Evaluation of SCTP as transport layer protocol for firewall control

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

Workshop "Neue Herausforderungen in der Netzsicherheit"
an der Universität Duisburg-Essen
06/07.10.2005

Outline

- **Motivation**
- **Overview of problems with SIP and firewalls**
- **Introduction to IETF MIDCOM/SIMCO**
- **Overview of 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

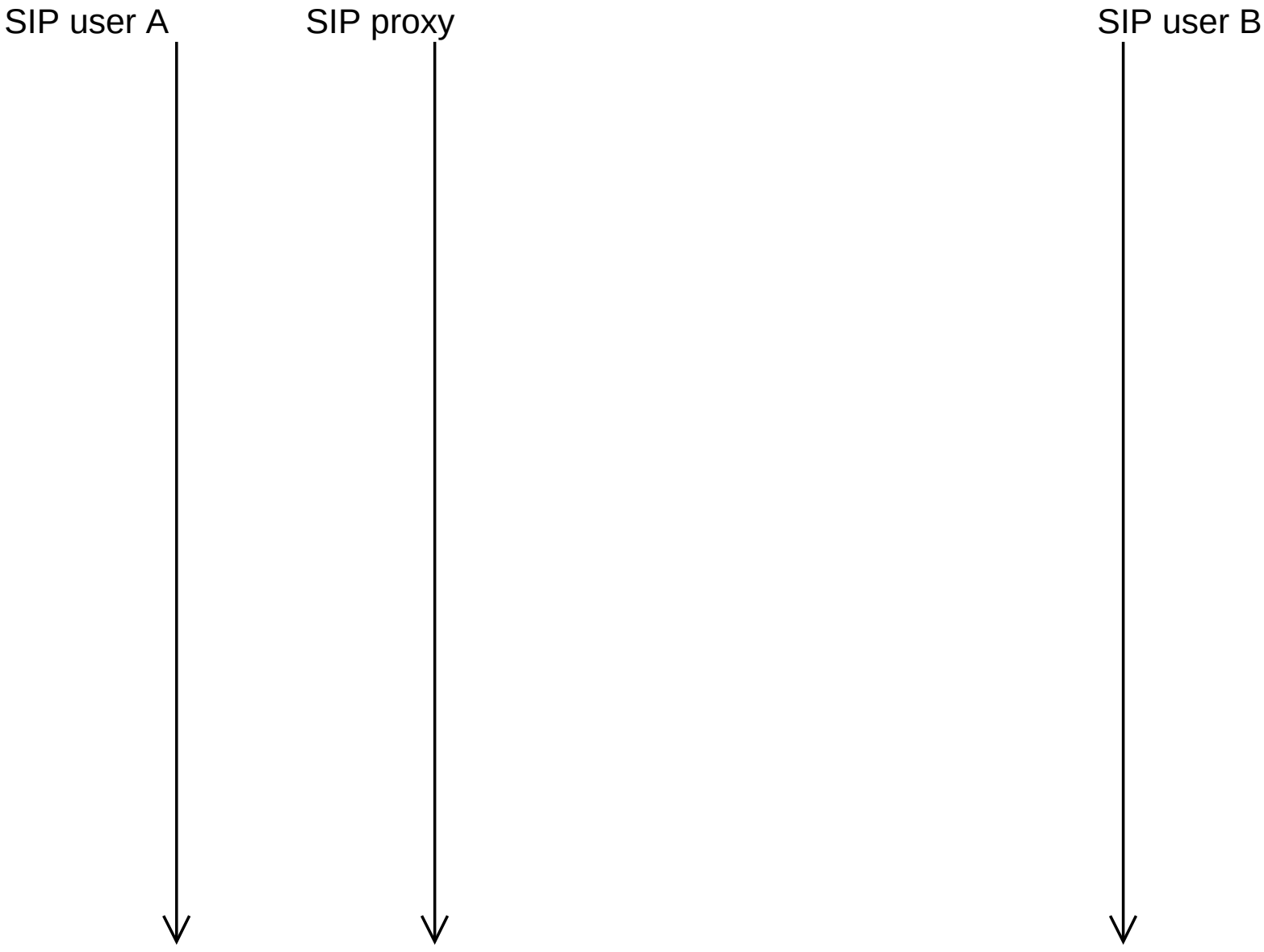
➥ **Signaling *and* media path secured by firewalls**

Firewalls

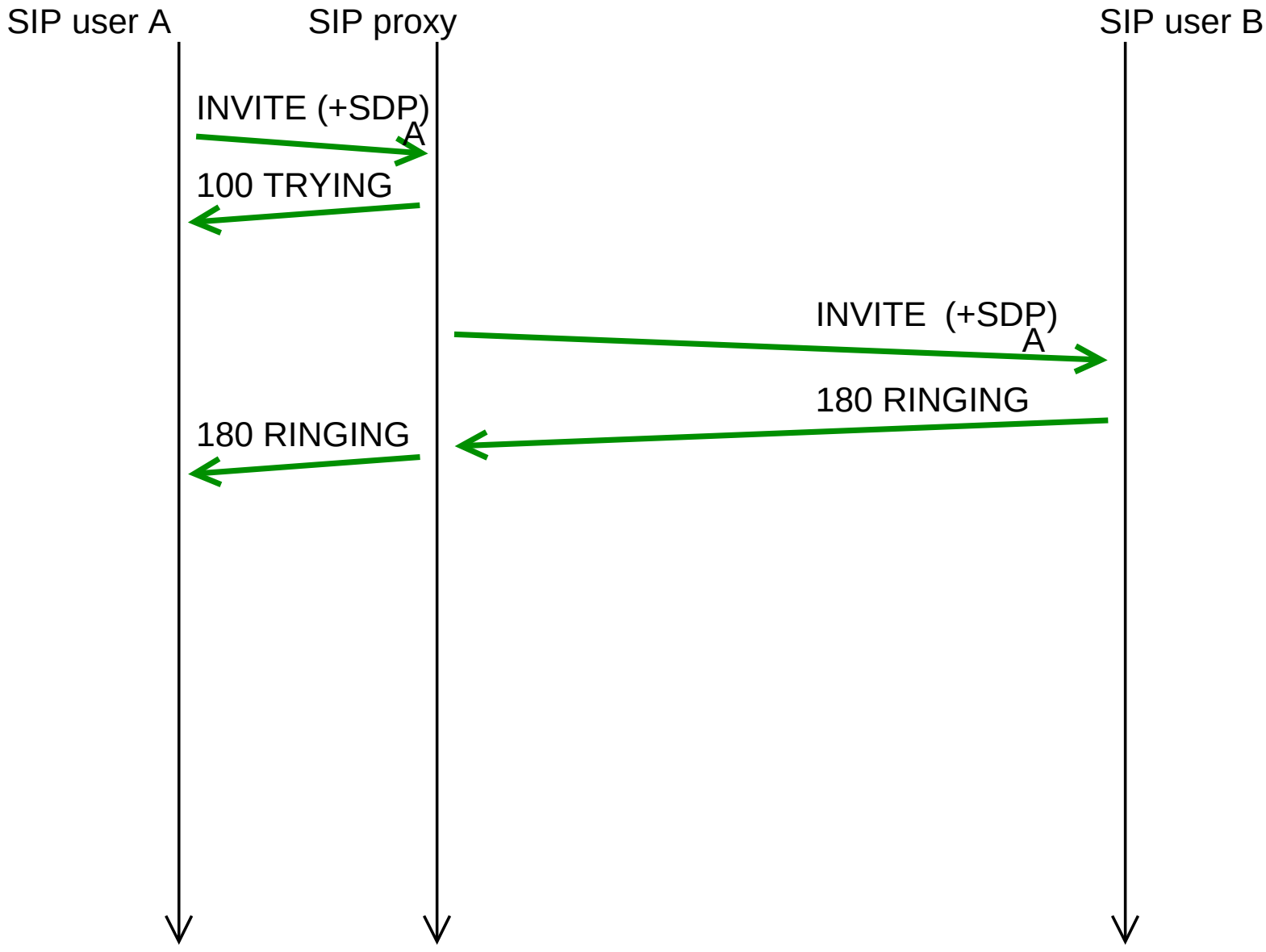
- **"A firewall is a system or group of systems that enforces an access control policy between two networks."**
- **Realization by packet filter and/or proxies**

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

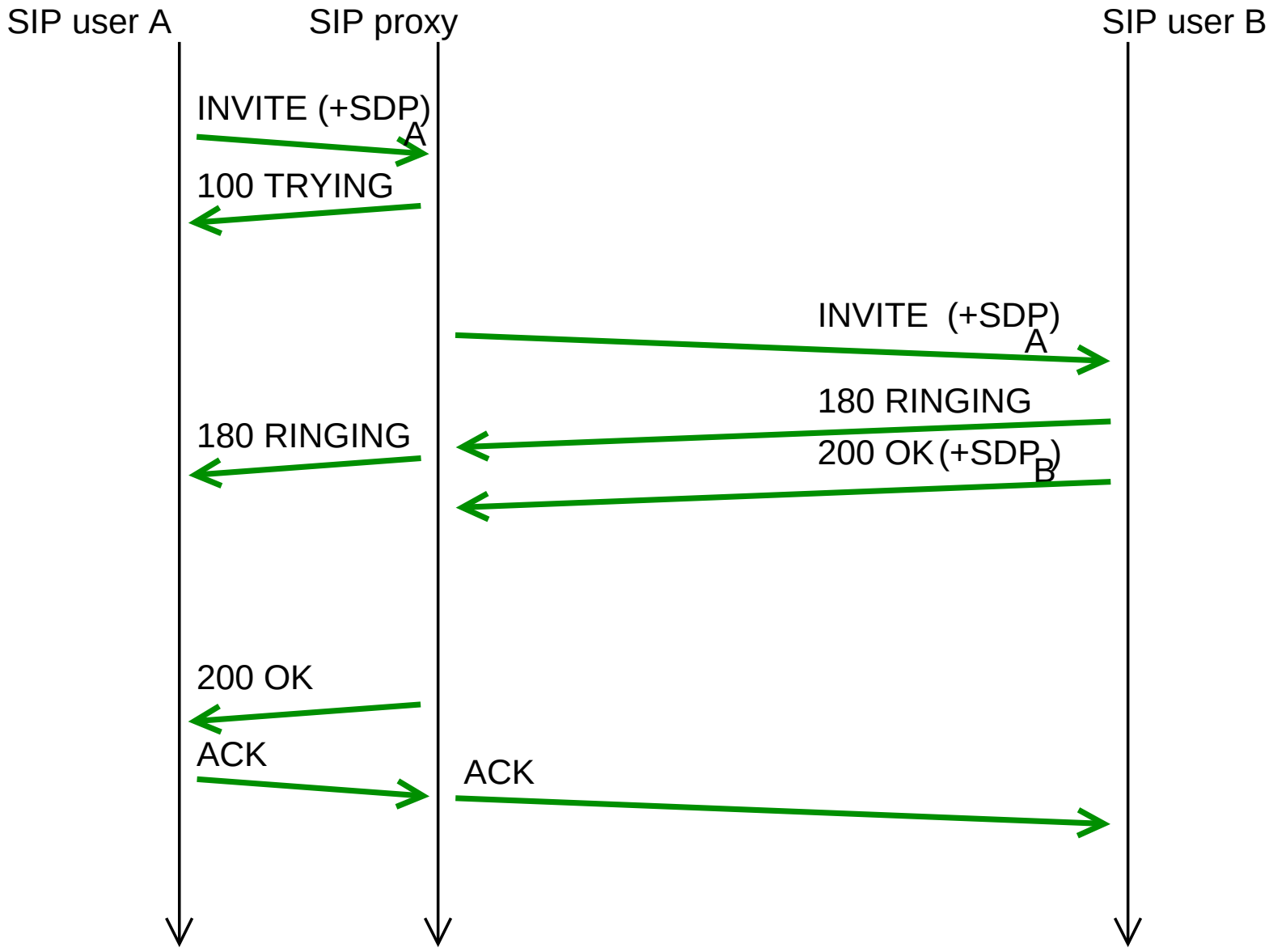
SIP/RTP: basic call flow



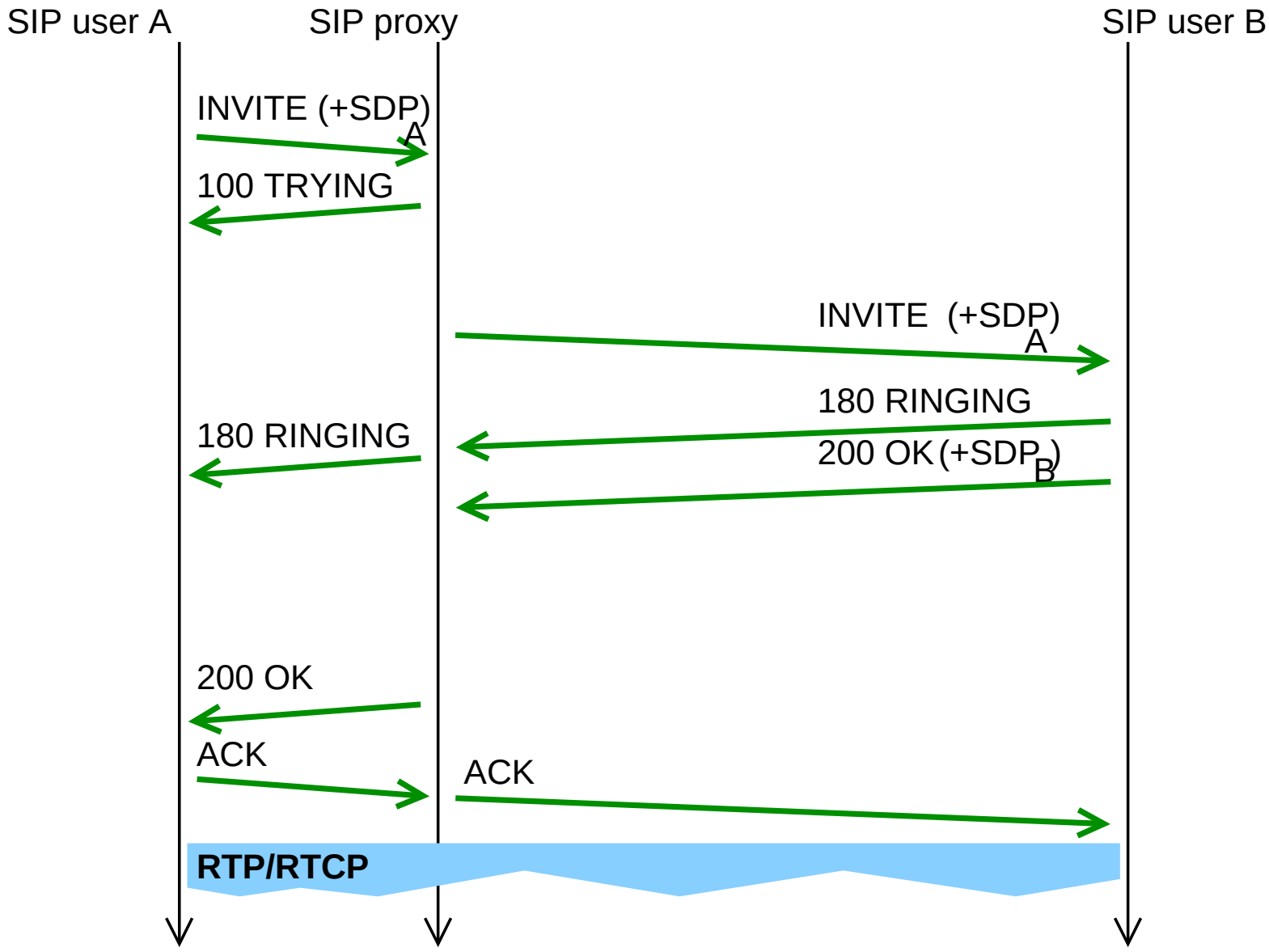
SIP/RTP: basic call flow



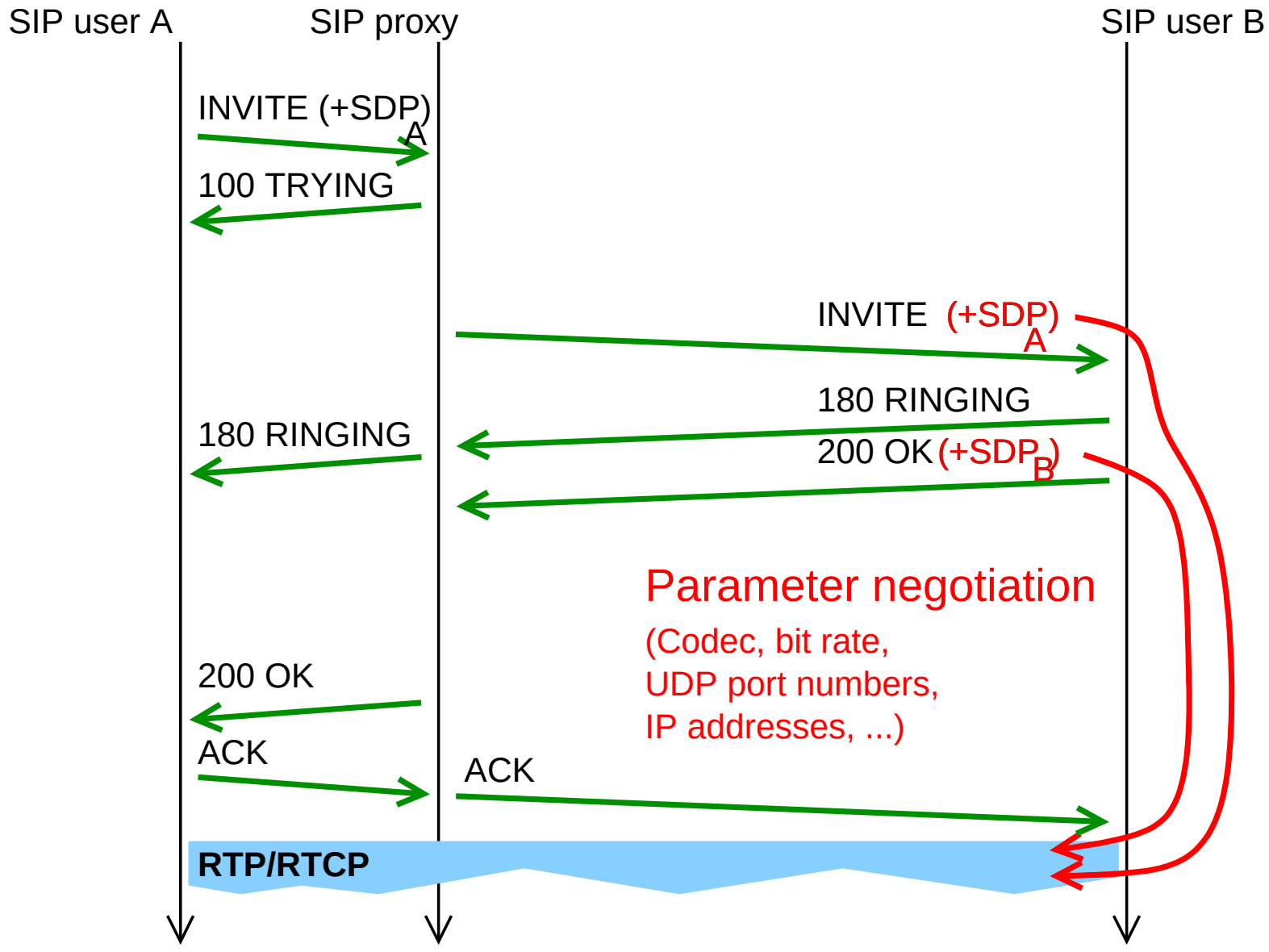
SIP/RTP: basic call flow



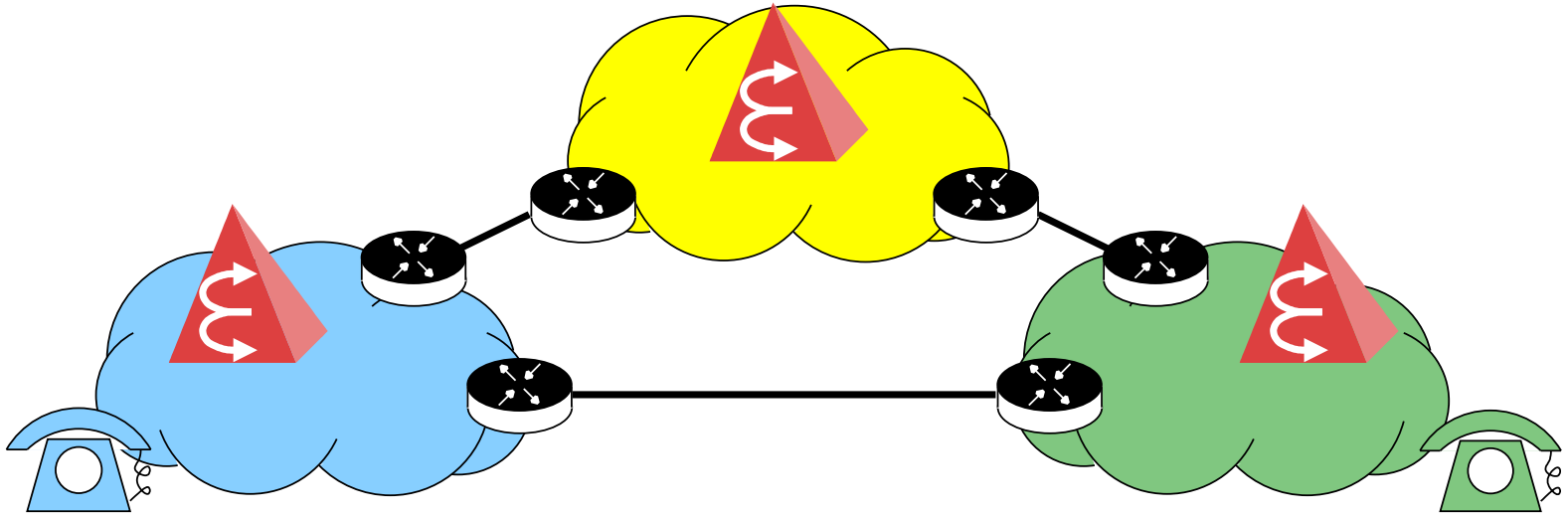
SIP/RTP: basic call flow



SIP/RTP: dyn. cross-layer parameter negotiation

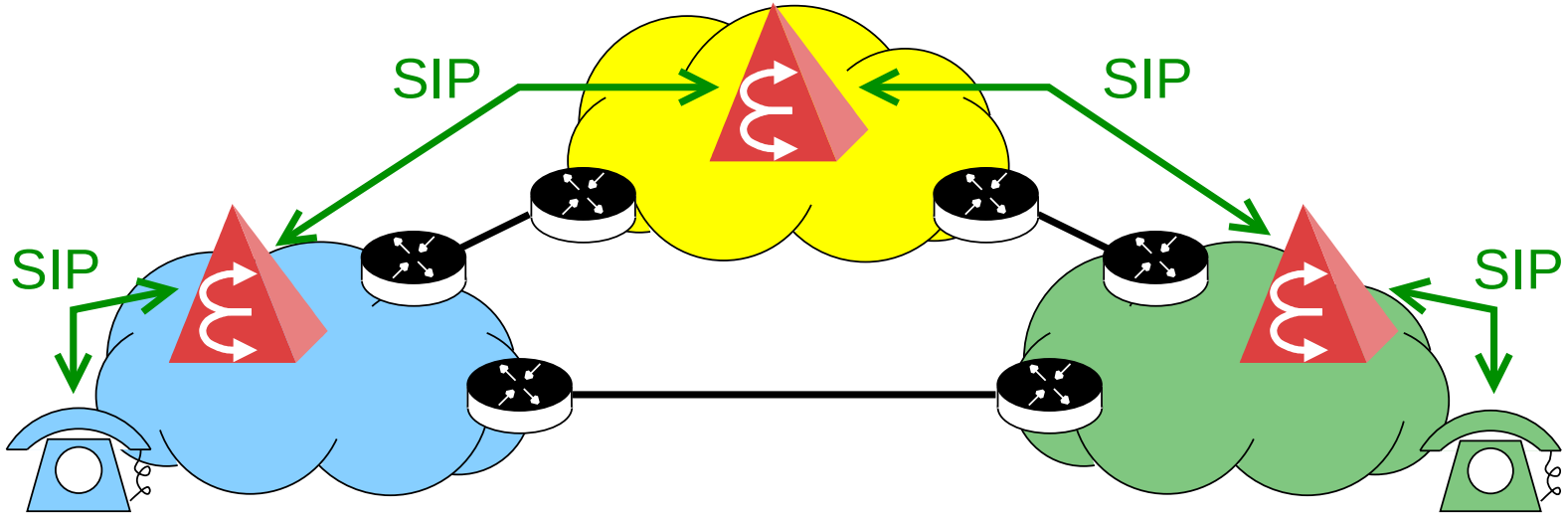


Firewalls and out-of-band signaling

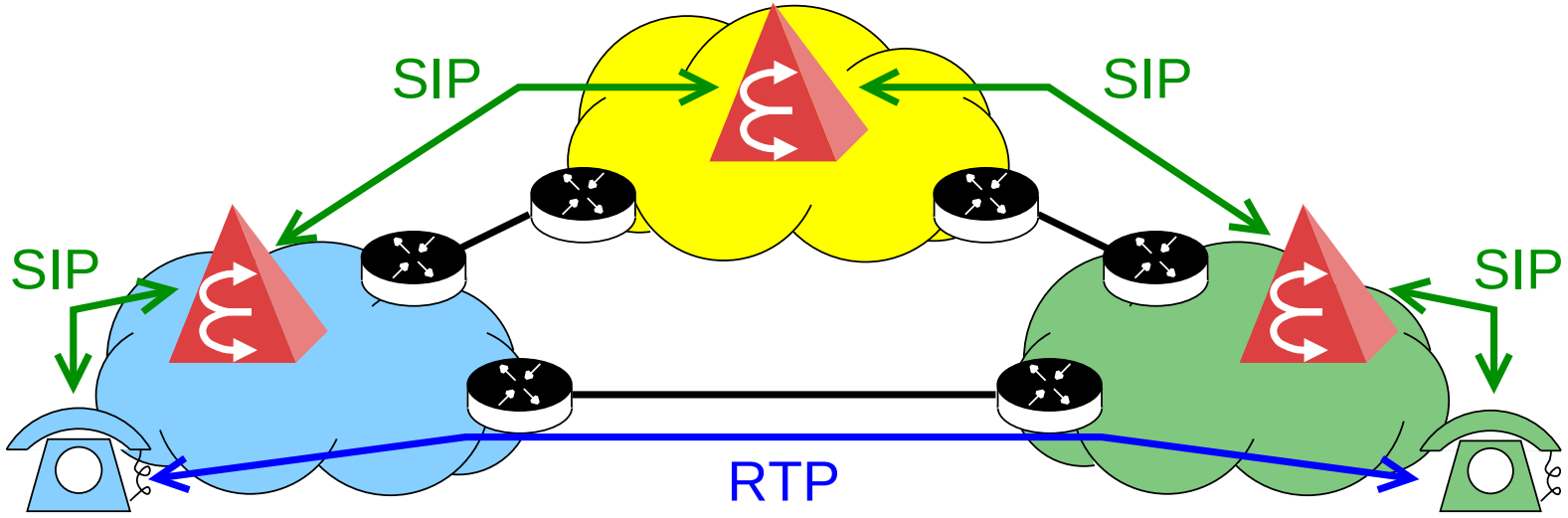


- **Clouds: IP based Operator Networks (e.g., NGN)**
- **Network interconnection based on bilateral agreements, protected by means of firewalls**

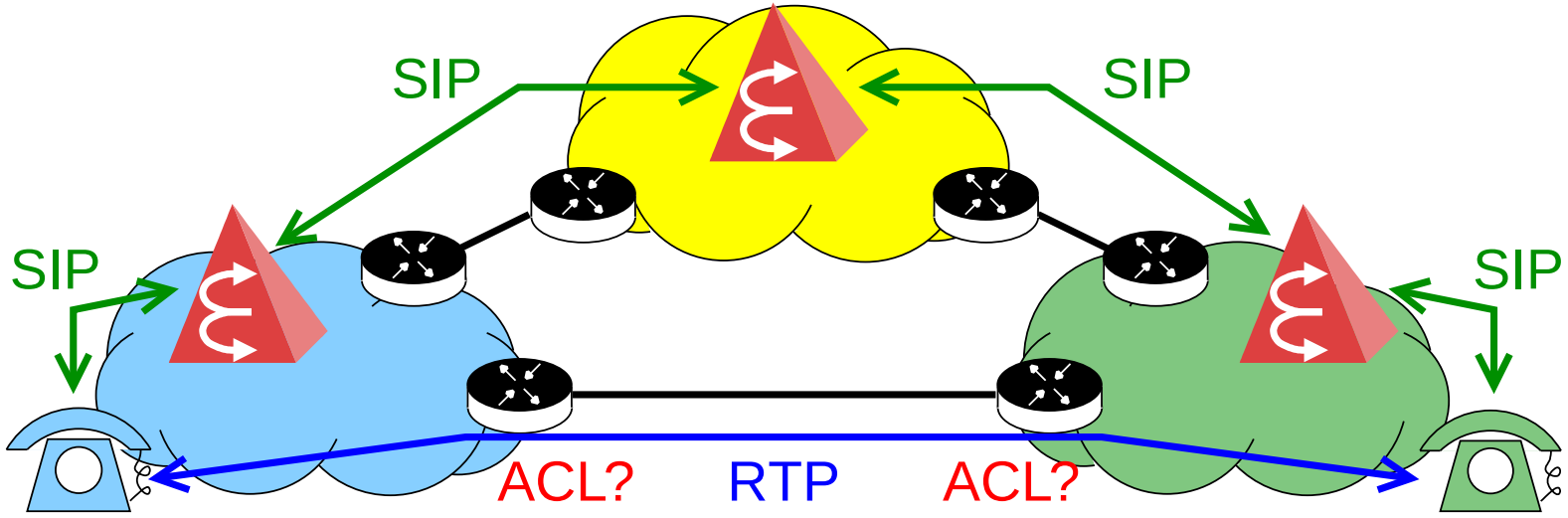
Firewalls and out-of-band signaling



Firewalls and out-of-band signaling



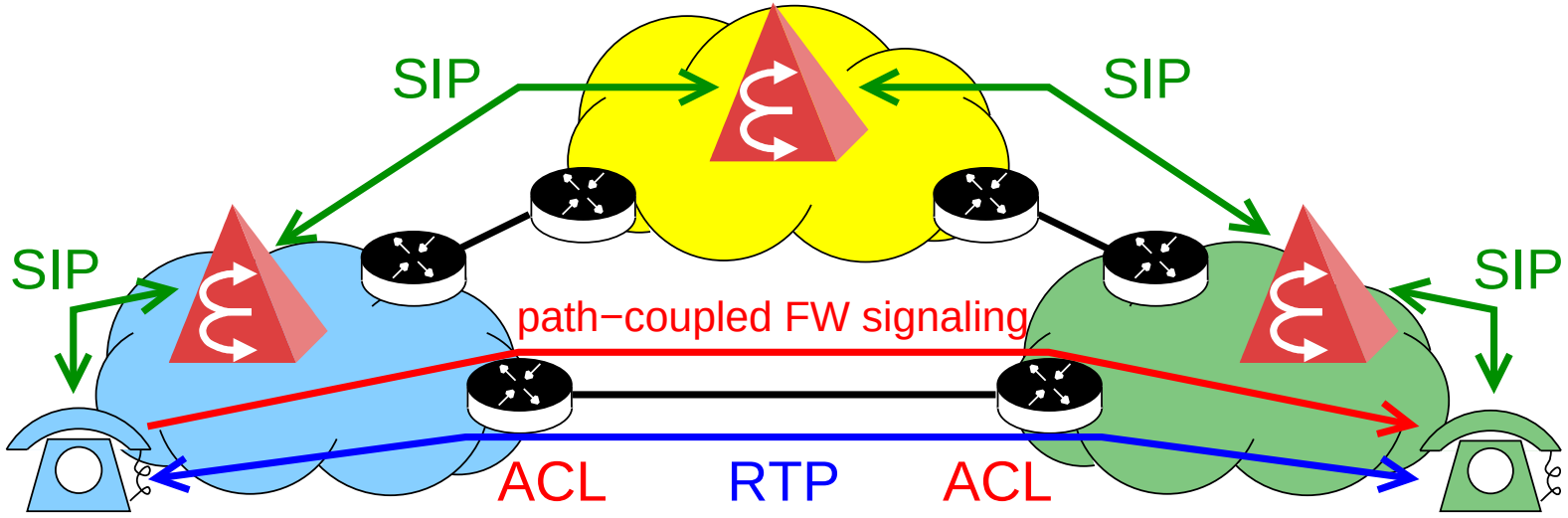
Firewalls and out-of-band signaling



Signaling messages may travel on different path through network than media streams do

➥ **How to open pinholes in firewalls on media path?**

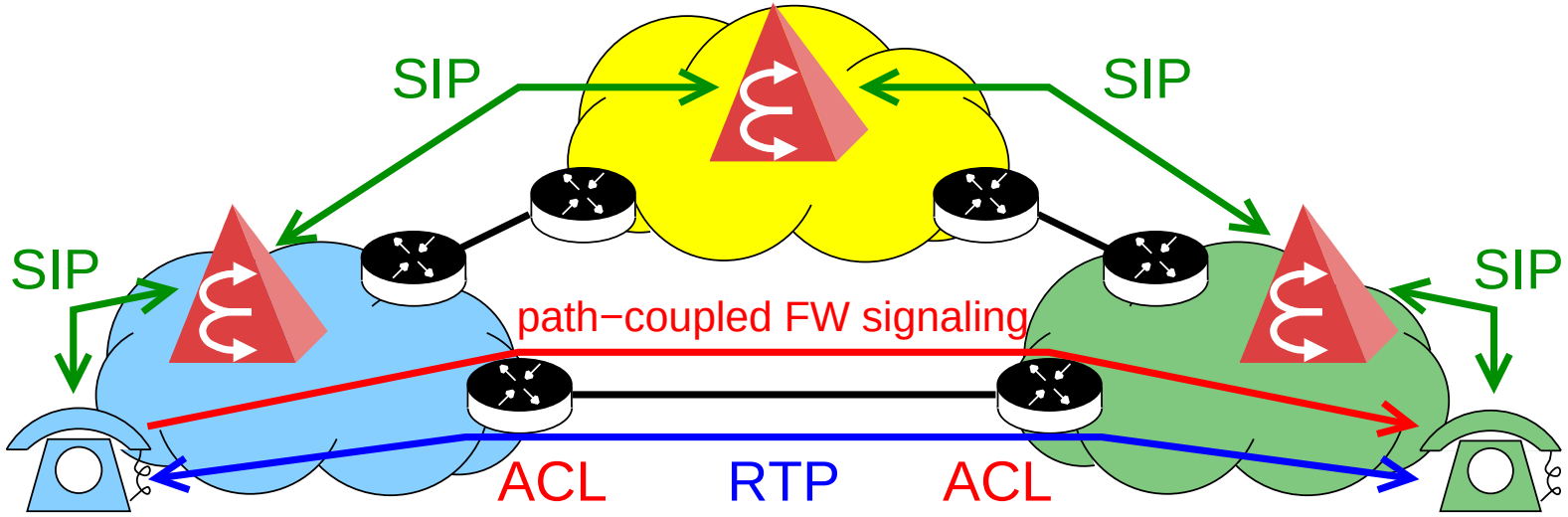
Firewalls and out-of-band signaling

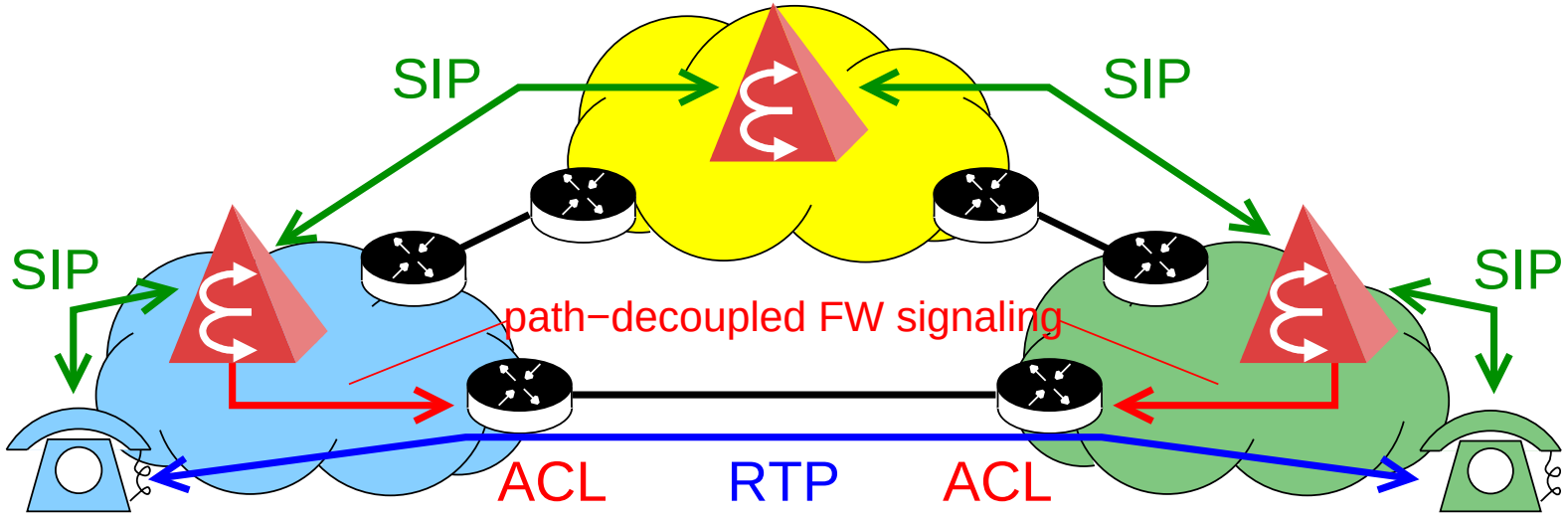


Examples for path-coupled firewall signaling:

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

Firewalls and out-of-band signaling

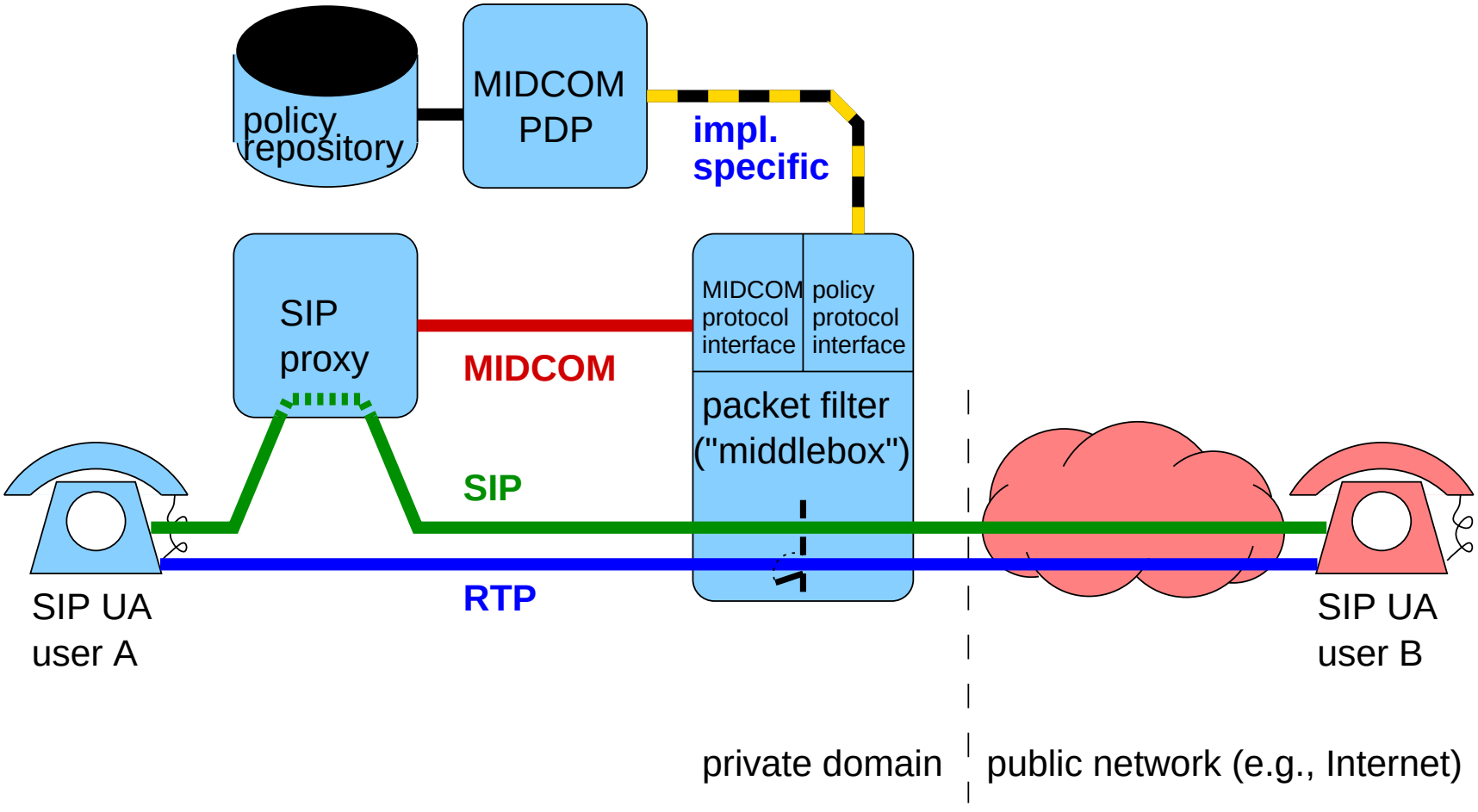




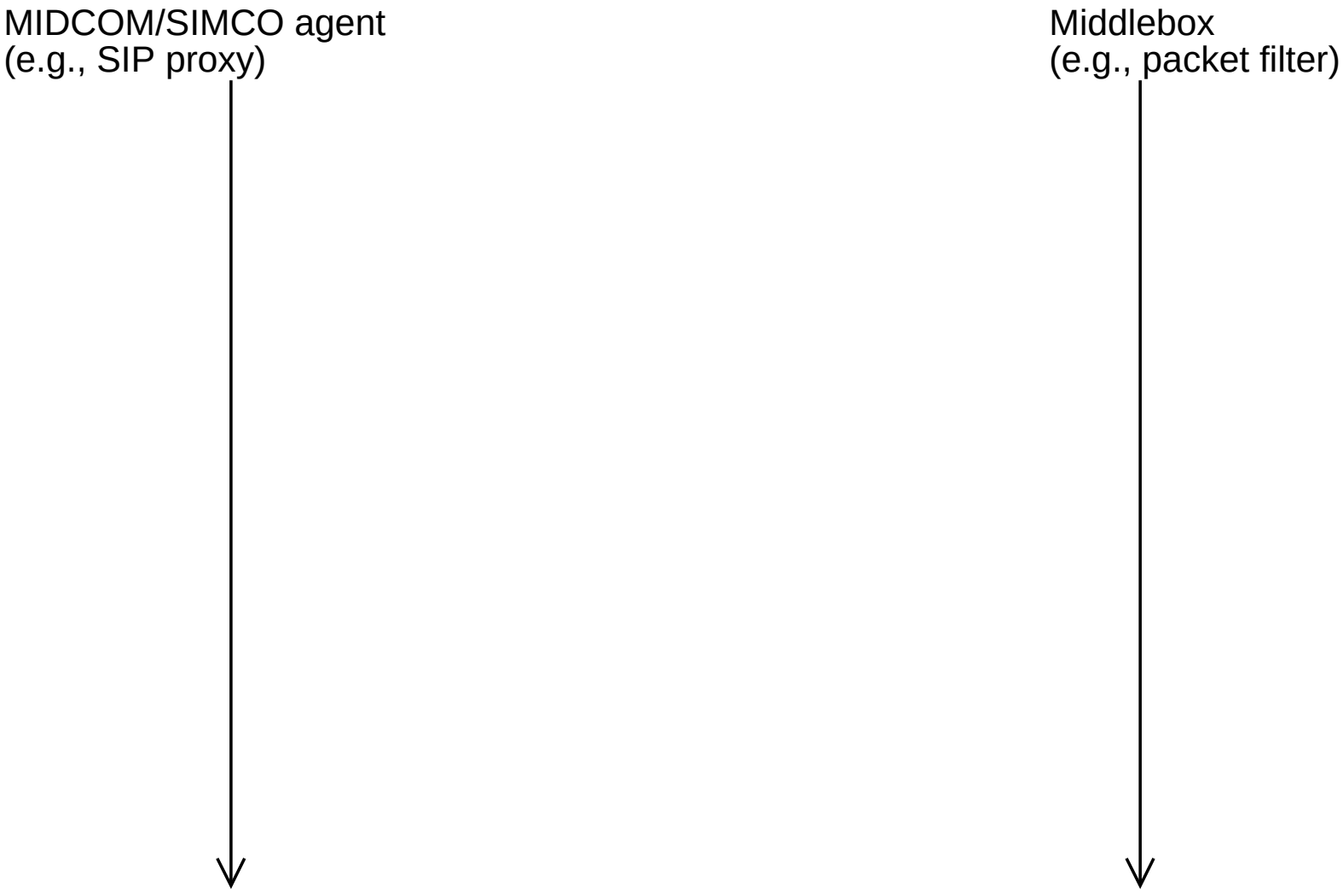
IETF MIDCOM - SIMCO

Examples for path-decoupled firewall signaling:

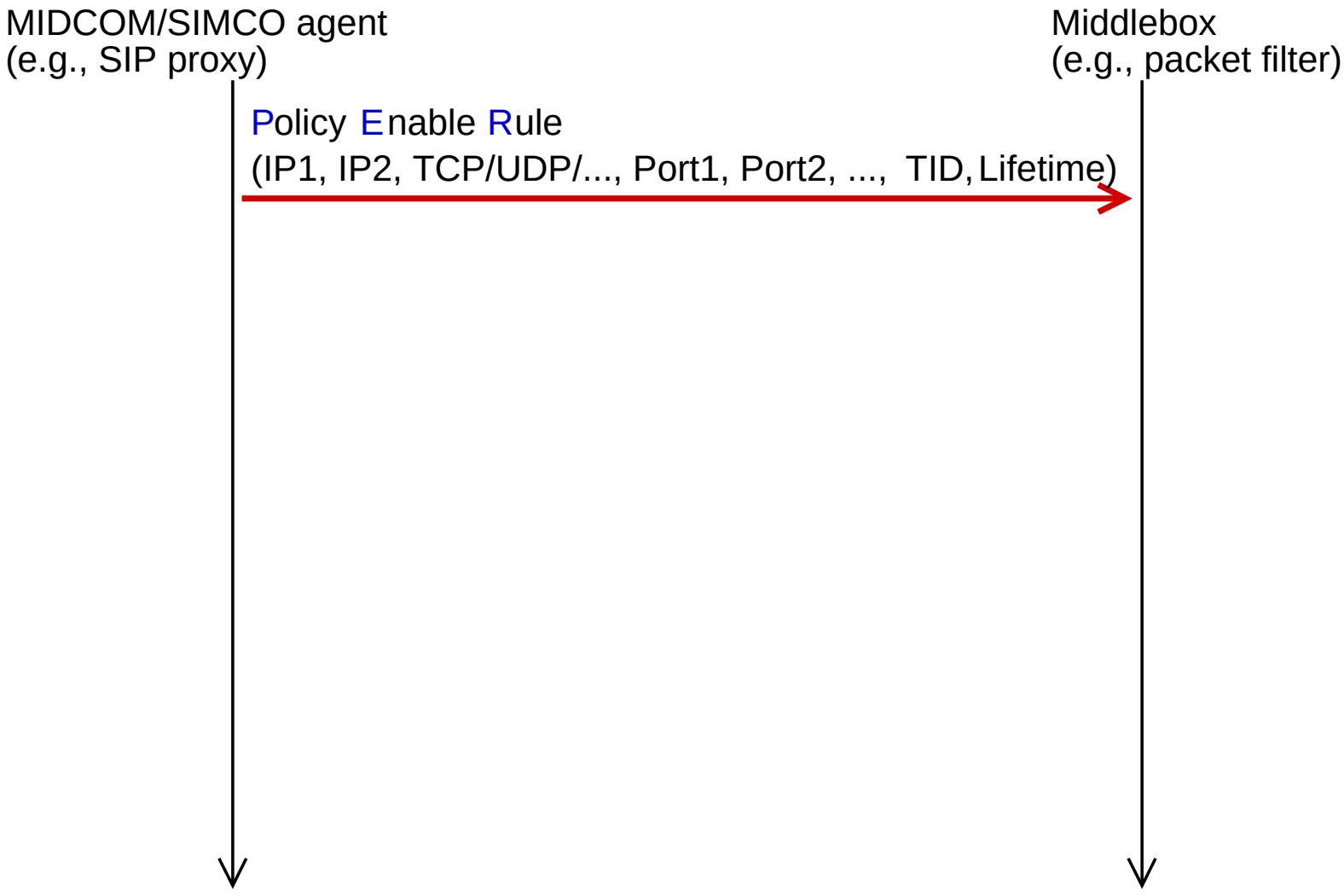
- **UPnP (home and small office LANs only)**
- **IETF MIDCOM (framework architecture) -> MIDCOM MIB or SIMCO**



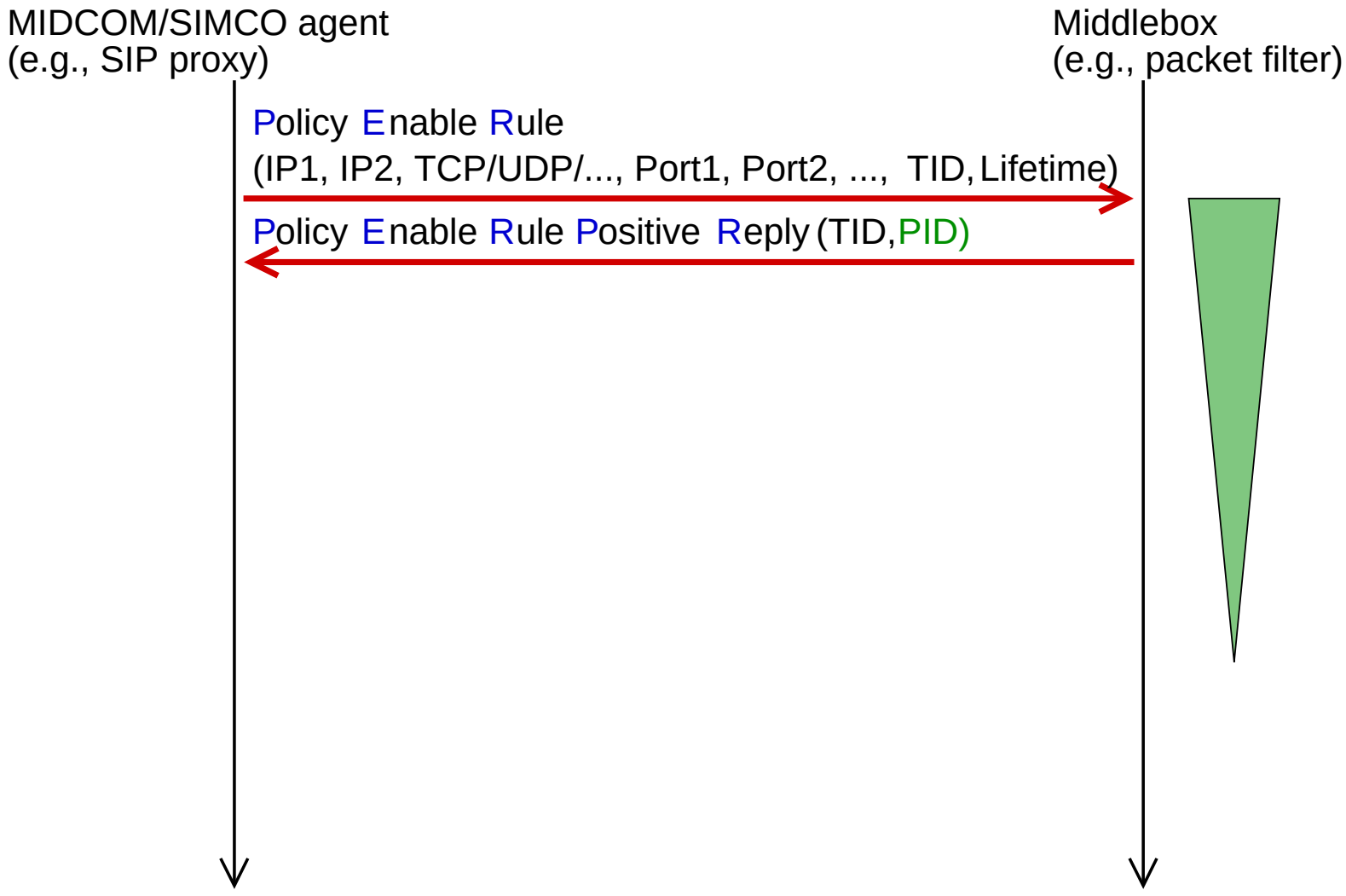
IETF MIDCOM - SIMCO



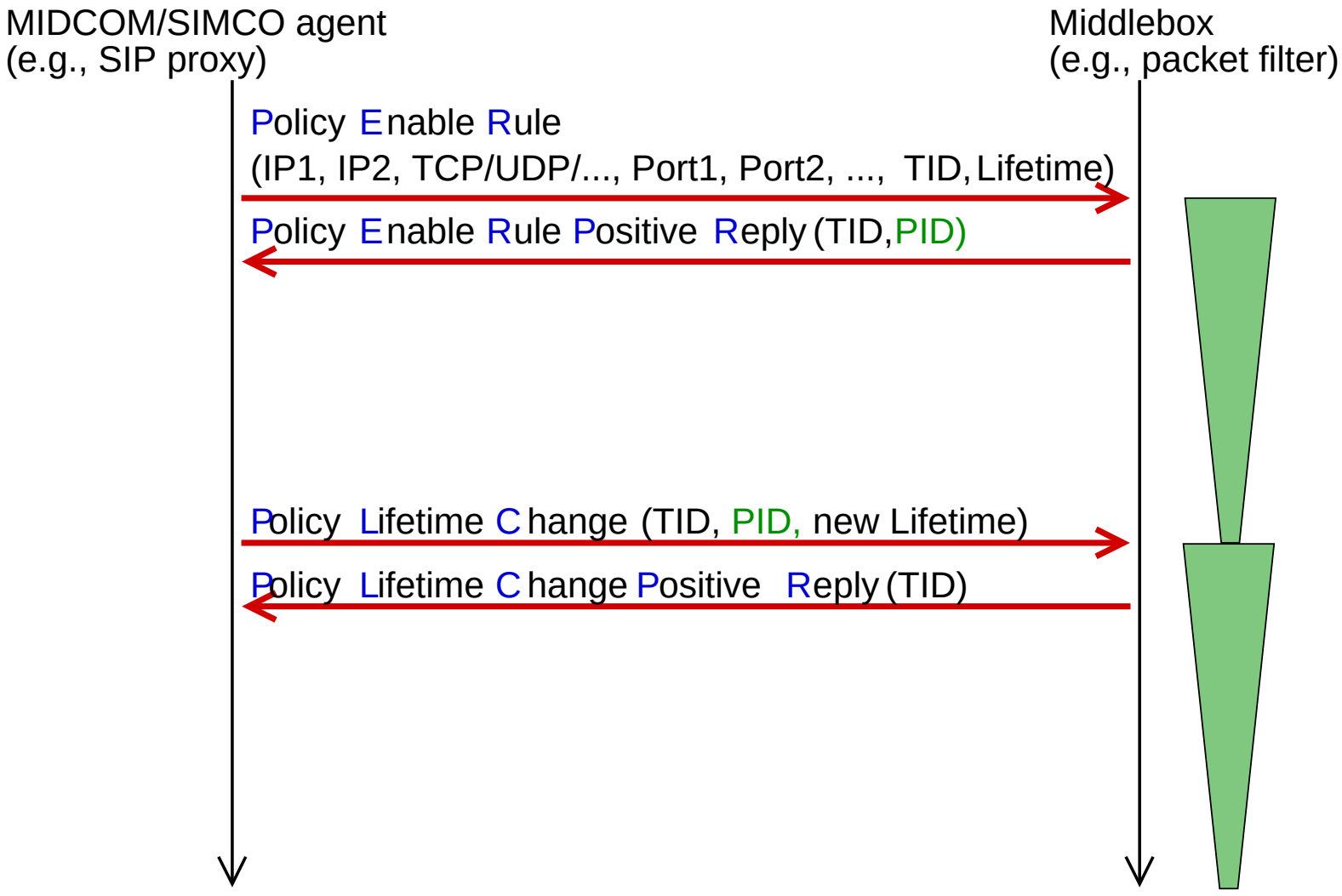
IETF MIDCOM - SIMCO



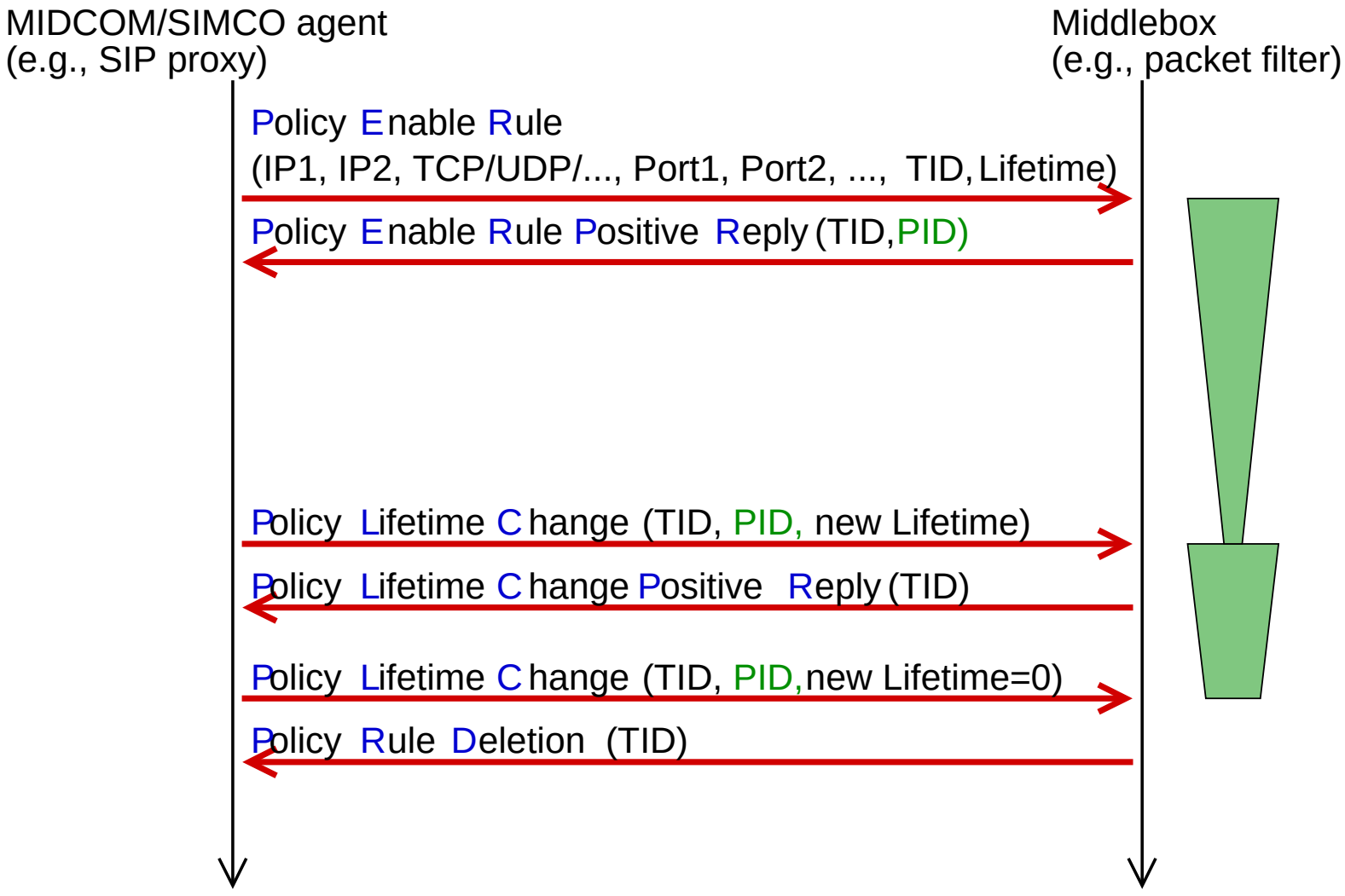
IETF MIDCOM - SIMCO



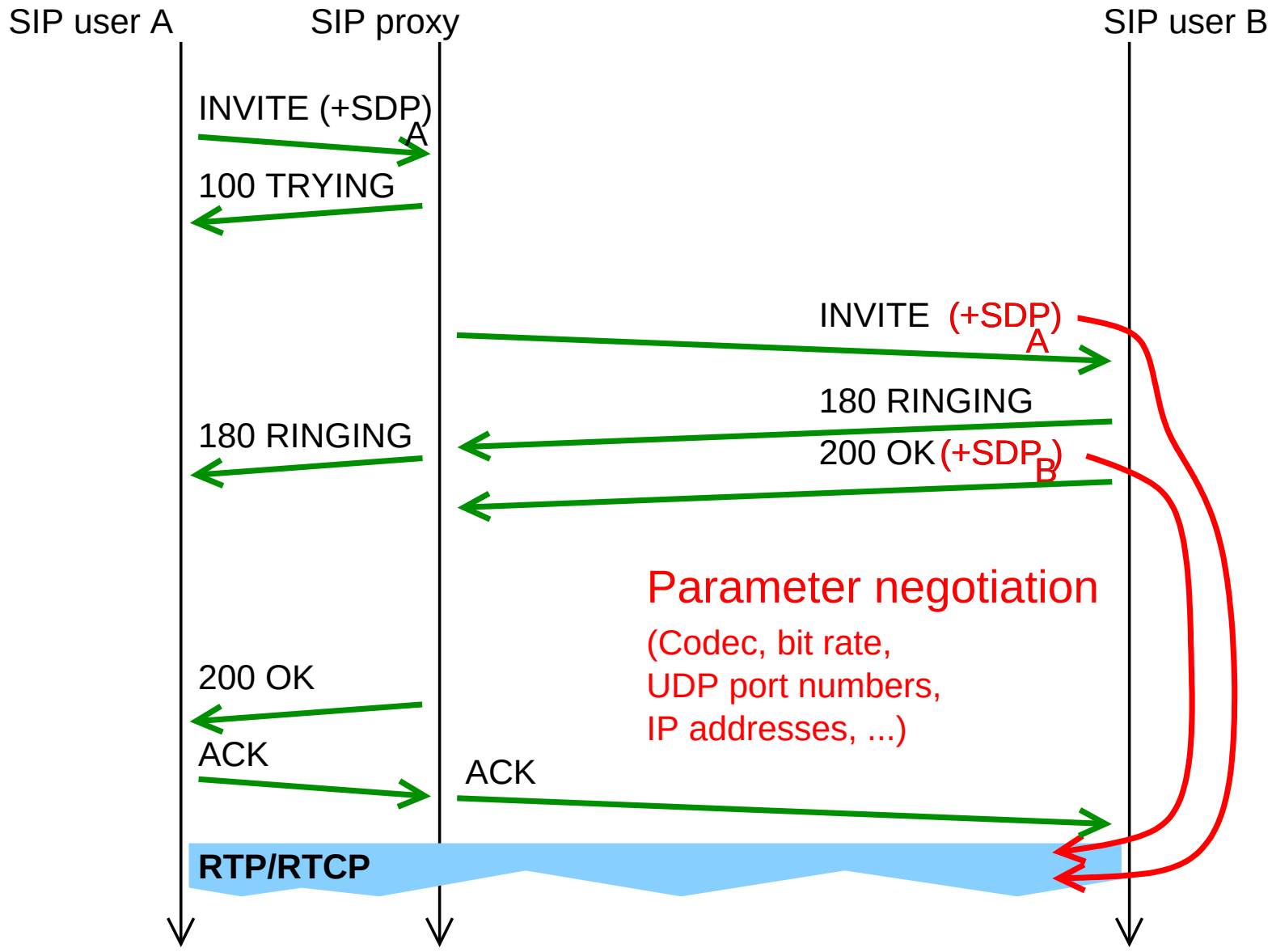
IETF MIDCOM - SIMCO



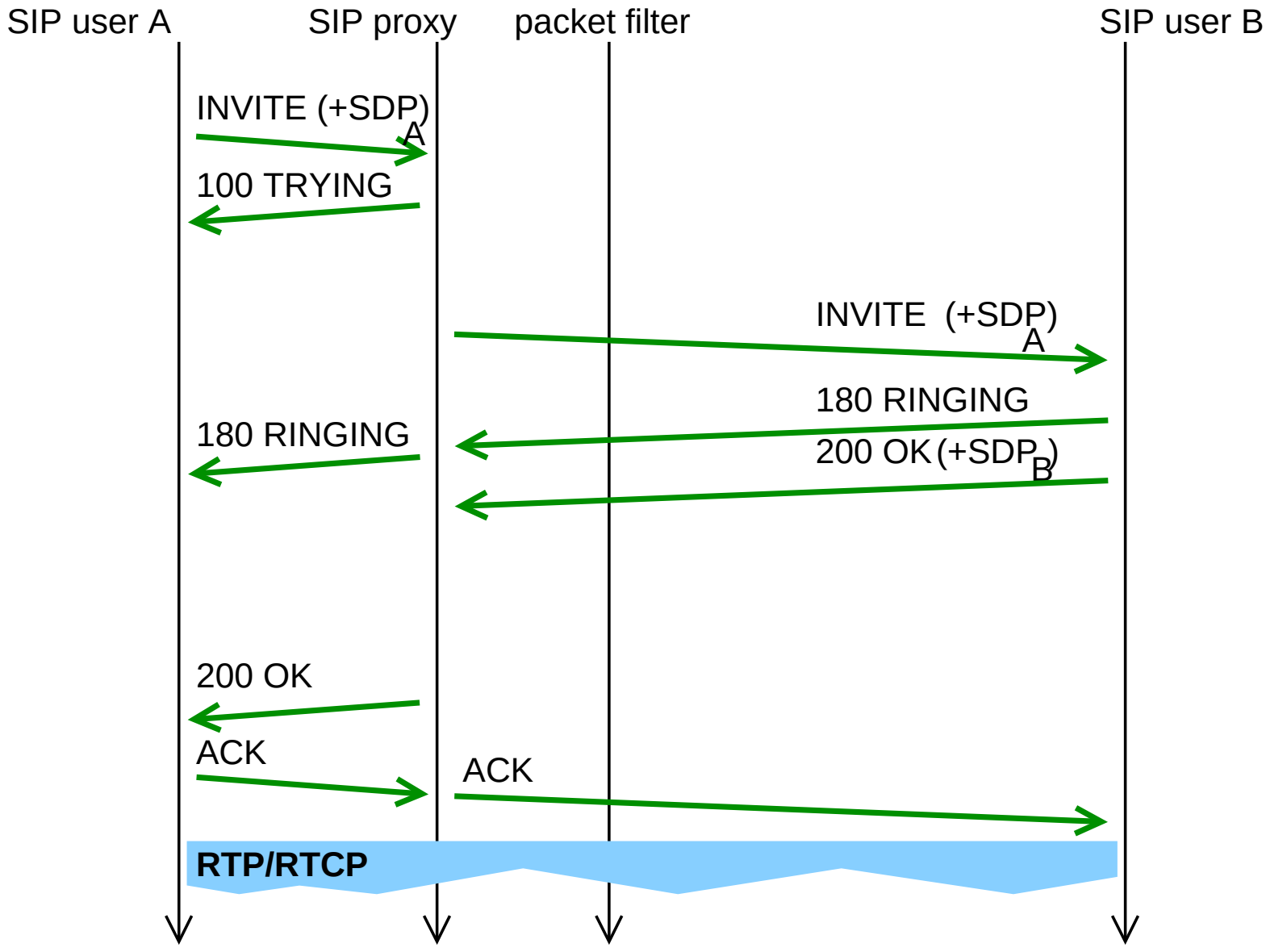
IETF MIDCOM - SIMCO



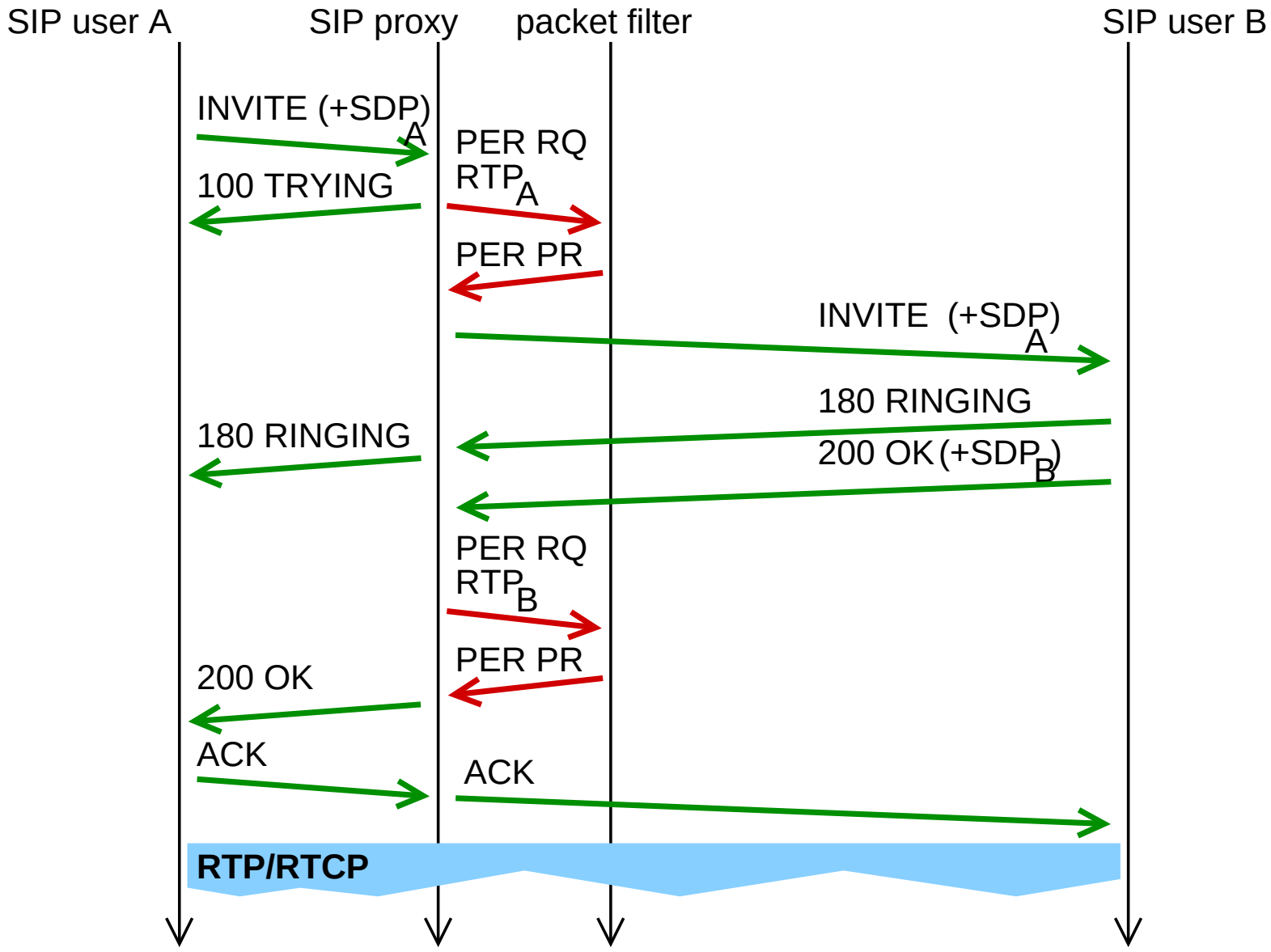
SIMCO - Interaction with SIP/RTP



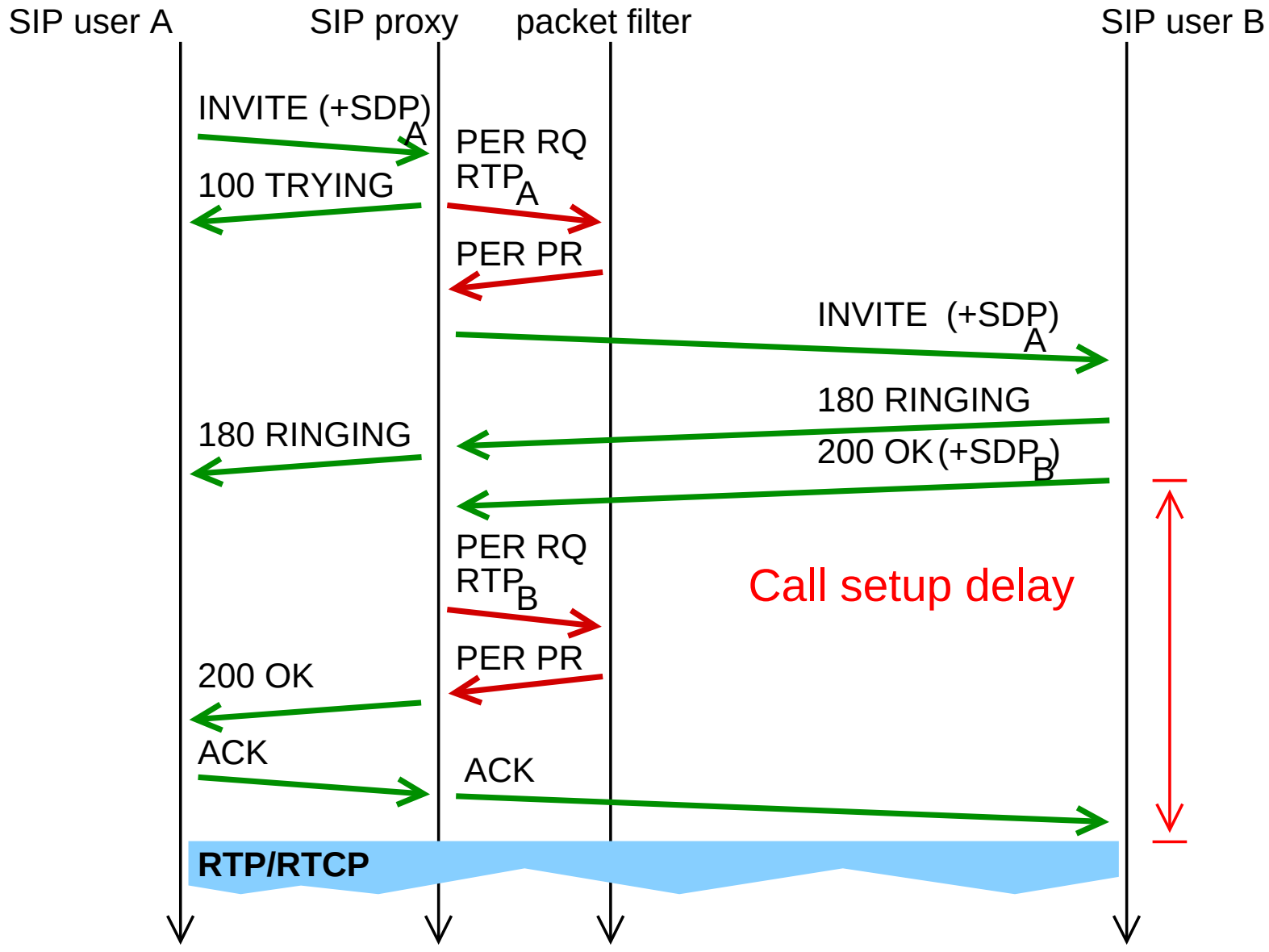
SIMCO - Interaction with SIP/RTP



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**
- **Prototype Implementations: NEC Europe, Ltd., Uni Stuttgart/IKR**

Stream Control Transmission Protocol

SCTP (Stream Control Transmission Protocol, RFC 2960)

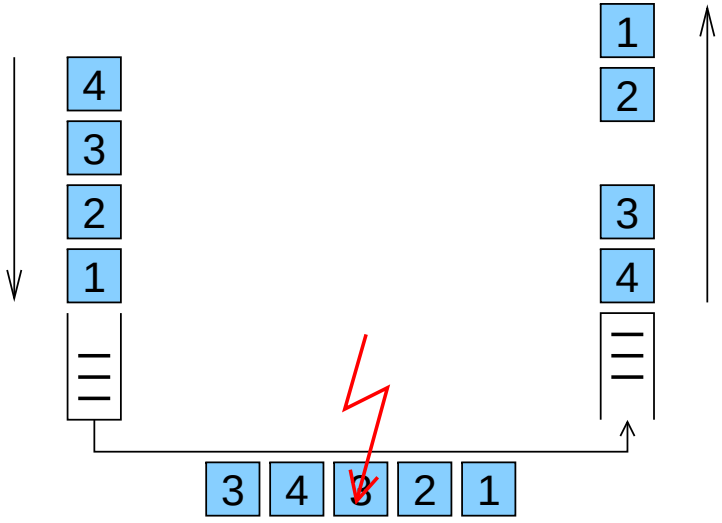
- **Generic transport layer protocol optimized for signaling purposes, originally developed as part of the SIGTRAN stack for "SS7 over IP"**
- **Connection oriented: "SCTP association"**
  - Reliable transmission (checksums, flow-control, etc.)
  - "TCP friendly" congestion control
  - Message-oriented 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



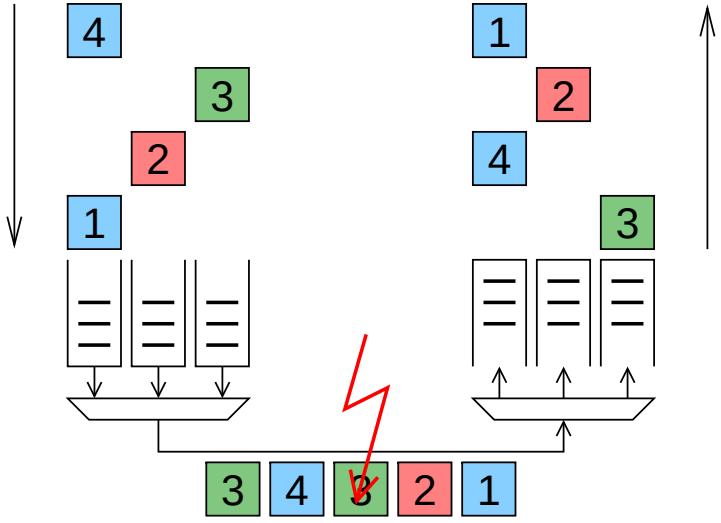
- **IP packet 3 lost or corrupted**

➥ **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**

Basic idea:

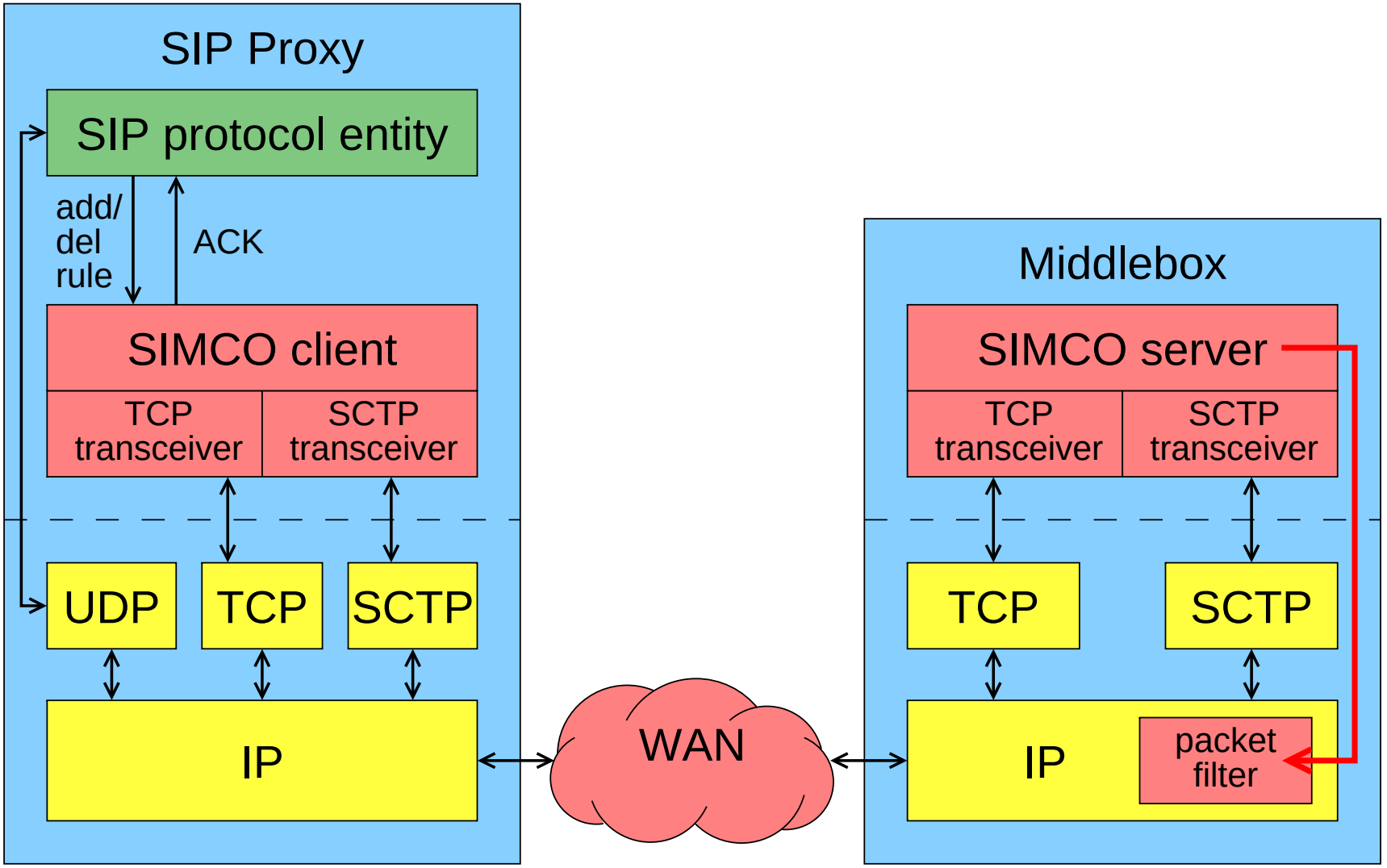
Agent and middlebox agree to use N bidirectional stream pairs upon session establishment

Distribution of messages to streams:

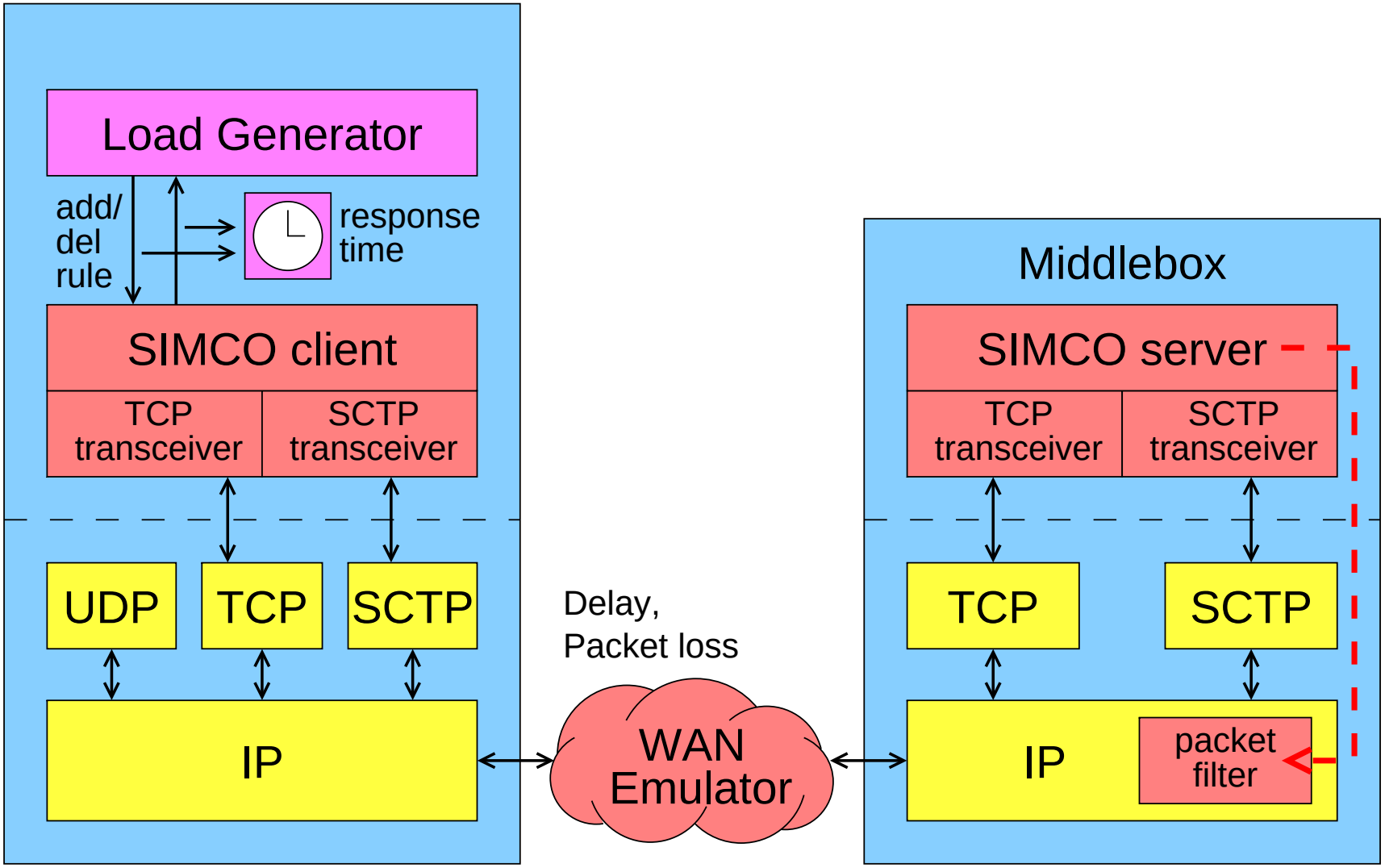
- **SIMCO Agent ("client")**
  - Create new policy rules: use round-robin scheme to distribute requests on streams, once decided save mapping PID - stream ID
  - Modify/Delete existing policy rule: reuse saved mapping
- **Middlebox ("server")**
  - Send answer on same stream number than request was received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

Specification needs to consider some special cases

SIMCO over SCTP: Prototypical implementation

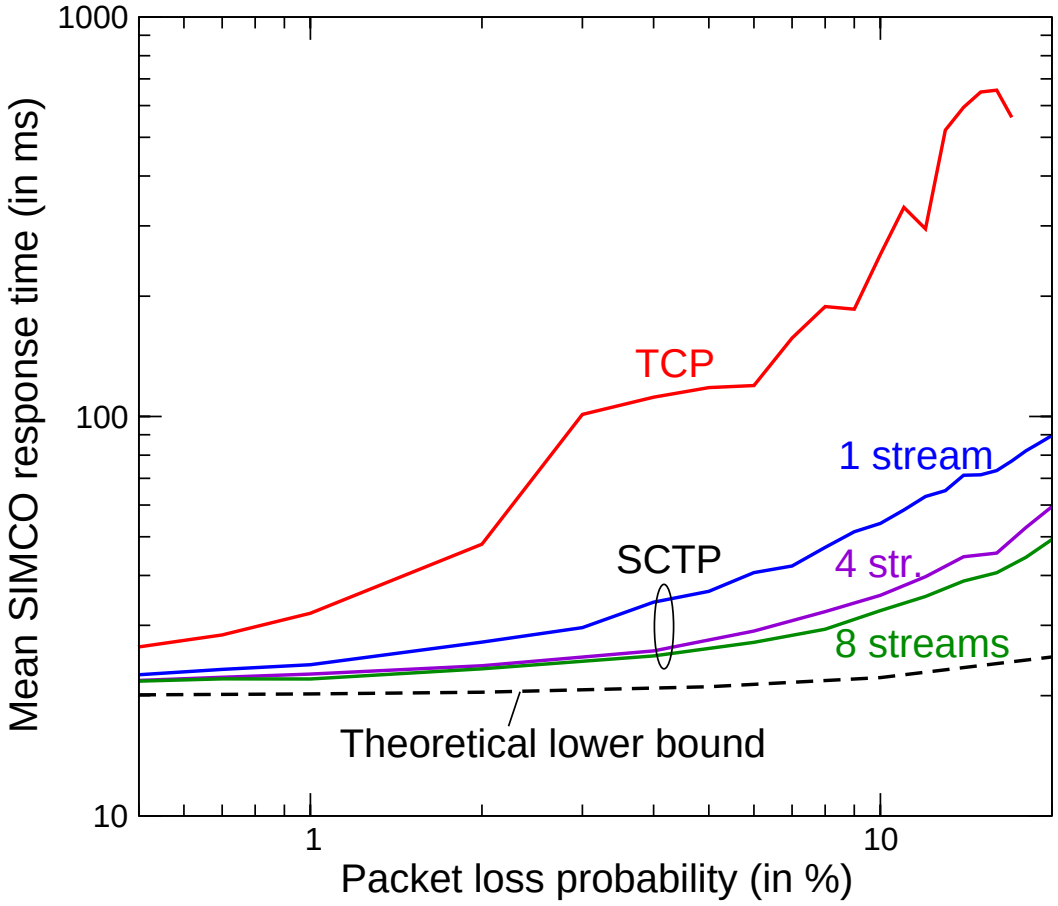


SIMCO over SCTP: Measurement testbed



Measurement results

Comparison of mean response time



System load

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

➥ **100 transactions/s**

Network

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

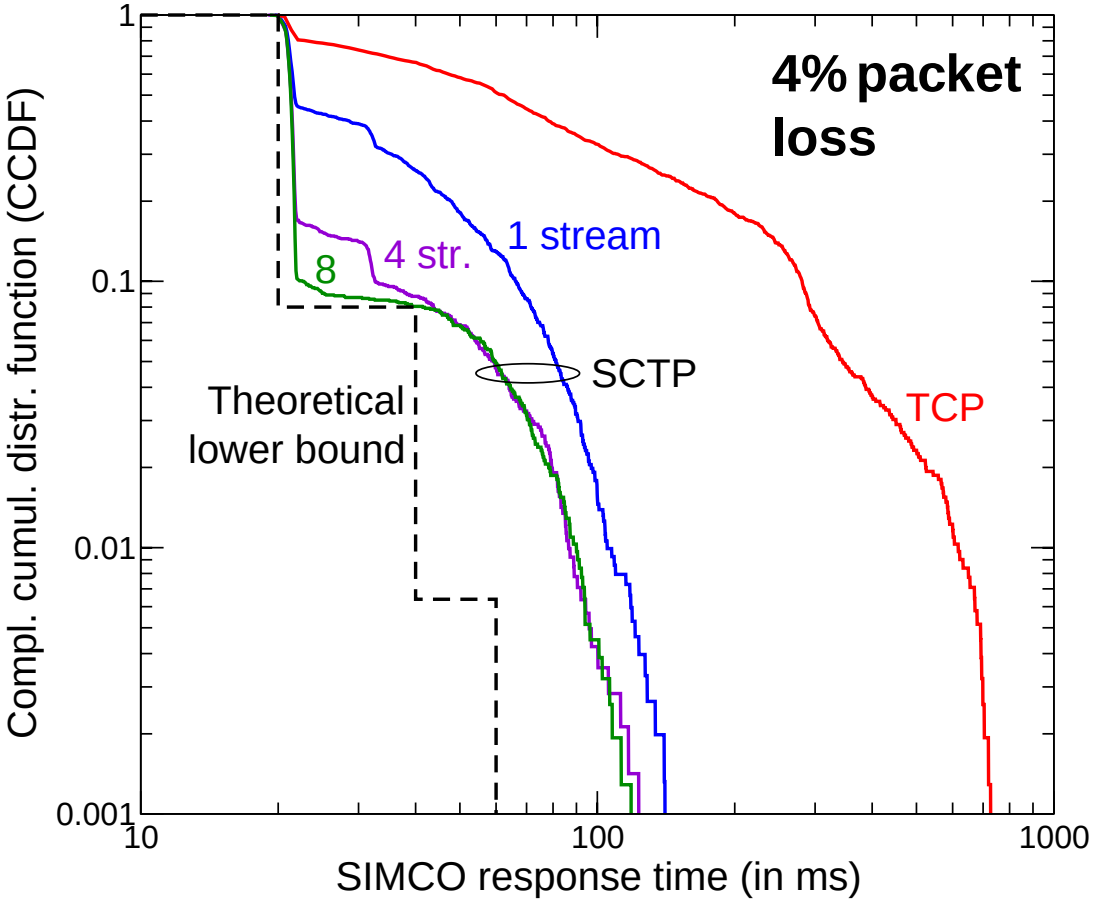
Linux 2.6.11 TCP/SCTP

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

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

Measurement results

Response time distribution



System load

- **30 ms call IAT (neg.-exp.)**
- **180 s call duration (neg.-exp.)**
- **Equiv. to 120,000 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

➥ **More than 8 SCTP streams will not significantly improve performance**

Conclusions

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**

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?
- **Explanation of observed TCP performance problems**