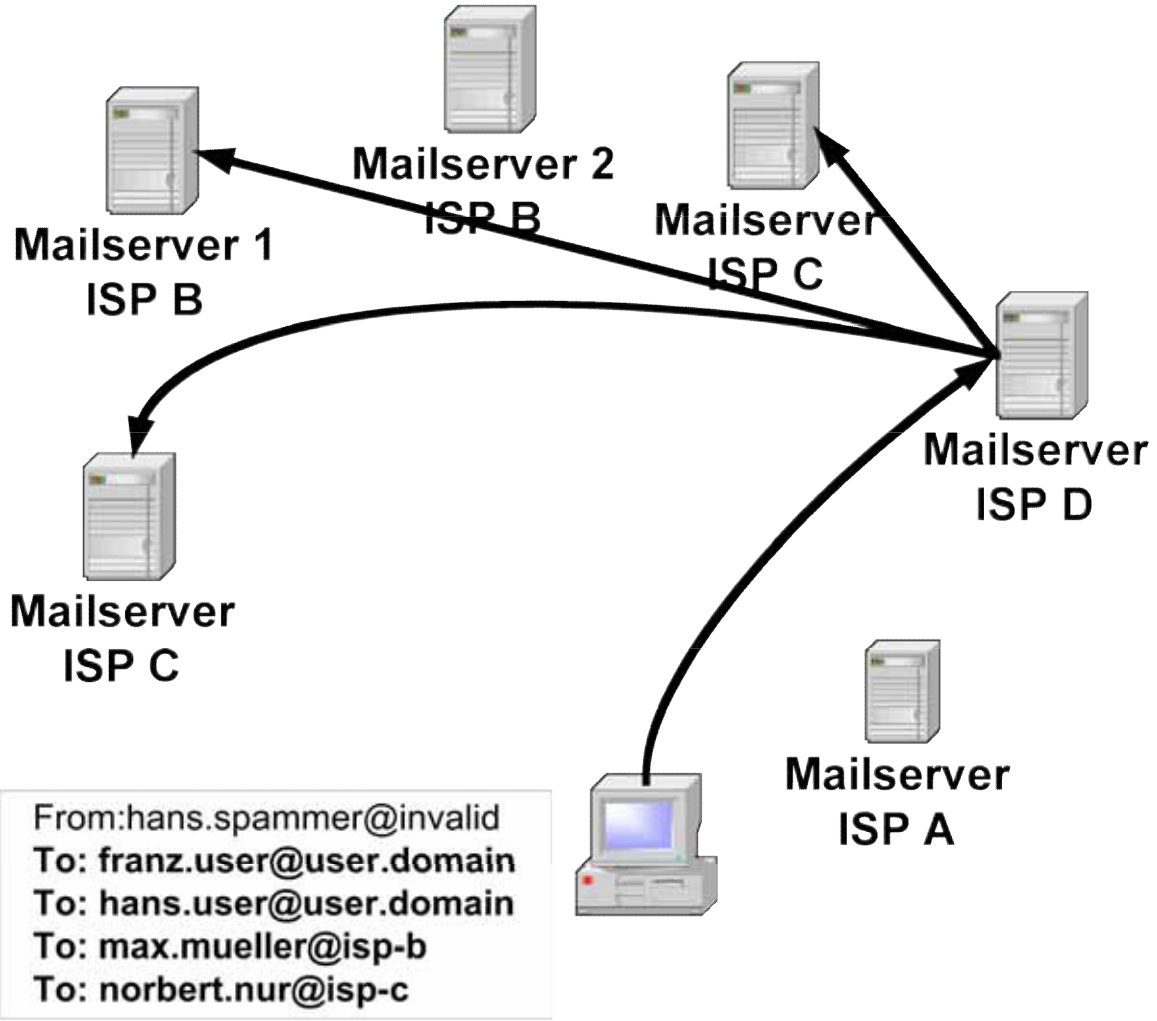
SMTP (MX)

```
>host -t MX franken.de
franken.de mail is handled by 10 laurel.franken.de.
franken.de mail is handled by 30 lara.franken.de.
franken.de mail is handled by 50 faui45.informatik.uni-
    erlangen.de.
```

SMTP Relay


Mailserver 1
ISP B
Mailserver 2
ISP B
Mailserver
ISP C
Mailserver
ISP D
Mailserver
ISP C
Mailserver
ISP A
From:hans.spammer@invalid
To: franz.user@user.domain

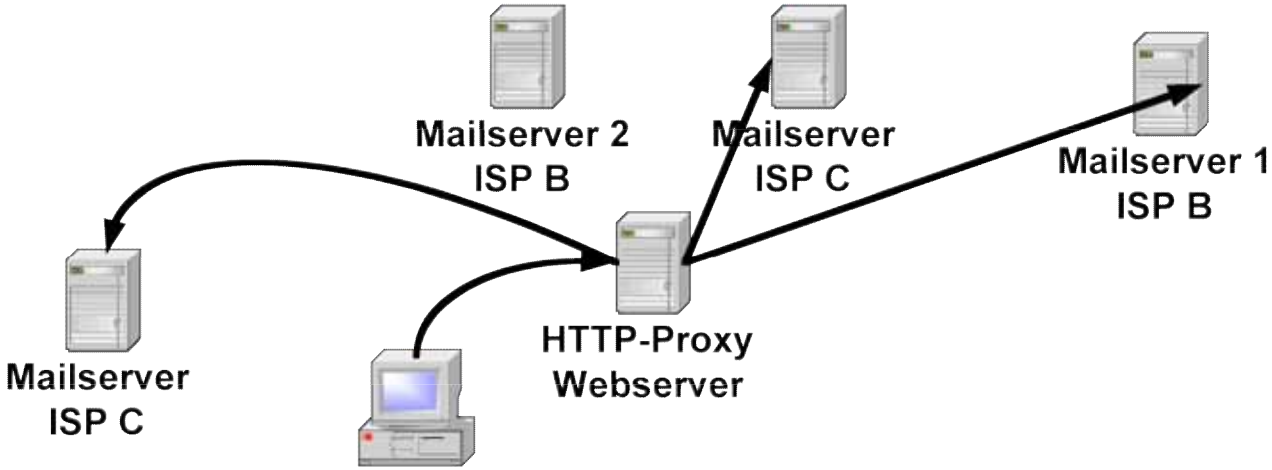
SMTP Relay


Mailserver 1
ISP B
Mailserver 2
ISP B
Mailserver
ISP C
Mailserver
ISP D
Mailserver
ISP C
Mailserver
ISP A
From:hans.spammer@invalid
To: franz.user@user.domain
To: hans.user@user.domain
To: max.mueller@isp-b
To: norbert.nur@isp-c

Anti-Relay

- Mailserver korrekt konfigurieren
  - Relay nur für bekannte IP-Adressen
  - Authentisierung von Nutzern fremder IP-Adressen
  - Korrekte Erkennung von Routing
- Ablehnen bekannter Relayserver
  - NJABL
  - SORBS
  - OPM
  - Maps

Mehr Relay



- SMTP durch Web-Proxy
- Ausnutzen von Sicherheitslücken in CGI-Skripten

=> Blocklist für Open Proxies/CGI-Servern

Blocken beim Empfang

- Sender-IP in Blacklist
- Absender in Blacklist
- Protokollfehler
- Untersuchung des Inhalts:
  - Received-Zeilen passen nicht zu Absender
  - Fehler im Header
  - Eindeutige Spam-Kennwörter (z.B. MMF)
  - Bayes-Untersuchung

RBL

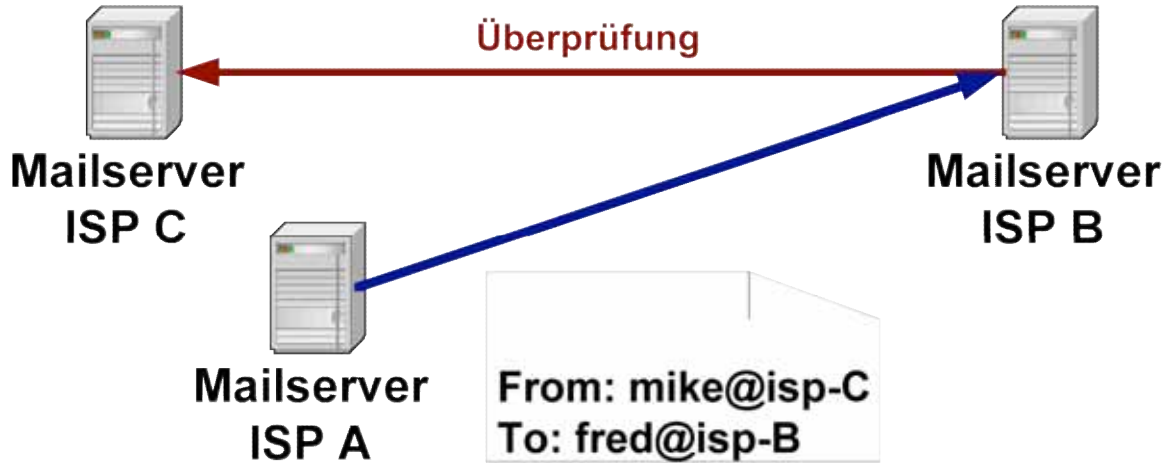
- Schnelle Listung von „bösen“ maileinliefernden IP-Adressen
- Kann präventiv durch „gescannte“ Daten gefüttert werden
- Kann sehr leicht falsche Daten enthalten
- Zentraler Angriffspunkt
- Oft missbraucht für persönliche Abneigungen

Razor & DCC

- Sammlung von Signaturen von erkannten Spam-Mails bzw. Signaturen gehäuft auftretenden Mails
- Bewertung von beitragenden Parteien
- Mittels Spam-Traps automatisiert betreibbar und daher sehr Zeitnah

Senderüberprüfung

- Existiert Absenderdomain?
- Ist eine Auslieferung an den Absender möglich (VRFY)
  - Verwendung fremder „gefundener“ Absender
  - Last auf eigentlich unbeteiligten Mailservern



RMX / DMP / SPF

Reverse MX proposal

Designated Mailer Protocol

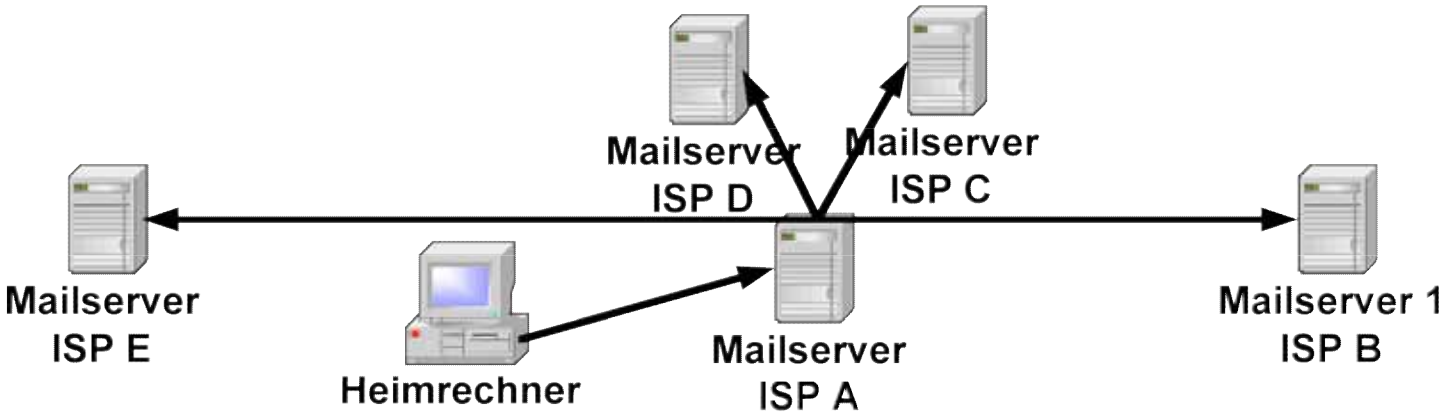
Senders Permitted From

- Einschränkung der erlaubten Sender für Adressen einer Domain
- Daten werden im DNS gespeichert
- Verhindert freie Verwendung von Absender-Adressen bei Relay über beliebige Mail-Server

Dumme Ideen

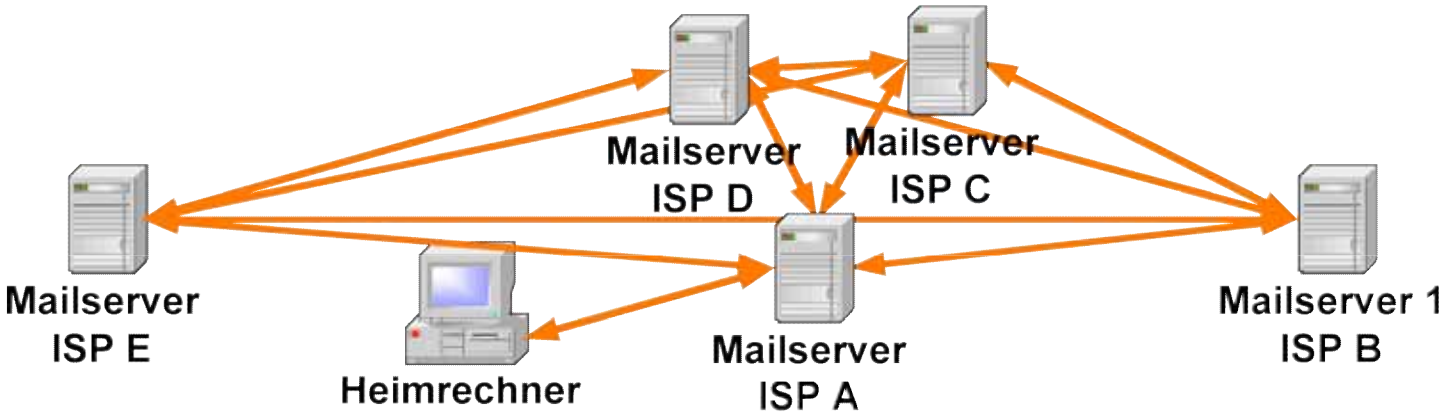
- Spam „zum Absender“ zurückschicken
- „Versender von Viren“ zu benachrichtigen
- Automatisierte Beschwerden über Spam
- Beschwerde über Spam an jede Abuse-Adresse aus im Header vorkommenden Hosts zu schicken
- Ungültige Mail-Adressen veröffentlichen
- „Tarpits“

SMTP-Auth



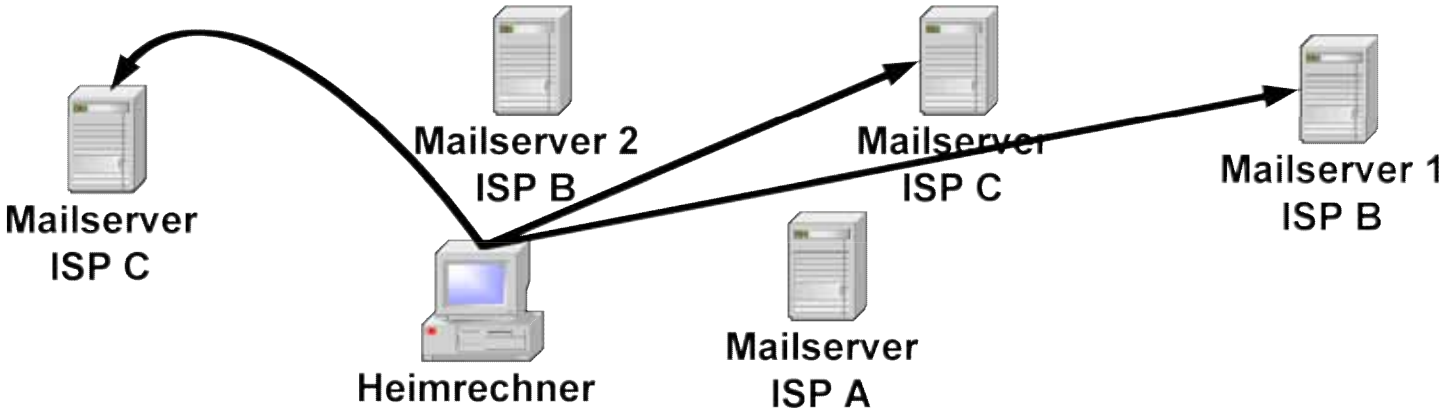
- Mails werden vom MTA nur angenommen, wenn der Einlieferer sich identifizieren konnte

SMTP-Auth



- Alle ISPs, die miteinander Mails austauschen wollen, müssen sich gegenseitig kennen und vertrauen
- Alternativ muss eine hierarchische Struktur geschaffen werden

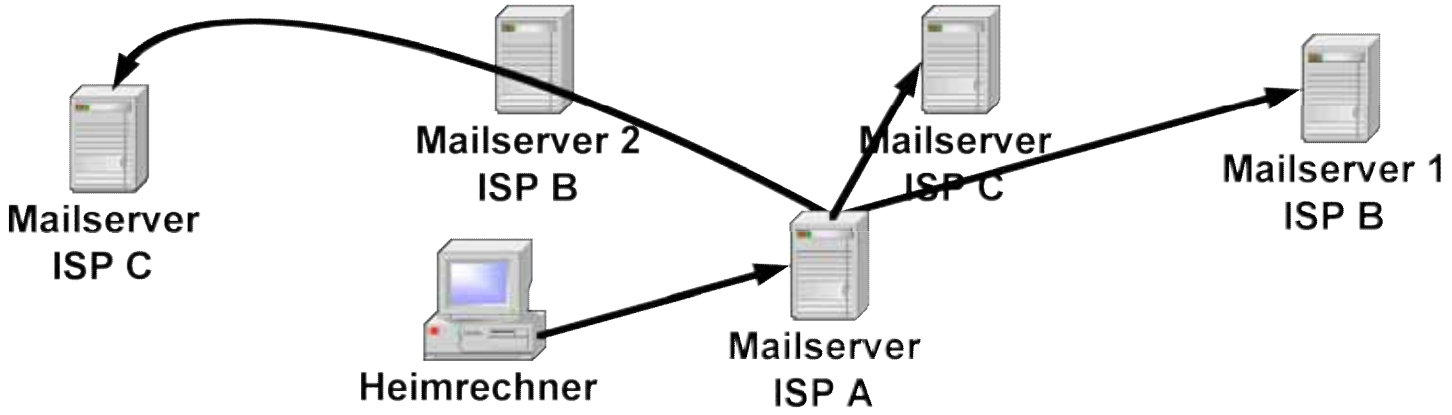
Relay über Enduser



- Ungepatchte Software auf Heim-PCs
- Mit Viren und Würmern Verseuchte Heim-PCs

- => Blocken von Dialup-IPs (DUL)

Relay via User-ISP



- Wenn „Home-PC“ gehackt ist, kann auch „auf übliche Weise“ relayed werden

Viren/Würmer

- Schwächstes Glied bleibt Nutzer-Rechner
  - SoBig.[a-f]
  - ProxyGuzu
  - Lovegate
  - Jeem
  - IRC/Backdoor.g
  - AnalogX-Proxy.ldr
  - Illusion Mailer
- Teilweise Web-Server auf Heim-Rechner
  - Installation via Wurm/Virus
  - Management z.B. über IRC
  - Link via Spam & DynDNS