



# SPAM

**Patrik Fältström**  
**Corporate Consulting Engineer**

**Member Internet Architecture Board**

# 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**

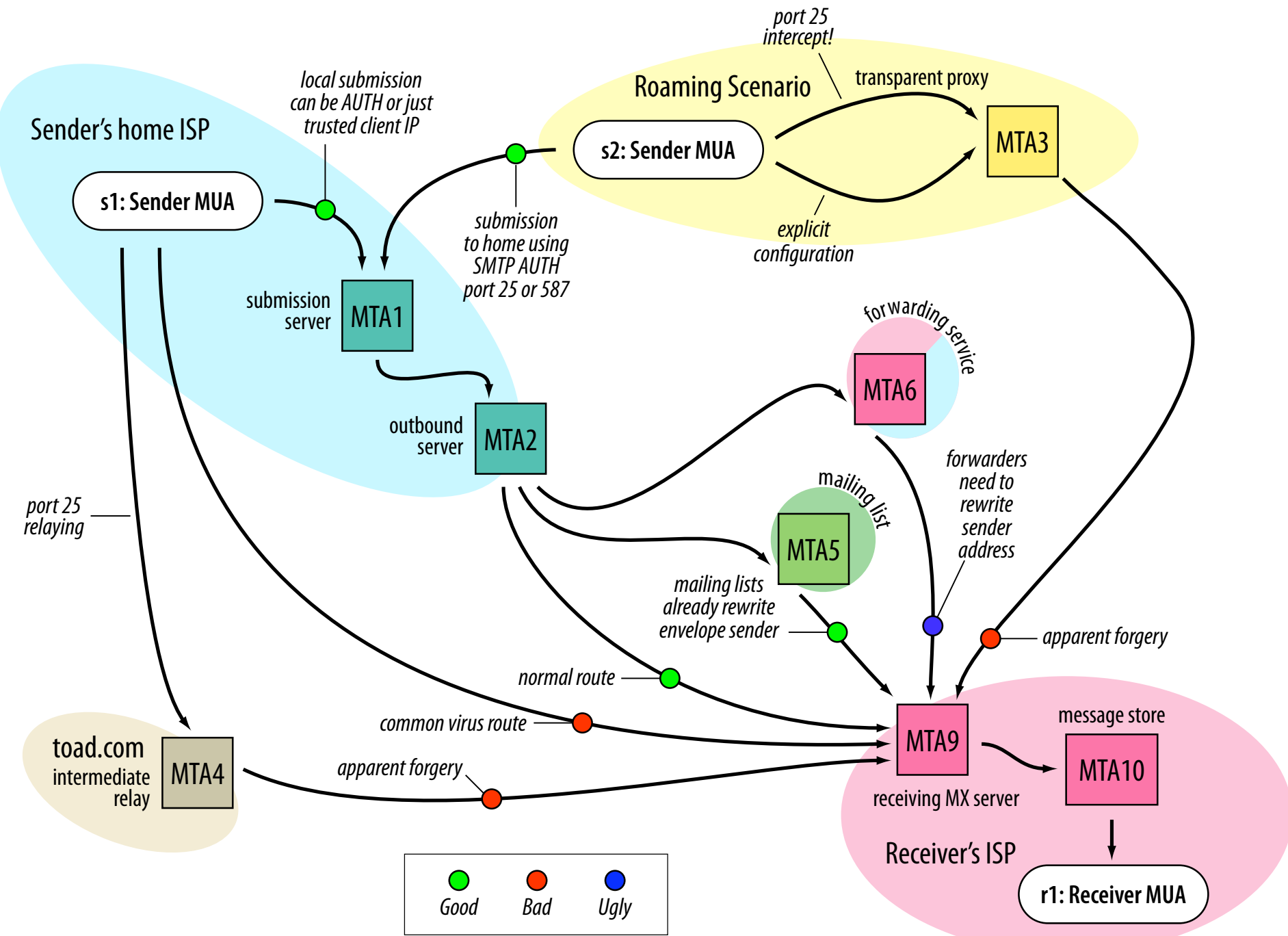
**Look for a problem the solution solves**

# Alternative method

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

# How is SMTP used?

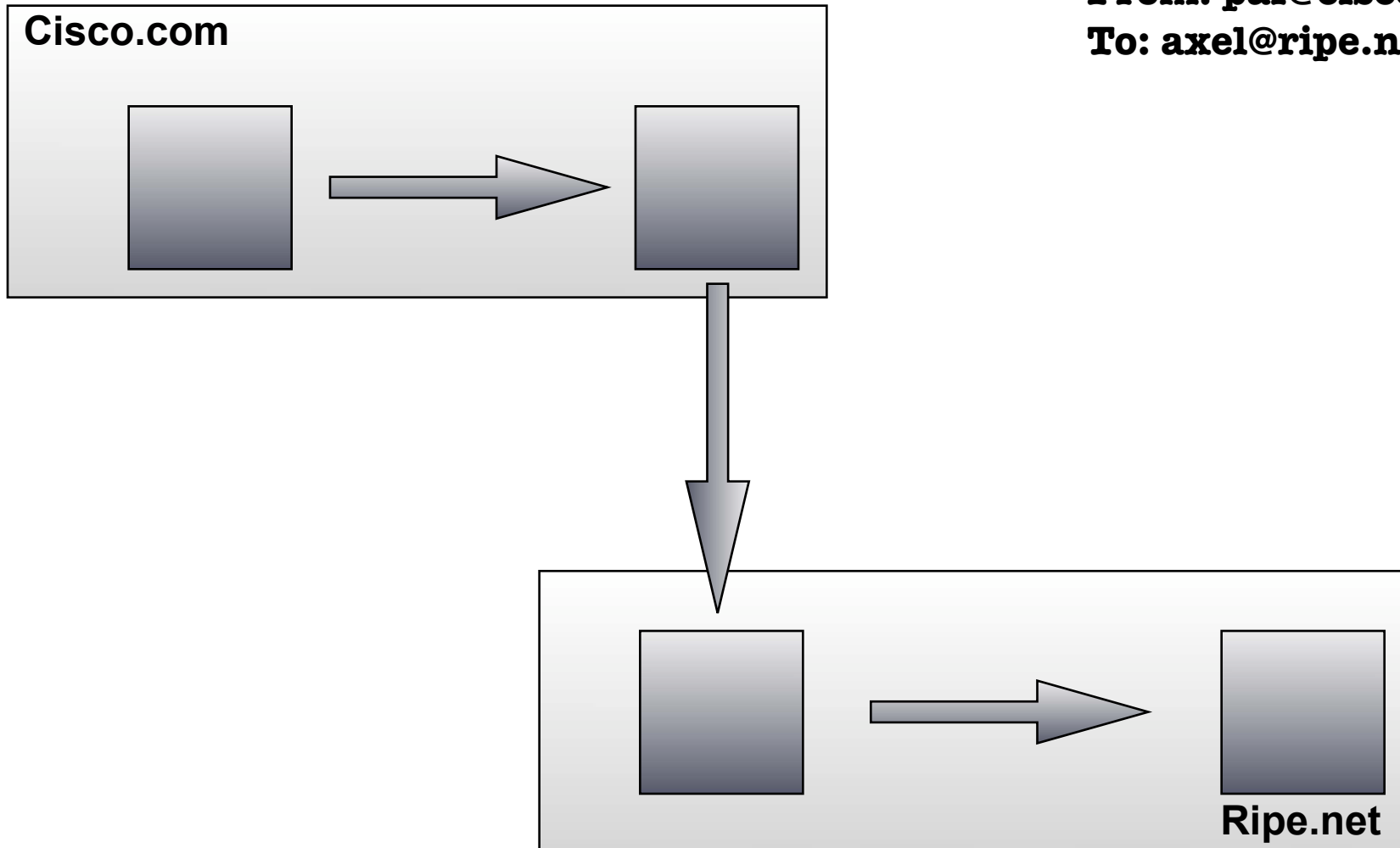
- **In many ways...**
- **Between many different entities...**
- **Spam, worms, trojans etc are injected in a “proper” mail flow...**
- **How, when where?**



# Basic flow

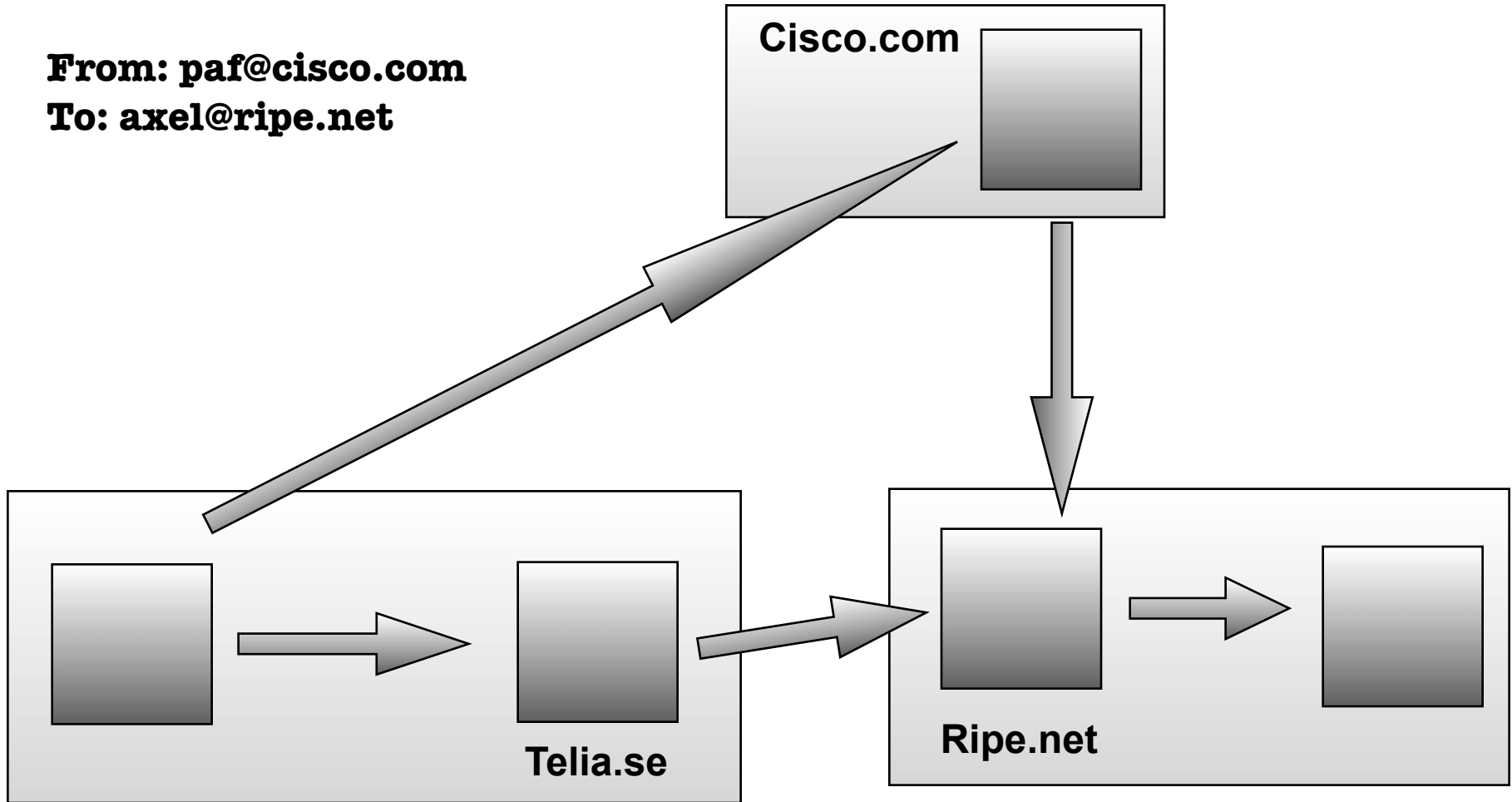
Cisco.com

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



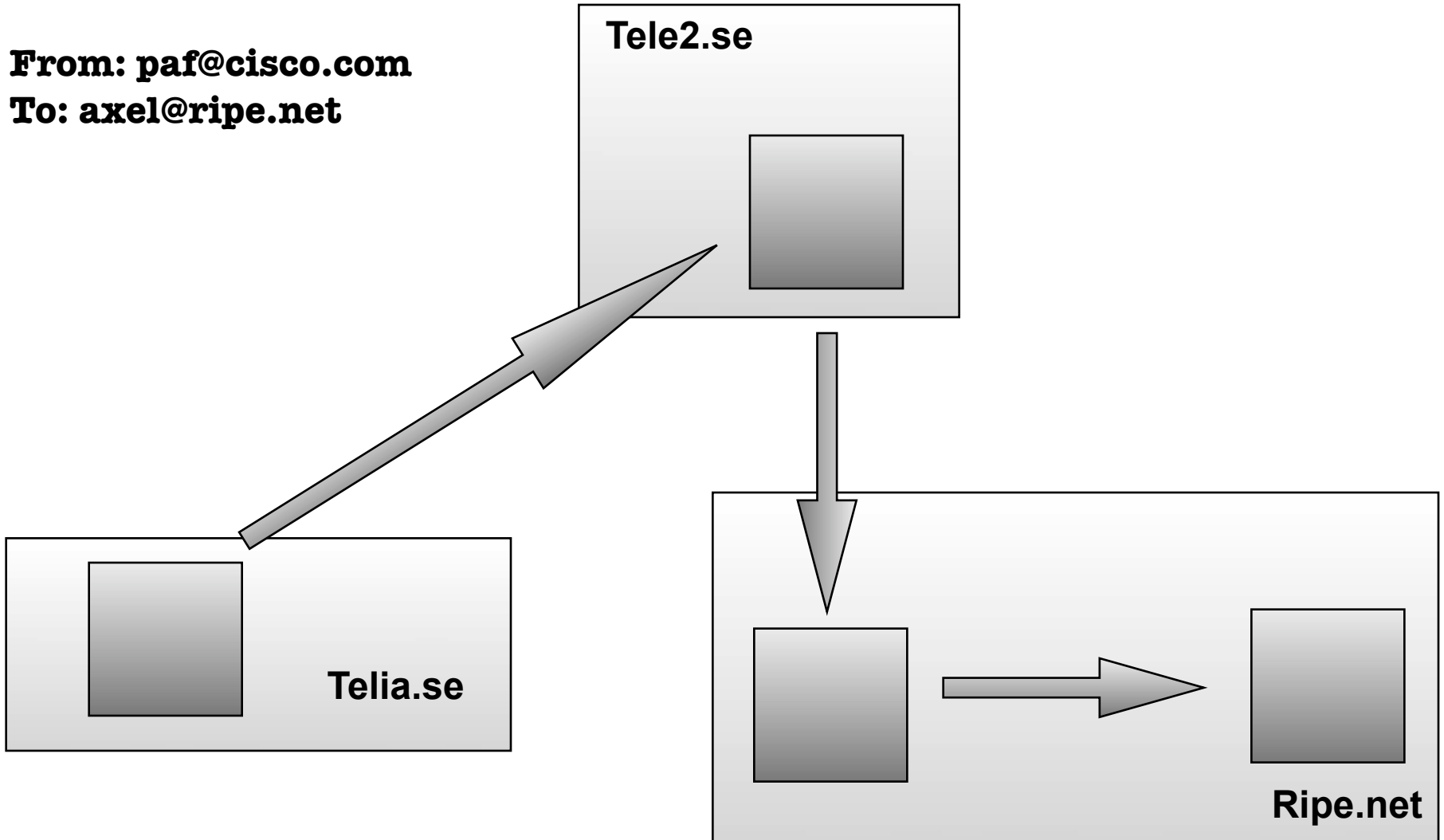
# From foreign domain

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



# Open relay

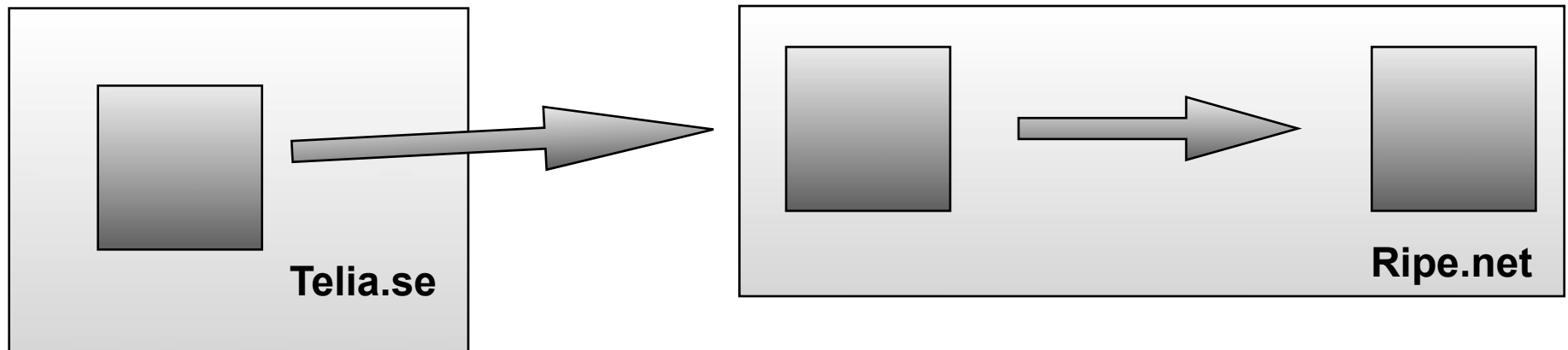
**From: paf@cisco.com**  
**To: axel@ripe.net**



# Direct

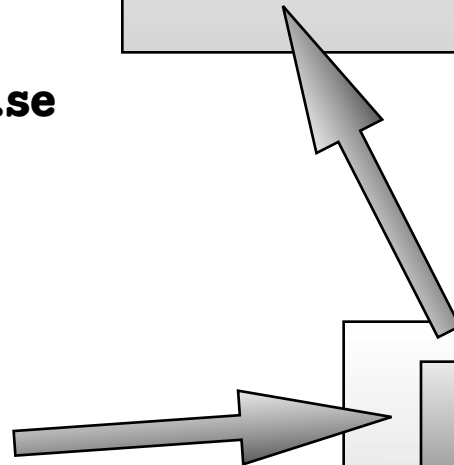
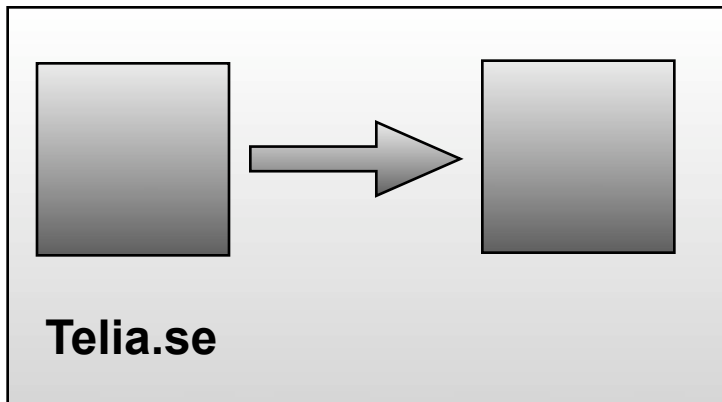
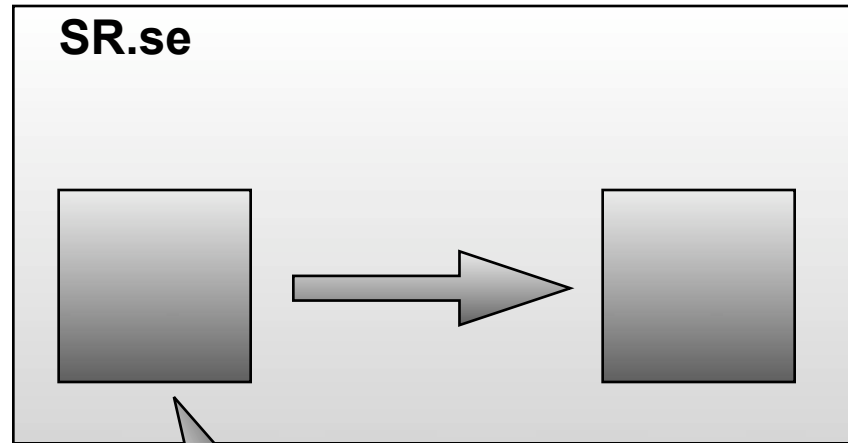
**From: paf@cisco.com**

**To: axel@ripe.net**



# Bounce

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

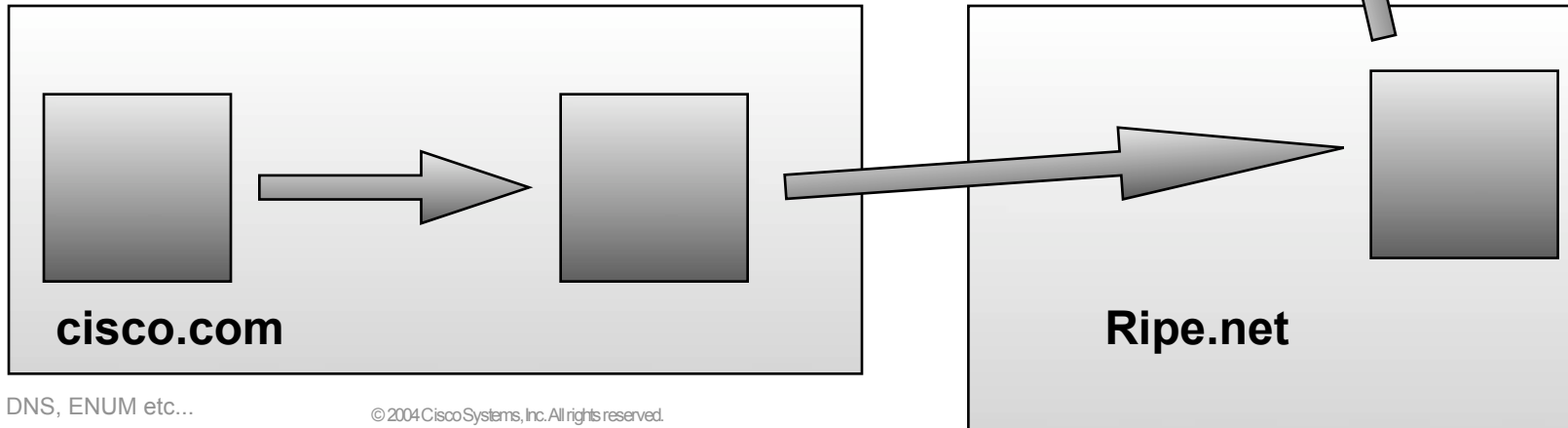


# MTA Forwarding

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

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

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

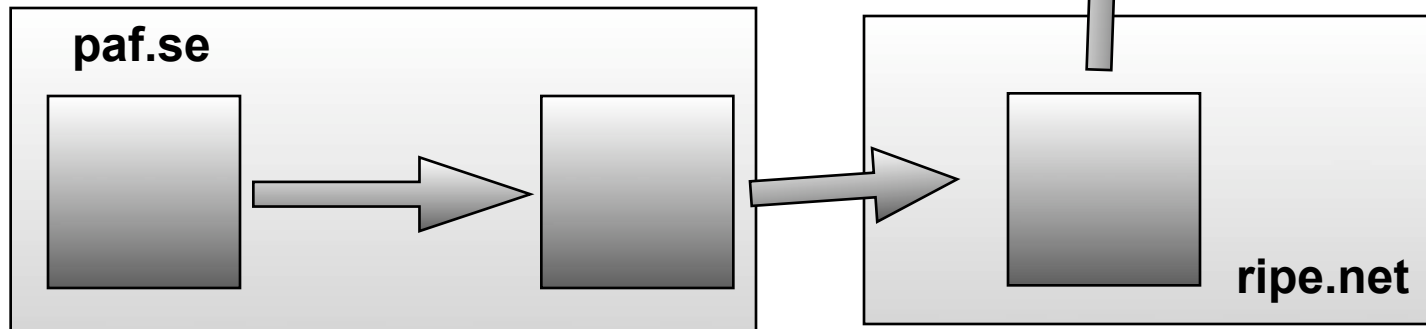


# Mailing list

**From: paf@paf.se**  
**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					
	primary	helo 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						✓		✓

# What's next?

- **IETF will most certainly look at DNS based verification mechanism**
- **IETF continue work with the SPAM problem in general**

**What should the policy description language look like?**

**Can this be expanded to other protocols than mail?**

- **Should we do SMTP Next Generation?**