Universität Stuttgart

INSTITUT FÜR
KOMMUNIKATIONSNETZE
UND RECHNERSYSTEME
Prof. Dr.-Ing. Dr. h. c. mult. P. J. Kühn

Efficient Transport of VoIP Firewall Control Signaling

Sebastian Kiesel, Michael Scharf
Institute of Communication Networks and Computer Engineering
University of Stuttgart
kiesel@ikr.uni-stuttgart.de, scharf@ikr.uni-stuttgart.de

IKR - VFF IND - Workshop
Dienste im Next Generation Network (NGN)
Universität Stuttgart, 3. März 2006

Outline

- **Motivation**
- **Overview of problems with SIP and firewalls**
- **Introduction to IETF MIDCOM/SIMCO**
- **Overview of SCTP**
- **"SIMCO over SCTP"**
- **Testbed and measurement results**
- **Conclusions and future work**

Motivation

Next Generation Networks

- **Carrier operated VoIP networks (SIP, RTP)**
- **Multi-operator scenarios**
- **Requirements**
  - Protection against denial-of-service attacks and VoIP spam
  - Accountability

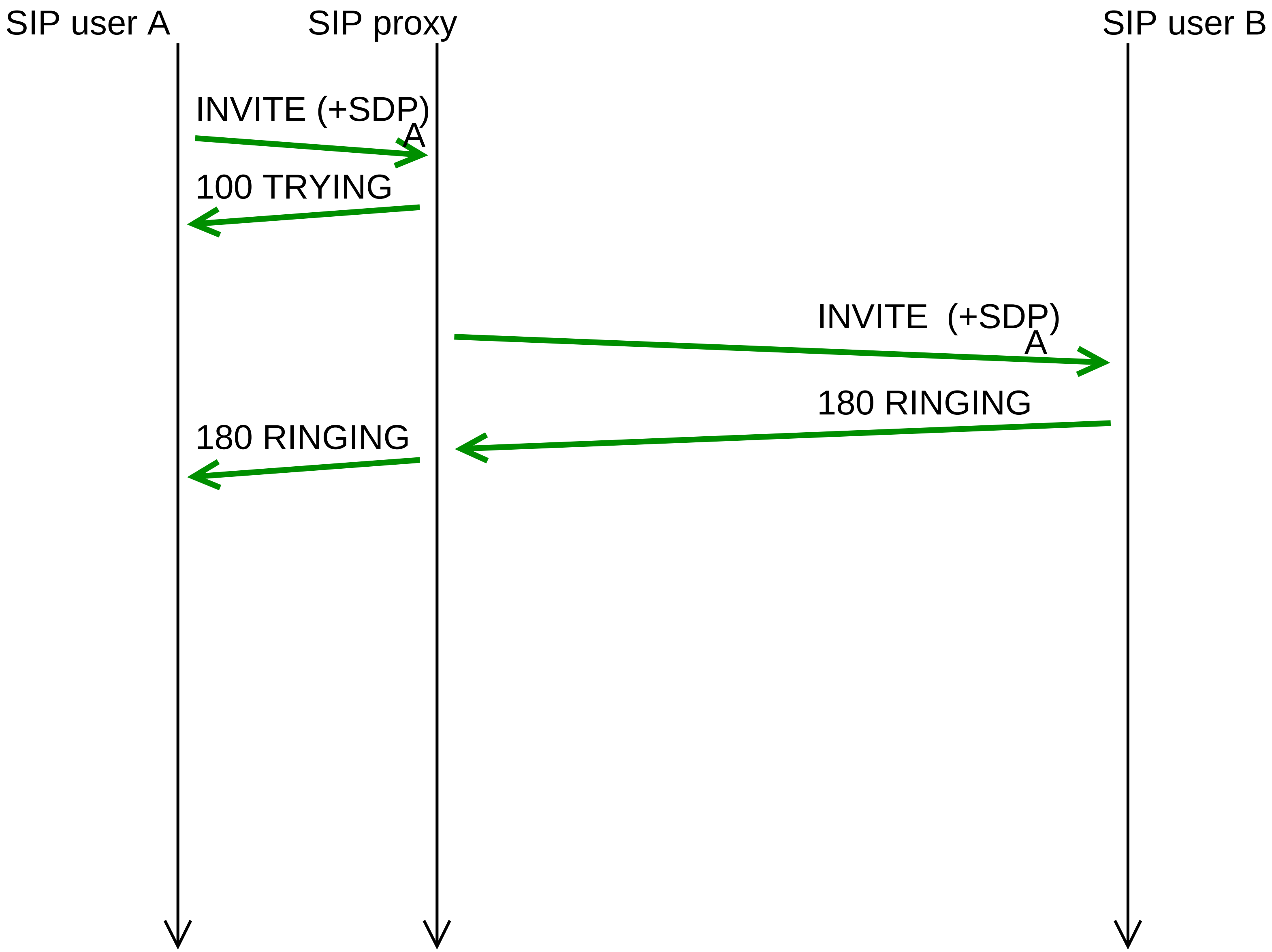
➥ **No full end-to-end connectivity on IP layer,
Signaling *and* media path secured by firewalls,**

Firewalls

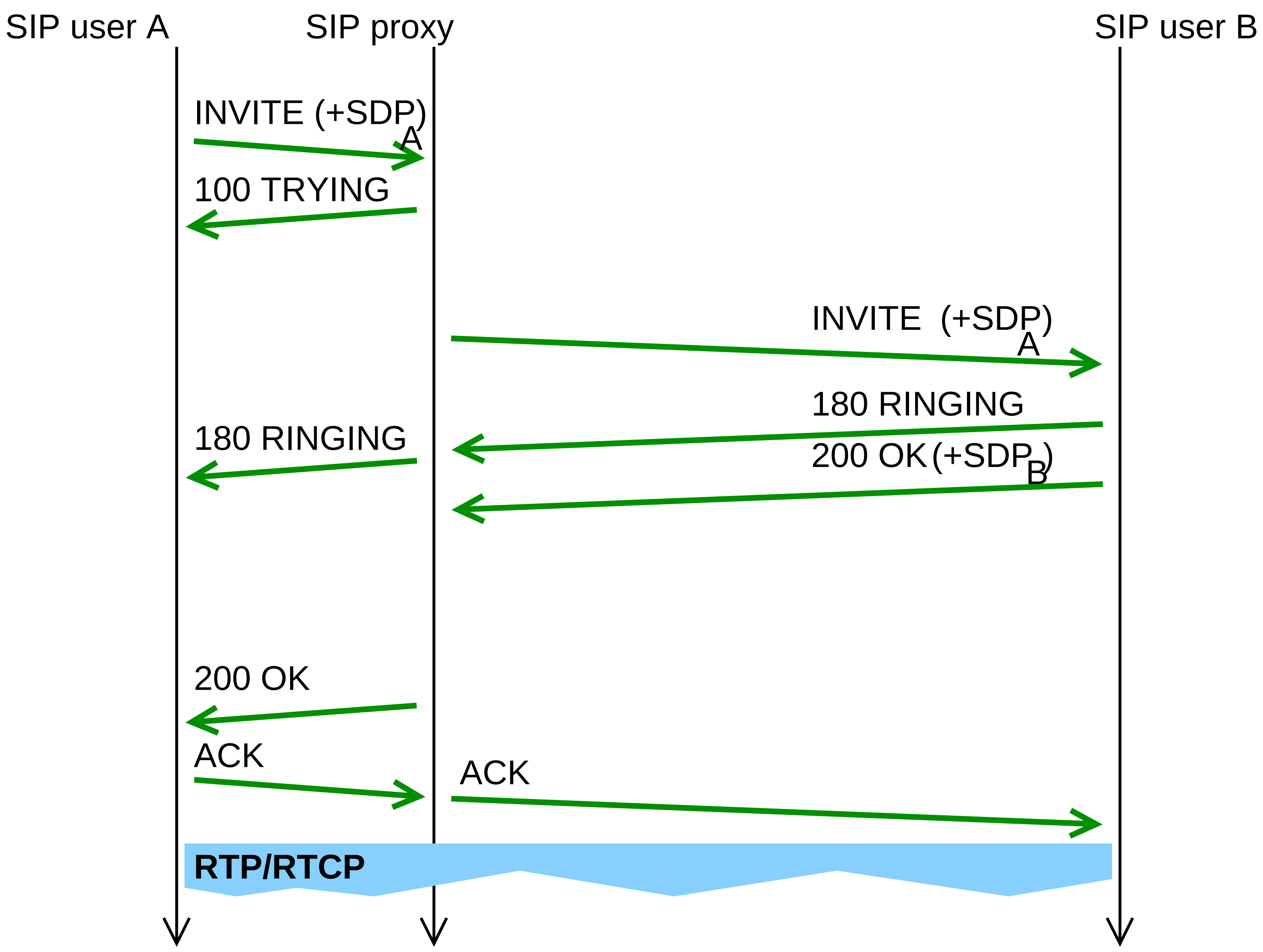
- **"A firewall is a system or group of systems that enforces an access control policy between two networks."**
- **Realization by packet filter and/or proxies**

➥ **Firewalls in media path have to interact with session signaling**

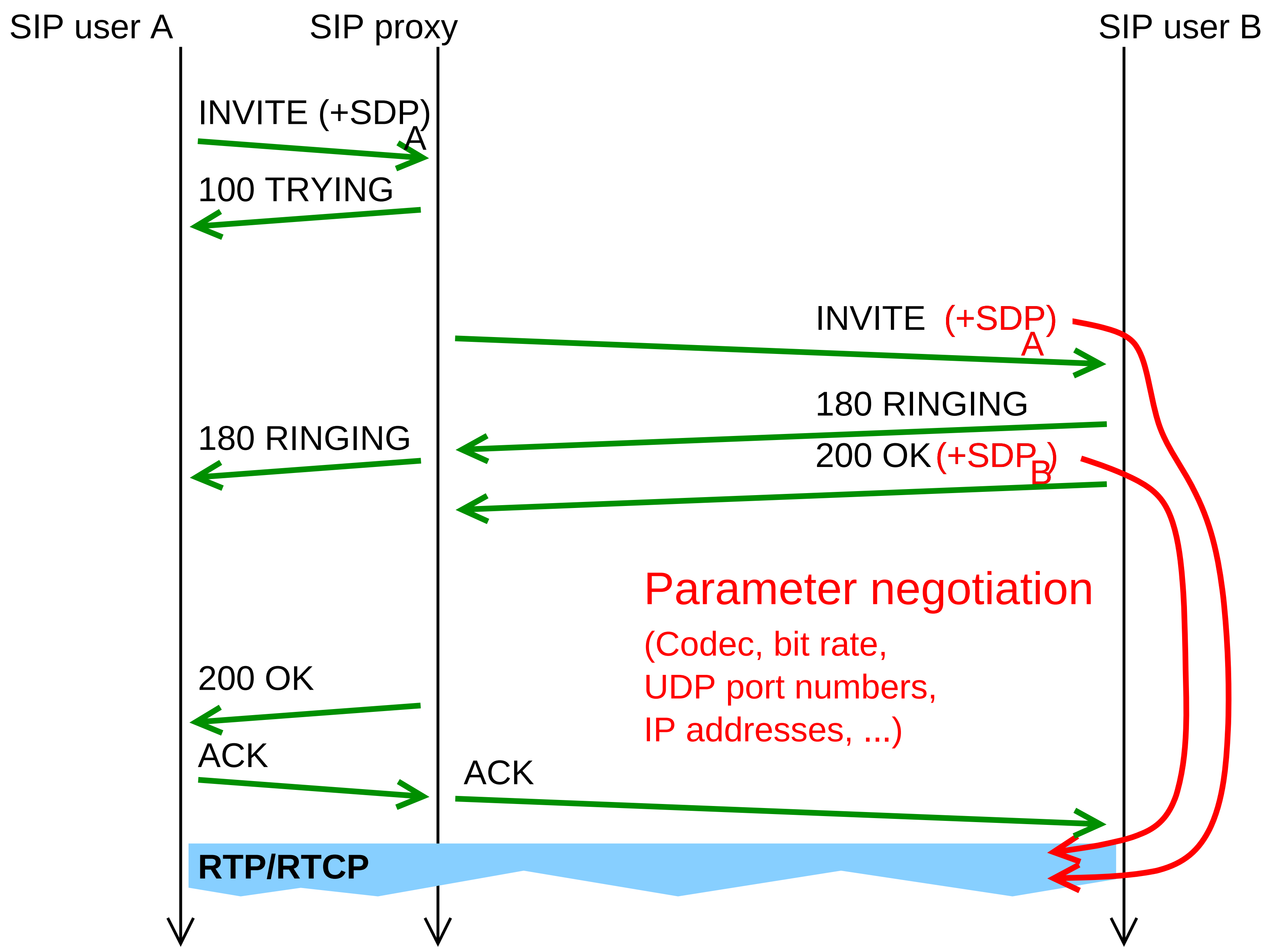
SIP/RTP: basic call flow



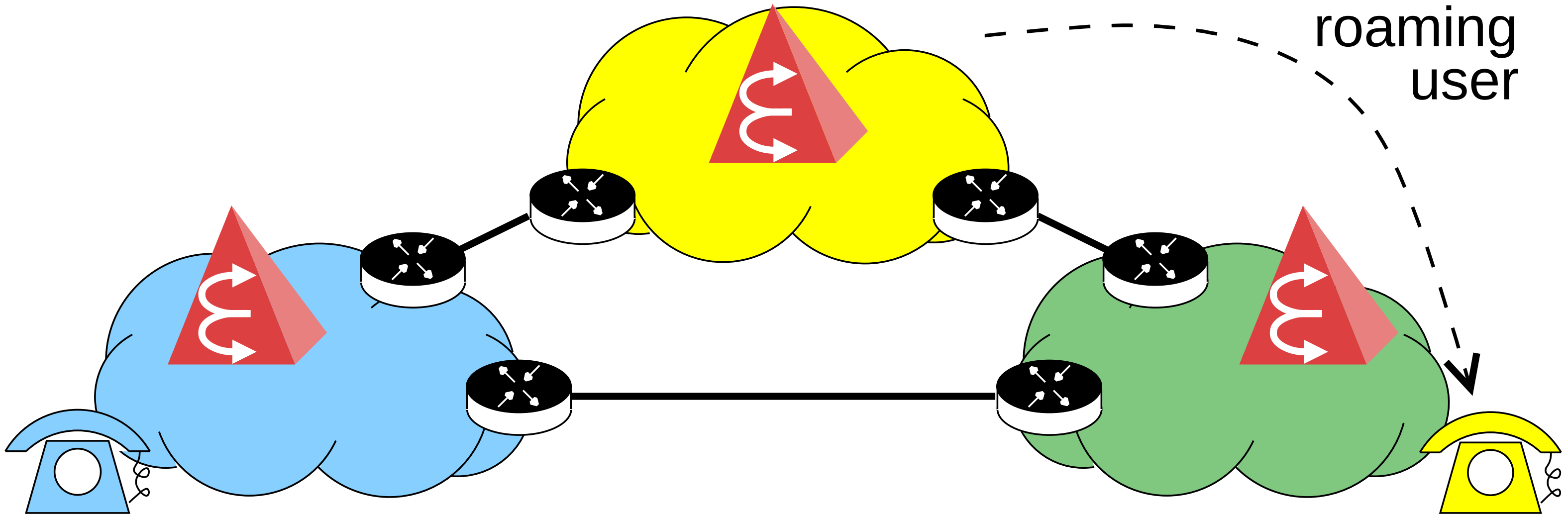
SIP/RTP: basic call flow



SIP/RTP: dyn. cross-layer parameter negotiation

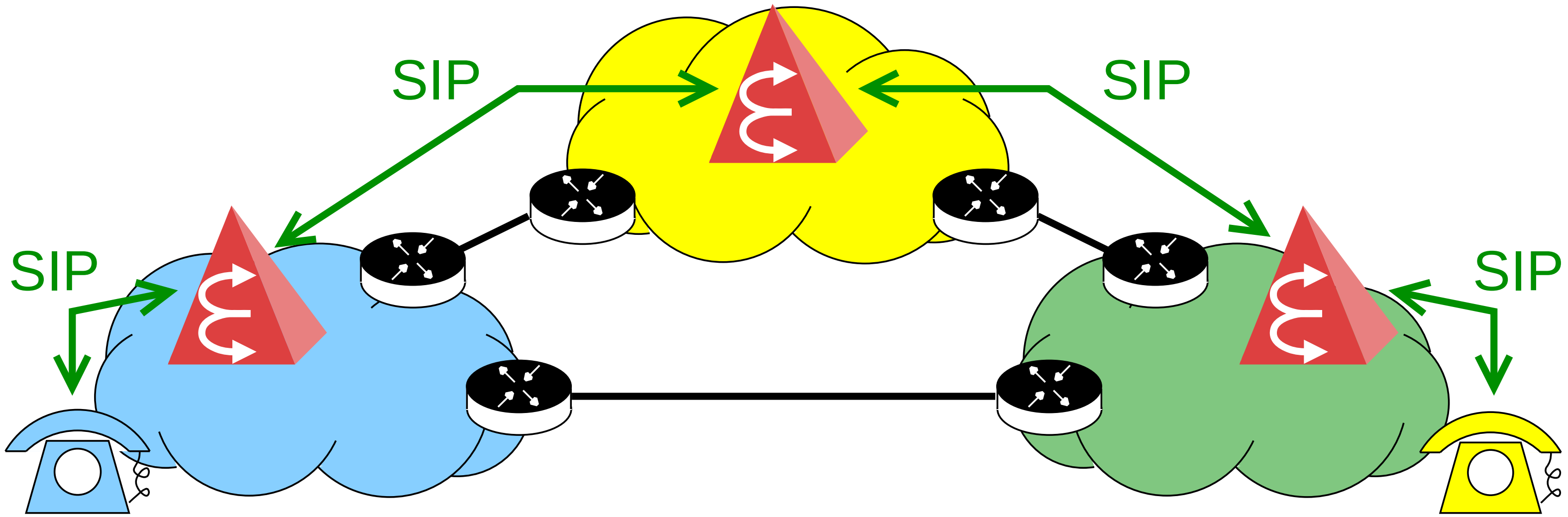


Firewalls and out-of-band signaling

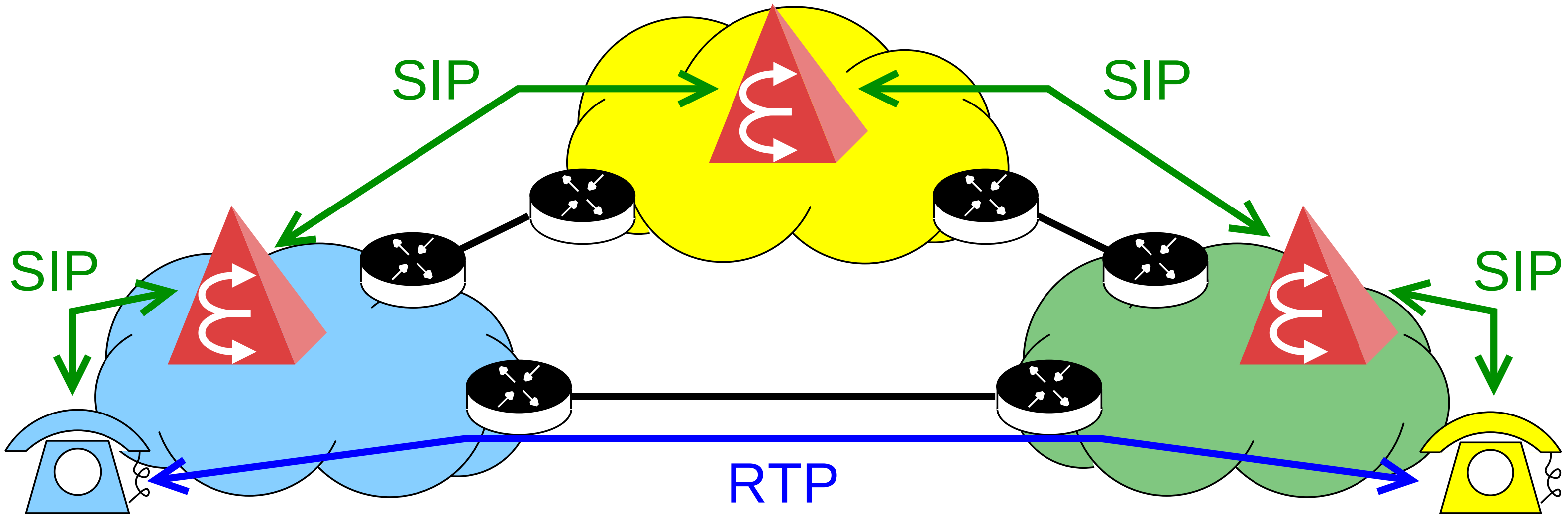


- **Clouds: IP based Operator Networks (e.g., NGN)**
- **Network interconnection based on bilateral agreements, protected by means of firewalls**

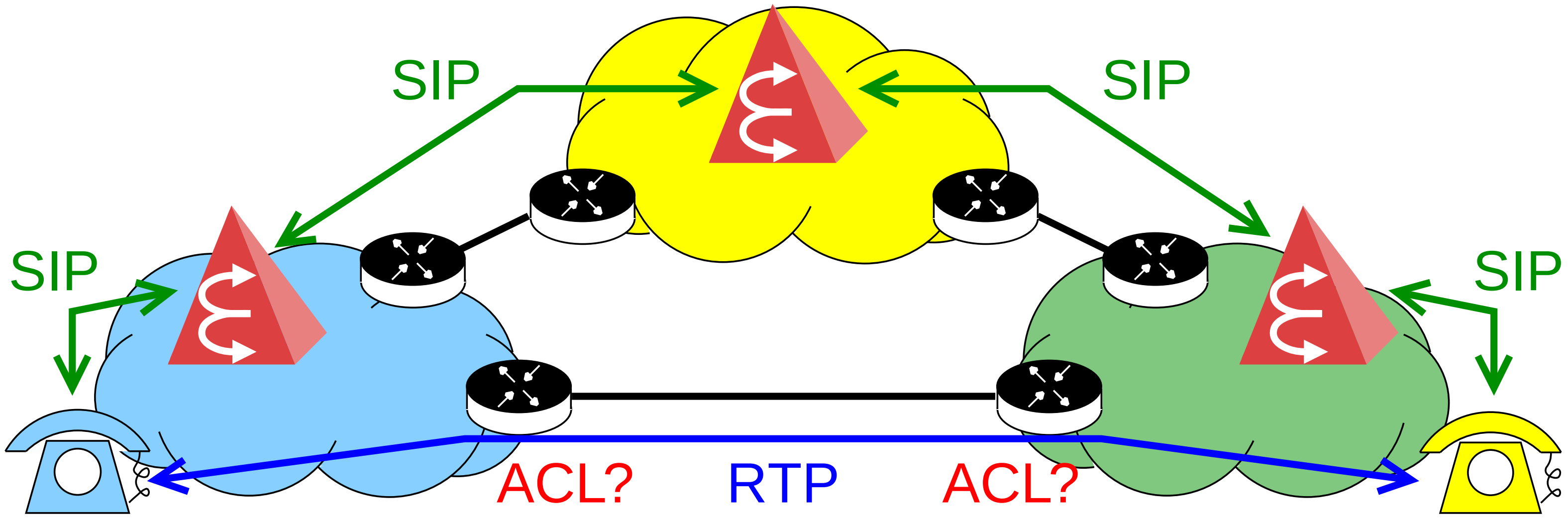
Firewalls and out-of-band signaling



Firewalls and out-of-band signaling



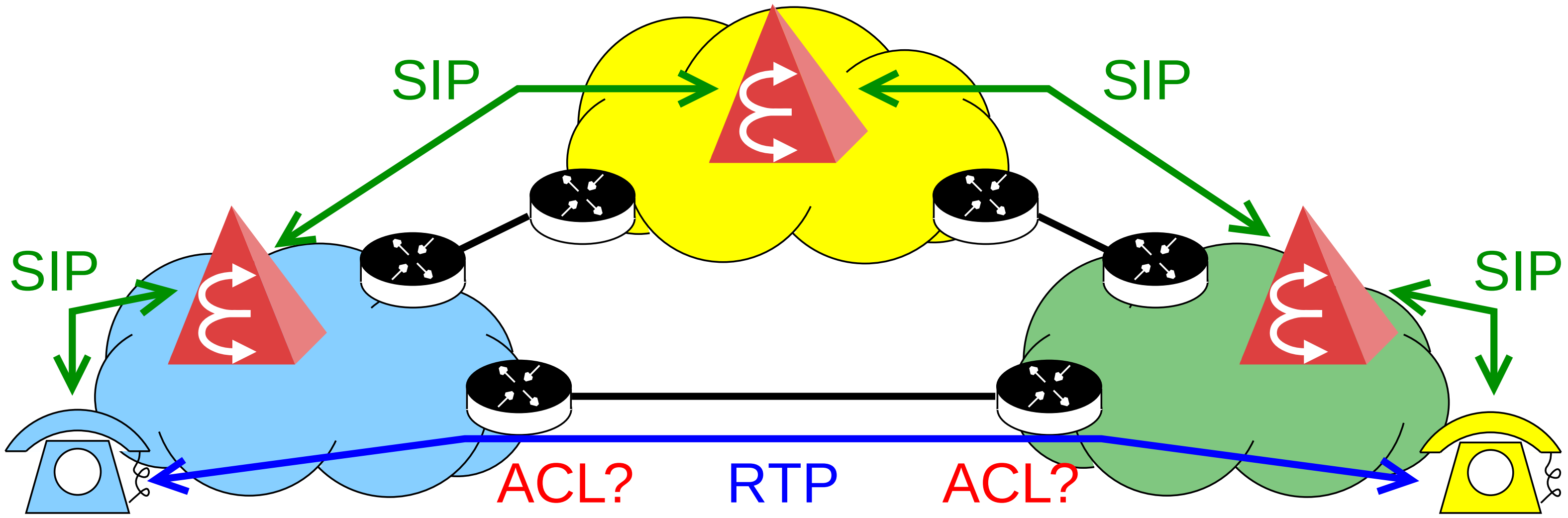
Firewalls and out-of-band signaling



- **Signaling messages negoitate parameters for media streams**
- **Signaling messages may travel on different path through network than media streams do**

➥ **SIP/RTP firewall traversal problem**

Firewalls and out-of-band signaling

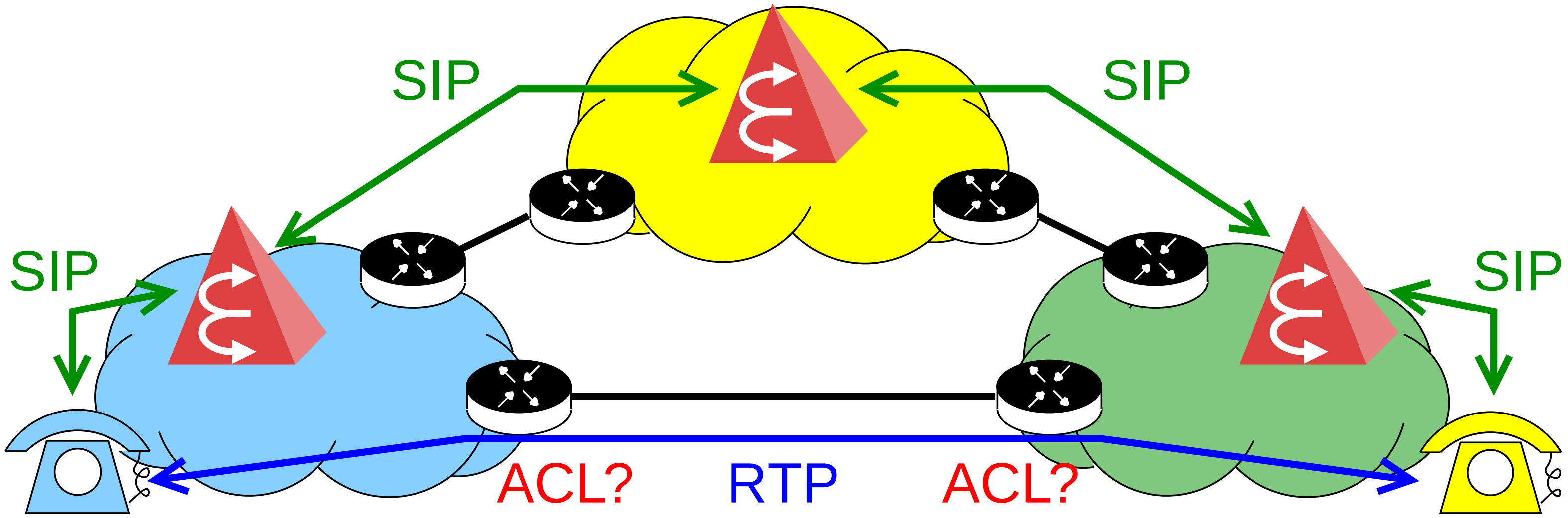


SIP/RTP firewall traversal problem - solution approaches

- **Remove firewall**
- **Static, permissive firewall configuration**
- **(HTTP) tunnel through firewall**

➥ **Secure?**

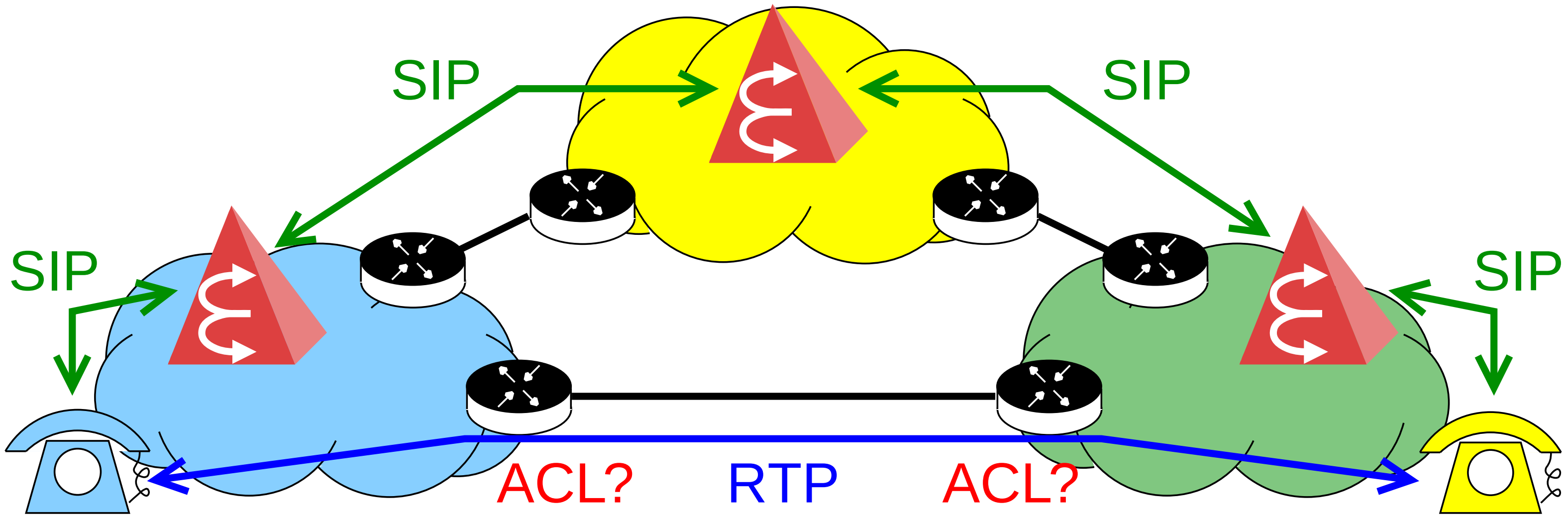
Firewalls and out-of-band signaling



SIP/RTP firewall traversal problem - solution approaches (cont.)

- **SIP decoder in packet filter (e.g., Linux Netfilter "Protocol Helper")**
  - ➥ Implementation difficult
  - ➥ Problem if signaling and media on different path
- **Application Layer Gateways (e.g., "Session Border Controller")**
  - ➥ Media will be forced to signaling path ➥ Efficiency? Latency?
  - ➥ Call state at network edge

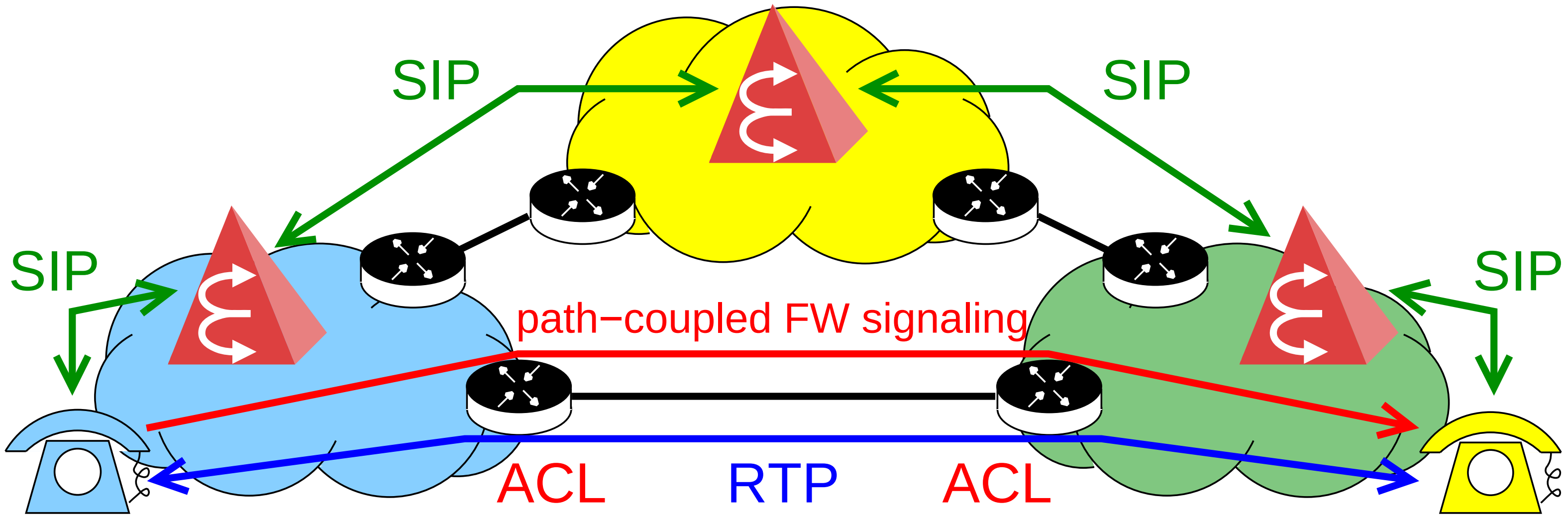
Firewalls and out-of-band signaling



<span>SIP/RTP firewall traversal problem</span> - solution approaches (cont.)

- **Use "firewall control protocol" for dynamic opening of "pinholes" in packet filter for media streams during call duration.**
  - ➥ Remote control of packet filter by means of signaling protocol
  - ➥ Where/Who is controlling entity? How to send signaling messages?
  - - Path-coupled firewall signaling
  - - Path-decoupled firewall signaling

Firewalls and out-of-band signaling



Examples for path-coupled firewall signaling:

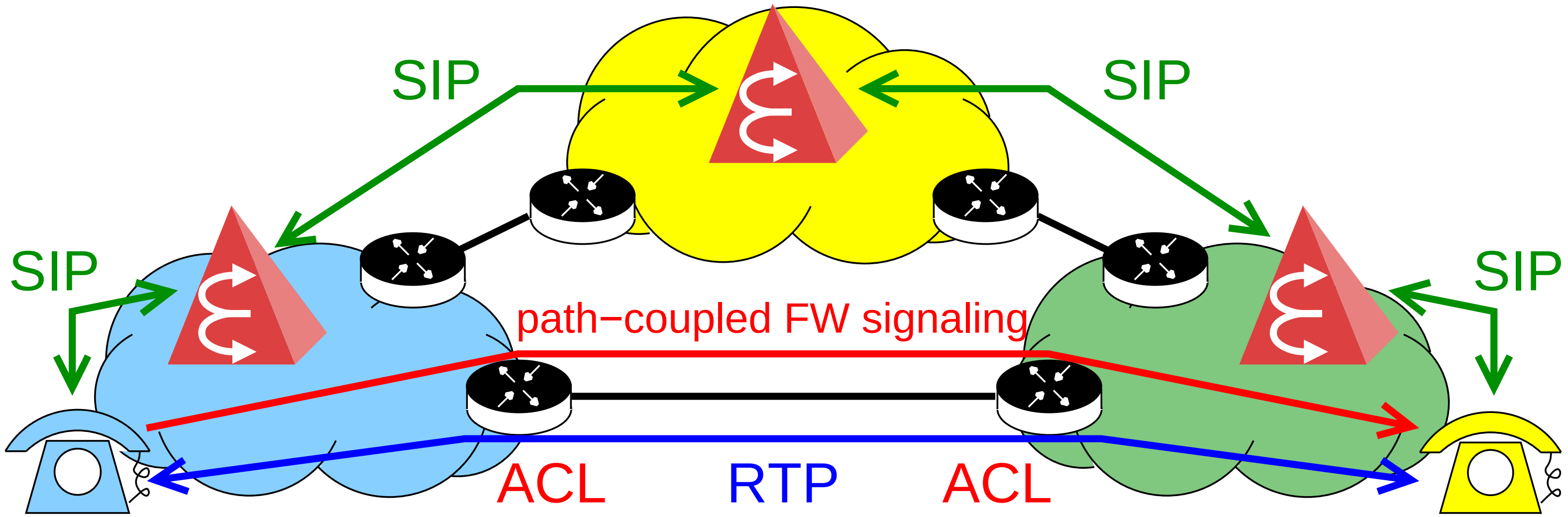
- **RSVP**
- **IETF NSIS (Next Steps In Signaling) - NAT/FW NSLP**

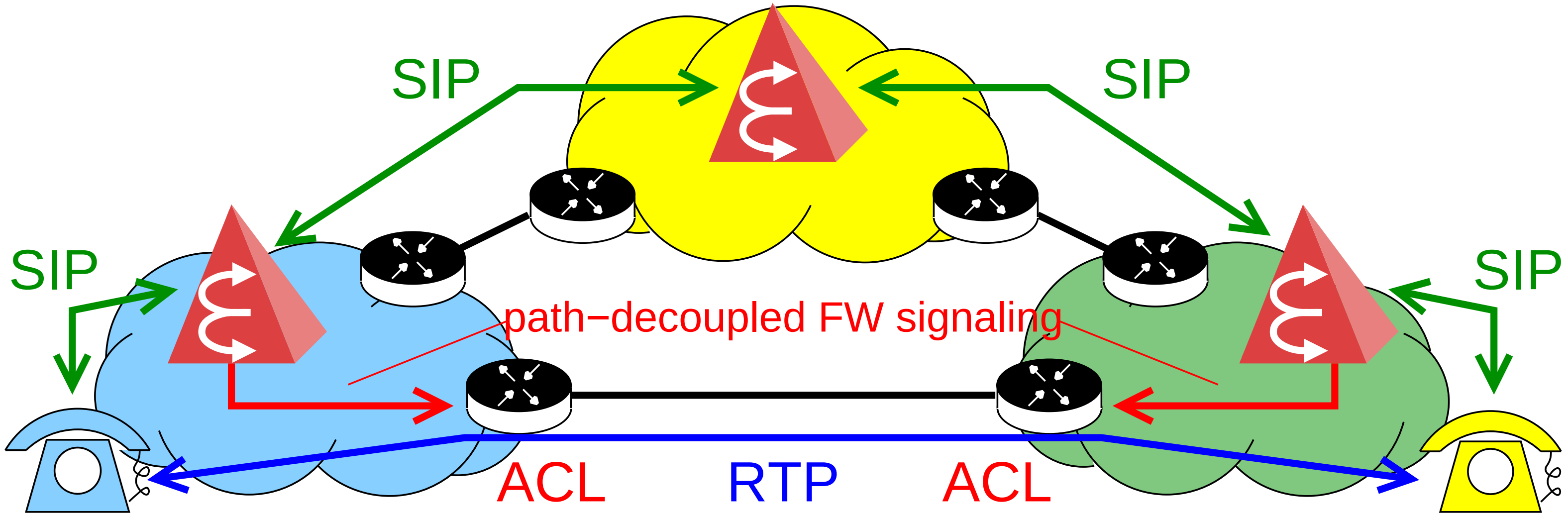
Signaling messages will be sent along the (future) media path

➥ No problem to find all firewalls on the path

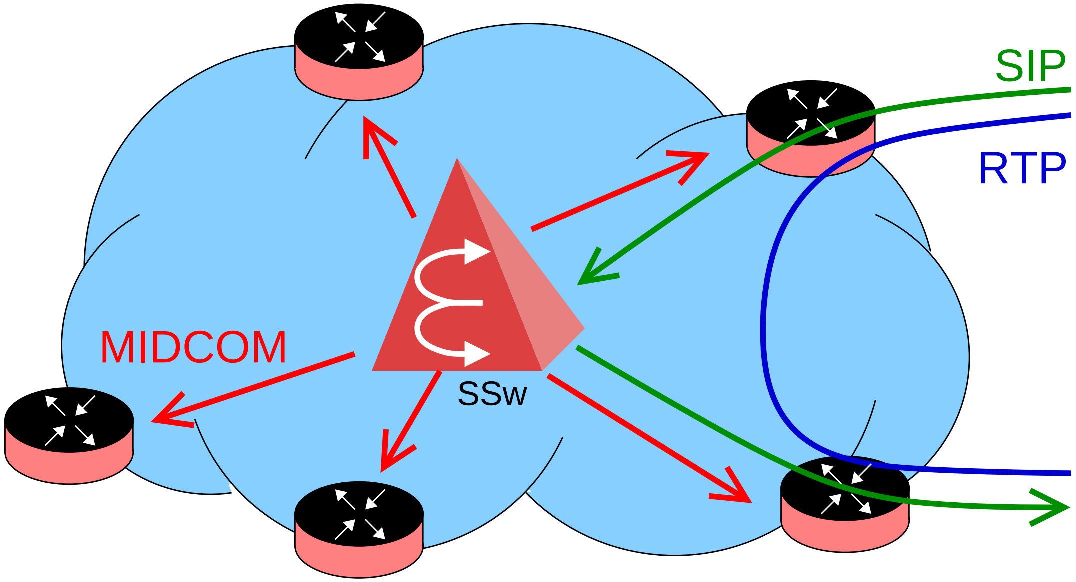
➥ Problem: secure and efficient (!) authorization of signaling messages

Firewalls and out-of-band signaling





Firewalls and out-of-band signaling



Examples for path-decoupled firewall signaling:

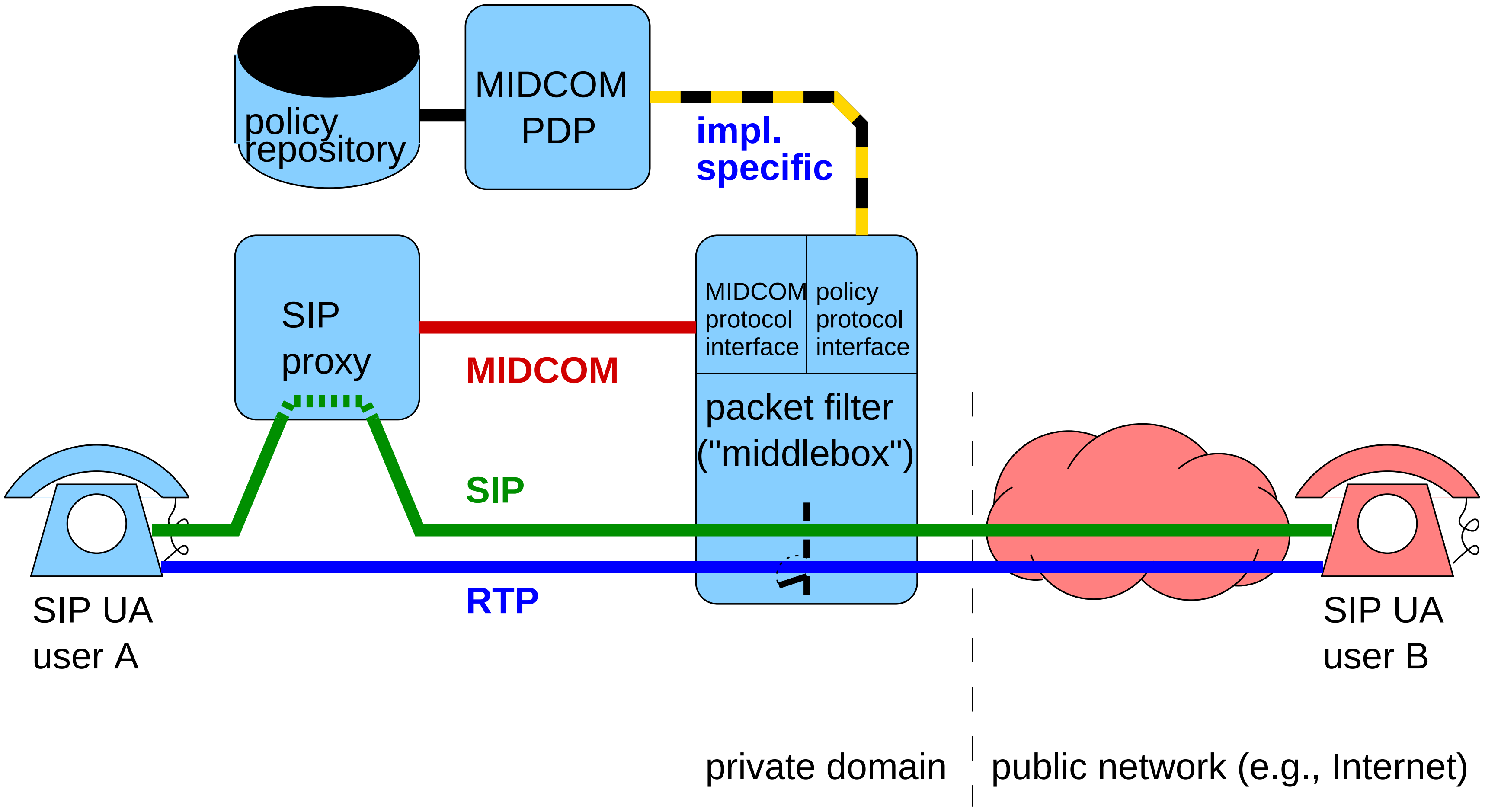
- **UPnP (home and small office LANs only)**
- **IETF MIDCOM**

Signaling messages will be sent from (centralized) softswitch (SSw)

➥ **Clear trust relationships (SSw: master, firewall: slave), pre-established IPsec/TLS security associations (➥ low latency)**

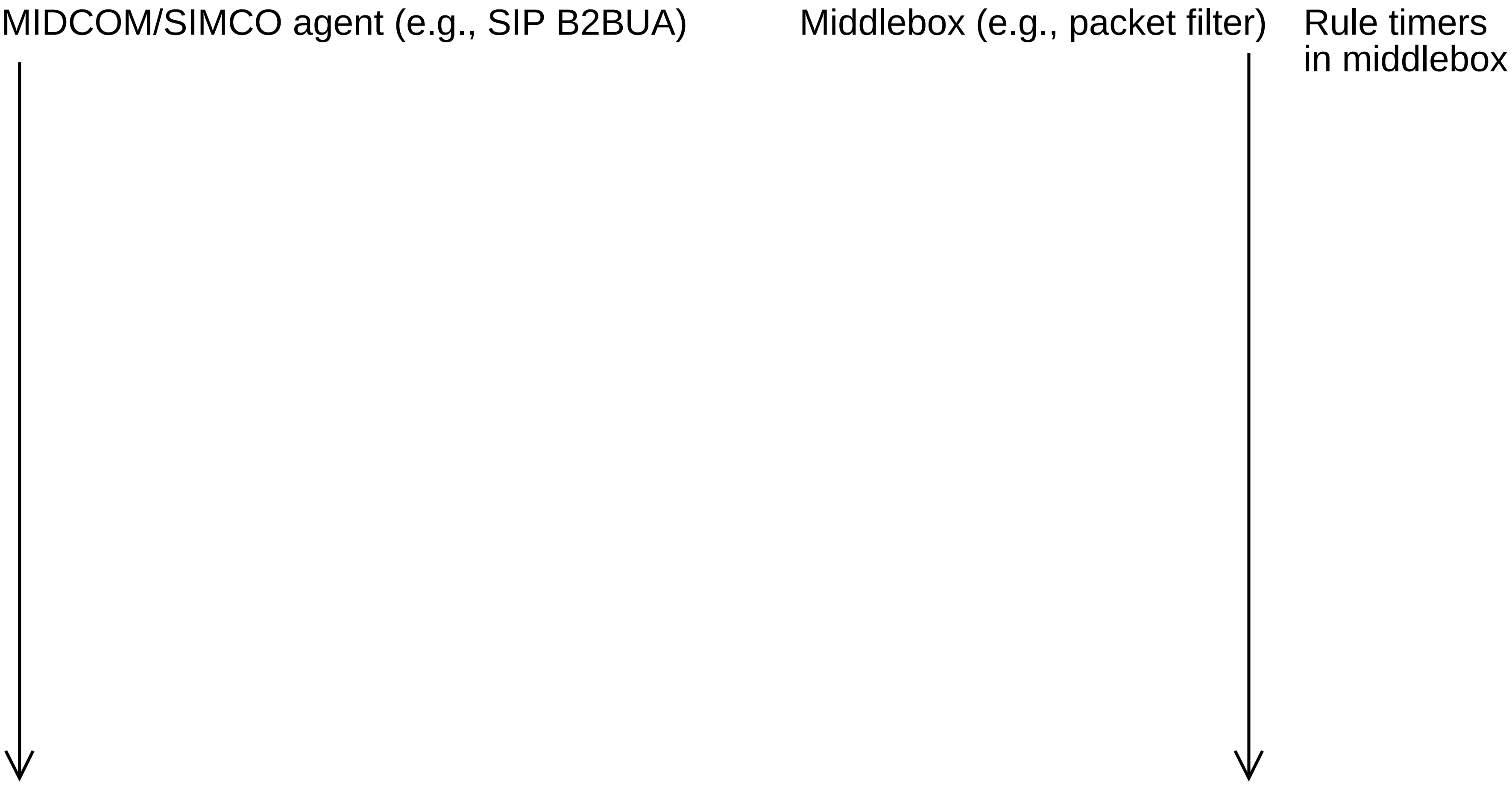
➥ **Problem: how to find firewalls on media path facing dynamic routing?**

IETF MIDCOM - SIMCO


policy repository
MIDCOM PDP
impl. specific
SIP proxy
MIDCOM
MIDCOM protocol interface
policy protocol interface
packet filter ("middlebox")
SIP
RTP
SIP UA user A
SIP UA user B
private domain
public network (e.g., Internet)

- **IETF MIDCOM is a framework architecture + protocol semantics**
- **Can be implemented using several protocols: SNMP, MEGACO, COPS, DIAMETER, SIMCO (SImple Middlebox COnfiguration) Protocol, ...**

IETF MIDCOM - SIMCO

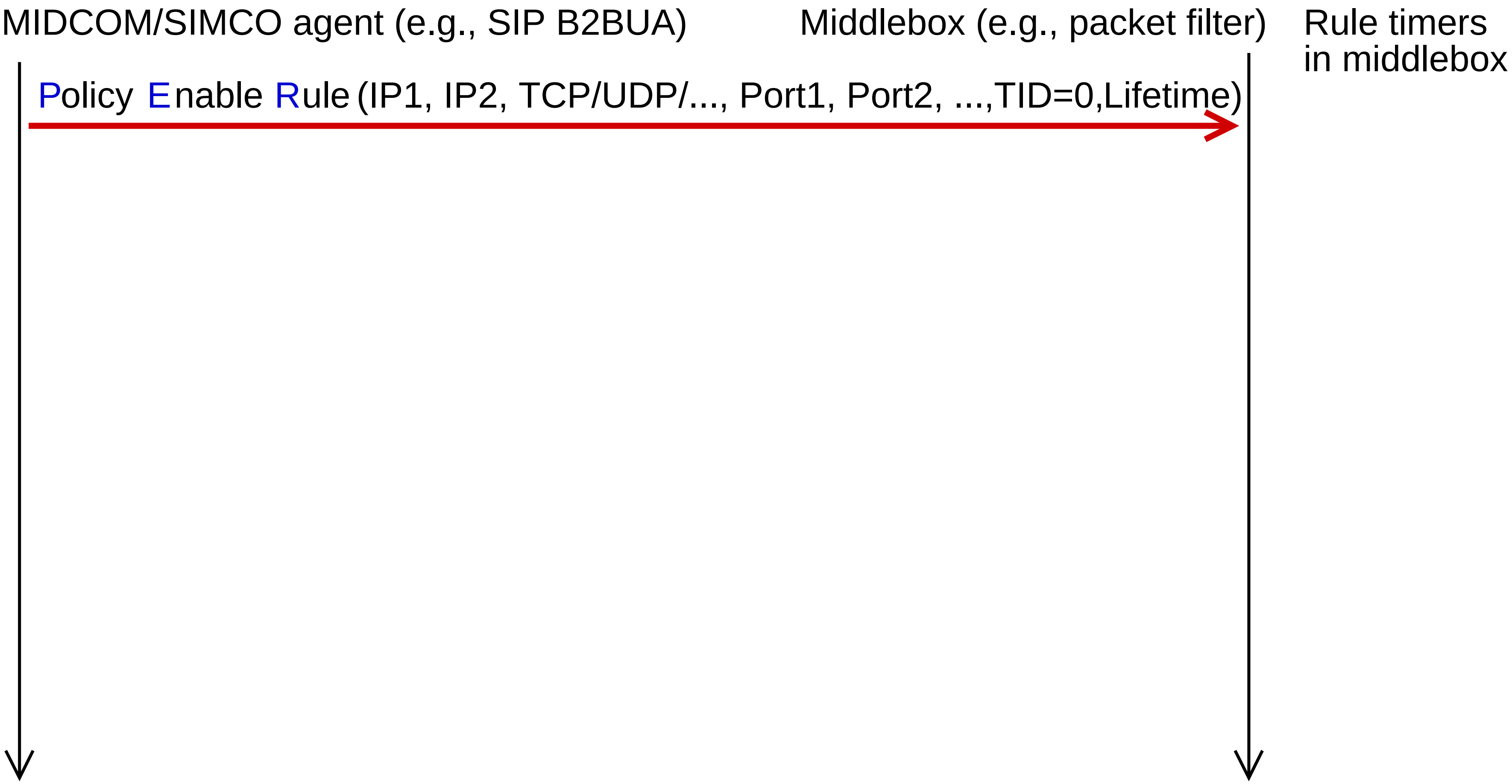


MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers
in middlebox

IETF MIDCOM - SIMCO



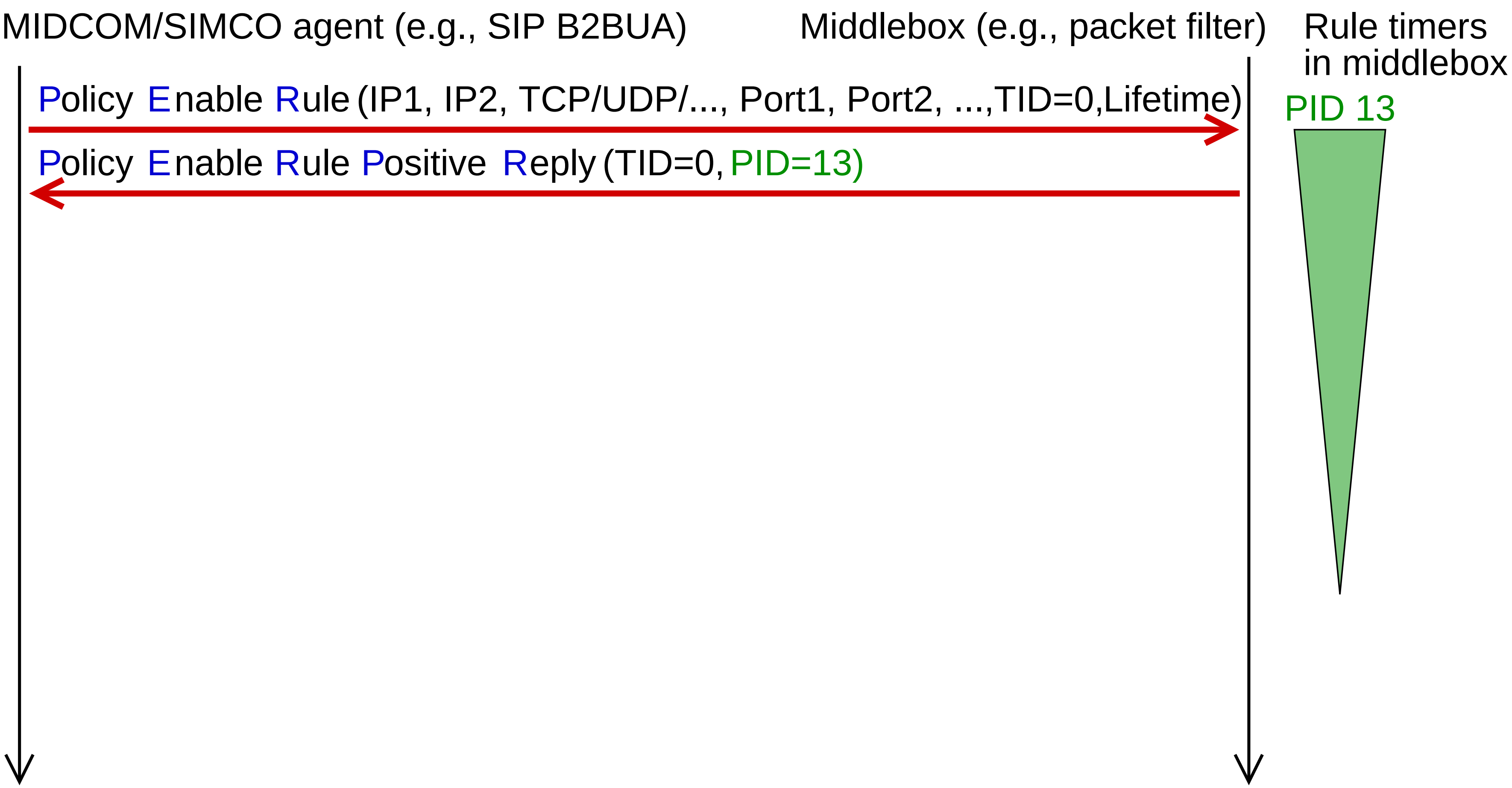
MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers
in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

IETF MIDCOM - SIMCO



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

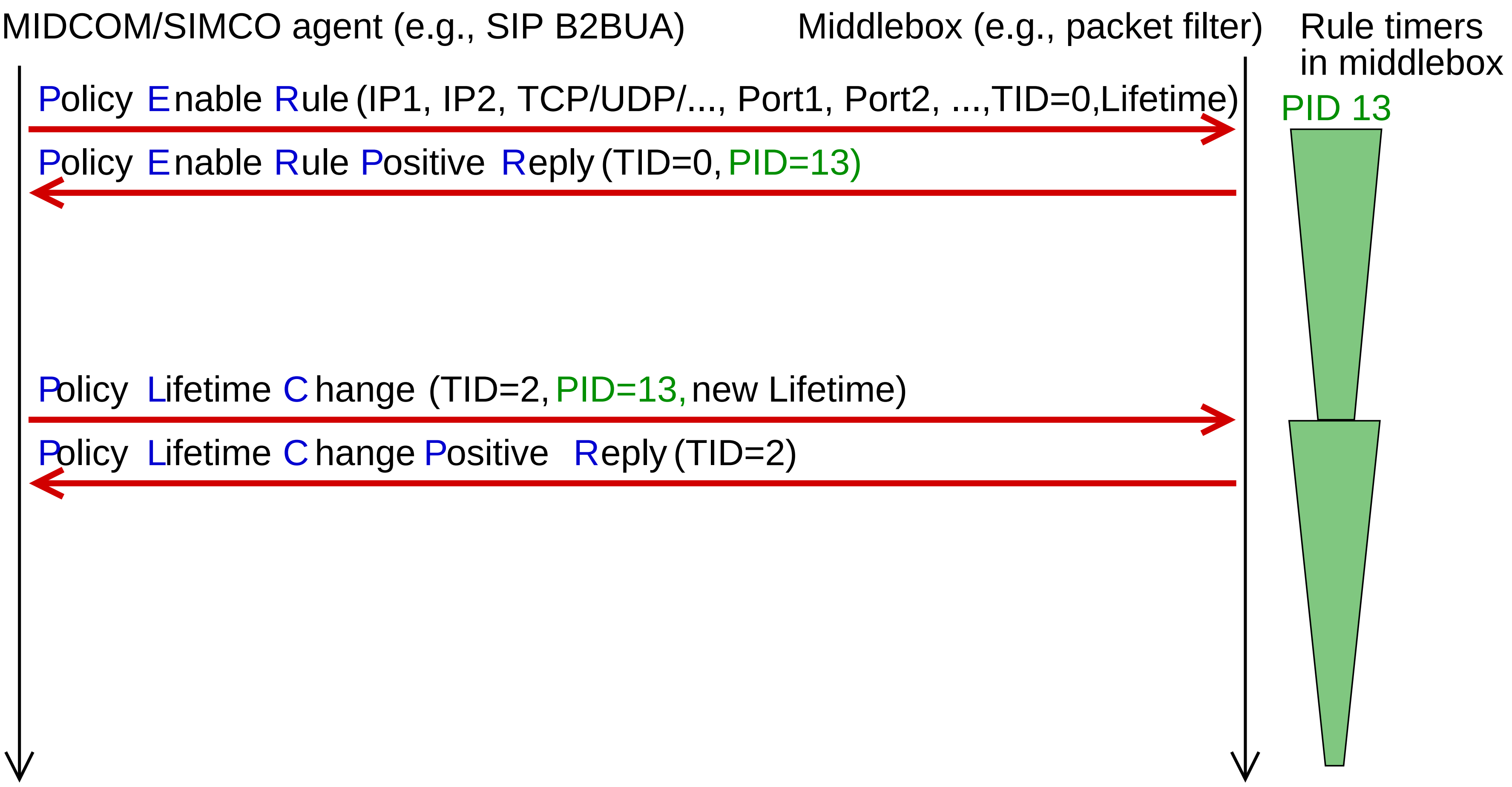
Rule timers
in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

Policy Enable Rule Positive Reply (TID=0, PID=13)

PID 13

IETF MIDCOM - SIMCO



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers
in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

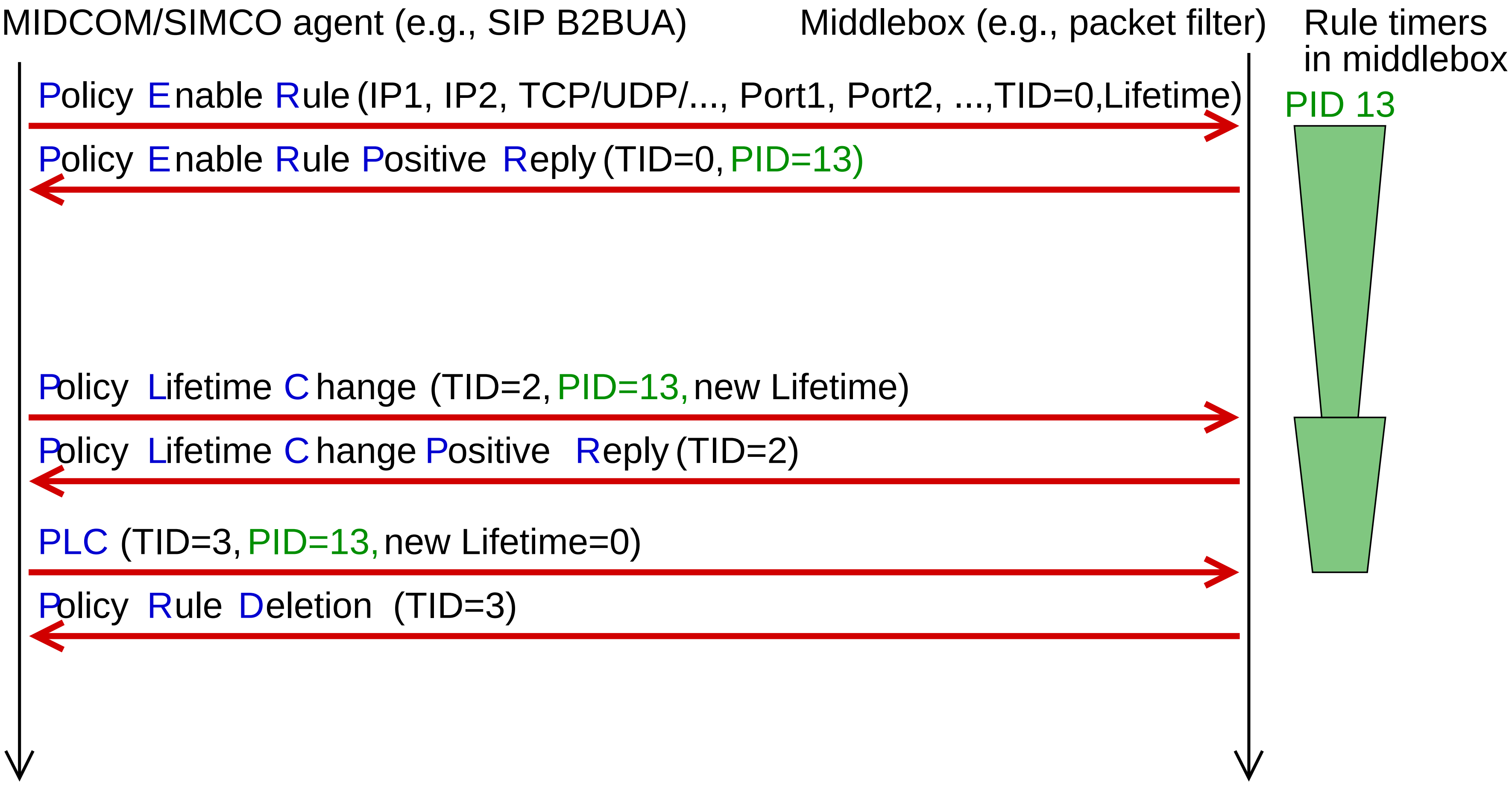
PID 13

Policy Enable Rule Positive Reply (TID=0, PID=13)

Policy Lifetime Change (TID=2, PID=13, new Lifetime)

Policy Lifetime Change Positive Reply (TID=2)

IETF MIDCOM - SIMCO



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers in middlebox

PID 13

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

Policy Enable Rule Positive Reply (TID=0, PID=13)

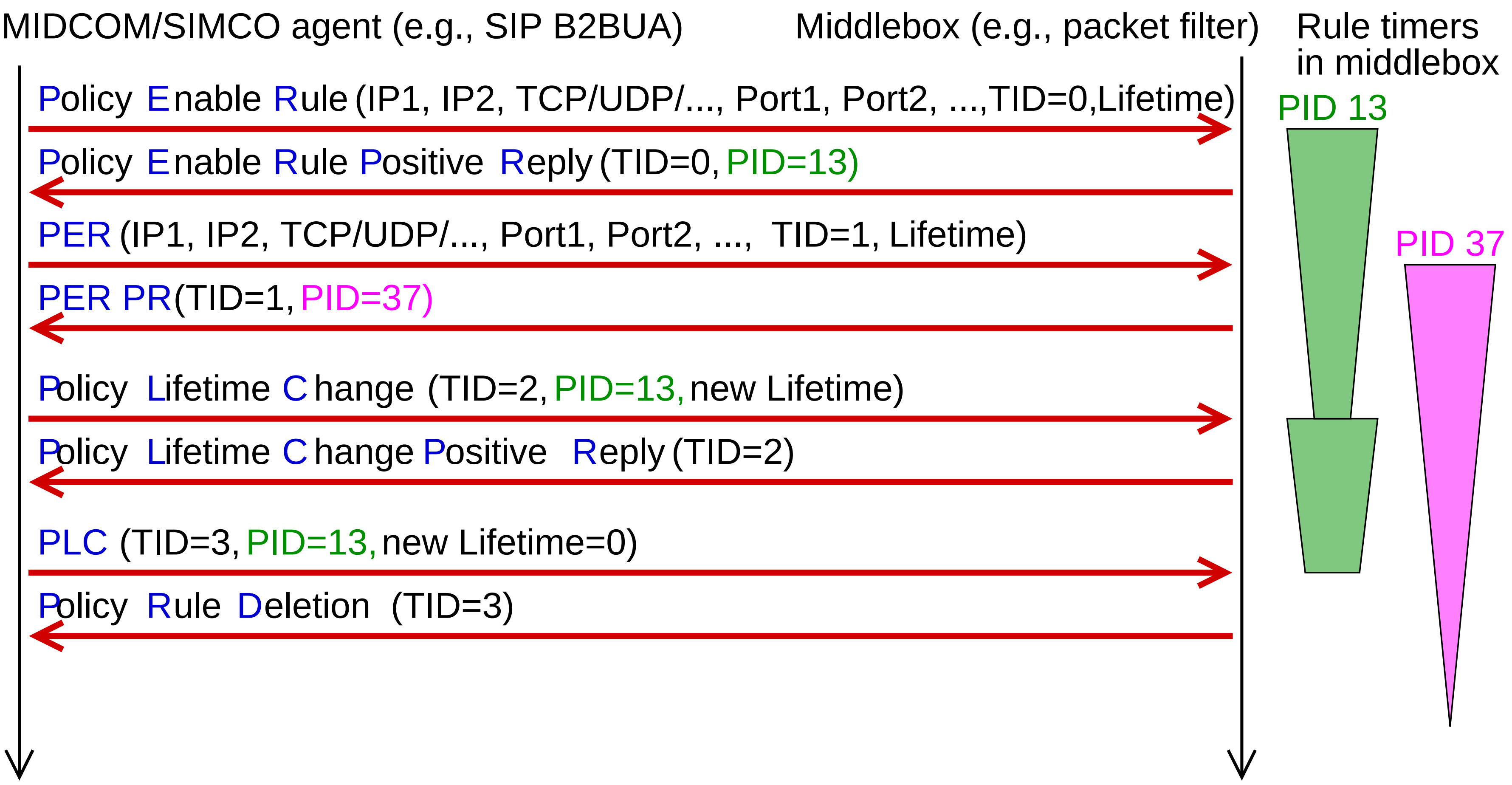
Policy Lifetime Change (TID=2, PID=13, new Lifetime)

Policy Lifetime Change Positive Reply (TID=2)

PLC (TID=3, PID=13, new Lifetime=0)

Policy Rule Deletion (TID=3)

IETF MIDCOM - SIMCO



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

Policy Enable Rule Positive Reply (TID=0, PID=13)

PER (IP1, IP2, TCP/UDP/..., Port1, Port2, ..., TID=1, Lifetime)

PER PR(TID=1, PID=37)

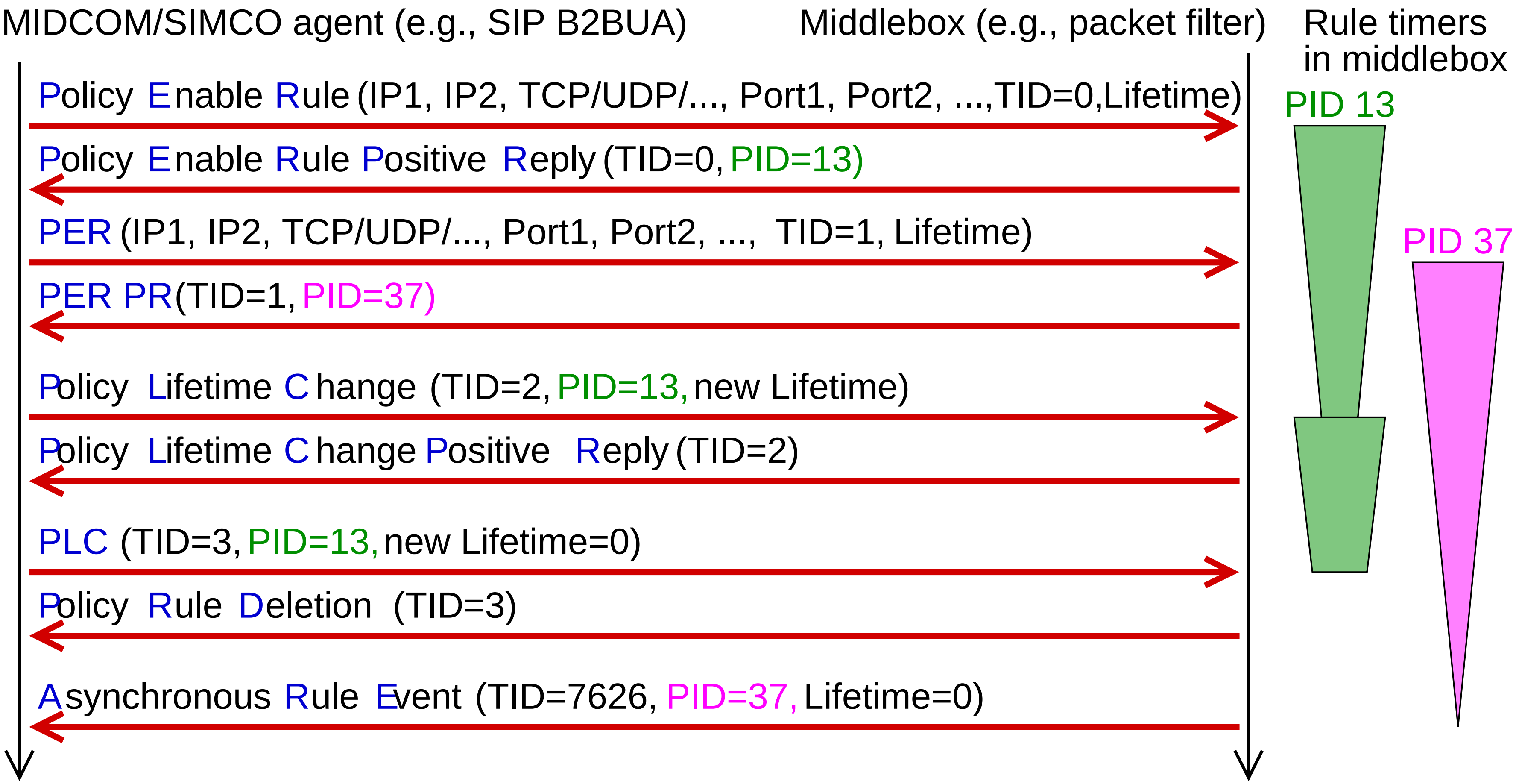
Policy Lifetime Change (TID=2, PID=13, new Lifetime)

Policy Lifetime Change Positive Reply (TID=2)

PLC (TID=3, PID=13, new Lifetime=0)

Policy Rule Deletion (TID=3)

IETF MIDCOM - SIMCO



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

Policy Enable Rule Positive Reply (TID=0, PID=13)

PER (IP1, IP2, TCP/UDP/..., Port1, Port2, ..., TID=1, Lifetime)

PER PR(TID=1, PID=37)

Policy Lifetime Change (TID=2, PID=13, new Lifetime)

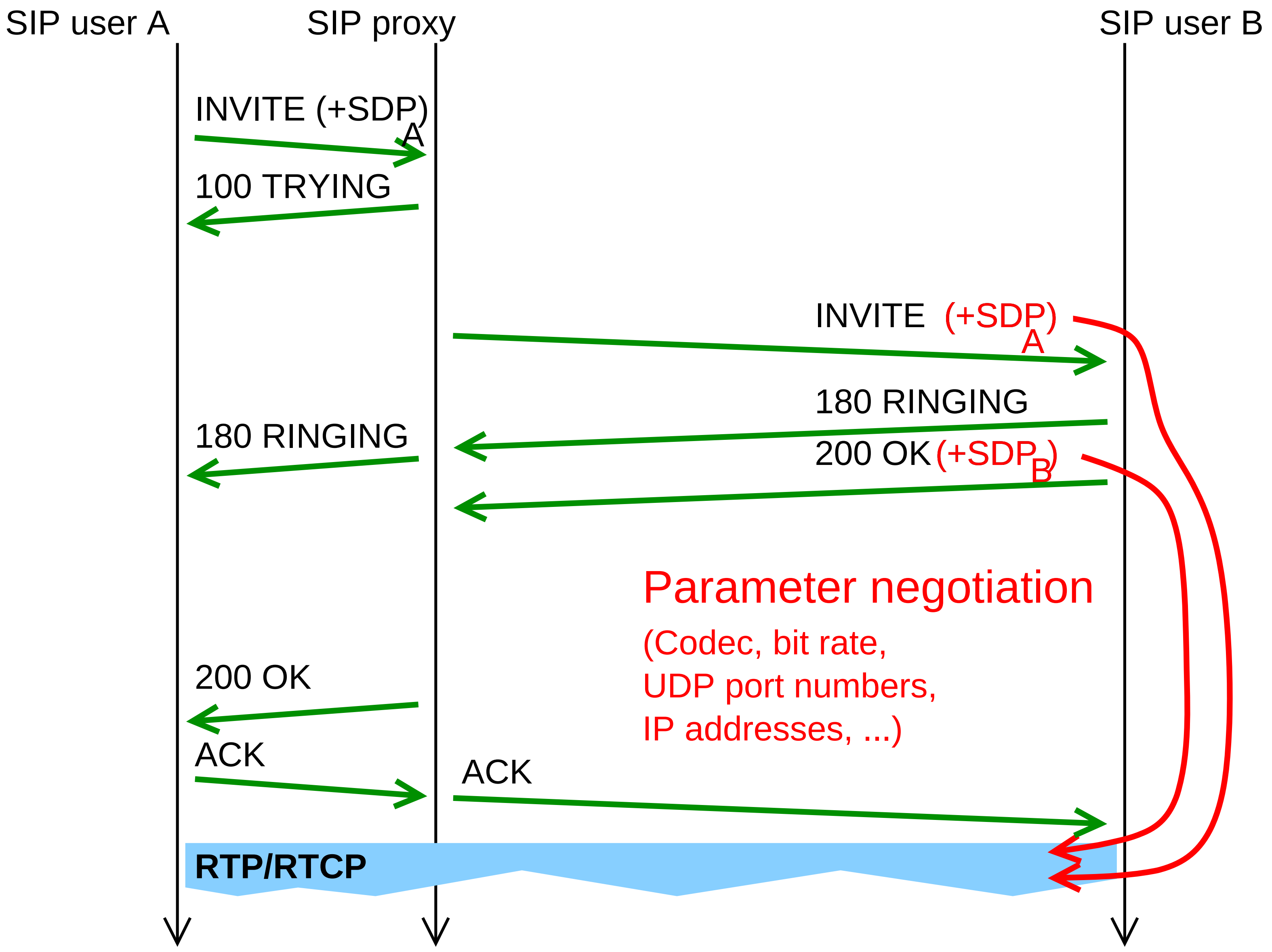
Policy Lifetime Change Positive Reply (TID=2)

PLC (TID=3, PID=13, new Lifetime=0)

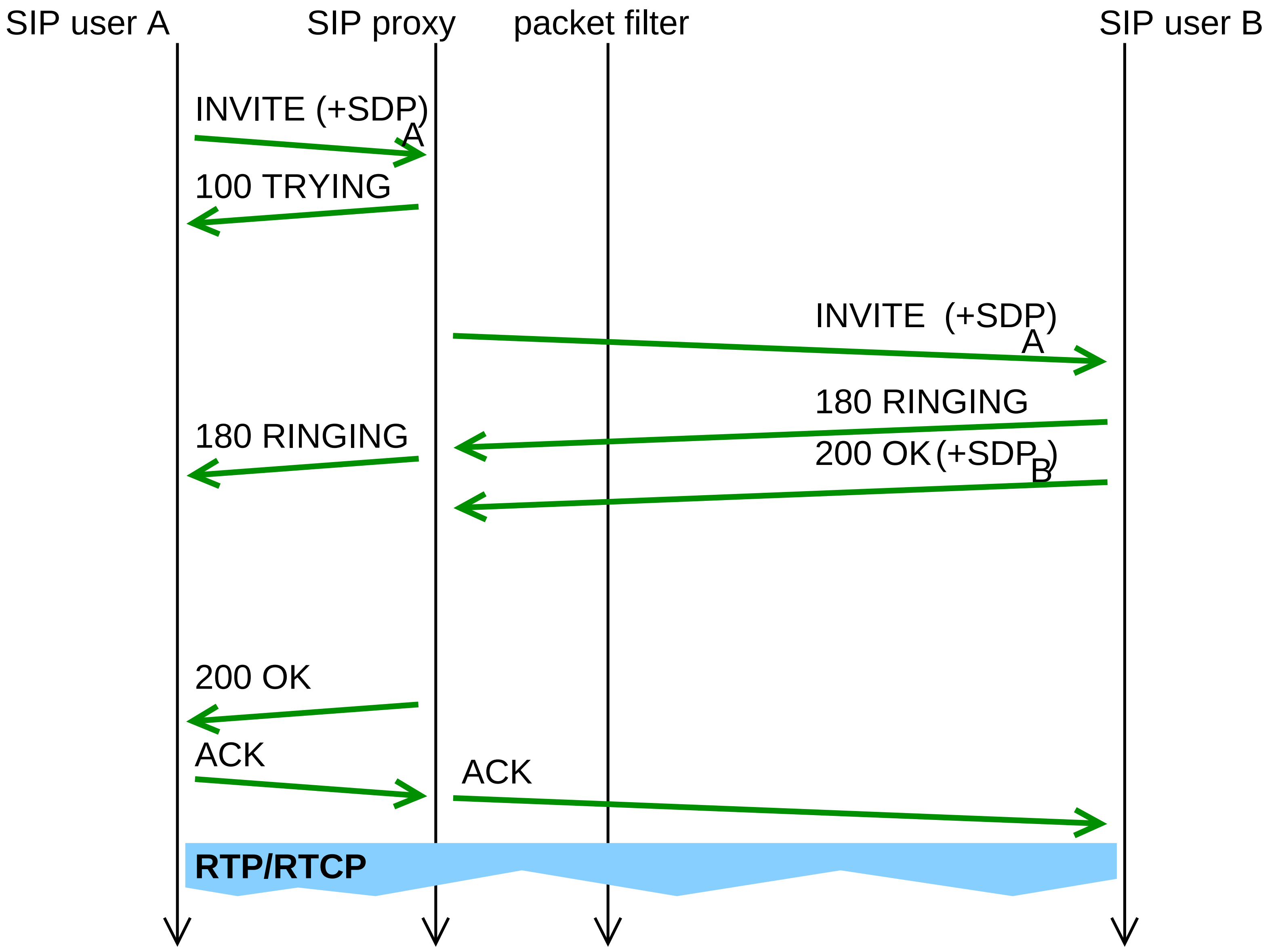
Policy Rule Deletion (TID=3)

Asynchronous Rule Event (TID=7626, PID=37, Lifetime=0)

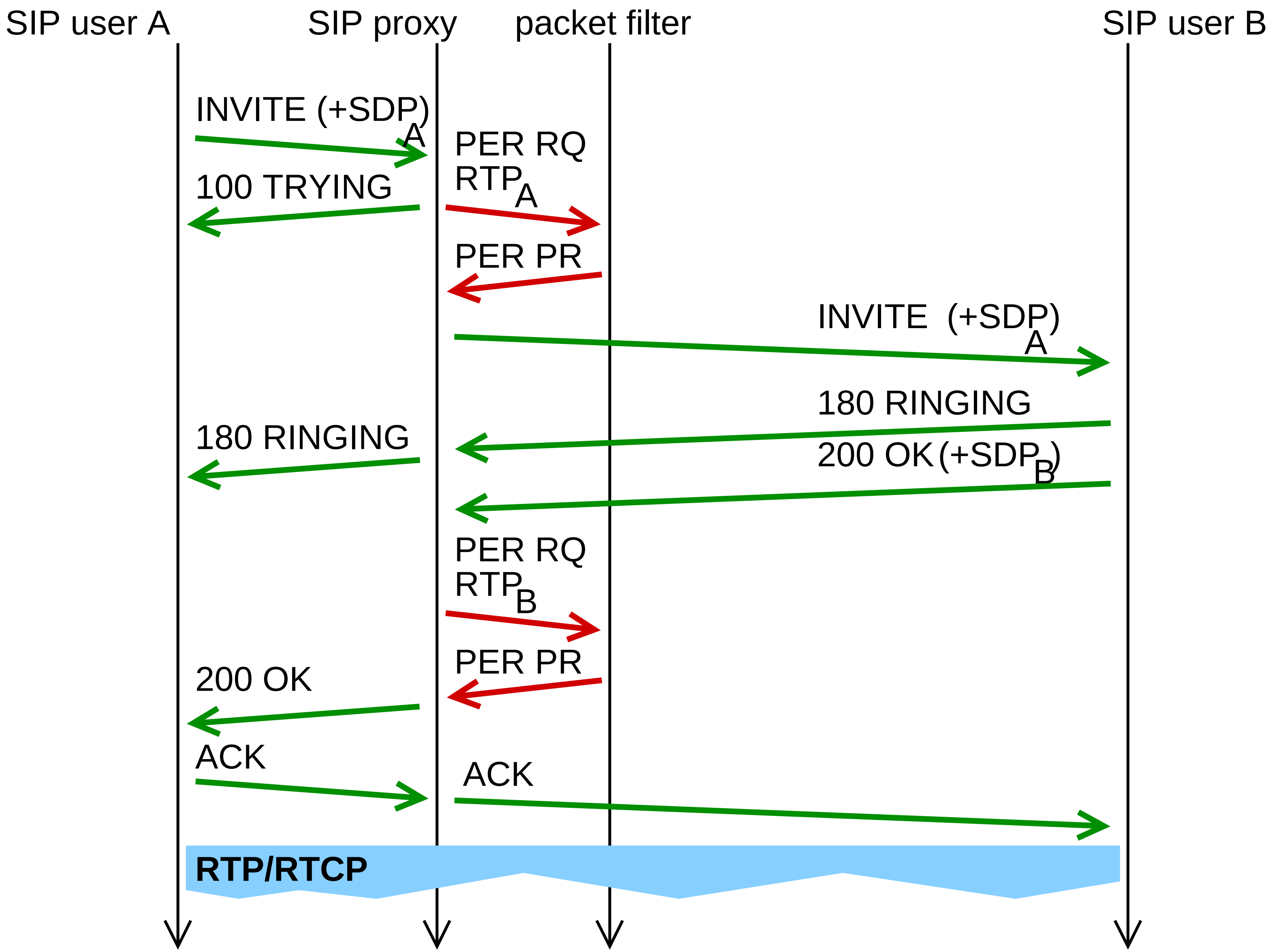
SIMCO - Interaction with SIP/RTP



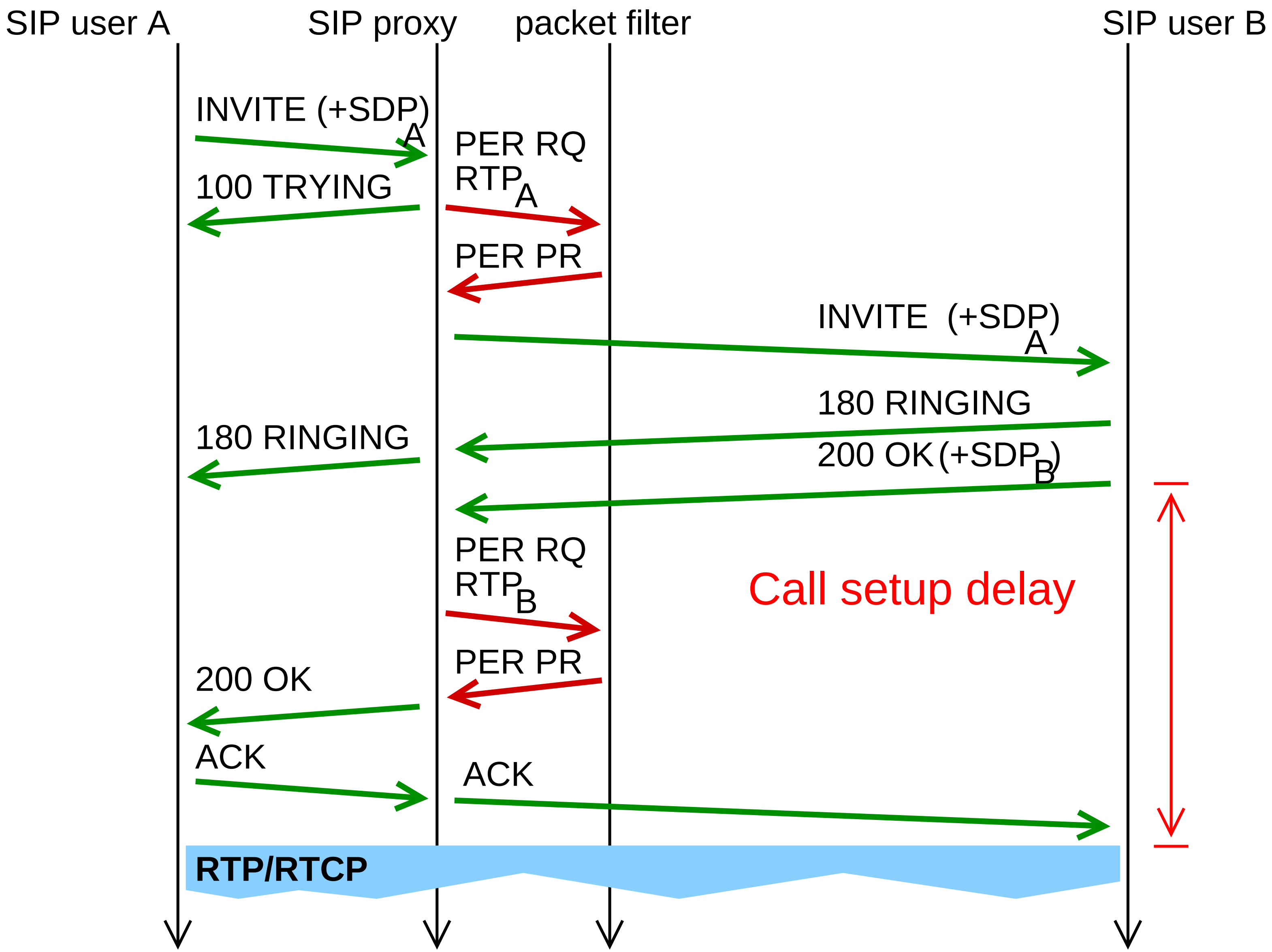
SIMCO - Interaction with SIP/RTP



SIMCO - Interaction with SIP/RTP



SIMCO - Interaction with SIP/RTP



Summary SIMCO

- **Signaling protocol for Firewall and NAT control**
- **Implements (abstract) IETF MIDCOM architecture and semantics**
- **Policy Rules**
  - Generalized representation of packet filter rules, NAT bindings, etc.
  - Soft state
- **Messages**
  - Session management
  - **Create, modify, delete policy rules** by means of transactions
  - Status query transactions
  - Asynchronous notifications
- **Current status: Internet Draft**
  `draft-stiemerling-midcom-simco-08.txt`
- **Prototype Implementations: NEC Europe, Ltd., Uni Stuttgart/IKR**

Summary SIMCO

- **Signaling protocol for Firewall and NAT control**
- **Implements (abstract) IETF MIDCOM architecture and semantics**
- **Policy Rules**
  - Generalized representation of packet filter rules, NAT bindings, etc.
  - Soft state
- **Messages**
  - Session management
  - **Create, modify, delete policy rules** by means of transactions
  - Status query transactions
  - Asynchronous notifications
- **Current status: Internet Draft**
  `draft-stiemerling-midcom-simco-08.txt`
- **Prototype Implementations: NEC Europe, Ltd., Uni Stuttgart/IKR**
- **Default transport protocol: TCP (Transmission Control Protocol)**

➥ **Reduced latency by using SCTP (Stream Control Transmission P.)?**

Stream Control Transmission Protocol

SCTP (Stream Control Transmission Protocol, RFC 2960)

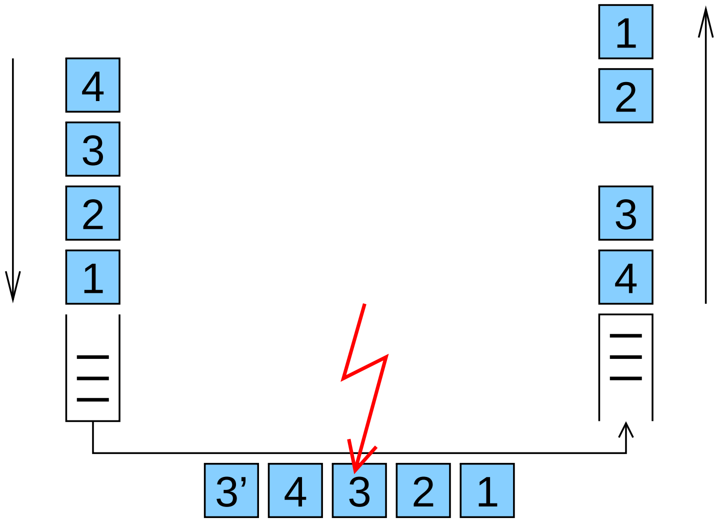
- **Generic transport layer protocol optimized for signaling purposes, originally developed as part of the SIGTRAN stack for "SS7 over IP"**
- **Connection oriented: "SCTP association"**
  - Reliable transmission (checksums, flow-control, etc.)
  - "TCP friendly" congestion control
  - Message-oriented interface to upper layers (no continous byte-stream)
- **Protocol mechanisms for deployment in high-reliability environments**
  - Multihoming, heartbeat/keepalive messages for automatic changeover
  - Protection against "blind spoofing" and DoS attacks
- **SCTP association subdivided in several "SCTP streams"**
  - Flow & congestion control applied to whole SCTP association

  ➥ More efficient than parallel TCP connections
  - In-order delivery of messages ensured only within same stream

  ➥ Reduced head-of-line blocking

Head-of-line blocking: Illustration

TCP



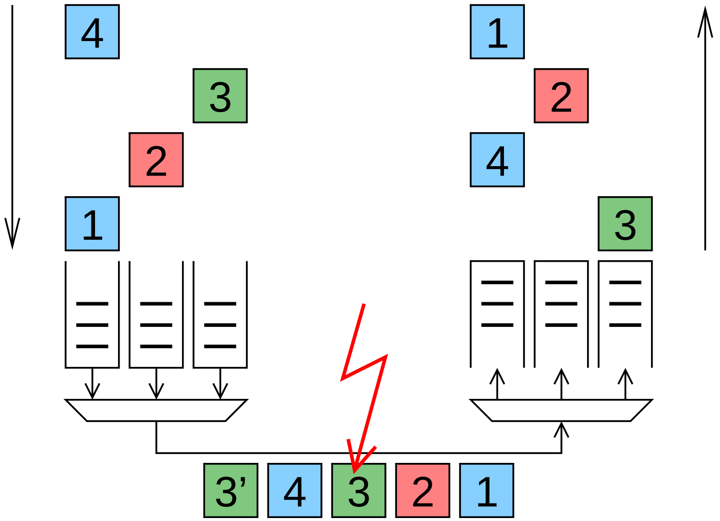
- **IP packet 3 lost or corrupted**

➥ **Retransmission**

- **Packet 4 has to wait in resequencing queue at receiver until packet 3 is retransmitted**

➥ **Head-of-line blocking**

SCTP with 3 streams



- **IP packet 3 lost or corrupted**

➥ **Retransmission**

- **Packets in other streams (e.g., packet 4) not affected by head-of-line blocking**

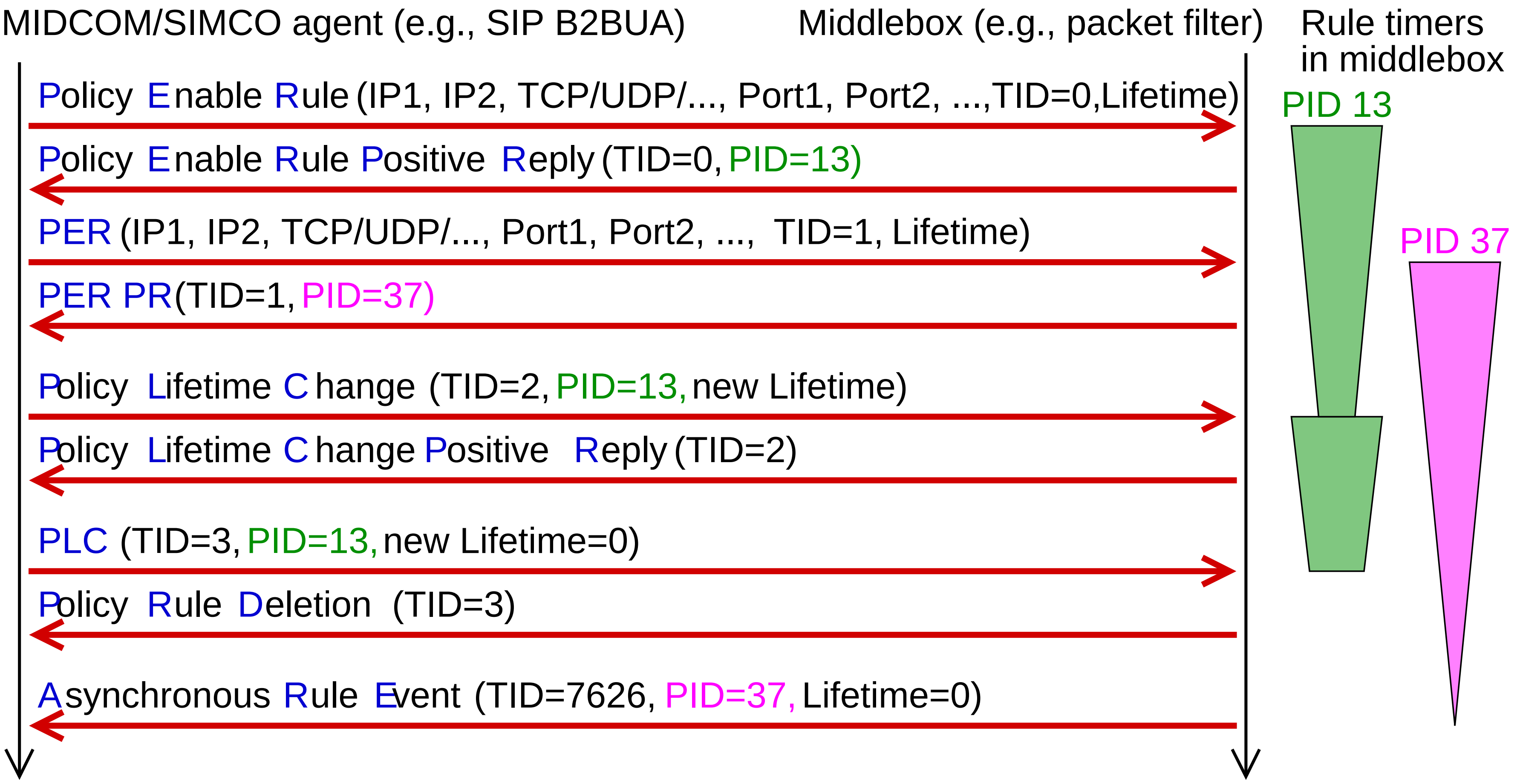
SIMCO over SCTP

Basic Question:	**how to leverage SCTP’s multiple streams feature?**
Constraint:	**retain causality for SIMCO**

SIMCO over SCTP

Basic Question: **how to leverage SCTP's multiple streams feature?**

Constraint: **retain causality for SIMCO**



MIDCOM/SIMCO agent (e.g., SIP B2BUA)

Middlebox (e.g., packet filter)

Rule timers in middlebox

Policy Enable Rule (IP1, IP2, TCP/UDP/..., Port1, Port2, ...,TID=0,Lifetime)

Policy Enable Rule Positive Reply (TID=0, PID=13)

PER (IP1, IP2, TCP/UDP/..., Port1, Port2, ..., TID=1, Lifetime)

PER PR (TID=1, PID=37)

Policy Lifetime Change (TID=2, PID=13, new Lifetime)

Policy Lifetime Change Positive Reply (TID=2)

PLC (TID=3, PID=13, new Lifetime=0)

Policy Rule Deletion (TID=3)

Asynchronous Rule Event (TID=7626, PID=37, Lifetime=0)

SIMCO over SCTP

Basic Question: **how to leverage SCTP’s multiple streams feature?**

Constraint: **retain causality for SIMCO**

Basic idea:

Agent and middlebox agree to use N bidirectional stream pairs upon session establishment

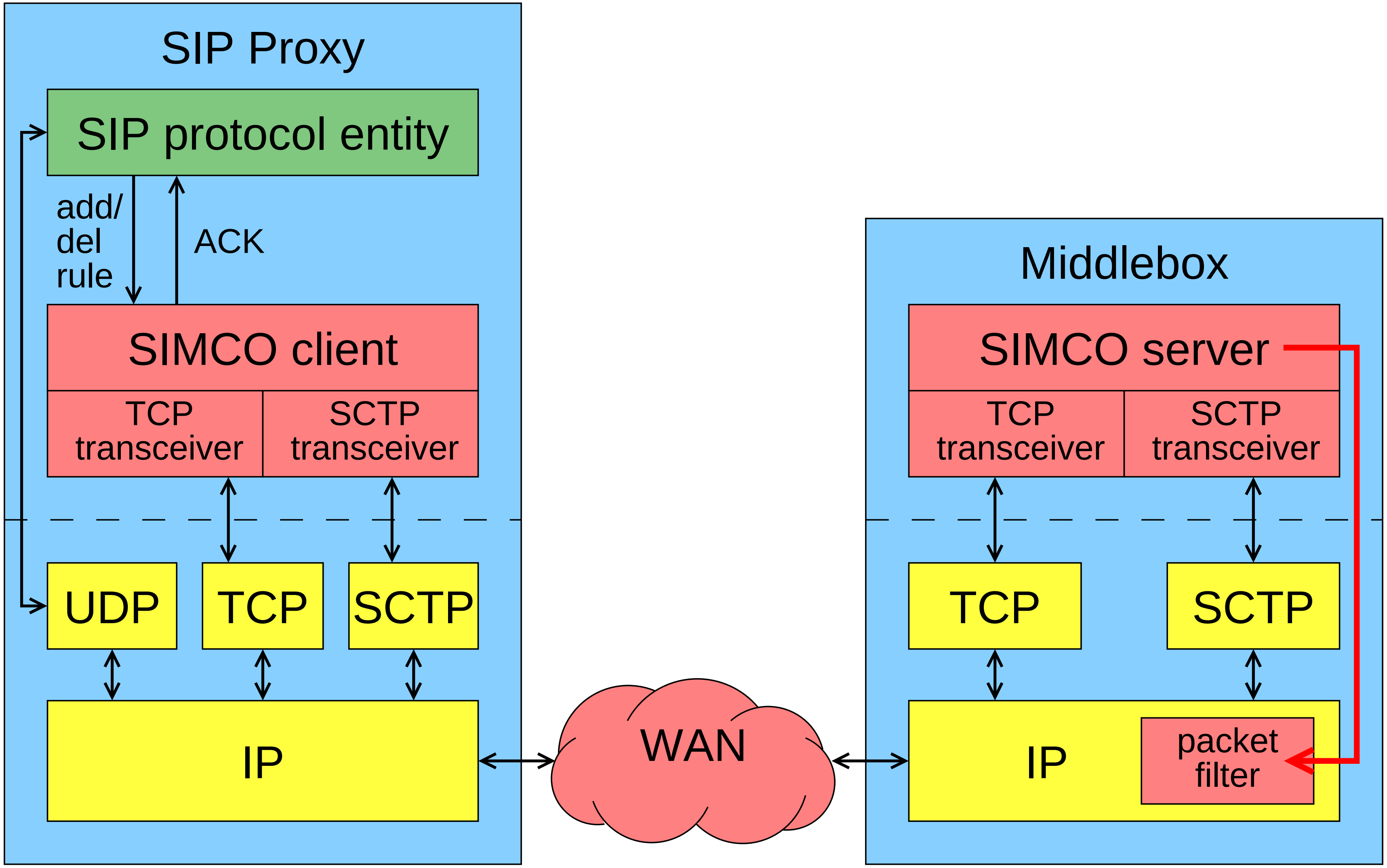
Distribution of messages to streams:

- **SIMCO Agent ("client")**
  - Create new policy rules: use round-robin scheme to distribute requests on streams, once decided save mapping PID - stream ID
  - Modify/Delete existing policy rule: reuse saved mapping
- **Middlebox ("server")**
  - Send answer on same stream number than request was received on

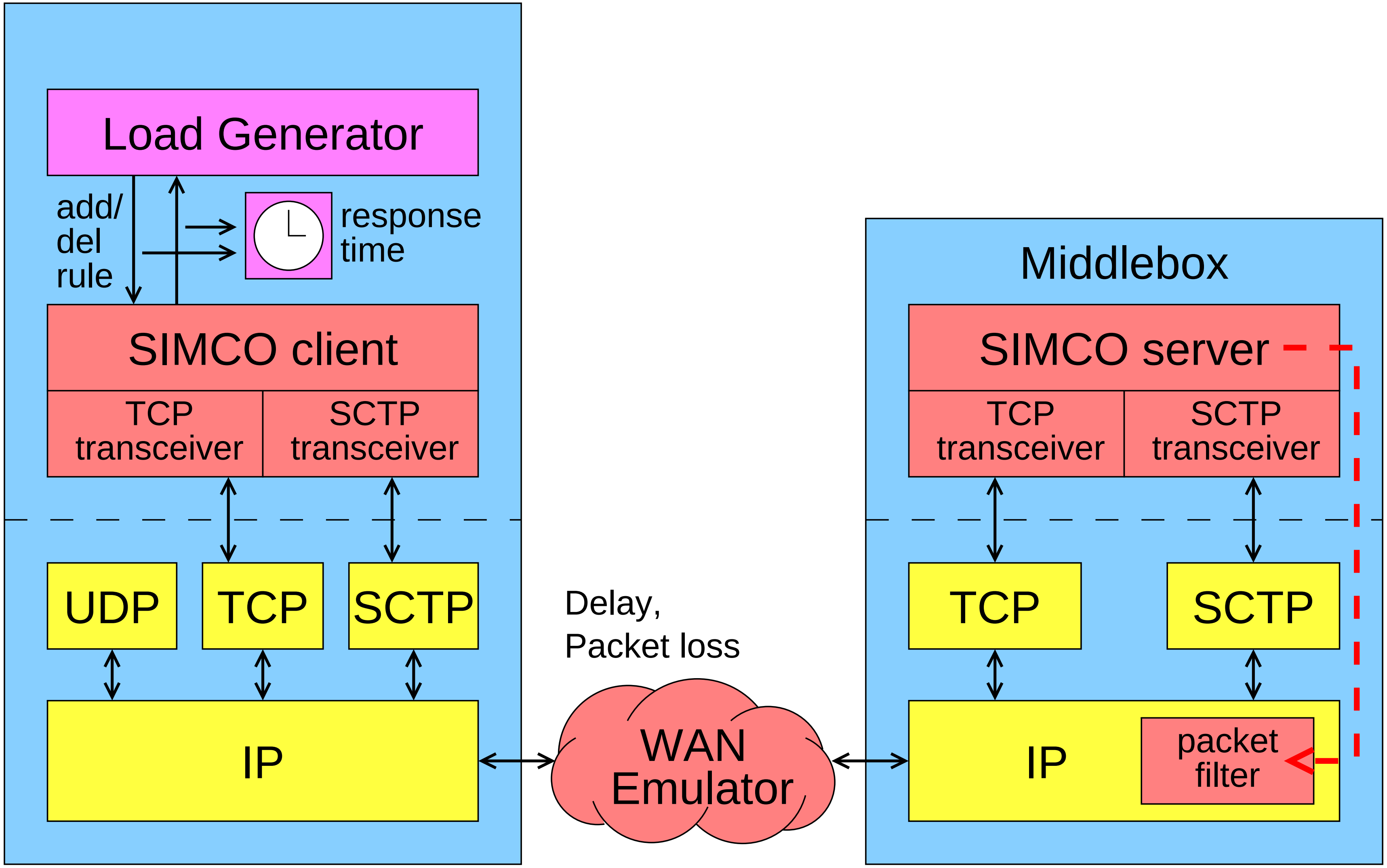
Specification needs to consider some special cases

`draft-kiesel-midcom-simco-sctp-00.txt`

SIMCO over SCTP: Prototypical implementation

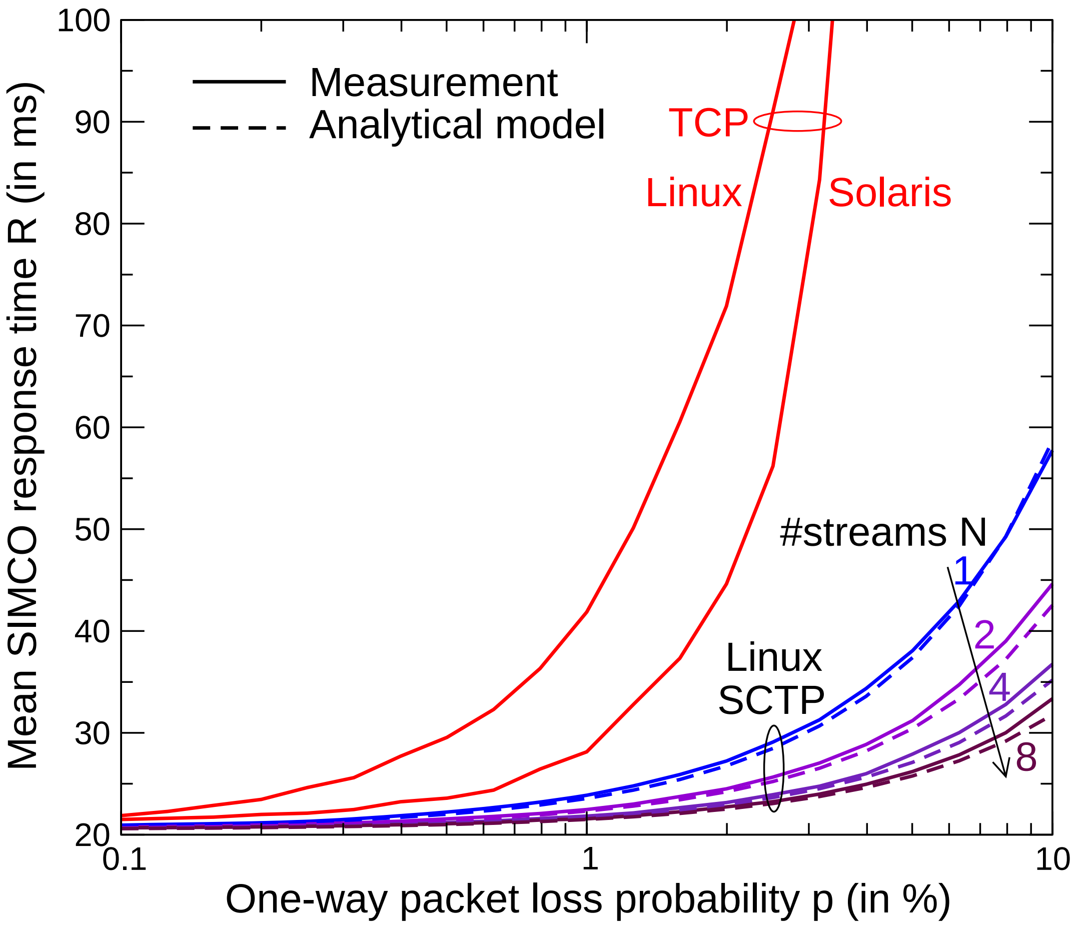


SIMCO over SCTP: Measurement testbed



Measurement results

Comparison of mean response time



System load

- 30 ms call IAT (neg.-exp.)
- 180 s call duration (neg.-exp.)
- PLC every 120s
- Equiv. to 60,000 users with 0.05 Erl.

➥ 100 transactions/s

Network

- 20 ms RTT
- 10 Mbps data rate
- Random packet loss

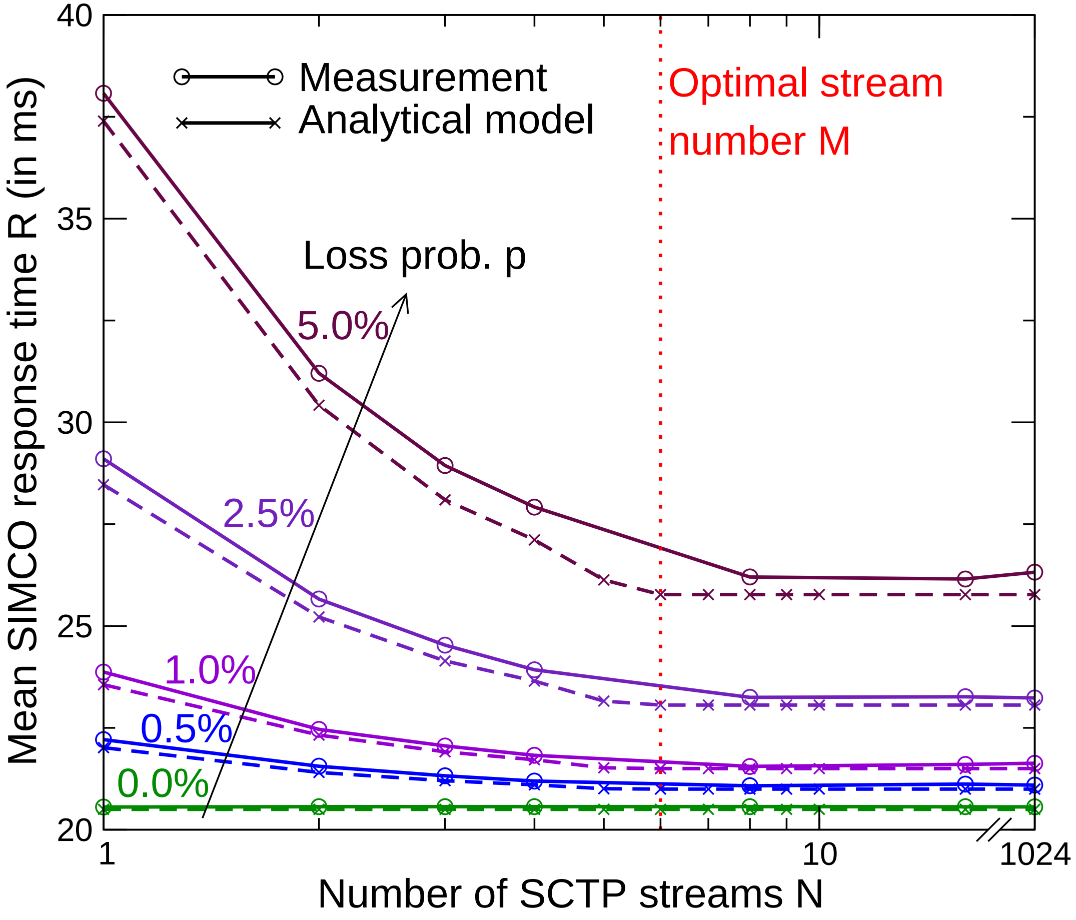
Linux 2.6.11 TCP/SCTP
Sun Microsystems Solaris 10

➥ **Several SCTP streams improve SIMCO response time**

➥ **Measured TCP performance much worse than SCTP**

Measurement results

Optimal number of streams



System load

- **30 ms call IAT (neg.-exp.)**
- **180 s call duration (neg.-exp.)**
- **PLC every 120s**
- **Equiv. to 60,000 users with 0.05 Erl.**

➥ **100 transactions/s**

Network

- **20 ms RTT**
- **10 Mbps data rate**
- **Random packet loss**

Linux 2.6.11 SCTP

➥ **No significant performance improvement for more than M=f(RTT, load)**

Usually a small number of streams is sufficient

Conclusions & Future Work

Conclusions

- **Firewalls in VoIP networks to achieve PSTN-like security model**
- **SIMCO is a signaling protocol for path-decoupled firewall control**
- **SCTP is beneficial as transport protocol for SIMCO**
  - Less implementation complexity
  - Protocol mechanisms for high-reliability environments
  - Reduced head-of-line blocking
- **Measurements with prototype implementation show that small number of SCTP streams is sufficient**
- **`draft-kiesel-midcom-simco-sctp-00.txt`**

Future Work

- **Performance impact of actually controlling a packet filter with SIMCO middlebox entity (e. g., Linux netfilter)**

  ➥ Performance optimization by rule grouping/reordering possible?
- **Compare response time with several parallel TCP connections**