How to get control over email?

Patrik Fältström

paf@cisco.com

The discussion is wrong!

- I am of the view people attack the spam problem from the wrong angle
  - Look for a solution
  - Fine-tune it
  - Look for a problem the solution solves

Alternative method

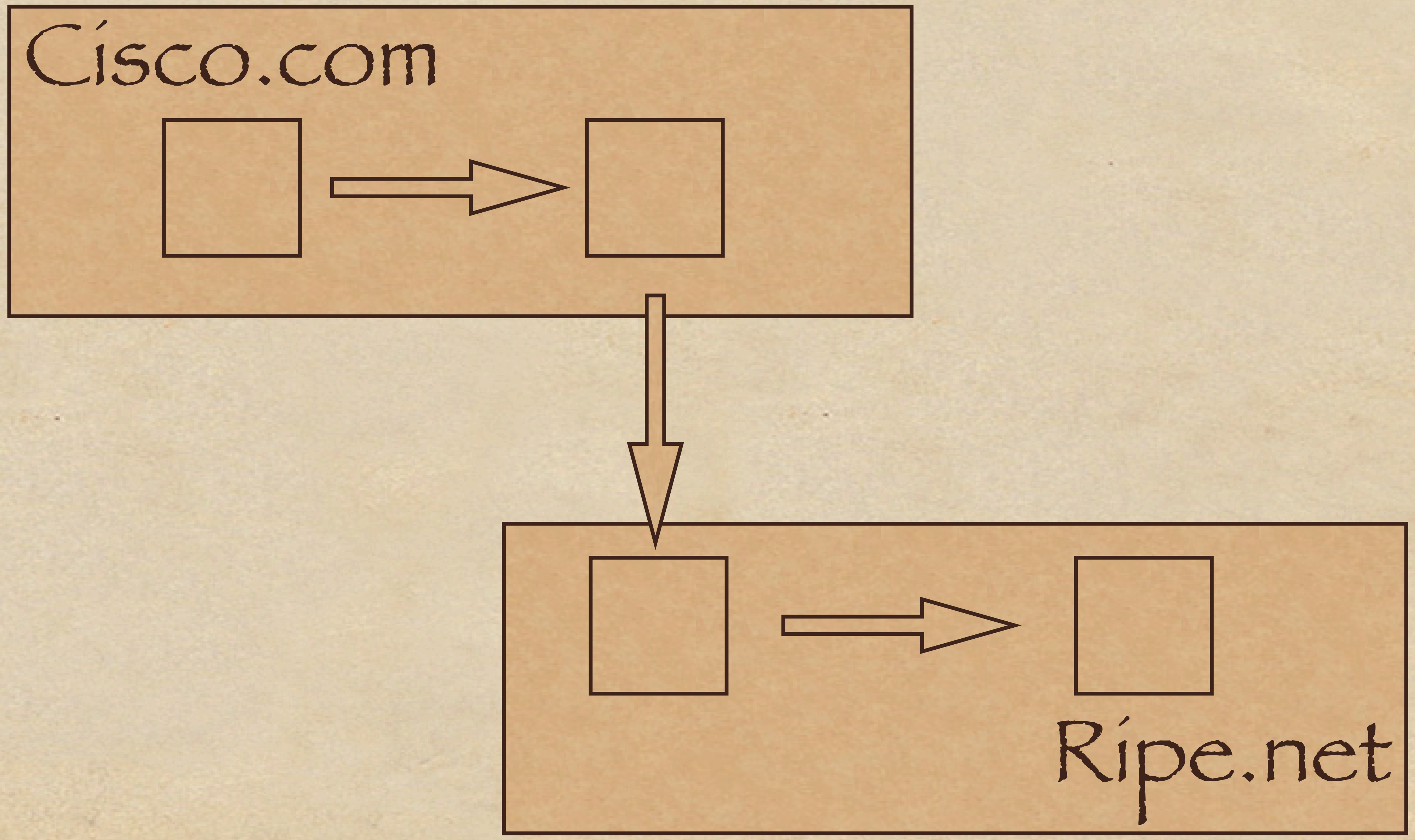
- Look at the problem
- Agree on what the problem is
- Find a solution to the problem

How is SMTP used?

- In many ways...
- Between many different entities...
- Spam, worms, trojans etc are injected in a "proper" mail flow...
- How, when where?

Basic flow

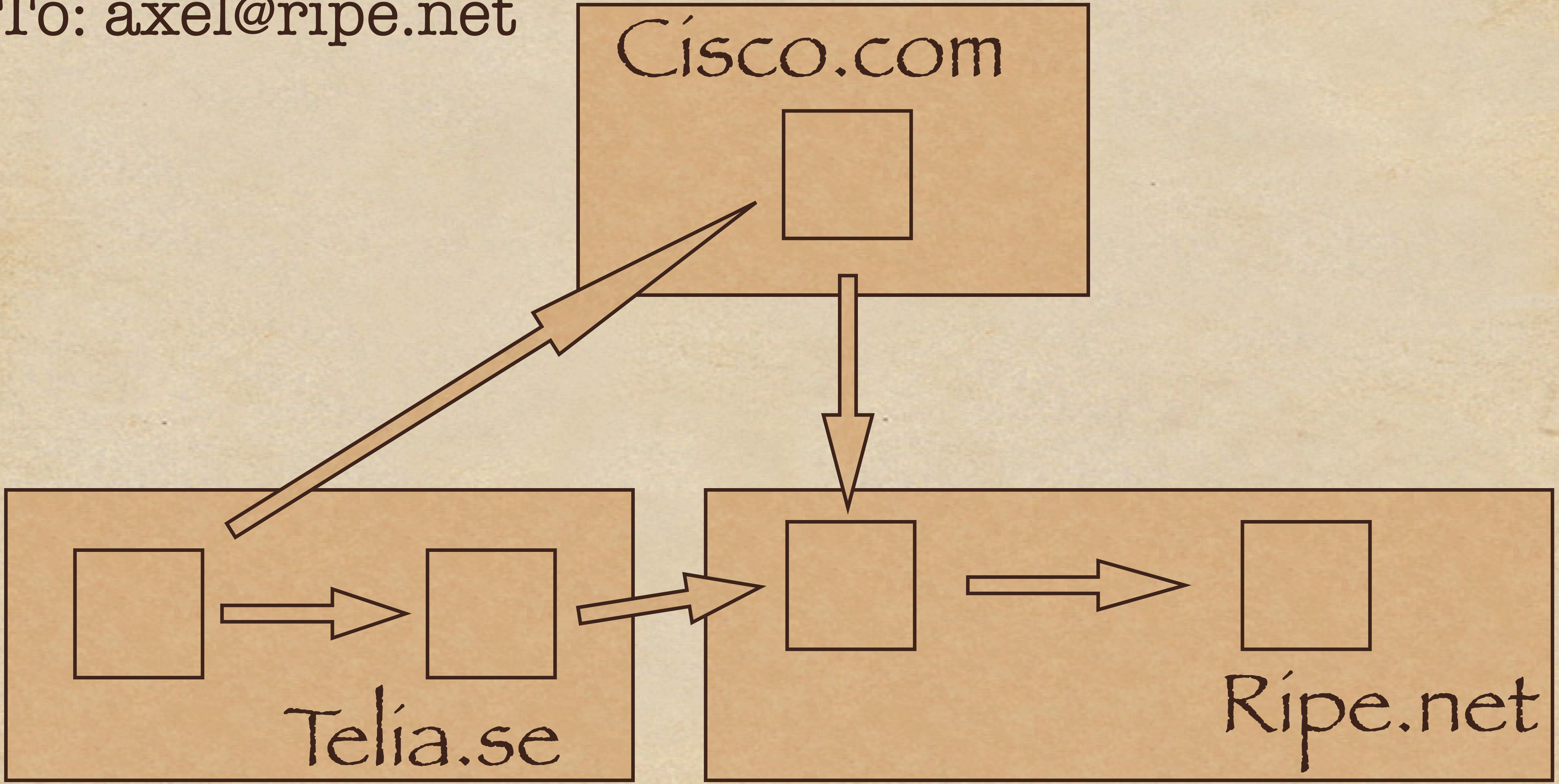
From: paf@cisco.com
To: axel@ripe.net



From foreign domain

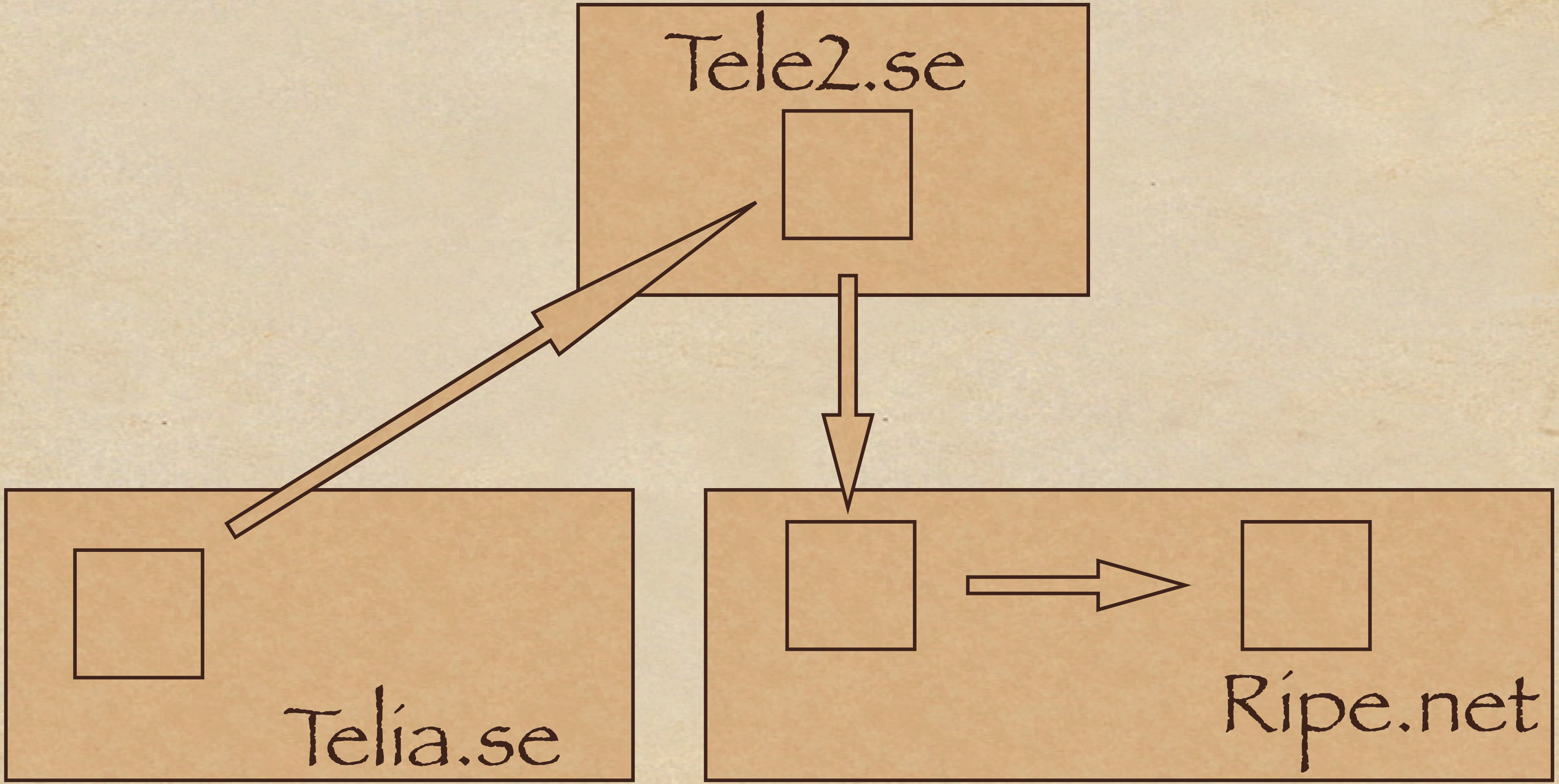
From: paf@cisco.com

To: axel@ripe.net



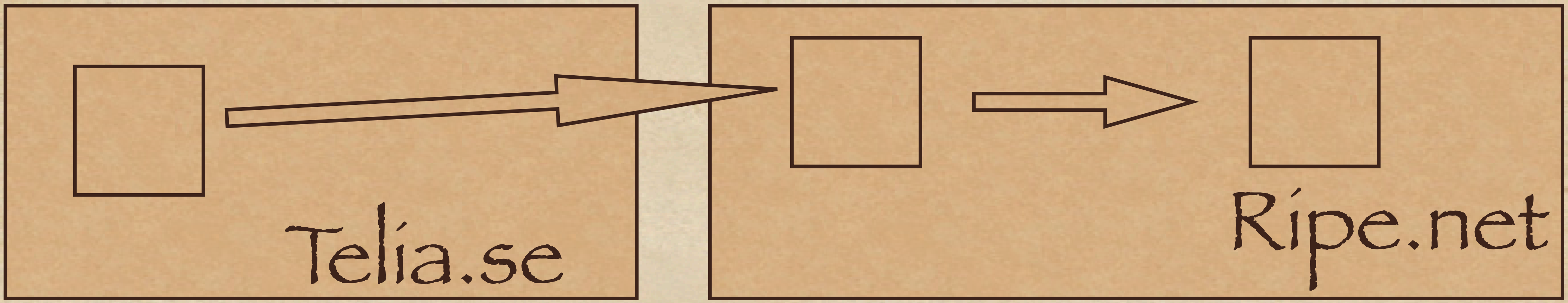
Open relay

From: paf@cisco.com
To: axel@ripe.net

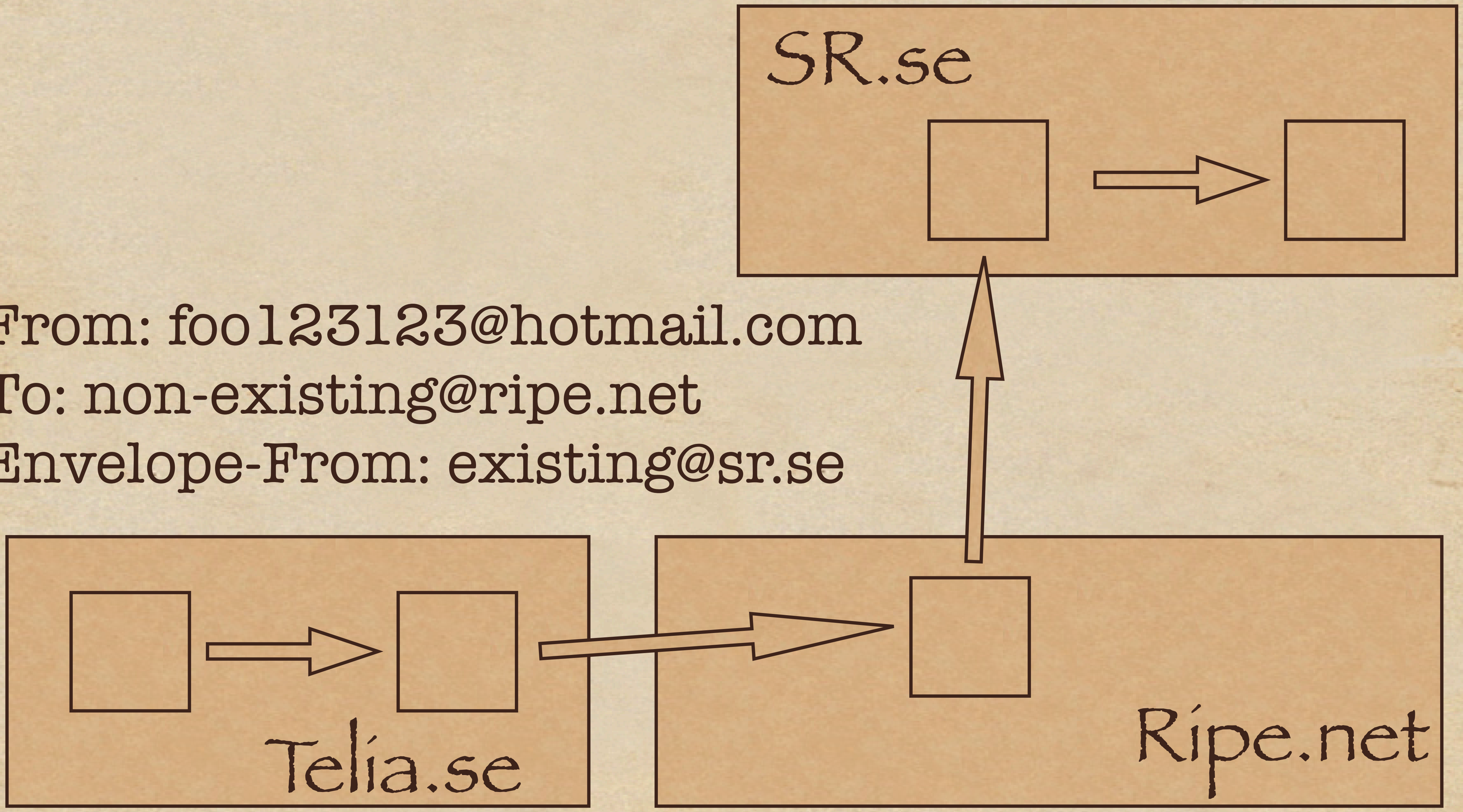


Direct

From: paf@cisco.com
To: axel@ripe.net



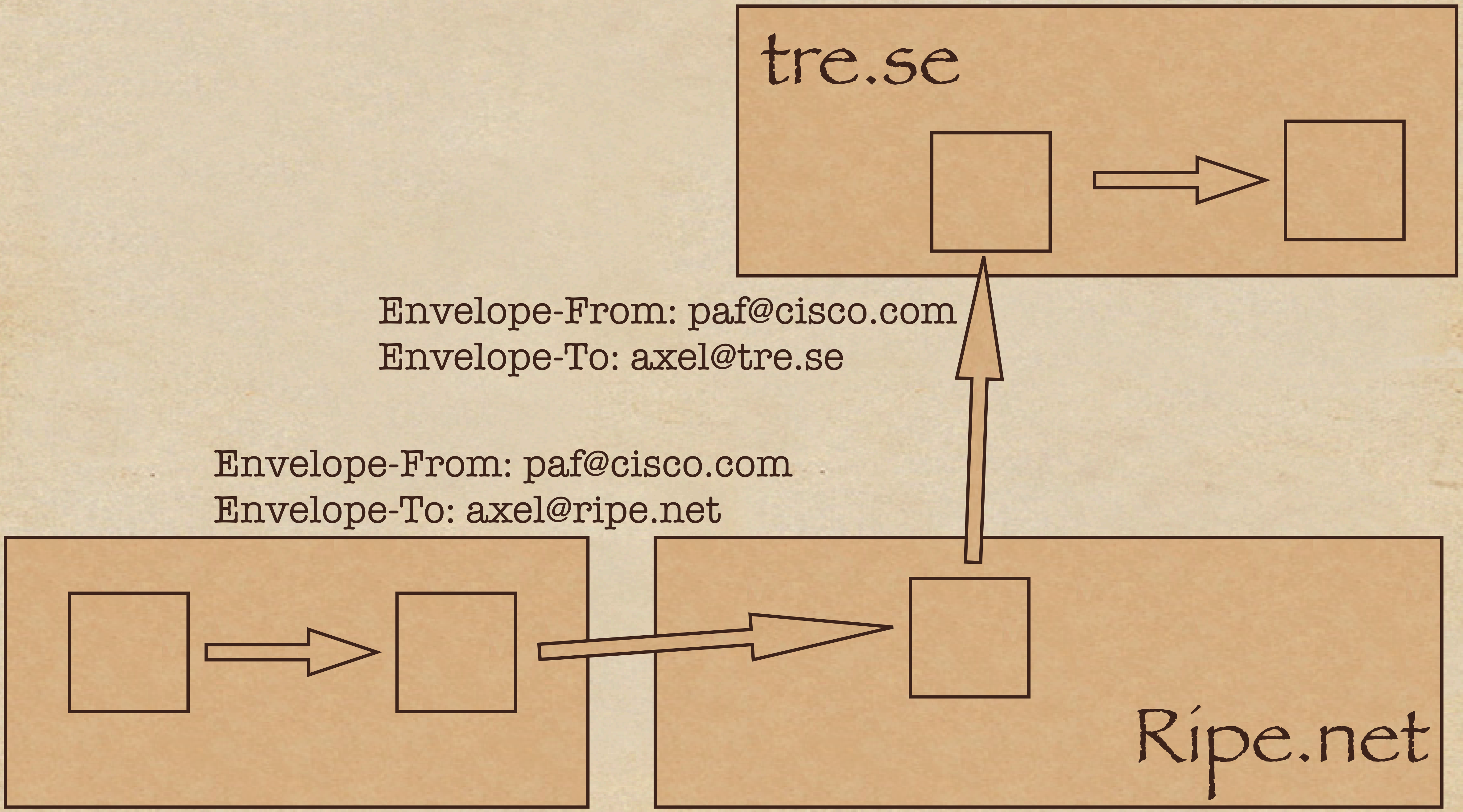
Bounce



From: foo123123@hotmail.com
To: non-existing@ripe.net
Envelope-From: existing@sr.se

Forwarding

From: paf@cisco.com
To: axel@ripe.net



tre.se

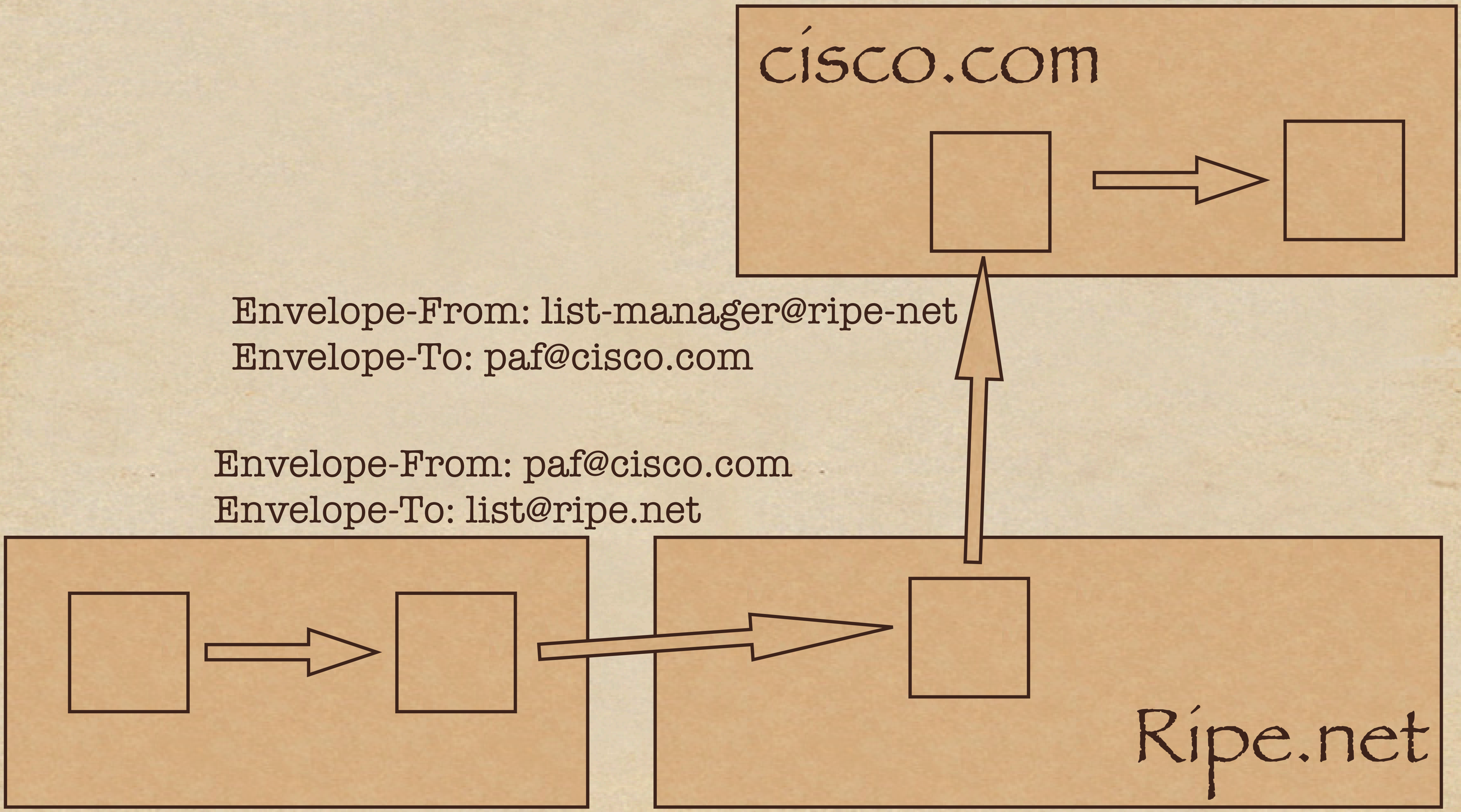
Envelope-From: paf@cisco.com
Envelope-To: axel@tre.se

Envelope-From: paf@cisco.com
Envelope-To: axel@ripe.net

Ripe.net

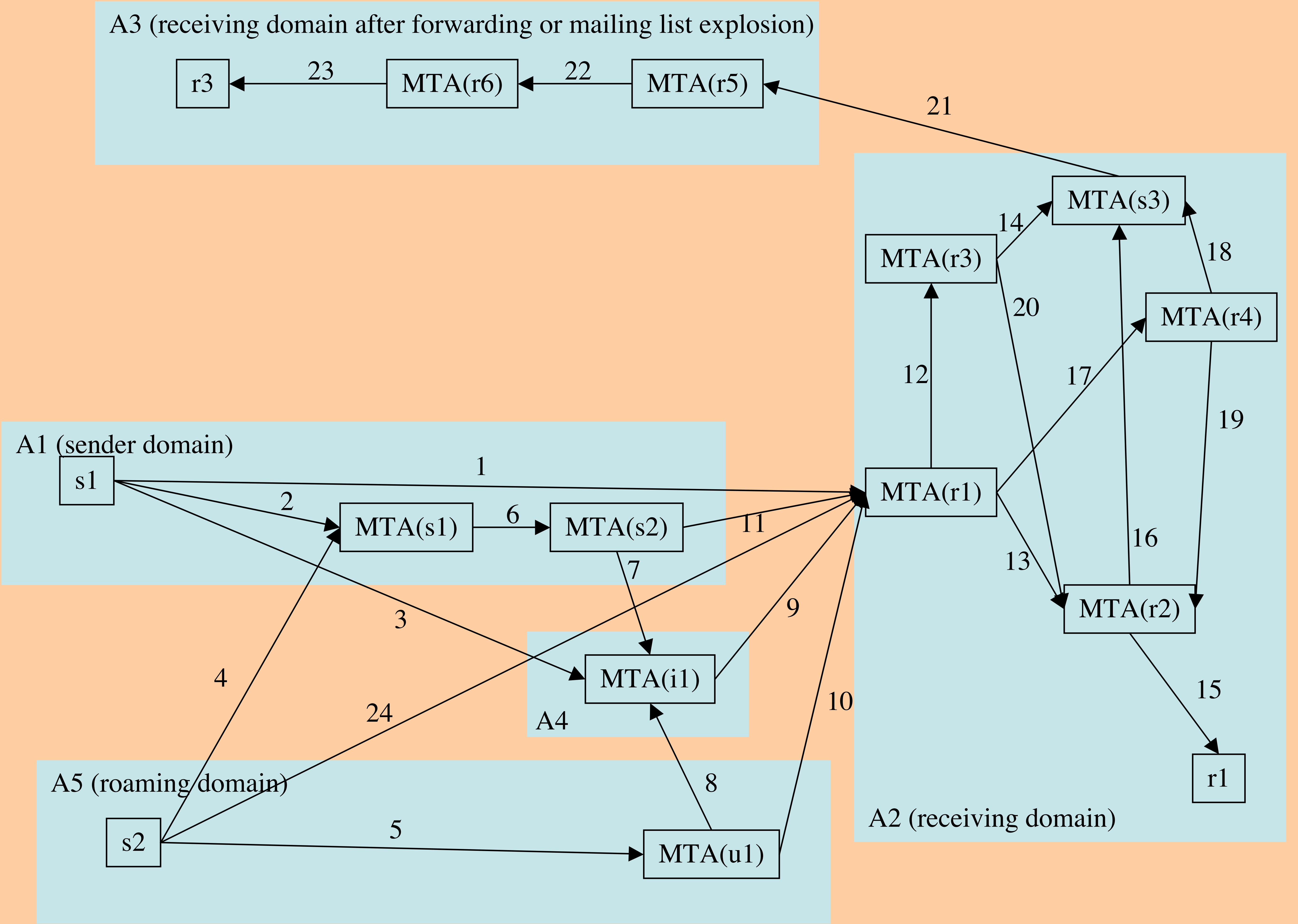
Mailing list

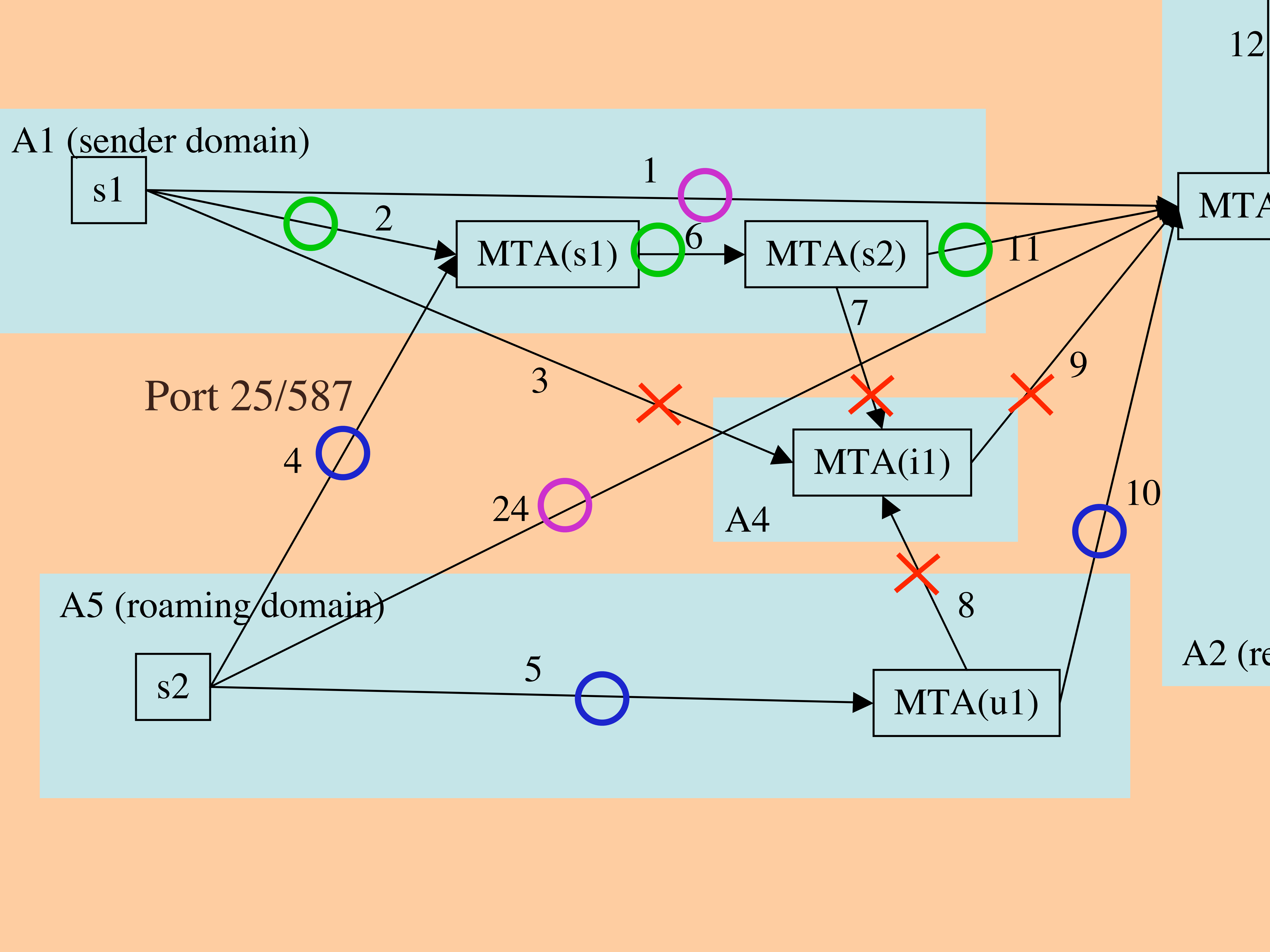
From: paf@cisco.com
To: list@ripe.net



Envelope-From: list-manager@ripe-net
Envelope-To: paf@cisco.com

Envelope-From: paf@cisco.com
Envelope-To: list@ripe.net


A3 (receiving domain after forwarding or mailing list explosion)
r3
23
MTA(r6)
22
MTA(r5)
21
MTA(s3)
14
MTA(r3)
18
20
MTA(r4)
12
17
19
A1 (sender domain)
s1
1
MTA(r1)
2
MTA(s1)
6
MTA(s2)
11
16
13
7
MTA(r2)
9
3
4
MTA(i1)
10
15
24
A4
8
r1
A5 (roaming domain)
s2
5
MTA(u1)
A2 (receiving domain)


12
A1 (sender domain)
s1
1
2
MTA(s1)
6
MTA(s2)
11
MTA
7
Port 25/587
3
9
MTA(i1)
4
24
A4
10
A5 (roaming domain)
8
A2 (re
5
s2
MTA(u1)

Open questions 1(3)

- Should open relays be blocked?
  - What to do with things like ieee.org?
- Personal view: Absolutely!
- Community view: Yes, but...

Open questions 2(3)

- Must an email always pass an outgoing SMTP-relay?
  - What about people having an MTA on their laptop?
- Personal view: Yes, if the policy of sending domain says so
- Community view: But but...

Open questions 3(3)

- Should an MUA use always “home” SMTP server, or the outgoing SMTP relay provided by the ISP he currently uses?
- Personal view: Always home MTA
- Community view: ISP’s are blocking traffic to port 25 today, but, but...

See RFC 2476 about SMTP submit port 587

Two kind of proposals

- Signing mail (authenticate sender)
- “Reverse MX” and other DNS based

Followup issues

- Proposals will “just” make it possible to know who the mail comes from
- Proposals work on envelope sender, but many people working with anti-spam don’t know the difference, or want to secure header-from…
    - (which I see as a much harder problem due to mailing lists etc)

Me think...

- We need:
  - Technical methods to track violators
  - Legislation
  - Police (etc) which do the tracking
- IETF (etc) only work with the 1st of these

Patrik Fältström

paf@cisco.com