MARID BOF

ietf-mxcomp@imc.org

The discussion is wrong!

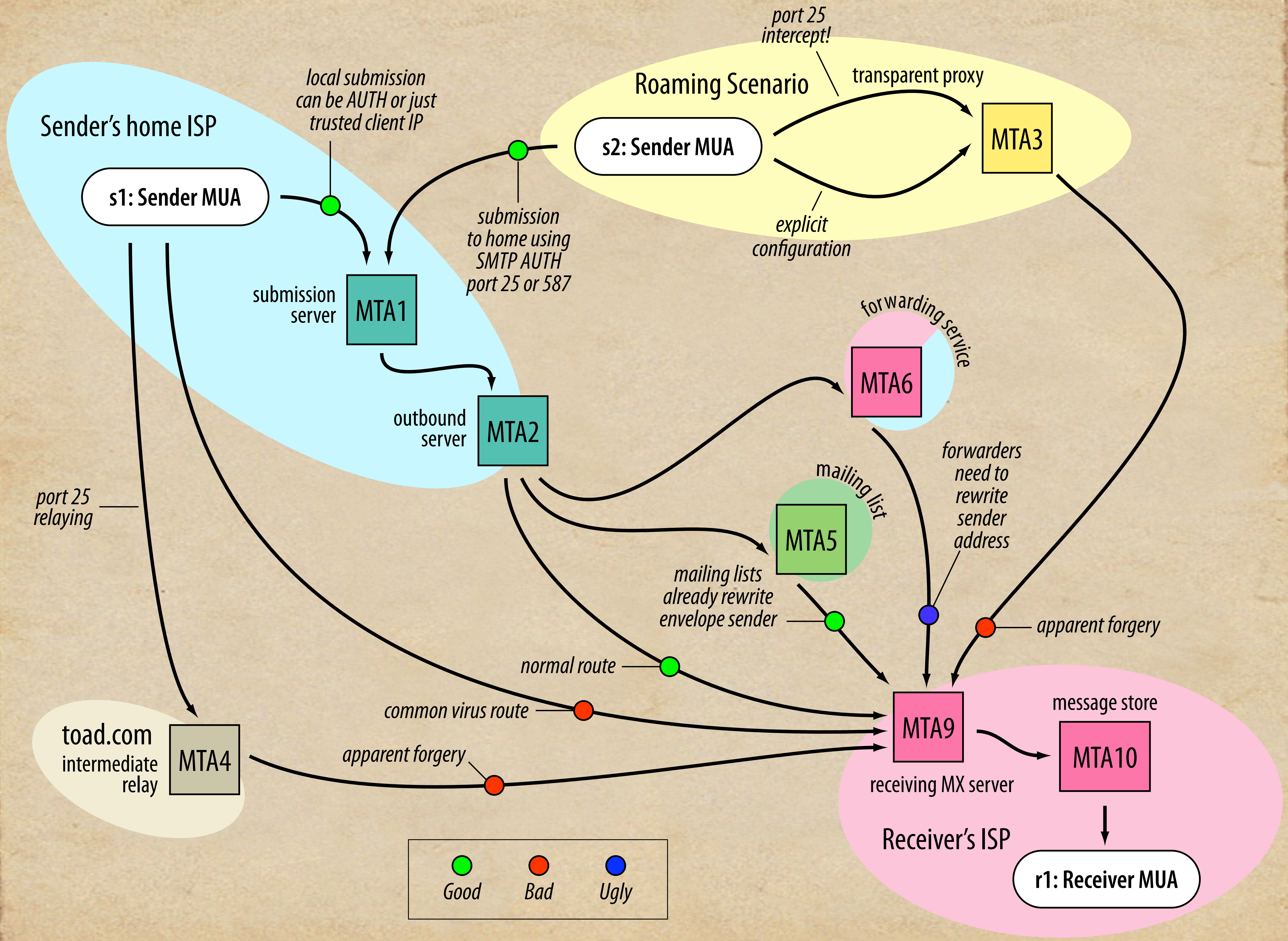
- I am of the view people attack the spam problem from the wrong angle
  - Look for a solution
  - Fine-tune it
  - Look for a problem the solution solves

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?



Sender's home ISP

s1: Sender MUA

local submission can be AUTH or just trusted client IP

submission server

MTA1

outbound server

MTA2

Roaming Scenario

s2: Sender MUA

port 25 intercept!

transparent proxy

MTA3

explicit configuration

submission to home using SMTP AUTH port 25 or 587

forwarding service

MTA6

forwarders need to rewrite sender address

mailing list

MTA5

mailing lists already rewrite envelope sender

port 25 relaying

normal route

common virus route

apparent forgery

apparent forgery

toad.com intermediate relay

MTA4

MTA9

receiving MX server

message store

MTA10

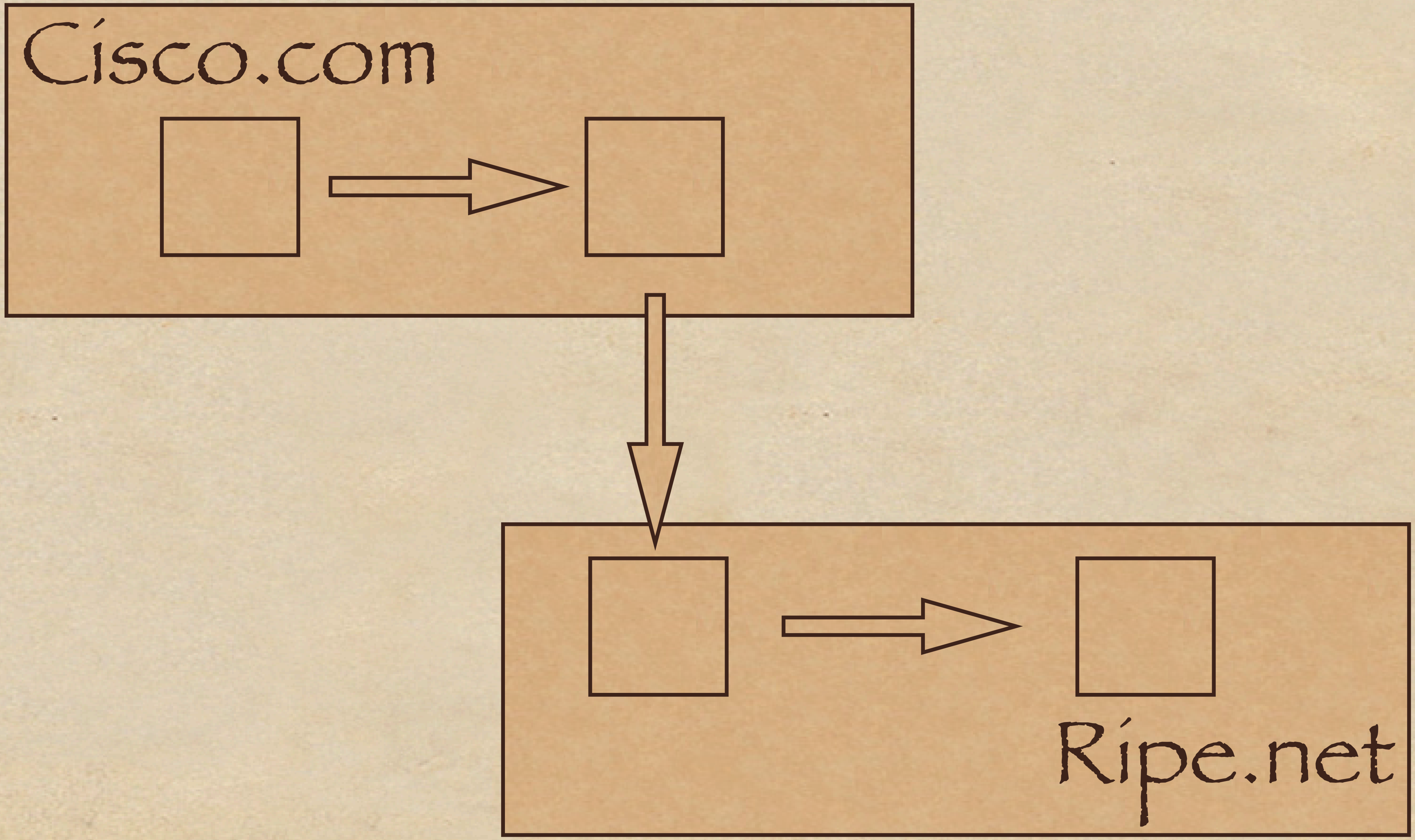
Receiver's ISP

r1: Receiver MUA

🟢	🔴	🔵
Good	Bad	Ugly

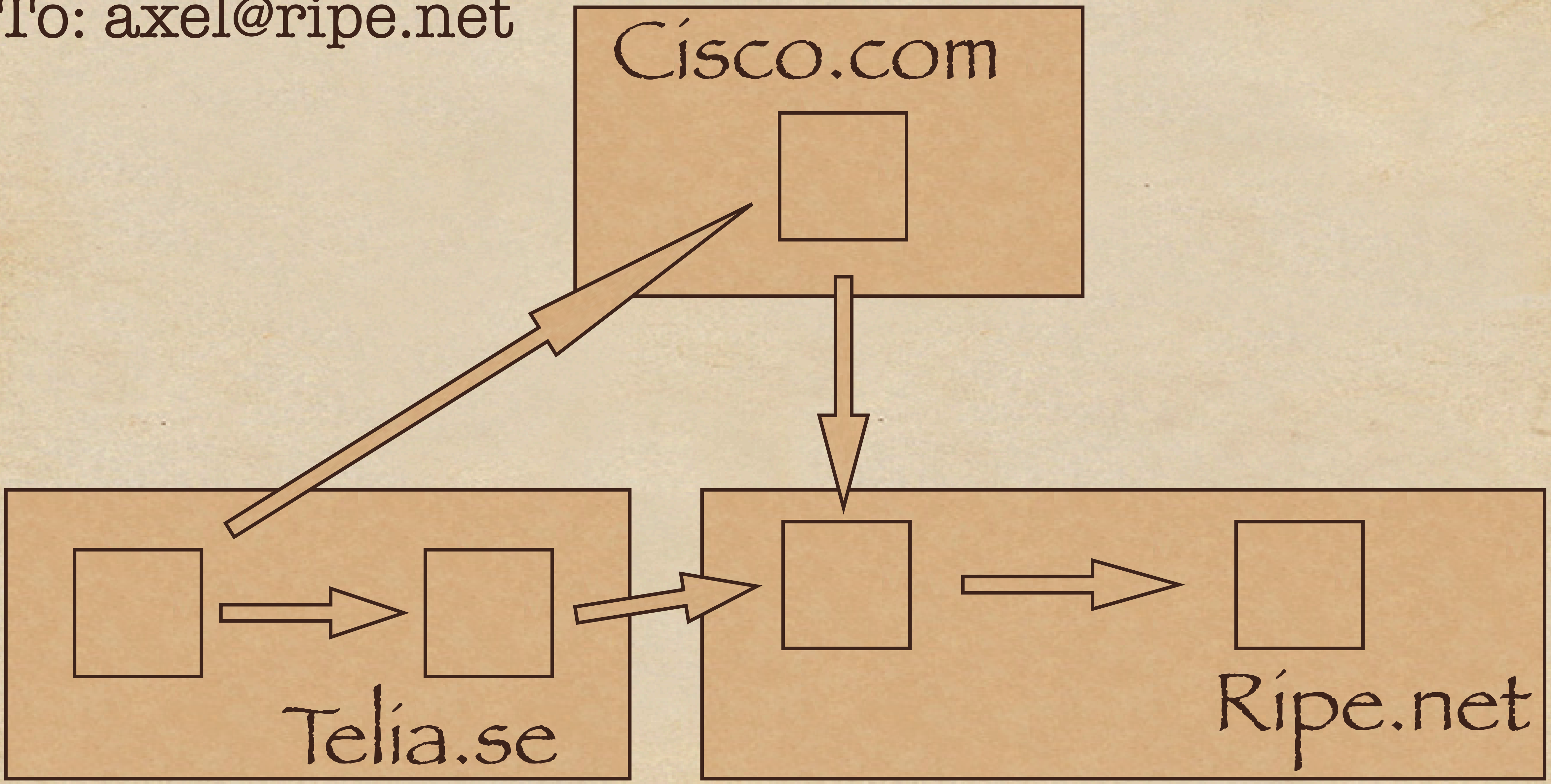
Basic flow

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



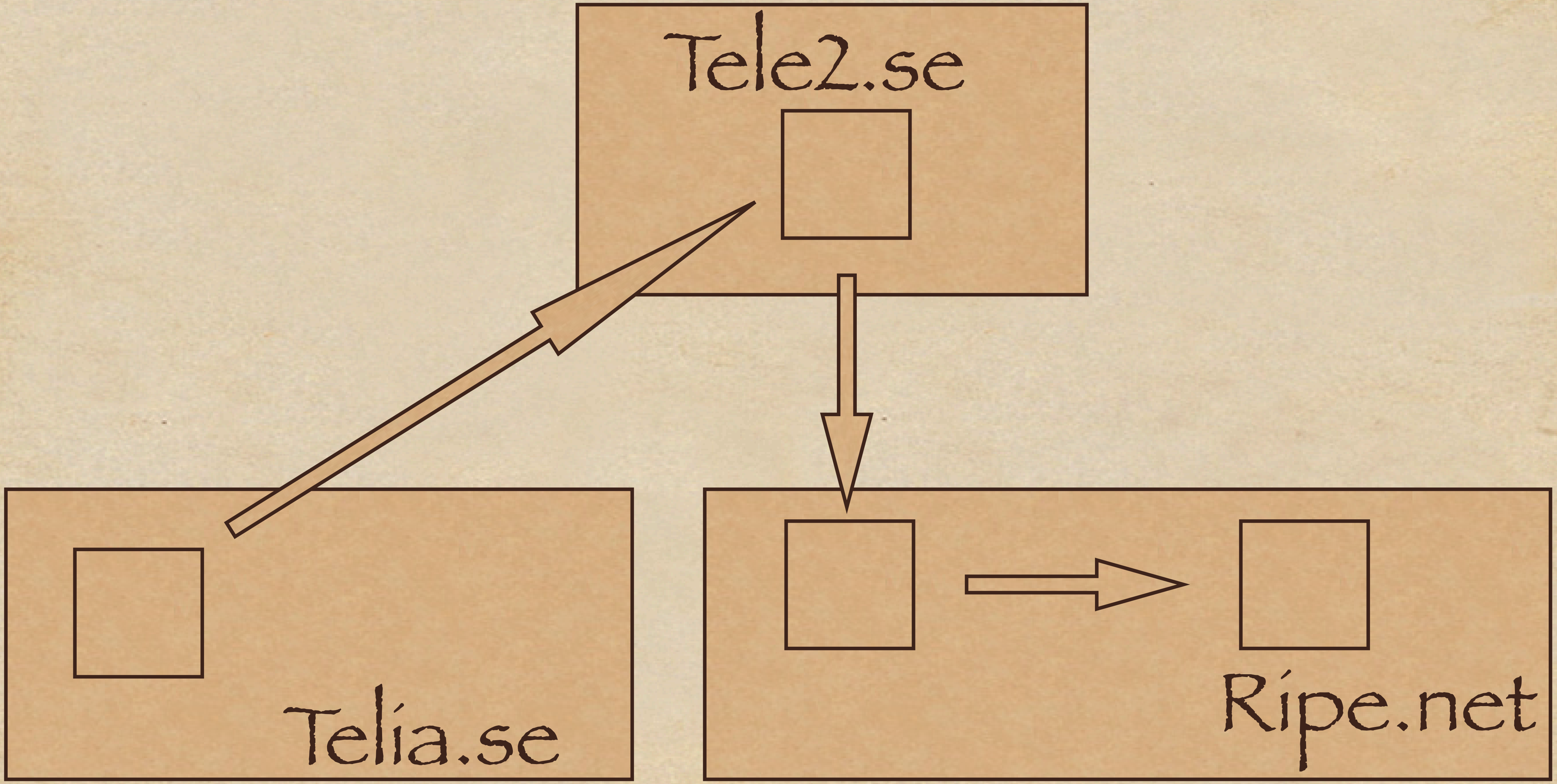
From foreign domain

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



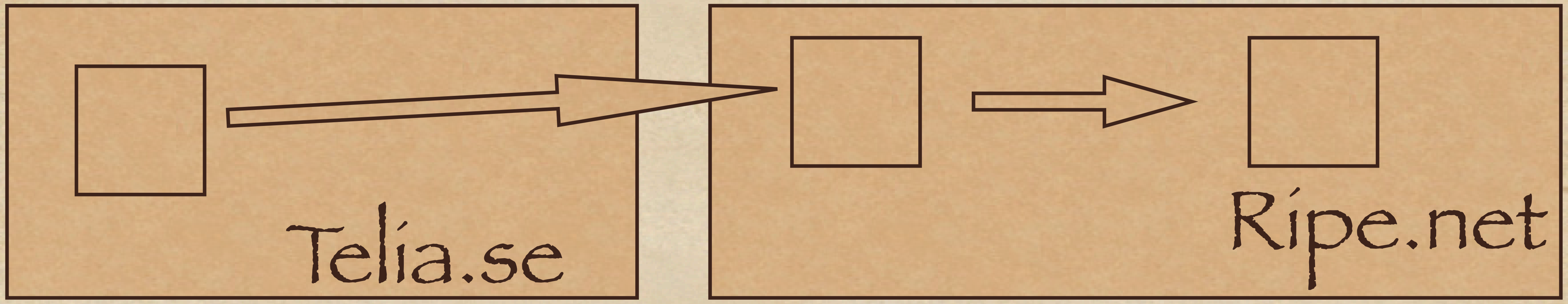
Open relay

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

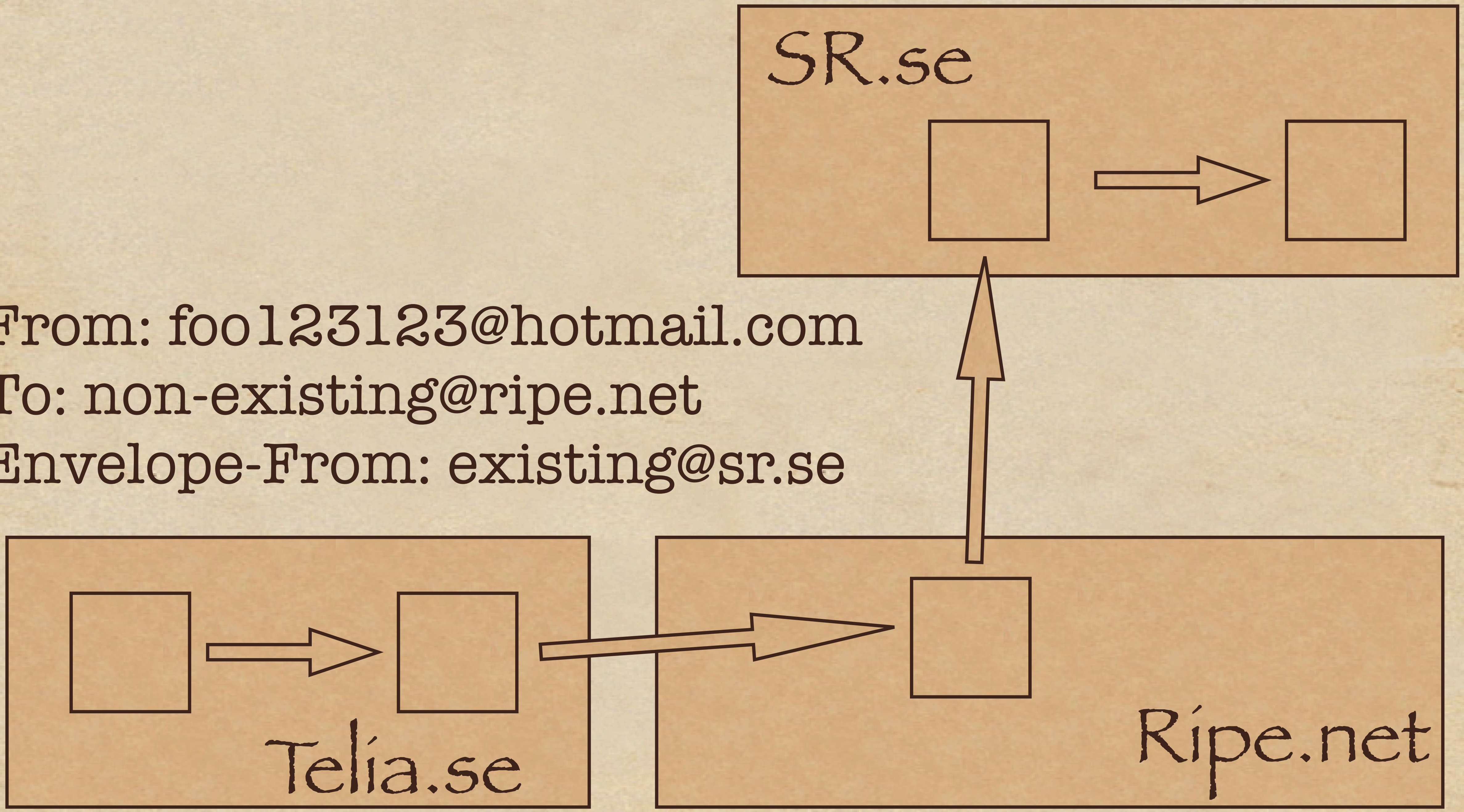


Direct

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



Bounce



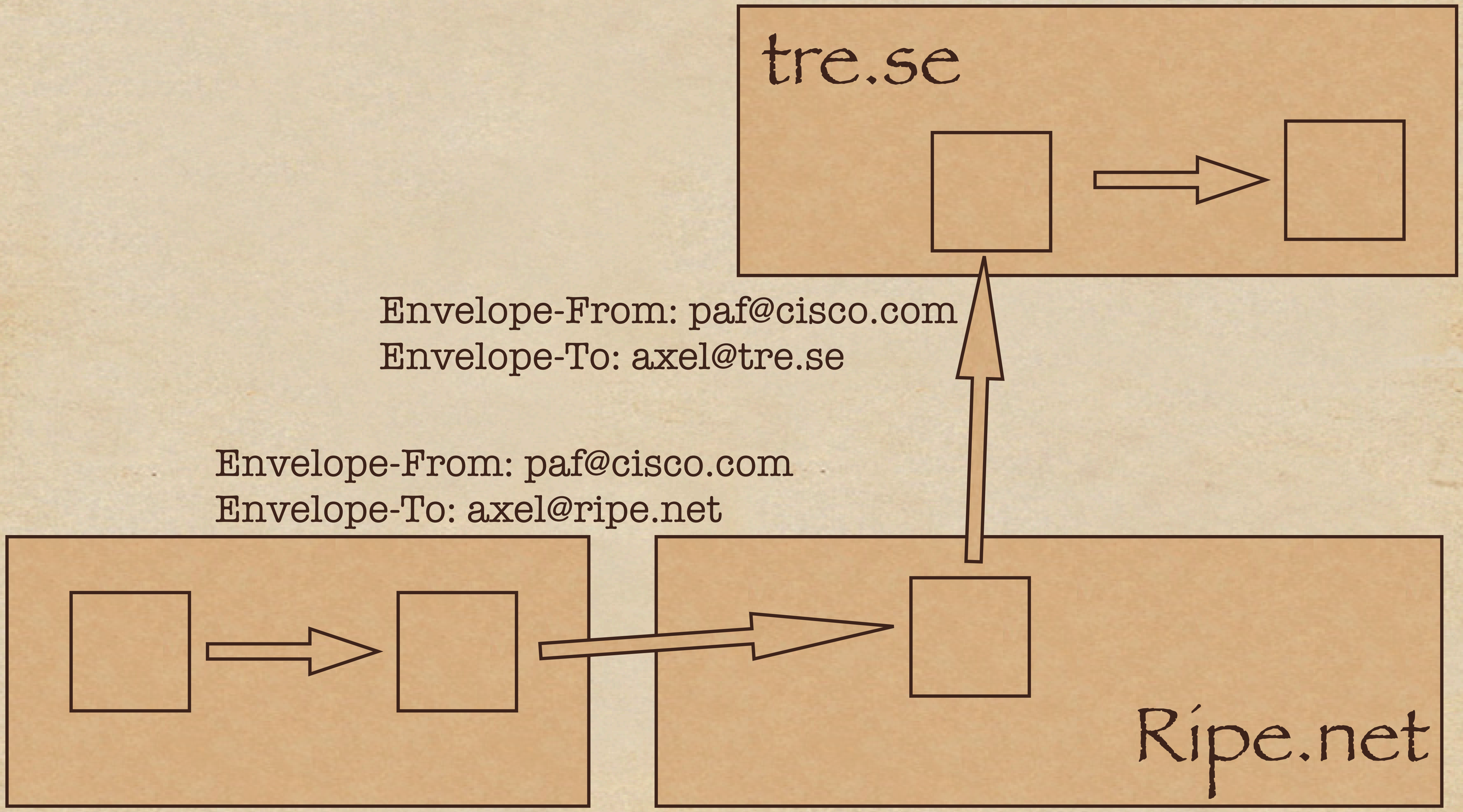
From: foo123123@hotmail.com

To: non-existing@ripe.net

Envelope-From: existing@sr.se

MTA Forwarding

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



tre.se

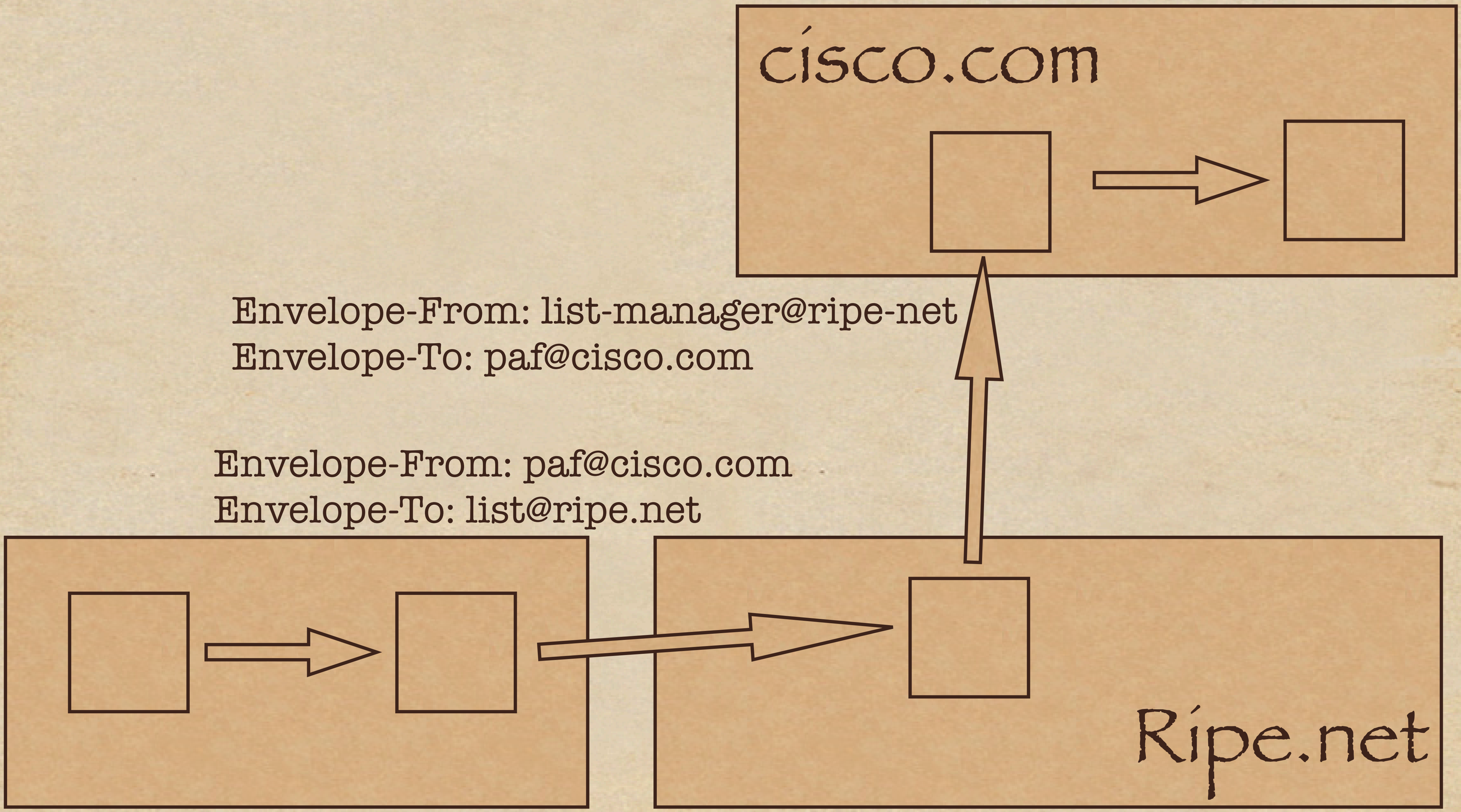
Envelope-From: paf@cisco.com
Envelope-To: axel@tre.se

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

Q1

- Will verification of SMTP peer help, and if so, what exactly is the problem that solves?
- Transition strategies?

Q2

- What will spammers do?

Q3

- Proposals have impact on what SMTP relay is used, one belonging to ISP, one to domain.
- Is RFC 2476 what should be used?
    - SMTP AUTH+port 587

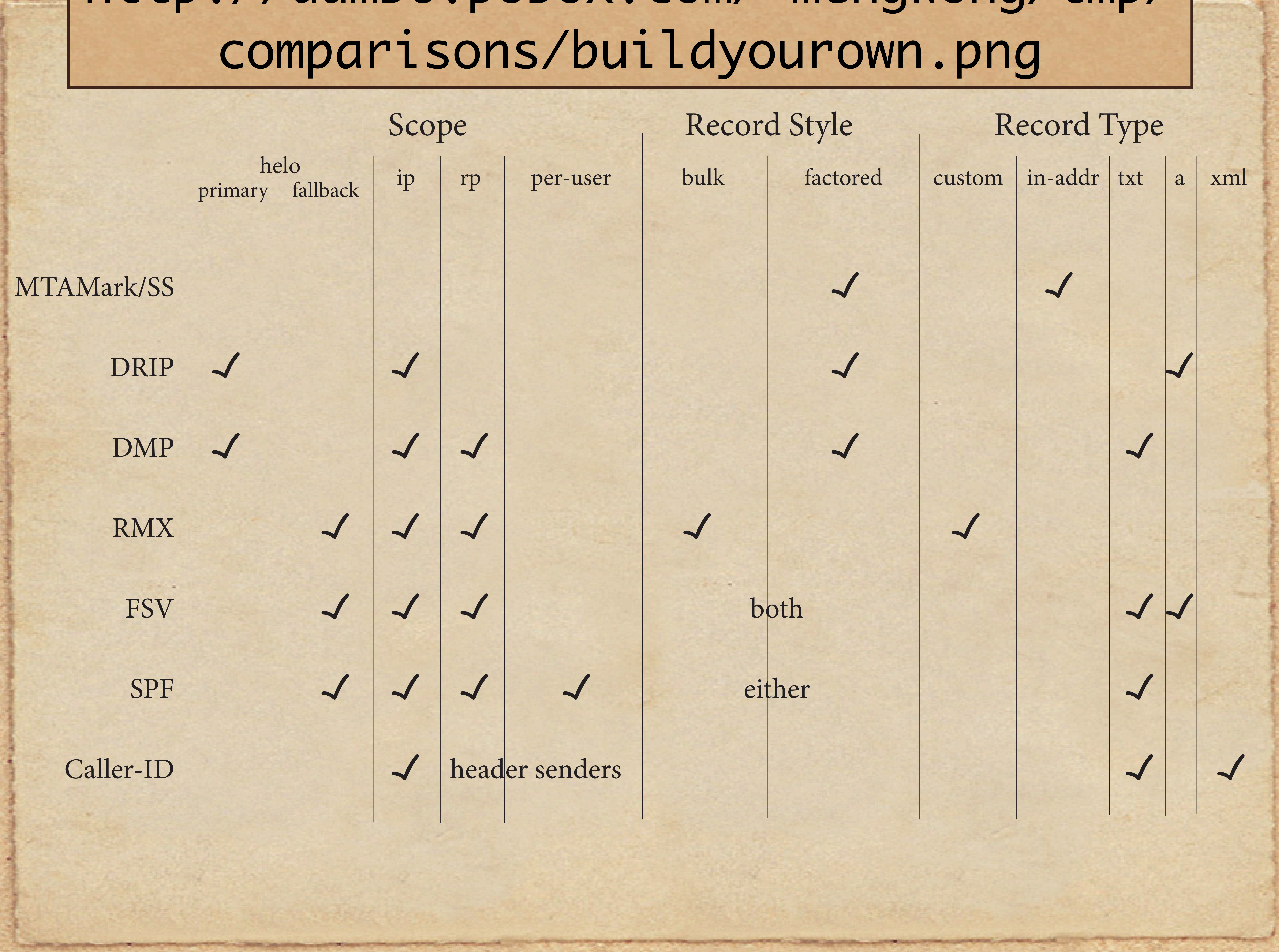
Q4

- Most proposals (?) force mailing lists and forwarders to a more strict behaviour.
- Is this something which will be deployed?

Q5

- What Resource Record Type should be used?

http://dumbo.pobox.com/~mengwong/tmp/comparisons/buildyourown.png



	Scope					Record Style		Record Type				
	helo											
	primary	fallback	ip	rp	per-user	bulk	factored	custom	in-addr	txt	a	xml
MTAMark/SS							✓		✓			
DRIP	✓		✓				✓				✓	
DMP	✓		✓	✓			✓			✓		
RMX		✓	✓	✓		✓		✓				
FSV		✓	✓	✓		both				✓	✓	
SPF		✓	✓	✓	✓	either				✓		
Caller-ID			✓	header senders						✓		✓

- Is there IETF work that we should take on to develop a mechanism that allows an MTA to use a DNS-based record to signal to peer MTA's that it is authorized to send mail?

MARID BOF

ietf-mxcomp@imc.org