

Spam

(auch: Mogelpost, Netzpest, Digipest,
Quälmail, E-Müll, ...)

... und was man dagegen tun kann

Timo Felbinger

05.08.2007

```
Return-Path: <mahoney_heather@bah.com>
Delivered-To: timof@uranos.local
Received: (qmail 31232 invoked from network); 6 Feb 2007 10:52:21 -0000
Received: from unknown (HELO cluster1a.us.message1abs.com) (86.35.192.41)
  by maia.quantum.physik.uni-potsdam.de with SMTP; 6 Feb 2007 10:52:21 -0000
Received: from 192.168.0.%RND_DIGIT
  (203-219-%DIGSTAT2-%STATDIG.%RND_FROM_DOMAIN [203.219.%DIGSTAT2.%STATDIG])
  by mail%SINGSTAT.%RND_FROM_DOMAIN (envelope-from %FROM_EMAIL)
  (8.13.6/8.13.6) with SMTP id %STATWORD for <%TO_EMAIL>; %CURRENT_DATE_TIME
Message-Id: <%RND_DIGIT[10].%STATWORD@mail%SINGSTAT.%RND_FROM_DOMAIN>
From: "%FROM_NAME" <%FROM_EMAIL>
Content-Length: 160
Lines: 9
%TO_CC_DEFAULT_HANDLER
Subject: %SUBJECT
Sender: "%FROM_NAME" <%FROM_EMAIL>
Mime-Version: 1.0
Content-Type: text/html
Date: %CURRENT_DATE_TIME

%MESSAGE_BODY
```

... was tun mit erkanntem Spam?

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!

Riskant: legitime aber falsch-positive E-mail geht verloren

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!

Riskant: legitime aber falsch-positive E-mail geht verloren

- Zurück an Absender!

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!

Riskant: legitime aber falsch-positive E-mail geht verloren

- Zurück an Absender!

Gar keine gute Idee: Absender ist bei Spam fast immer gefälscht:

- Spam wird an anderes Opfer weitergeleitet
- Eigener Server kann als Spam-Schleuder eingestuft werden

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!
Riskant: legitime aber falsch-positive E-mail geht verloren
- Zurück an Absender!
Gar keine gute Idee: Absender ist bei Spam fast immer gefälscht:
 - Spam wird an anderes Opfer weitergeleitet
 - Eigener Server kann als Spam-Schleuder eingestuft werden
- Als Spam markieren, Zustellen (in Spam-Ordner)

... was tun mit erkanntem Spam?

- Entsorgen nach **/dev/null!**

Riskant: legitime aber falsch-positive E-mail geht verloren

- Zurück an Absender!

Gar keine gute Idee: Absender ist bei Spam fast immer gefälscht:

- Spam wird an anderes Opfer weitergeleitet
- Eigener Server kann als Spam-Schleuder eingestuft werden

- Als Spam markieren, Zustellen (in Spam-Ordner)

Nicht wirklich befriedigend:

Weiterhin manuelle Filterung nötig, Problem ist nicht wirklich gelöst!

... was tun mit erkanntem Spam?

- Entsorgen nach `/dev/null`!

Riskant: legitime aber falsch-positive E-mail geht verloren

- Zurück an Absender!

Gar keine gute Idee: Absender ist bei Spam fast immer gefälscht:

- Spam wird an anderes Opfer weitergeleitet
- Eigener Server kann als Spam-Schleuder eingestuft werden

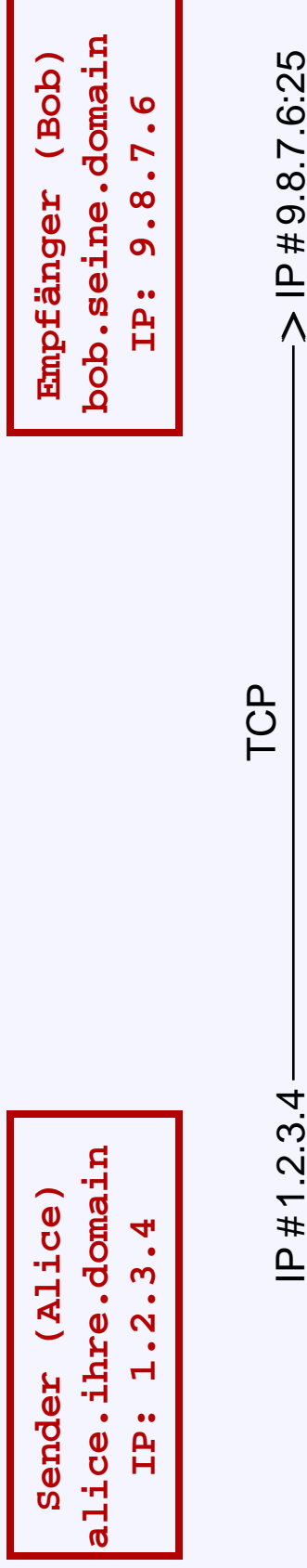
- Als Spam markieren, Zustellen (in Spam-Ordner)

Nicht wirklich befriedigend:

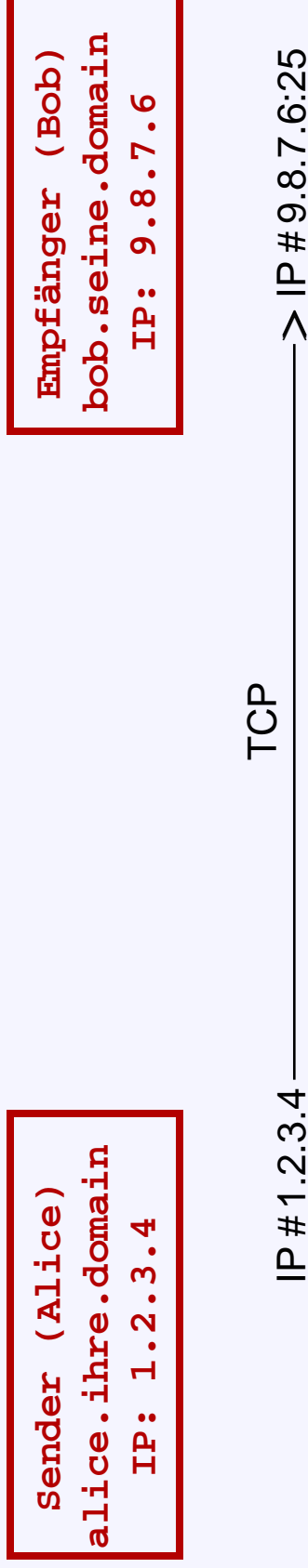
Weiterhin manuelle Filterung nötig, Problem ist nicht wirklich gelöst!

- Wohl die beste Lösung: Annahme von Spam verweigern!

SMTP: Simple Mail Transfer Protocol

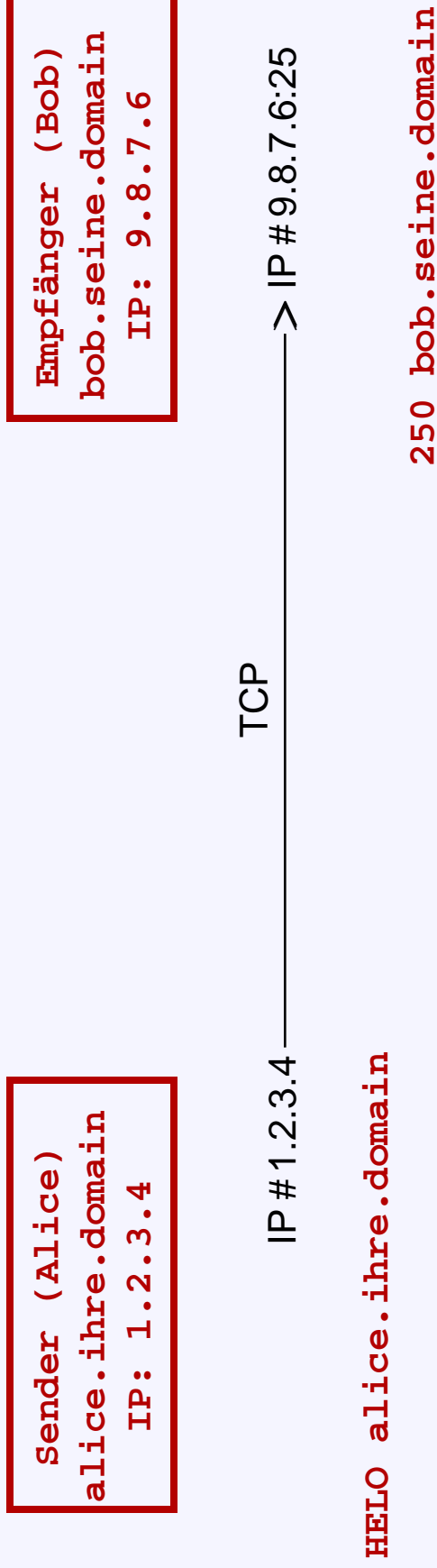


SMTP: Simple Mail Transfer Protocol



HELO alice.ihre.domain

SMTP: Simple Mail Transfer Protocol



SMTP: Simple Mail Transfer Protocol

4

Sender (Alice)
alice.ihre.domain
IP: 1.2.3.4

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

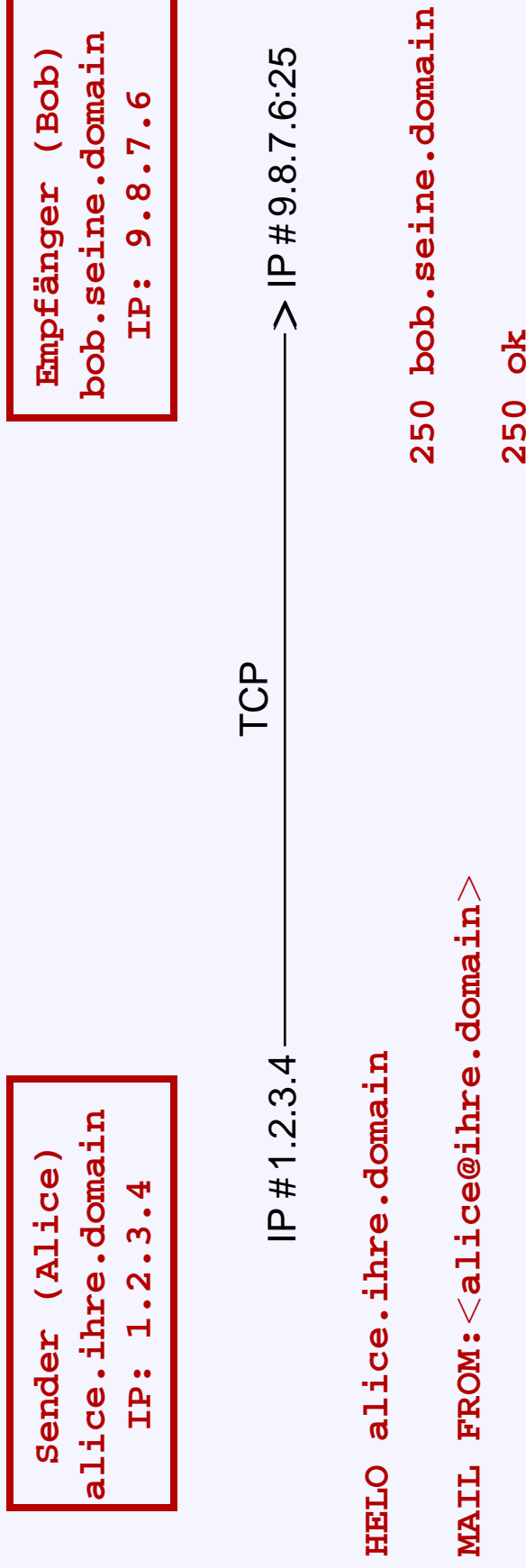
IP # 1.2.3.4 ——— TCP ———> IP # 9.8.7.6:25

HELO alice.ihre.domain

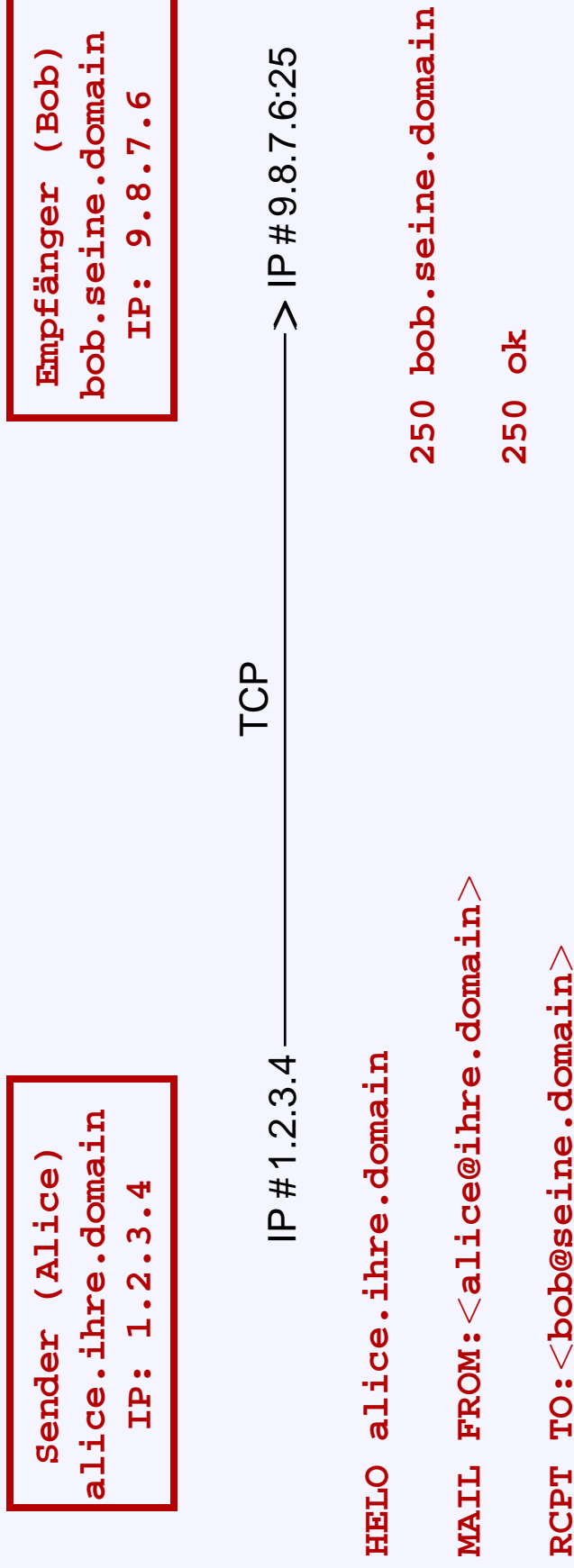
MAIL FROM:<alice@ihre.domain>

250 bob.seine.domain

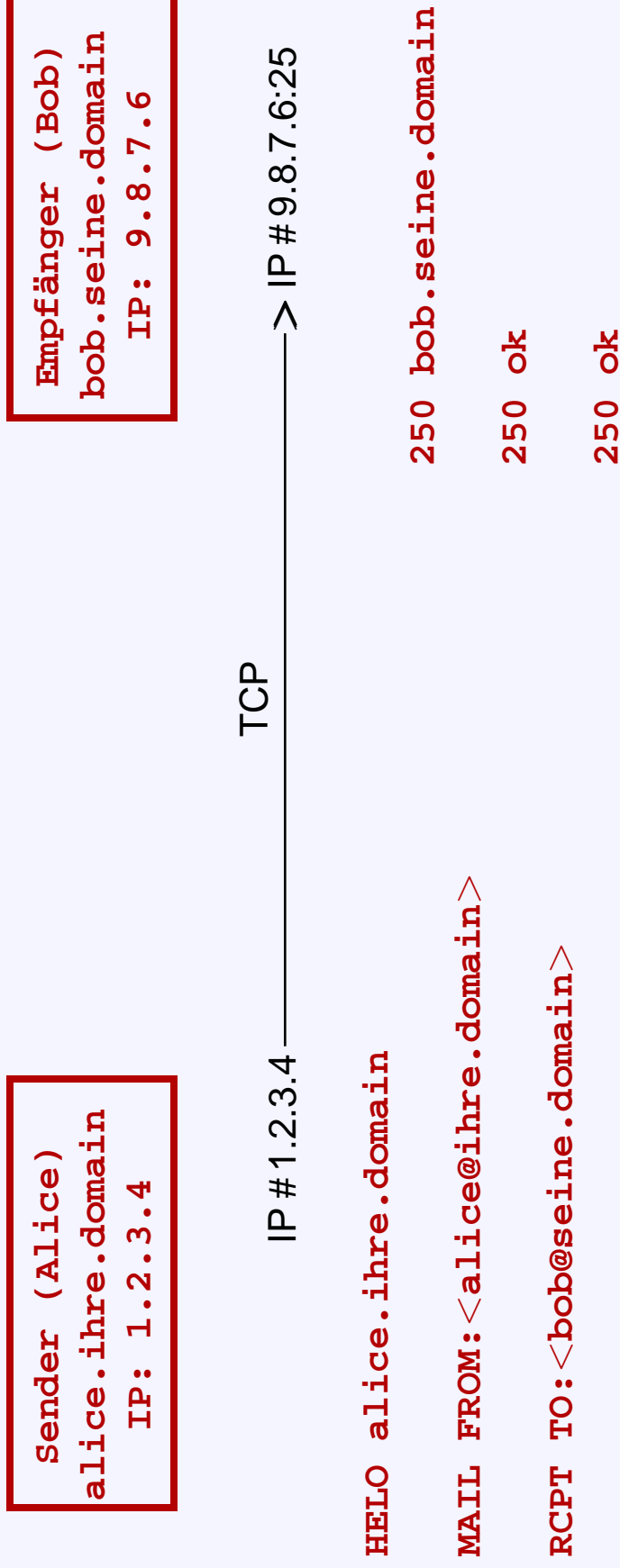
SMTP: Simple Mail Transfer Protocol



SMTP: Simple Mail Transfer Protocol

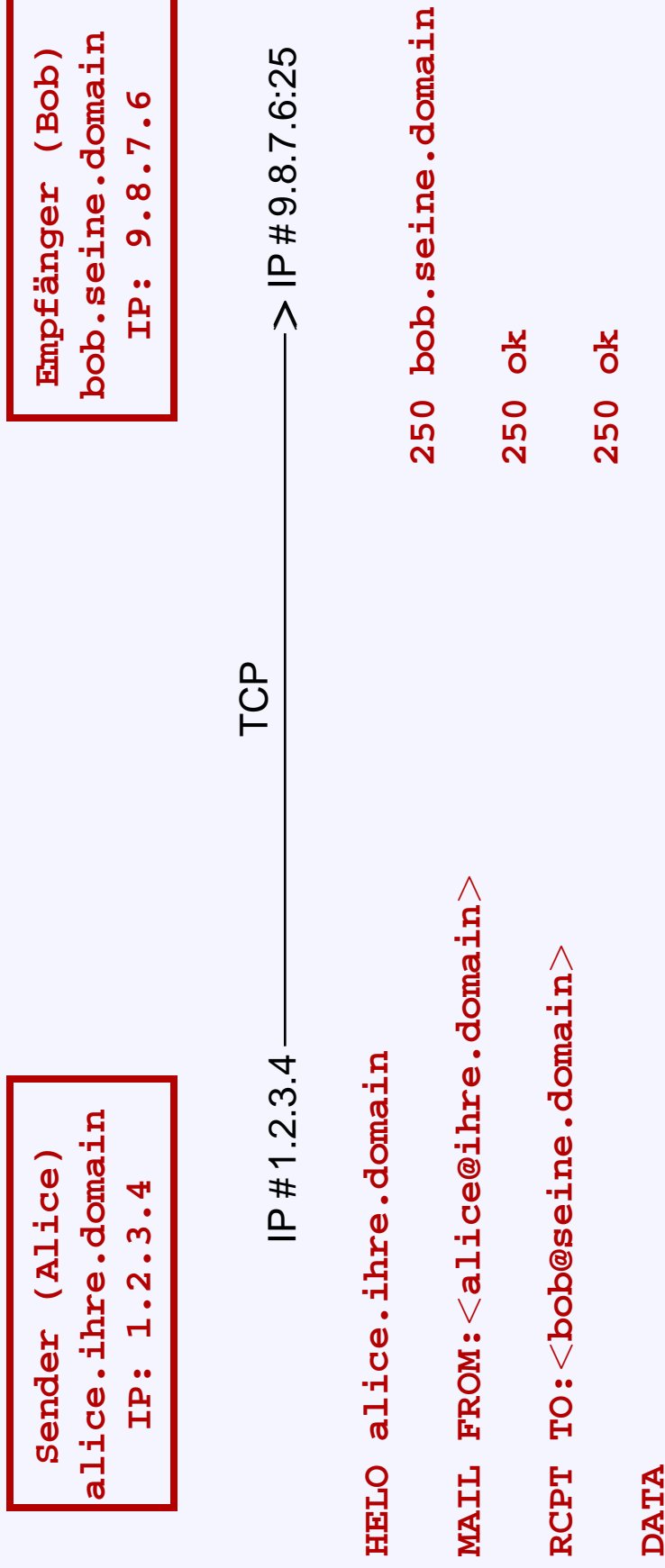


SMTP: Simple Mail Transfer Protocol

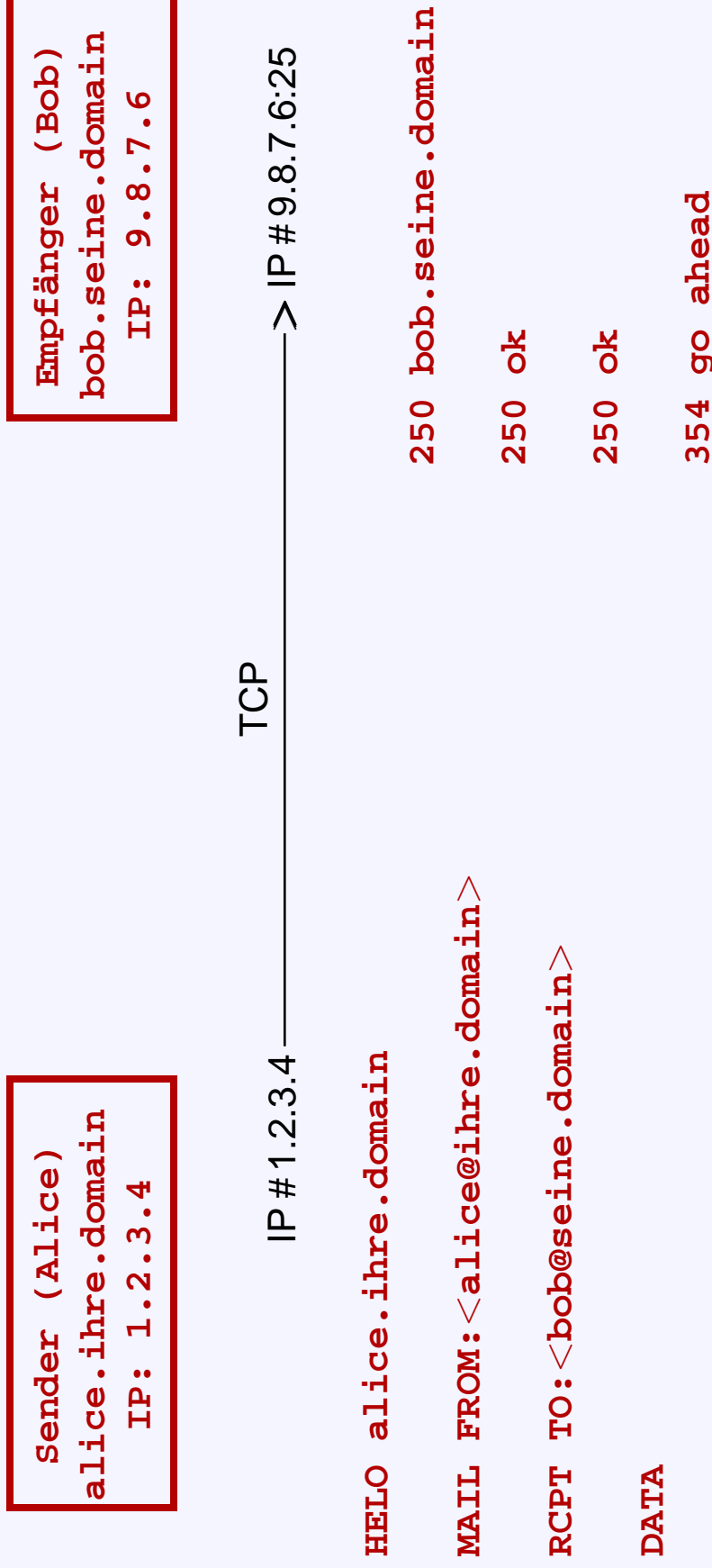


SMTP: Simple Mail Transfer Protocol

4

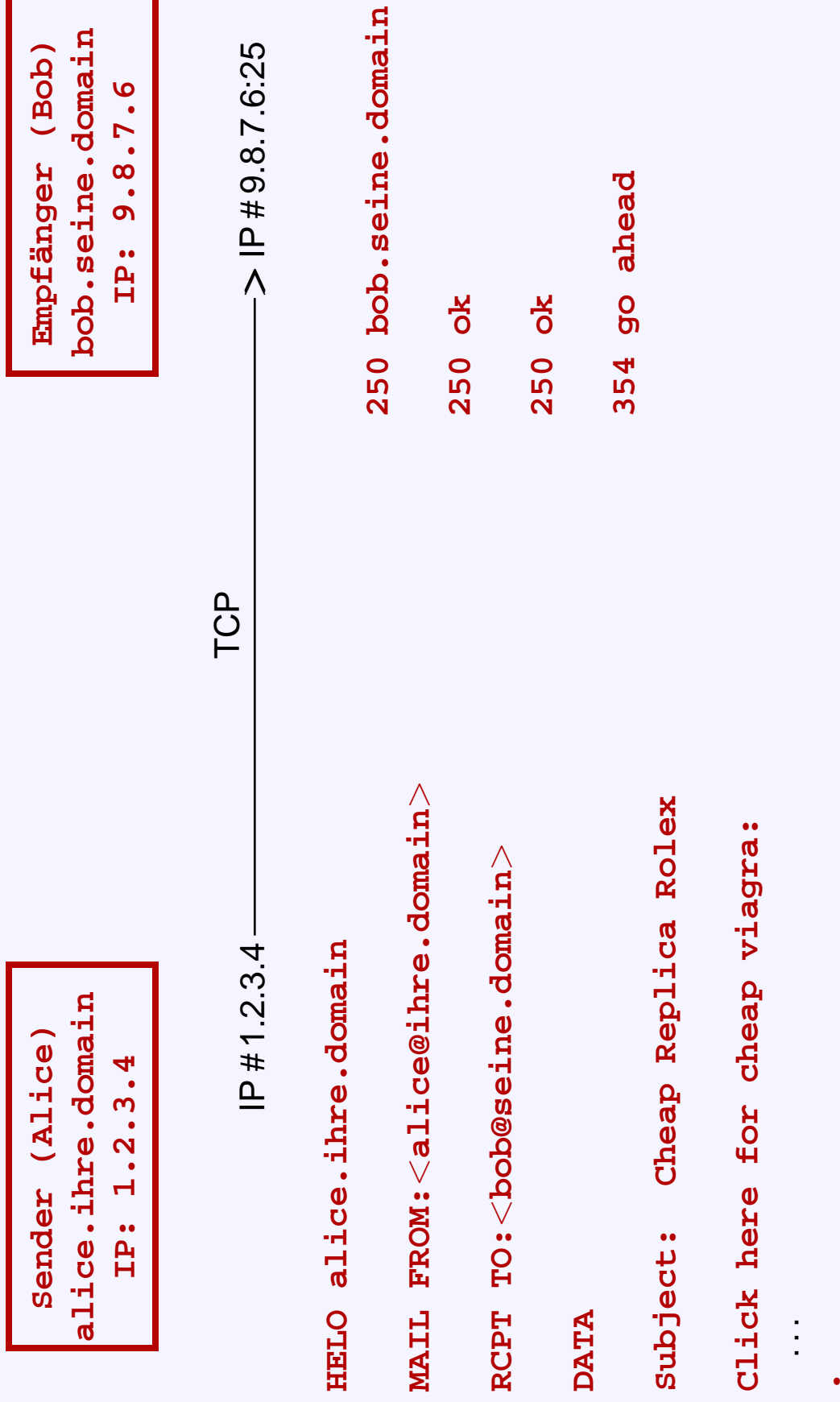


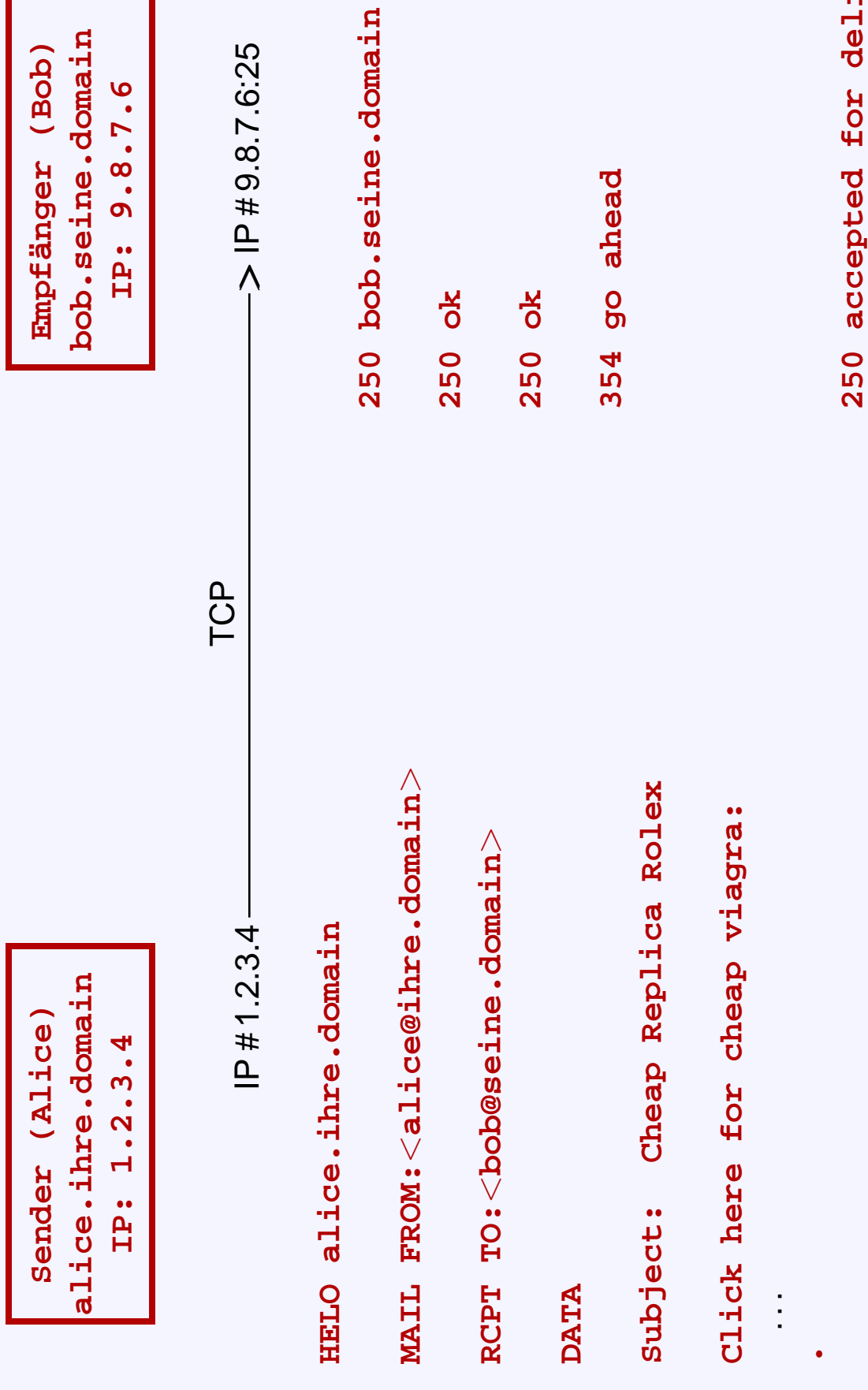
SMTP: Simple Mail Transfer Protocol



SMTP: Simple Mail Transfer Protocol

4





- ab jetzt ist Bob für die Nachricht verantwortlich!

- E-Mail in der Regel nicht authentifiziert

- E-Mail in der Regel nicht authentifiziert
- E-Mail von Jedem an Jeden soll jederzeit möglich bleiben

- E-Mail in der Regel nicht authentifiziert
- E-Mail von Jedem an Jeden soll jederzeit möglich bleiben
- Kompatibilität mit existierendem Prototoll muss gewahrt bleiben

- E-Mail in der Regel nicht authentifiziert
- E-Mail von Jedem an Jeden soll jederzeit möglich bleiben
- Kompatibilität mit existierendem Prototoll muss gewahrt bleiben
- Dennoch: in jedem Protokollschritt sind Tests und Abbruch möglich!

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

RTBL Server
www.spamcannibal.org
www.sorbs.net
...

IP# 6.6.6.6 ——— TCP ———> IP# 9.8.7.6:25

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

RTBL Server
www.spamcannibal.org
www.sorbs.net
...

IP# 6.6.6.6 ———> IP# 9.8.7.6:25
TCP

DNS (UDP)

—————>
Anfrage: IP # 6.6.6.6 ?

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

RTBL Server
www.spamcannibal.org
www.sorbs.net
...

IP# 6.6.6.6 ———> IP# 9.8.7.6:25
TCP

DNS (UDP)

→
Anfrage: IP # 6.6.6.6 ?

<

Antwort: Warnung: 6.6.6.6 ist Spamschleuder!

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

RTBL Server
www.spamcannibal.org
www.sorbs.net
...

TCP

IP# 6.6.6.6 → IP# 9.8.7.6:25

DNS (UDP)

→
Anfrage: IP # 6.6.6.6 ?

←

Antwort: Warnung: 6.6.6.6 ist Spamschleuder!

HELO alice.ihre.domain

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

RTBL Server
www.spamcannibal.org
www.sorbs.net
...

IP# 6.6.6.6 ———> IP# 9.8.7.6:25
TCP

DNS (UDP)

Anfrage: IP # 6.6.6.6 ?

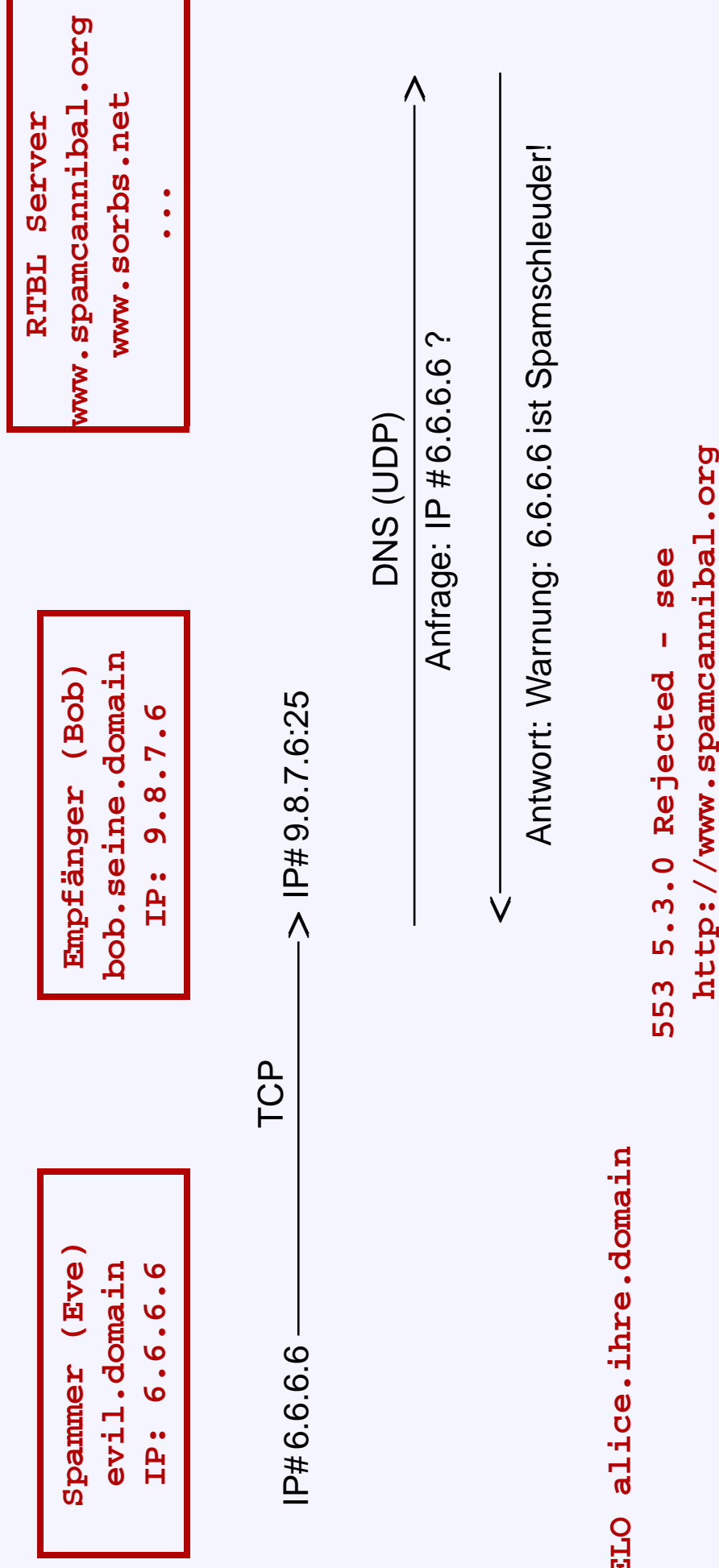
<

Antwort: Warnung: 6.6.6.6 ist Spamschleuder!

HELO alice.ihre.domain

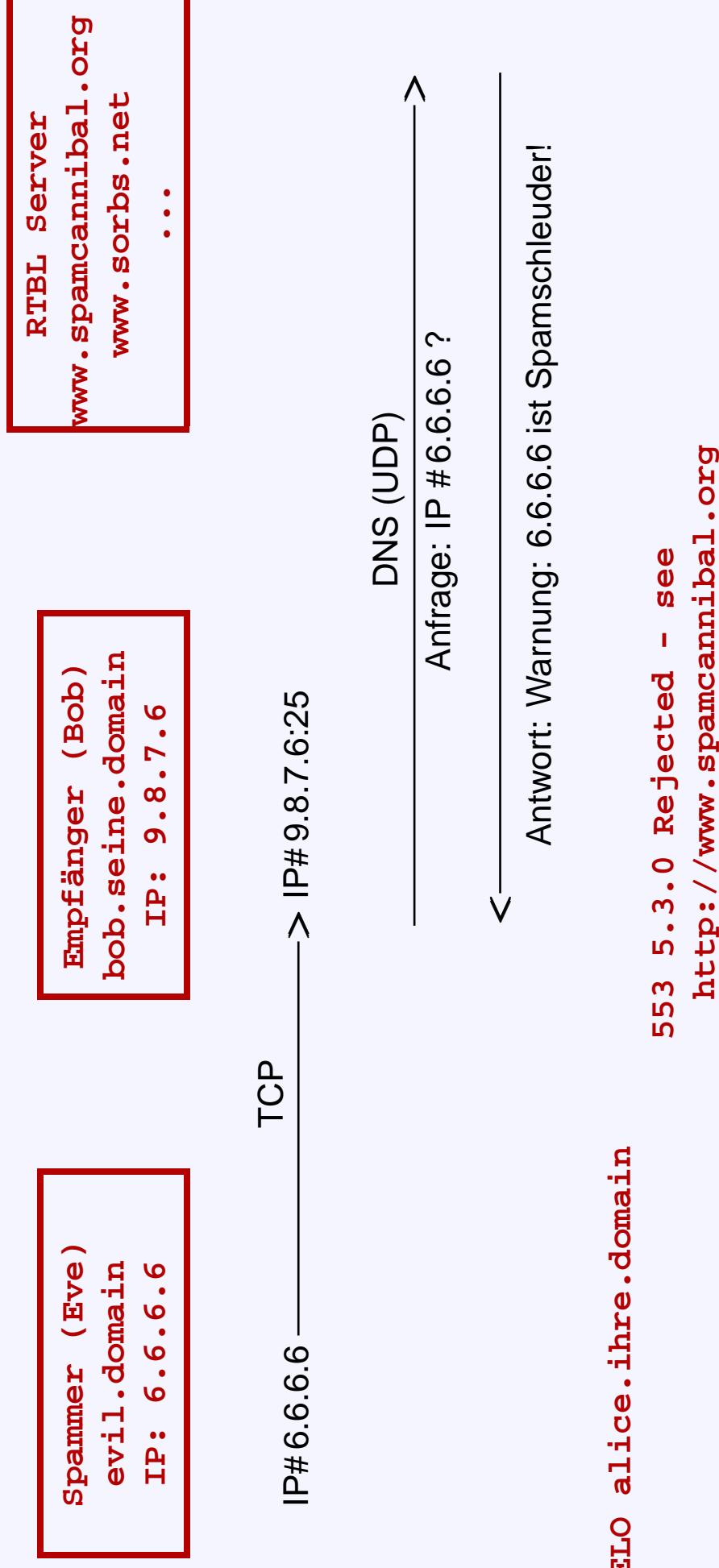
553 5.3.0 Rejected - see
<http://www.spamcannibal.org>

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6



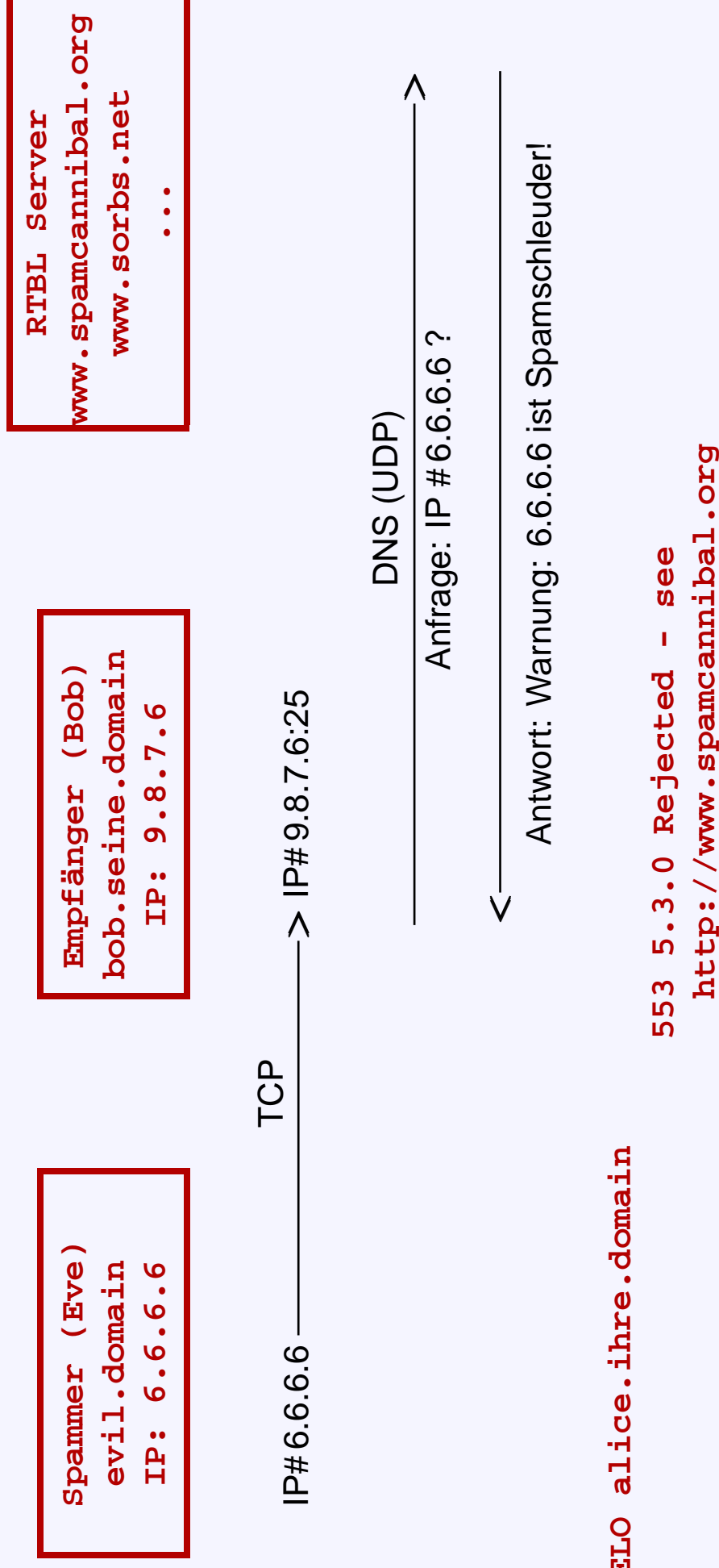
- möglichst rasche (“Echtzeit”, also “RTBL”) Reaktion auf neue Spamschleudern ist nötig

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6



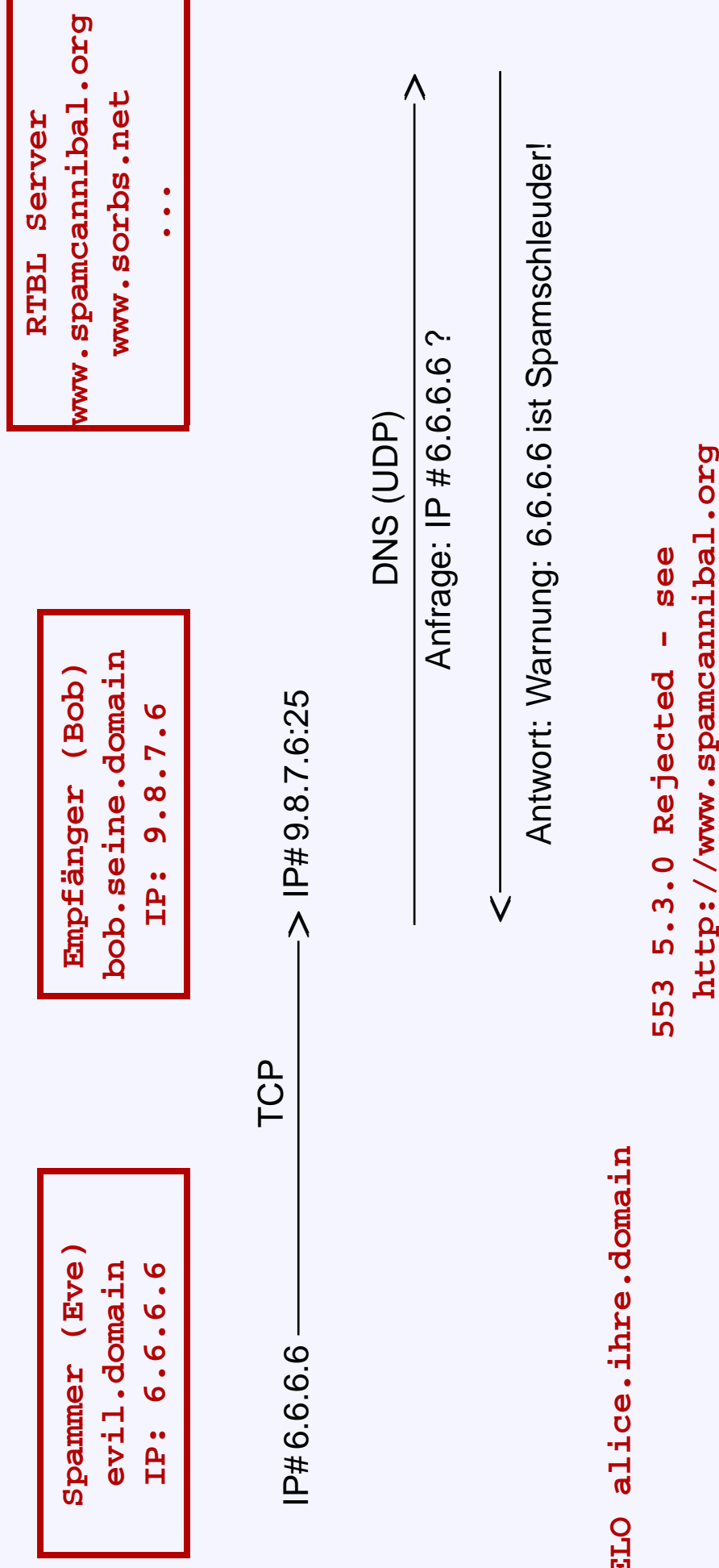
- möglichst rasche (“Echtzeit”, also “RTBL”) Reaktion auf neue Spamschleudern ist nötig
- Daher oft: vollautomatische Einstufung durch E-Mail an “Köderadressen”

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6



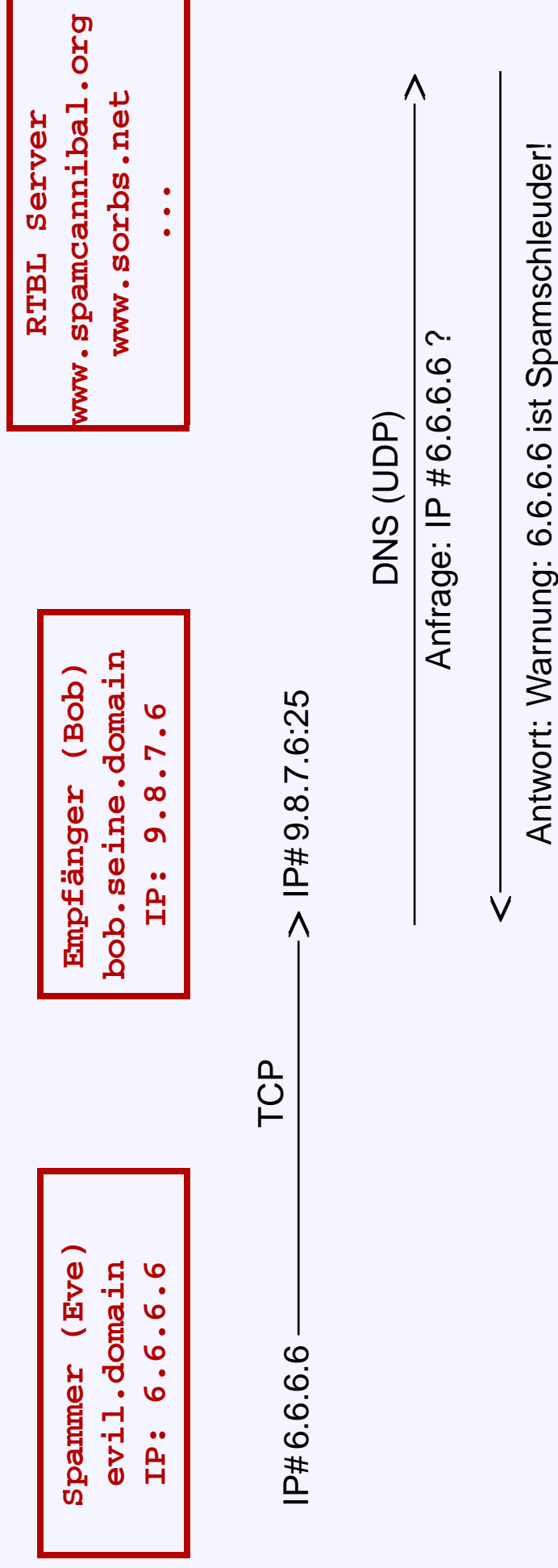
- möglichst rasche (“Echtzeit”, also “RTBL”) Reaktion auf neue Spamschleudern ist nötig
- Daher oft: vollautomatische Einstufung durch E-Mail an “Köderadressen”
- Gefahr: auch legitime Sender können (fast) unschuldig als Spammer gelistet werden

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6



- möglichst rasche (“Echtzeit”, also “RTBL”) Reaktion auf neue Spamschleudern ist nötig
- Daher oft: vollautomatische Einstufung durch E-Mail an “Köderadressen”
- Gefahr: auch legitime Sender können (fast) unschuldig als Spammer gelistet werden
- Entfernung von der Sperrliste kann kostenpflichtig sein (www.sorbs.net)

Blacklisting: Sperrt IP-Nummern bekannter Spammer 6



HELO `alice.ihre.domain`

553 5.3.0 Rejected - see

<http://www.spamcannibal.org>

- möglichst rasche (“Echtzeit”, also “RTBL”) Reaktion auf neue Spamschleudern ist nötig
- Daher oft: vollautomatische Einstufung durch E-Mail an “Köderadressen”
- Gefahr: auch legitime Sender können (fast) unschuldig als Spammer gelistet werden
- Entfernung von der Sperrliste kann kostenpflichtig sein (www.sorbs.net)
- ... oder auch einfach sehr langwierig...

Zum Beispiel am 18.Juni 2007:

```
This is the Postfix program at host mail2.pdi-berlin.de.  
<martin.wilkens@quantum.physik.uni-potsdam.de>: host  
hp.rz.uni-potsdam.de[141.89.64.1] said: 553 5.3.0 Rejected - see  
http://www.spamcannibal.org (in reply to MAIL FROM command)
```

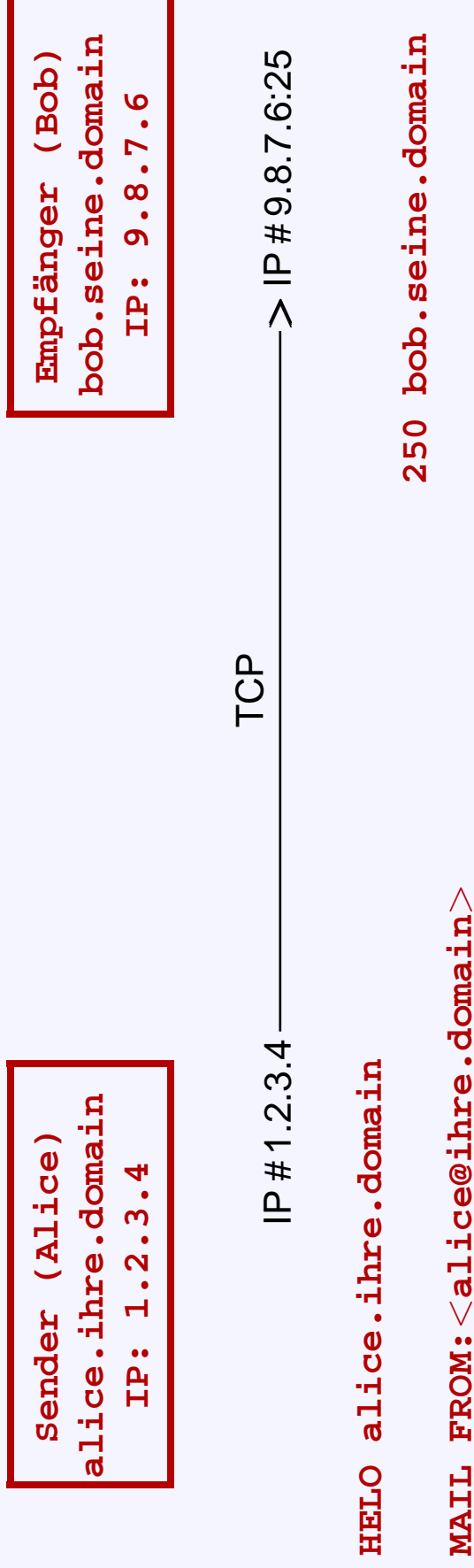
Zum Beispiel am 18.Juni 2007:

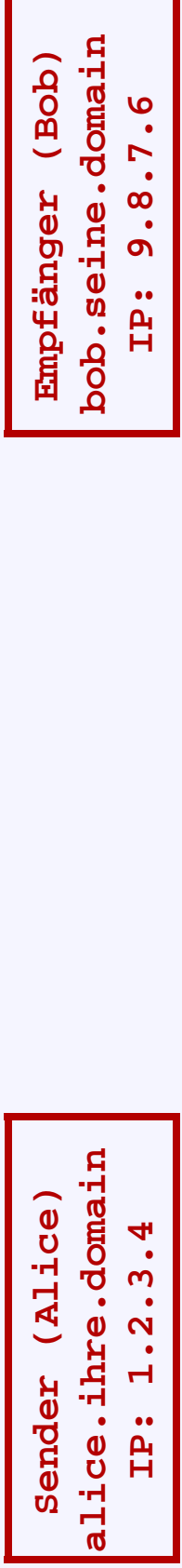
```
This is the Postfix program at host mail2.pdi-berlin.de.  
<martin.wilkens@quantum.physik.uni-potsdam.de>: host  
hp.rz.uni-potsdam.de[141.89.64.1] said: 553 5.3.0 Rejected - see  
http://www.spamcannibal.org (in reply to MAIL FROM command)
```

Ursache (laut www.spamcannibal.org) war eine einzige(!) email vom 23. Mai 2004(!) an eine Köderadresse:

```
...  
Received: from mail2.pdi-berlin.de (mail2.pdi-berlin.de [62.141.165.111])  
by ns2.is.bizsystems.com (8.12.11/8.12.11) with ESMTP id i4NBED1b018311  
for <michael@bizsystems.com>; Sun, 23 May 2004 04:14:16 -0700  
Received: from localhost (localhost [127.0.0.1])  
...  
Subject: VIRUS (I-Worm.LovGate.w ) IN MAIL FROM YOU  
VIRUS ALERT  
Our content checker found  
virus: I-Worm.LovGate.w
```

... also eine gutgemeinte, aber an einen gefälschten Absender fehlgeleitete automatische Viruswarnung!





IP # 1.2.3.4 ——— TCP ———> IP # 9.8.7.6:25

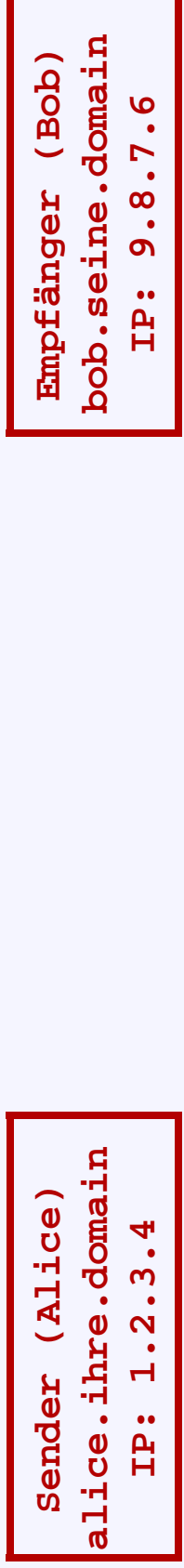
HELO **alice.ihre.domain**

250 bob.seine.domain

MAIL FROM: <**alice@ihre.domain**>

Die Argumente von

- **HELO** (Name des sendenden Servers) und, vor allem,
 - **MAIL FROM** (Absenderadresse)
- können überprüft werden:



IP # 1.2.3.4 ————— TCP —————> IP # 9.8.7.6:25

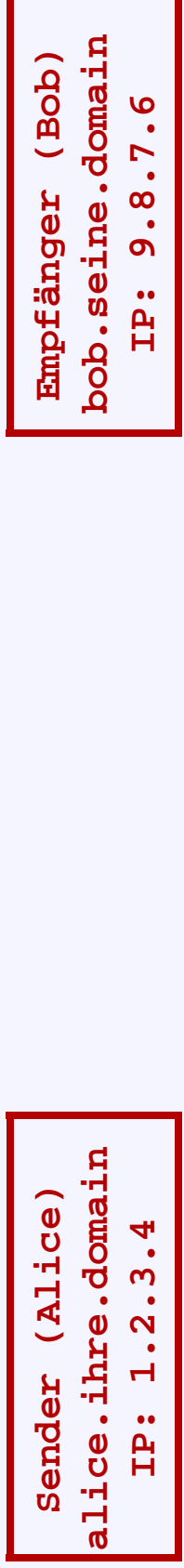
HELO **alice.ihre.domain**

250 bob.seine.domain

MAIL FROM: <**alice@ihre.domain**>

Die Argumente von

- **HELO** (Name des sendenden Servers) und, vor allem,
- **MAIL FROM** (Absenderadresse) können überprüft werden:
- Existiert die angegebene Domain überhaupt? (einfache DNS-Anfrage)



IP # 1.2.3.4 ————— TCP —————> IP # 9.8.7.6:25

HELO alice.ihre.domain
MAIL FROM: <alice@ihre.domain>
250 bob.seine.domain

Die Argumente von

- **HELO** (Name des sendenden Servers) und, vor allem,
- **MAIL FROM** (Absenderadresse)
können überprüft werden:
- Existiert die angegebene Domain überhaupt?
(einfache DNS-Anfrage)
- Passt die Domain zur IP-Nummer des Senders?
(ebenfalls per DNS: SPF-Einträge)

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

Nameserver
ns.ihre.domain

IP# 6.6.6.6 ———> IP# 9.8.7.6:25
TCP

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

Nameserver
ns.ihre.domain

IP# 6.6.6.6 ———> TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

250 ok bob.seine.domain

MAIL FROM: <alice@ihre.domain>

UDP (DNS)

—————>
wer sendet mail für ihre.domain?

SPF: Sender Policy Framework

9

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

Nameserver
ns.ihre.domain

IP# 6.6.6.6 ———> TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

250 ok bob.seine.domain

MAIL FROM:<alice@ihre.domain>

UDP (DNS)

wer sendet mail für ihre.domain?

<----->
Antwort: nur IP # 1.2.3.4!

SPF: Sender Policy Framework

9

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

Nameserver
ns.ihre.domain

IP# 6.6.6.6 ———> TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

250 ok bob.seine.domain

MAIL FROM:<alice@ihre.domain>

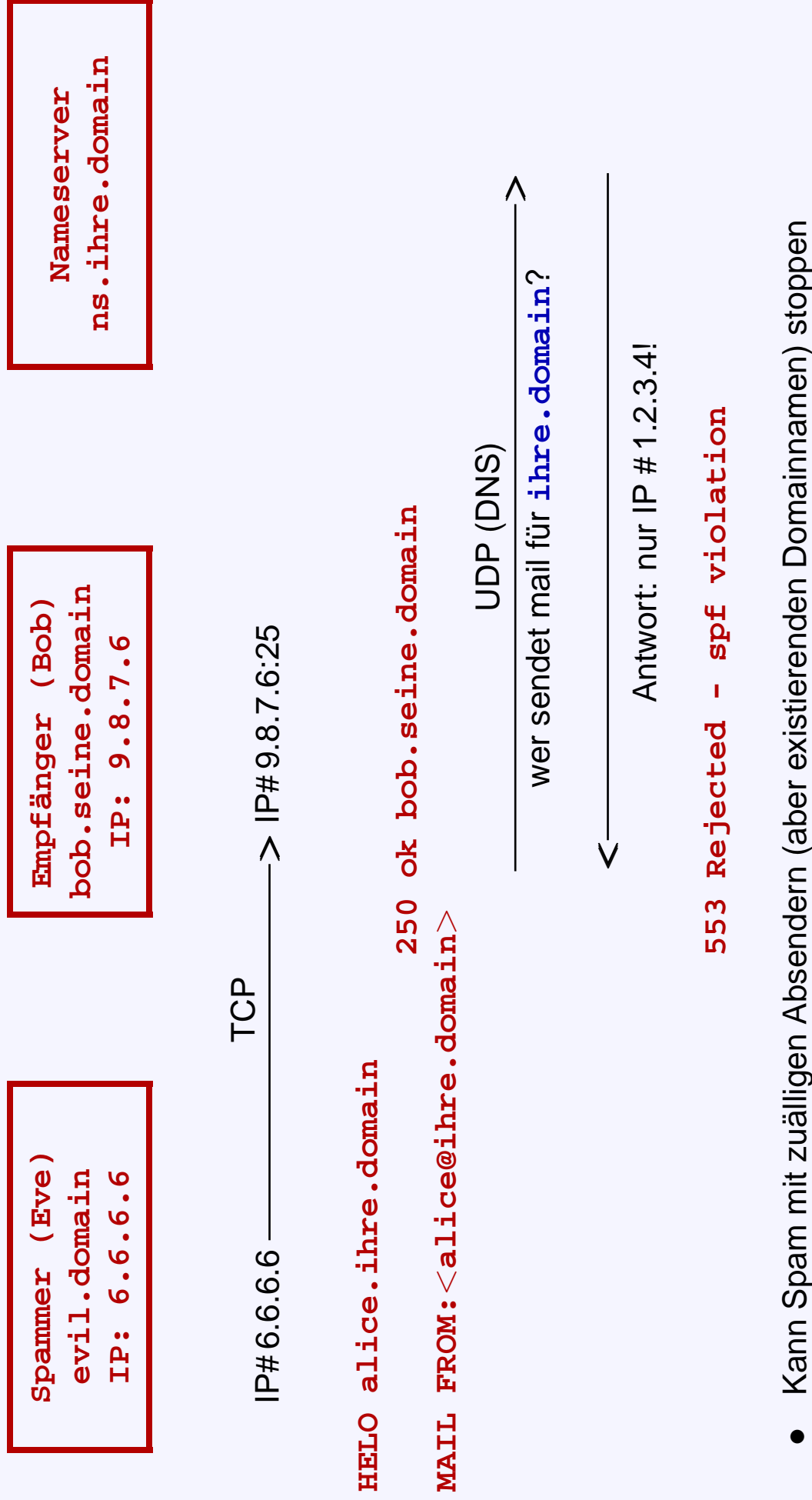
UDP (DNS)

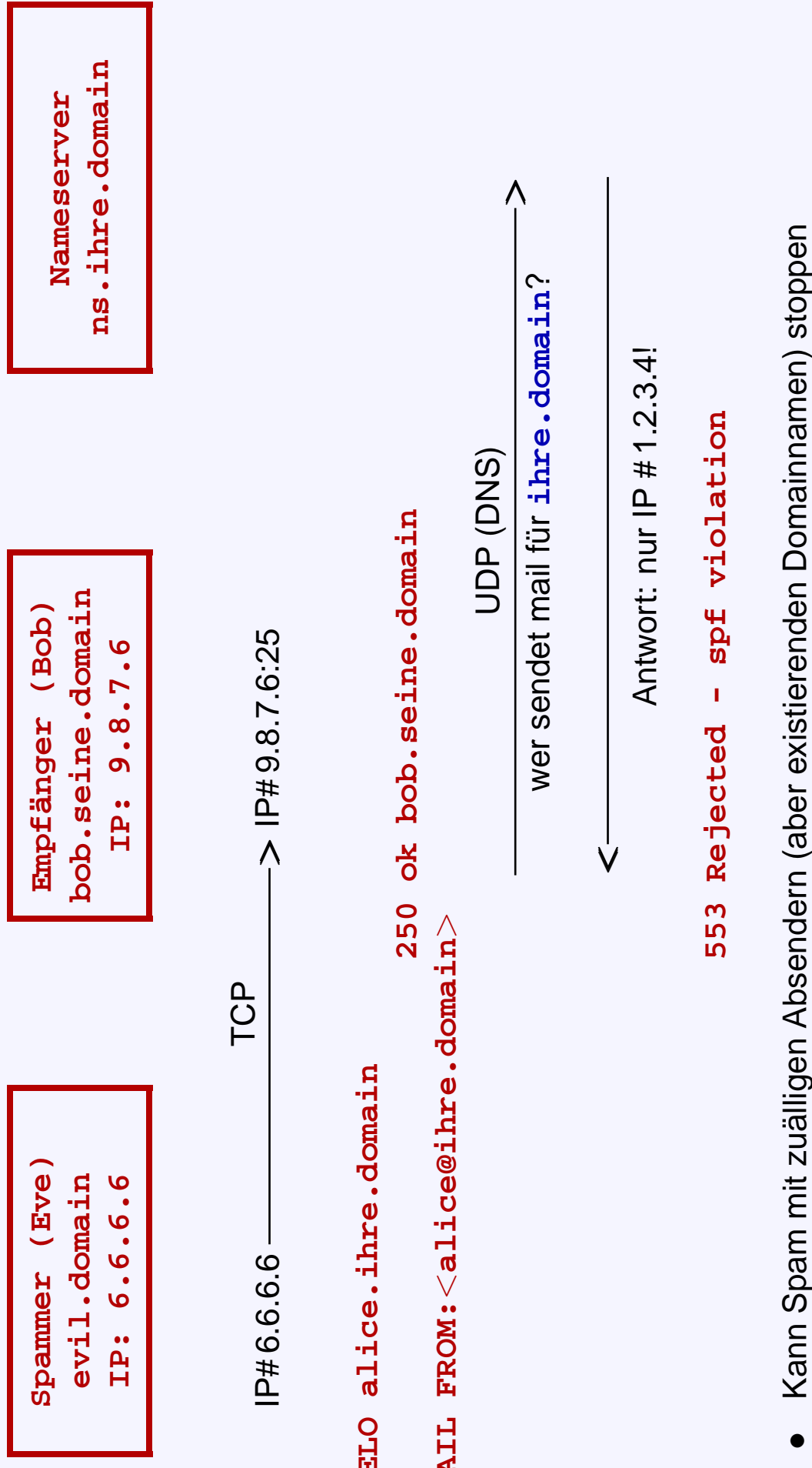
wer sendet mail für ihre.domain?

<—————>

Antwort: nur IP # 1.2.3.4!

553 Rejected - spf violation





- Kann Spam mit zufälligen Absendern (aber existierenden Domainnamen) stoppen
- Kann (im obigen Beispiel: Alice) vor “Bounce-Spam” schützen

SPF: Sender Policy Framework

9



IP# 6.6.6.6 ———> IP# 9.8.7.6:25
TCP

HELO `alice.ihre.domain`

250 ok `bob.seine.domain`

MAIL FROM: `<alice@ihre.domain>`

UDP (DNS)

wer sendet mail für `ihre.domain`?

<—————

Antwort: nur IP # 1.2.3.4!

553 Rejected - spf violation

- Kann Spam mit zufälligen Absendern (aber existierenden Domainnamen) stoppen
- Kann (im obigen Beispiel: Alice) vor “Bounce-Spam” schützen
- Problem: Weiterleitung von E-mail oder einfache Mailinglisten (per `.forward`) funktionieren nicht!

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<bob@seine.domain>

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<bob@seine.domain>

in .forward: charlie@charlies.domain

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

```
HELO alice.ihre.domain
```

```
MAIL FROM:<alice@ihre.domain>
```

```
RCPT TO:<bob@seine.domain>
```

```
in .forward: charlie@charlies.domain
```

```
HELO bob.seine.domain
```

```
MAIL FROM:<SRS0+XX=TT=ihre.domain=alice@seine.domain>
```

```
RCPT TO:<charlie@charlies.domain>
```

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

```
HELO alice.ihre.domain
```

```
MAIL FROM:<alice@ihre.domain>
```

```
RCPT TO:<bob@seine.domain>
```

```
in .forward: charlie@charlies.domain
```

```
HELO bob.seine.domain
```

```
MAIL FROM:<SRS0+XX=TT=ihre.domain=alice@seine.domain>
```

```
RCPT TO:<charlie@charlies.domain>
```

- Domain wird durch die eigene Domain ersetzt (so dass Weiterleitung ohne SPF-Verletzung möglich ist)

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

```
HELO alice.ihre.domain
```

```
MAIL FROM:<alice@ihre.domain>
```

```
RCPT TO:<bob@seine.domain>
```

```
in .forward: charlie@charlies.domain
```

```
HELO bob.seine.domain
```

```
MAIL FROM:<SRS0+XX=TT=ihre.domain=alice@seine.domain>
```

```
RCPT TO:<charlie@charlies.domain>
```

- Domain wird durch die eigene Domain ersetzt (so dass Weiterleitung ohne SPF-Verletzung möglich ist)
- Bisheriger Absender wird in den Lokalteil kodiert

Verfahren um bei Email-Weiterleitung die Senderadresse SPF-konform umzuschreiben:

```
Sender (Alice)  
alice.ihre.domain  
IP: 1.2.3.4
```

```
Empfänger (Bob)  
bob.seine.domain  
IP: 9.8.7.6
```

```
Empfänger (Charlie)  
pc.charlies.domain  
IP: 4.7.1.1
```

```
HELO alice.ihre.domain
```

```
MAIL FROM:<alice@ihre.domain>
```

```
RCPT TO:<bob@seine.domain>
```

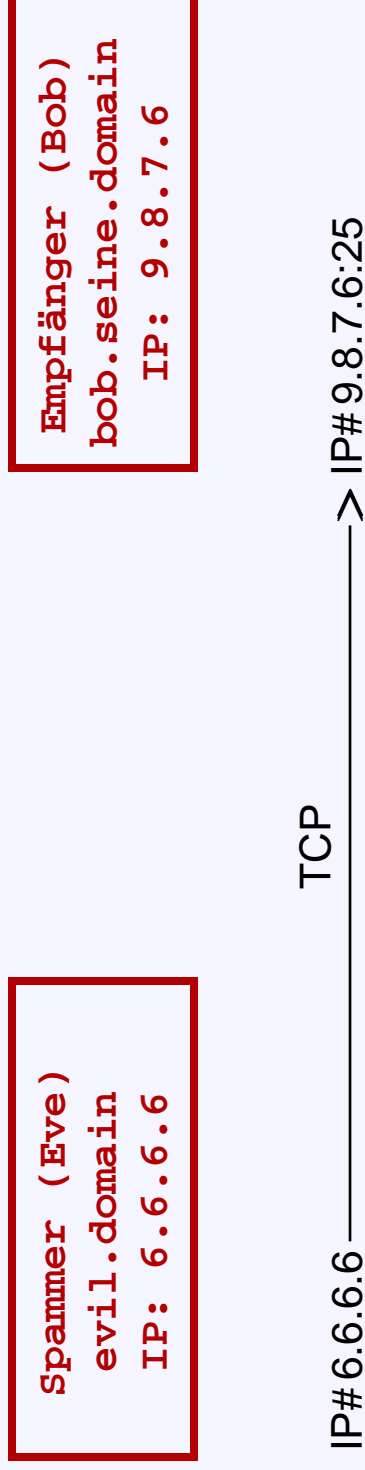
```
in .forward: charlie@charlies.domain
```

```
HELO bob.seine.domain
```

```
MAIL FROM:<SRS0+XX=TT=ihre.domain=alice@seine.domain>
```

```
RCPT TO:<charlie@charlies.domain>
```

- Domain wird durch die eigene Domain ersetzt (so dass Weiterleitung ohne SPF-Verletzung möglich ist)
- Bisheriger Absender wird in den Lokalteil kodiert
- und mit Zeitstempel (**TT**) und kryptografischer Signatur (**XX**) gesichert



Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ———> TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

250 ok bob.seine.domain

250 ok

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ————> IP# 9.8.7.6:25
TCP

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@charlies.domain>

250 ok bob.seine.domain

250 ok

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ————> IP# 9.8.7.6:25
TCP

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@charlies.domain>

250 ok bob.seine.domain

250 ok

554 I do not accept mail for this domain

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 —————> TCP —————> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@charlies.domain>

250 ok bob.seine.domain

250 ok

554 I do not accept mail for this domain

- Test auf erlaubte (eigene oder gehostete) Domain sollte auf jeden Fall erfolgen!
(Weiterleitung an fremde Domain sollte auf jeden Fall vermieden werden!)

Empfängerprüfung: lokaler Teil der Adresse

12

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ————> IP# 9.8.7.6:25
TCP

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

TCP

IP# 6.6.6.6 —————> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

250 ok bob.seine.domain

250 ok

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 —————> TCP —————> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@seine.domain>

250 ok bob.seine.domain

250 ok

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 —————> TCP —————> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@seine.domain>

250 ok bob.seine.domain

250 ok

Test: gibt es hier einen Charlie?

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ————> IP# 9.8.7.6:25
TCP

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@seine.domain>

250 ok bob.seine.domain

250 ok

Test: gibt es hier einen Charlie?

554 no such mailbox



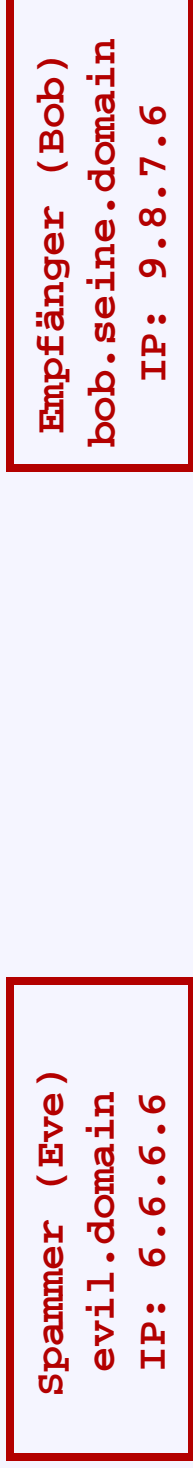
IP#6.6.6.6 —————> TCP —————> IP#9.8.7.6:25

```
HELO alice.ihre.domain
MAIL FROM:<alice@ihre.domain>
RCPT TO:<charlie@seine.domain>
250 ok bob.seine.domain
250 ok
```

Test: gibt es hier einen Charlie?

554 no such mailbox

- Scheint einfach, kann aber kompliziert sein und war aber früher unüblich



IP# 6.6.6.6 —————> TCP —————> IP# 9.8.7.6:25

```
HELO alice.ihre.domain
MAIL FROM:<alice@ihre.domain>
RCPT TO:<charlie@seine.domain>

250 ok bob.seine.domain
250 ok
```

Test: gibt es hier einen Charlie?

554 no such mailbox

- Scheint einfach, kann aber kompliziert sein und war aber früher unüblich
- Erfordert meist Abfrage einer lokalen Datenbank

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP#6.6.6.6 ————> TCP ————> IP#9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<charlie@seine.domain>

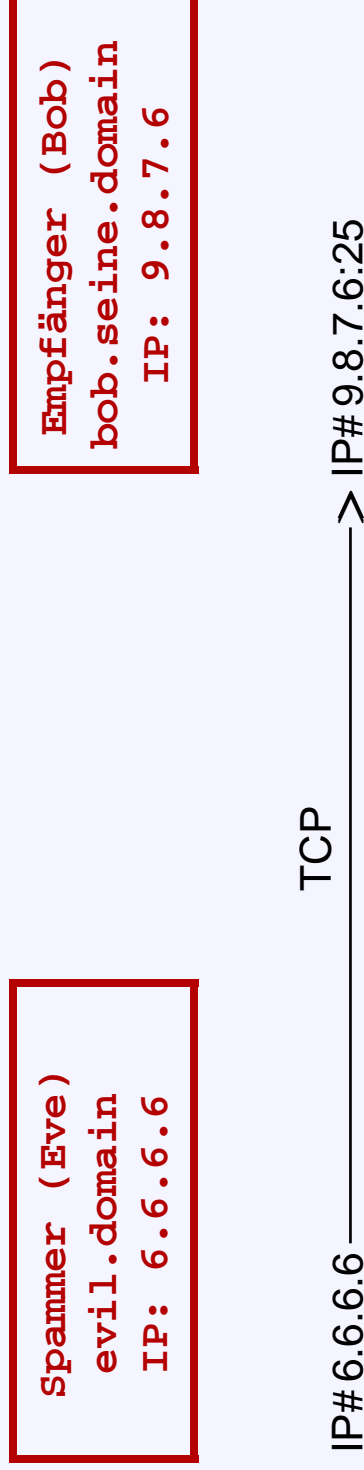
250 ok bob.seine.domain

250 ok

Test: gibt es hier einen Charlie?

554 no such mailbox

- Scheint einfach, kann aber kompliziert sein und war aber früher unüblich
- Erfordert meist Abfrage einer lokalen Datenbank
- Erspart aber massenhaft unzustellbare Email, und insbesondere “double-bounces”



Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ——— TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

MAIL FROM:<alice@ihre.domain>

RCPT TO:<bob@seine.domain>

250 ok bob.seine.domain

250 ok

250 ok

Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ——— TCP ———> IP# 9.8.7.6:25

HELO alice.ihre.domain

250 ok bob.seine.domain

MAIL FROM:<alice@ihre.domain>

250 ok

RCPT TO:<bob@seine.domain>

250 ok

DATA

354 go ahead

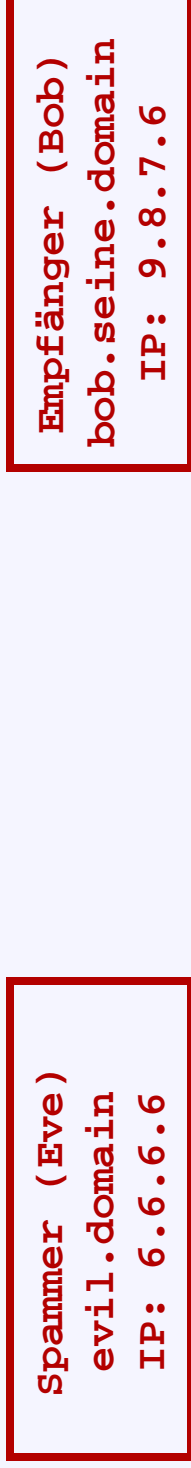
Spammer (Eve)
evil.domain
IP: 6.6.6.6

Empfänger (Bob)
bob.seine.domain
IP: 9.8.7.6

IP# 6.6.6.6 ——— TCP ———> IP# 9.8.7.6:25

```
HELO alice.ihre.domain
MAIL FROM:<alice@ihre.domain>
RCPT TO:<bob@seine.domain>
DATA
Subject: Cheap Replica Rolex
Click here for cheap viagra:
...
.
```

250 ok bob.seine.domain
250 ok
250 ok
354 go ahead

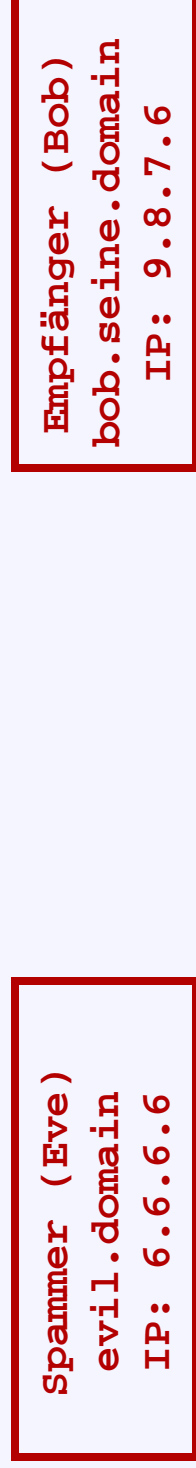


IP# 6.6.6.6 ——— TCP ———> IP# 9.8.7.6:25

```
HELO alice.ihre.domain
MAIL FROM:<alice@ihre.domain>
RCPT TO:<bob@seine.domain>
DATA
Subject: Cheap Replica Rolex
Click here for cheap viagra:
...
.
```

250 ok bob.seine.domain
250 ok
250 ok
354 go ahead

Filterung: Spam oder kein Spam?



IP# 6.6.6.6 —————> IP# 9.8.7.6:25

```
HELO alice.ihre.domain
MAIL FROM:<alice@ihre.domain>
RCPT TO:<bob@seine.domain>
DATA
Subject: Cheap Replica Rolex
Click here for cheap viagra:
...
.
```

250 ok bob.seine.domain
250 ok
250 ok
354 go ahead

Filterung: Spam oder kein Spam?

554 rejected: **this message is likely spam**

Filterung zum Beispiel durch **spamassassin** (<http://www.spamassassin.org>):

Kann Spam erkennen und markieren:

Filterung zum Beispiel durch **spamassassin** (<http://www.spamassassin.org>):
Kann Spam erkennen und markieren:

- sowohl zur Einordnung in Spam-Ordner durch Email-Client,

Filterung zum Beispiel durch **spamassassin** (<http://www.spamassassin.org>):

Kann Spam erkennen und markieren:

- sowohl zur Einordnung in Spam-Ordner durch Email-Client,
- als auch zur Zurückweisung durch SMTP-Server

```
physik.uni-potsdam.de:m4_rules(  
d  
 , fbin/gmail-spamfilter  
 , aemailbackup@local.host  
 , m4_ldapquery(  
     m4_peopledn ? physikmaildrop;mail ? sub  
     ? ( & ( | (objectclass=inetorgperson)  
         (objectclass=physikalias) )  
         ( | (mail=${LOCAL0}@physik.uni-potsdam.de)  
             (physikalias=${LOCAL0}@physik.uni-potsdam.de) )  
         )  
     ? preserveextension=1  
 )  
 , 5  
 )
```

Regeln für Adressen `physik.uni-potsdam.de`

Inhaltsfilter aktivieren (Spamassassin)

Empfänger per LDAP-Anfrage suchen

falls kein Treffer: Antwort 554 no such mailbox

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:
- Das reicht natürlich nicht: `Email`

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:
- Das reicht natürlich nicht: `Email`
- Beliebt: Bilder statt Klartext

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:
- Das reicht natürlich nicht: `Email`
- Belieb: Bilder statt Klartext
aber nicht so:
``

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:
- Das reicht natürlich nicht: `Email`
- Belieb: Bilder statt Klartext
aber nicht so:
``
- Dynamische Erzeugung durch Javascript

Mögliche Quellen, aus denen Spammer Email-Adressen erhalten können:

- Scannen von Webseiten
- Eingaben in Webformulare
- Adressbücher von durch Malware befallenen Rechner
(die dann oft selbst als Viren oder Spamschleuder benutzt werden)

Gegenmassnahmen:

- Verschleiern von Adressen auf Webseiten:
 - Das reicht natürlich nicht: `Email`
 - Beliebt: Bilder statt Klartext
aber nicht so:
``
- Dynamische Erzeugung durch Javascript
- Häufiger Wechsel der Email-Adresse

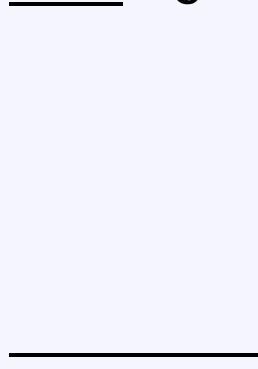
`nhrmrxr - jupp@29.09.2006.best-before.qipc.org`

nhrmrxr - jupp@29.09.2006.best-before.qipc.org



eigener Domainname

nhrmrxr - jupp@29.09.2006.best-before.qipc.org



eigener Domainname

Verfallsdatum kodiert als Subdomain

nhrmxxr - jupp@29.09.2006.best-before.qipc.org



eigener Domainname

Verfallsdatum kodiert als Subdomain

eigentliche Empfängeradresse

nhrmxxr - jupp@29.09.2006.best-before.qipc.org

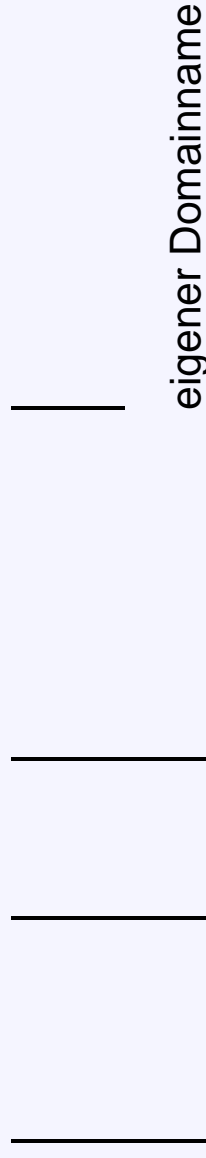


Verfallsdatum kodiert als Subdomain

eigentliche Empfängeradresse

Kryptografische Signatur der Adresse

nhrmxxr - jupp@29.09.2006.best-before.qipc.org



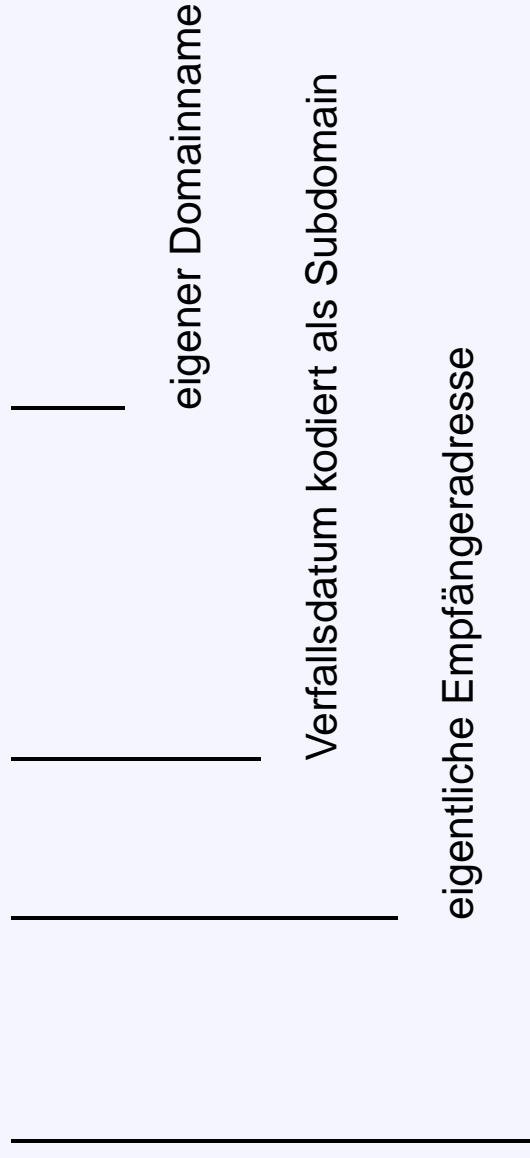
Verfallsdatum kodiert als Subdomain

eigentliche Empfängeradresse

Kryptografische Signatur der Adresse

- Sowohl Datum als auch Signatur sind sehr leicht verifizierbar
(patch für Qmail: <http://www.best-before.qipc.org> (demnächst...))

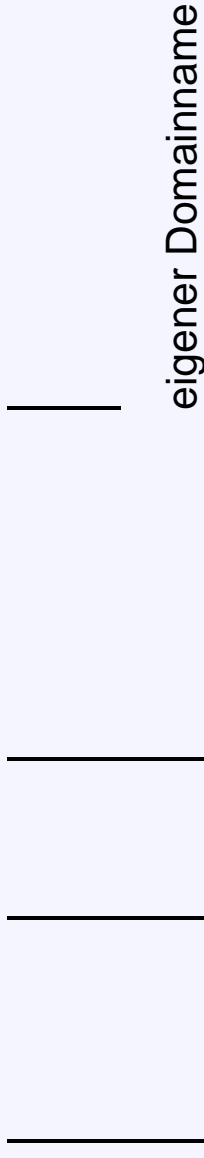
nhrmxxr - jupp@29.09.2006.best-before.qipc.org



Kryptografische Signatur der Adresse

- Sowohl Datum als auch Signatur sind sehr leicht verifizierbar (patch für Qmail: <http://www.best-before.qipc.org> (demnächst...))
- Nach Ablauf der Adresse: Löschung des DNS-Eintrags macht Adresse sofort unzustellbar

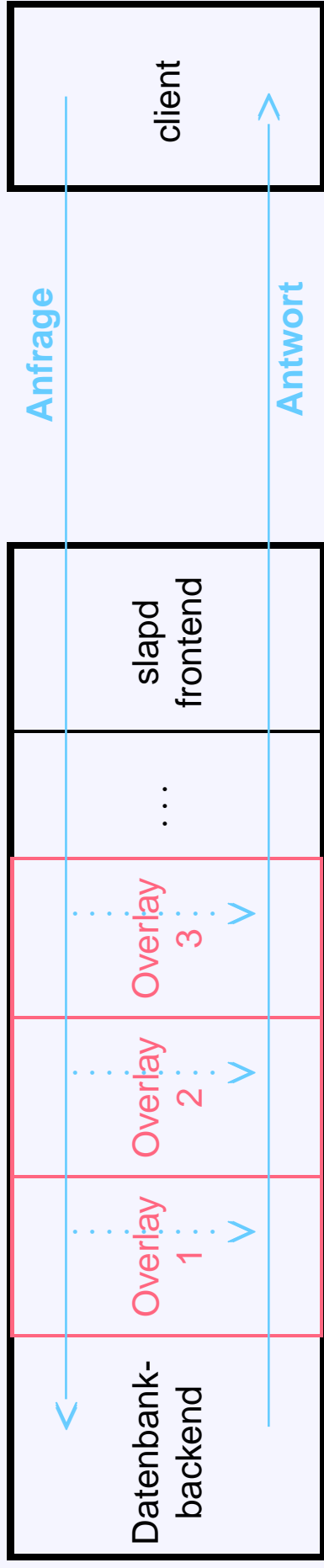
nhrmxxr - jupp@29.09.2006.best-before.qipc.org



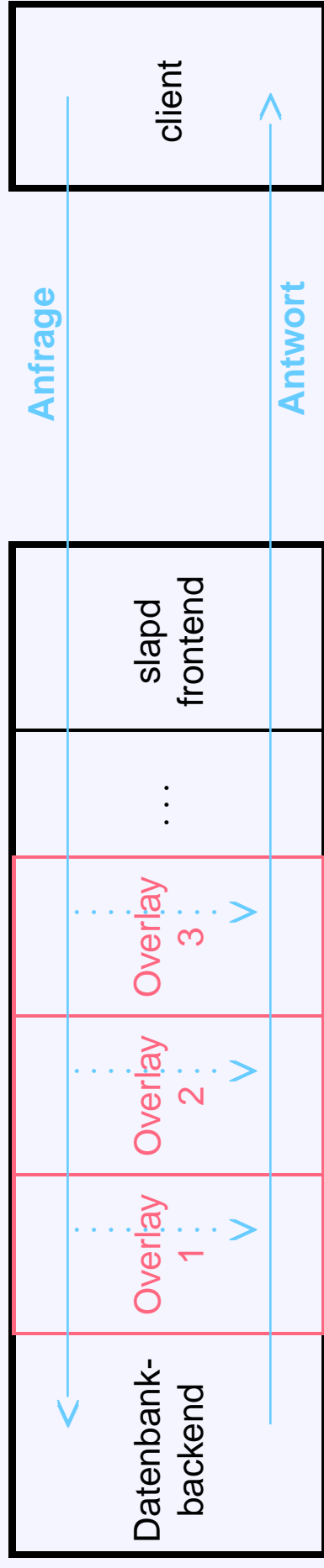
Kryptografische Signatur der Adresse

- Sowohl Datum als auch Signatur sind sehr leicht verifizierbar (patch für Qmail: <http://www.best-before.qipc.org> (demnächst...))
- Nach Ablauf der Adresse: Löschung des DNS-Eintrags macht Adresse sofort unzustellbar
- Adressen mit beliebiger Gültigkeitsdauer sind jederzeit erzeugbar

- Beliebige viele Overlays können zwischen slapd(-frontend) und Datenbank(-backend) gelegt werden.
- Anfrage und Antwort durchlaufen die Overlays, können modifiziert werden:



- Beliebige viele Overlays können zwischen slapd(-frontend) und Datenbank(-backend) gelegt werden.
- Anfrage und Antwort durchlaufen die Overlays, können modifiziert werden:



- Beispiel: **bbmail** (<http://www.best-before.qipc.org>):
Email-Adressen werden beim Lesen dynamisch mit "Verfallsdatum" und Signatur versehen:

mail: =====jupp@20.00.0000.best-before.qipc.org

wird zu

mail: snxdgt-jupp@25.08.2007.best-before.qipc.org

- Alternativen zu SMTP: IM2000, ..., ???
- Andere Ideen ?

- Alternativen zu SMTP: IM2000, ..., ???
- Andere Ideen ?
- Aber die sicherste Massnahme wäre...

- Alternativen zu SMTP: IM2000, ..., ???
- Andere Ideen ?
- Aber die sicherste Massnahme wäre...

Erziehung der Nutzer:

Kauft nicht bei Spammern!