

# SIP (and VoIP) Security Issues

Robert Sparks

VP - Research and Development



# Overview

- Quick discussion of VoIP landscape
- Threats
- Mechanisms to address threats
- Related challenges
- Goals:
  - Get a feel for the size of the problem and solution spaces
  - Stimulate questions

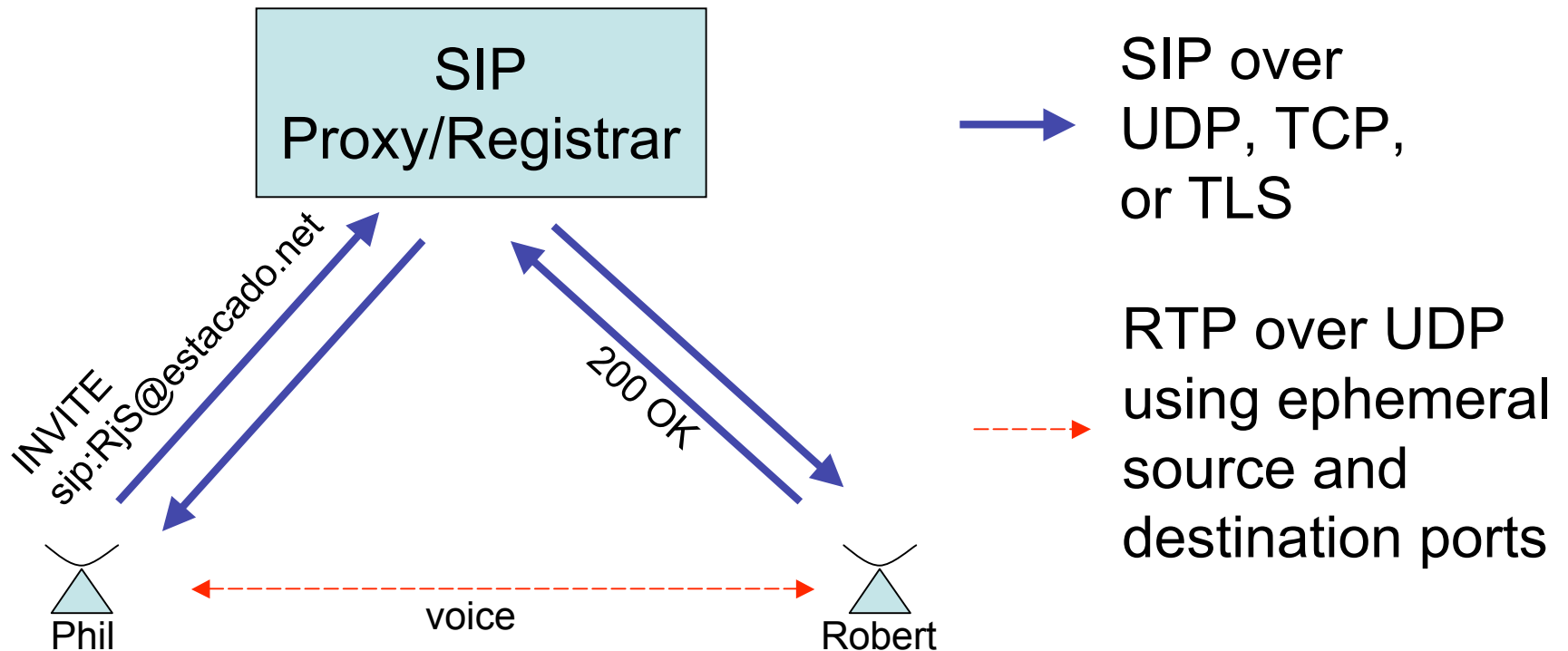
These are the tips of many icebergs

# What does VoIP mean?

- Many ways to carry Voice over IP
- Most solutions split setup and content
  - Signaling on one transport (wide range)
  - Media on another (typically RTP over UDP)
- Some solutions carry everything in one pipe
- Some solutions are one-way (streams)
- This session focuses on interactive real-time voice (and other) communication using SIP

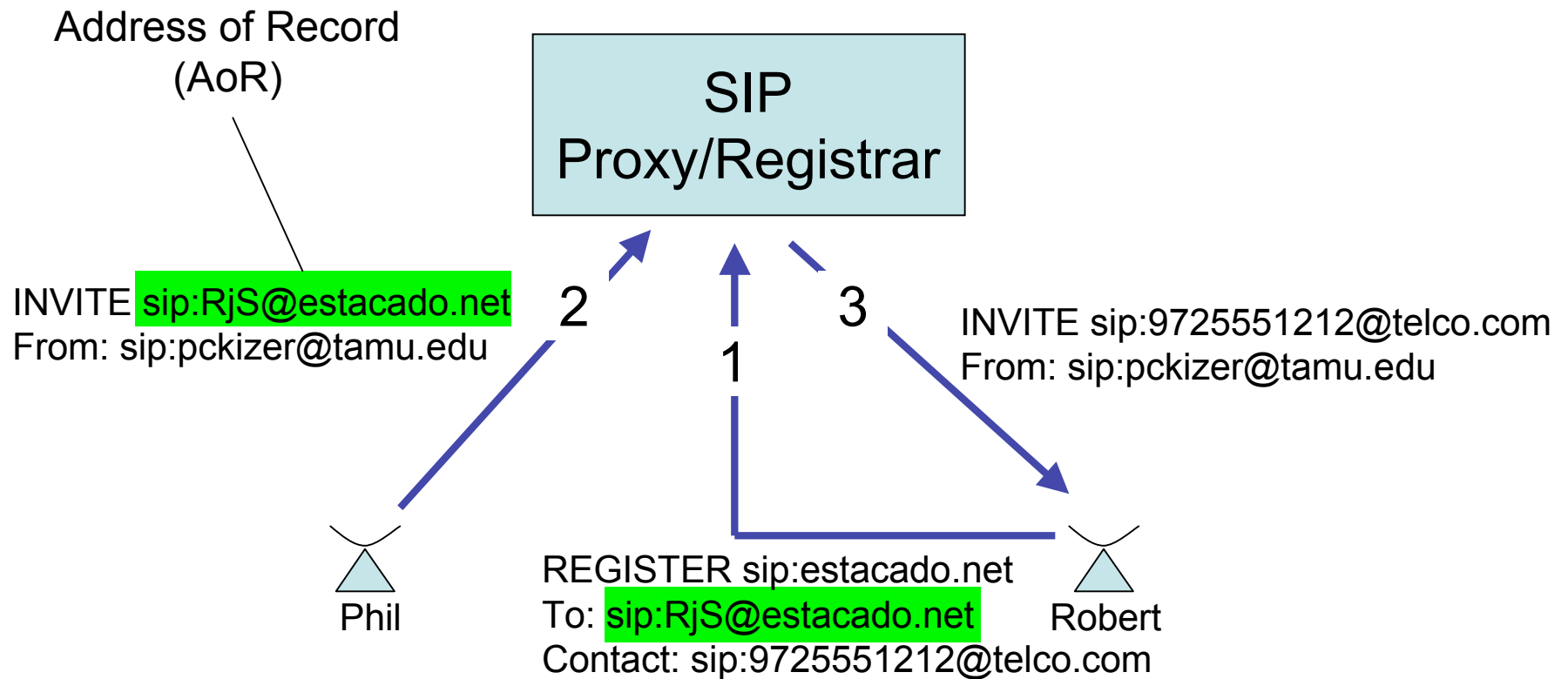
# The Landscape

## Basic Model



# The Landscape

## SIP Services Provide Rendezvous

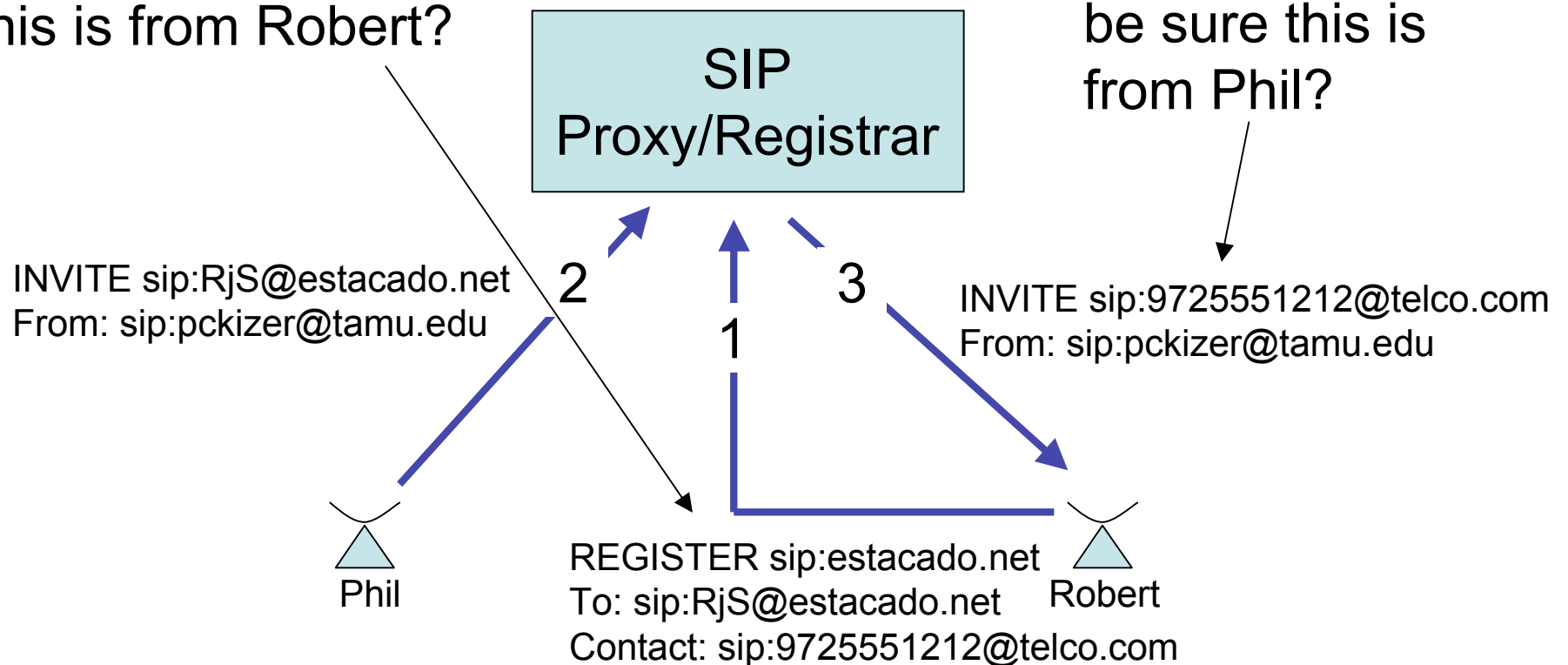


# The Landscape

## Identity is Crucial

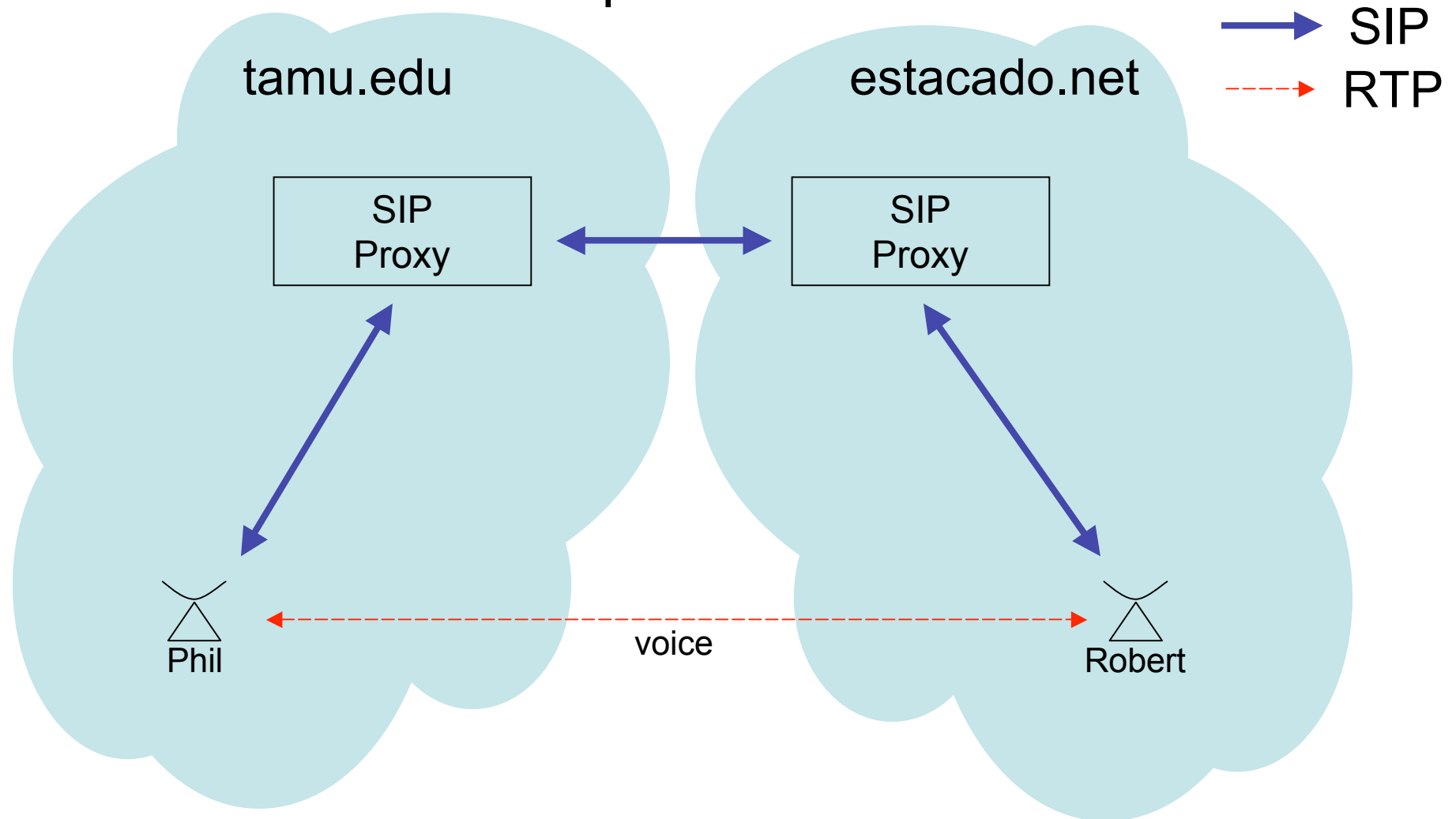
How does the server know  
this is from Robert?

How can Robert  
be sure this is  
from Phil?



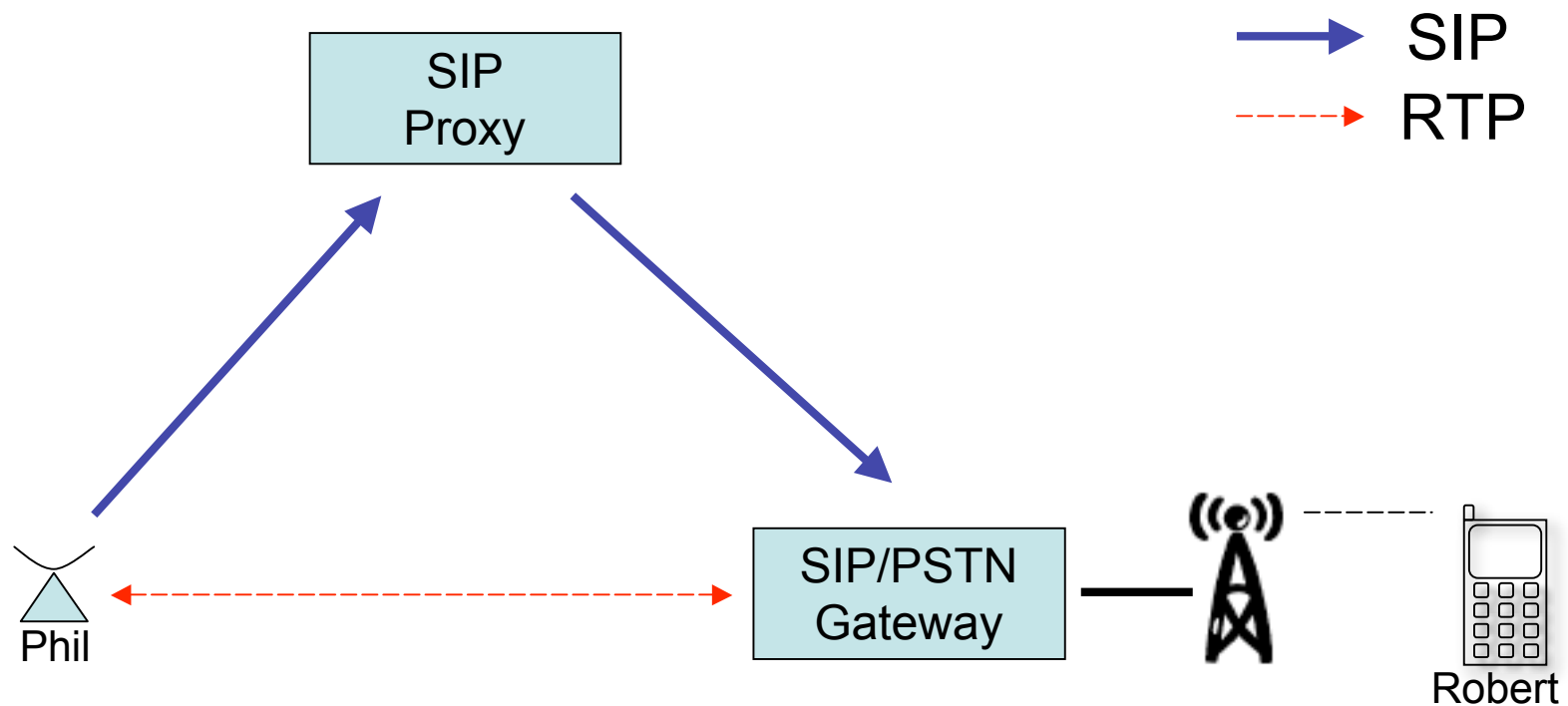
# The Landscape

## Trapezoid model



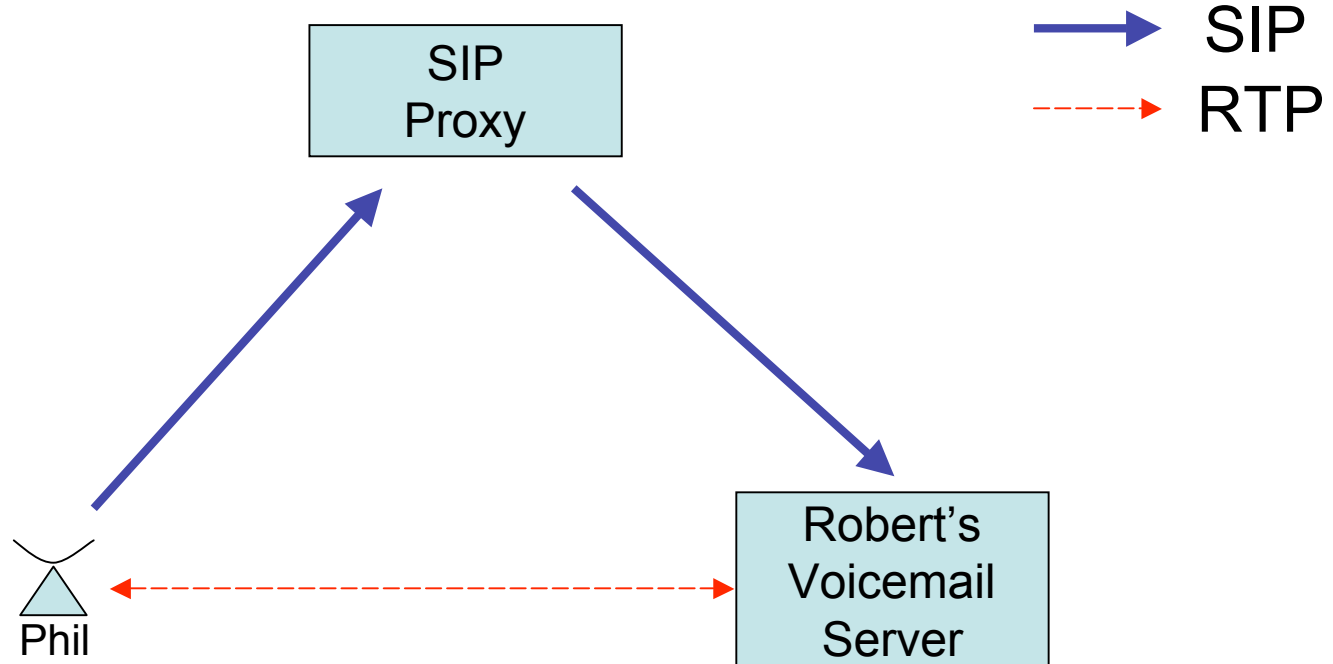
# Ecosystem Members

## PSTN Gateways



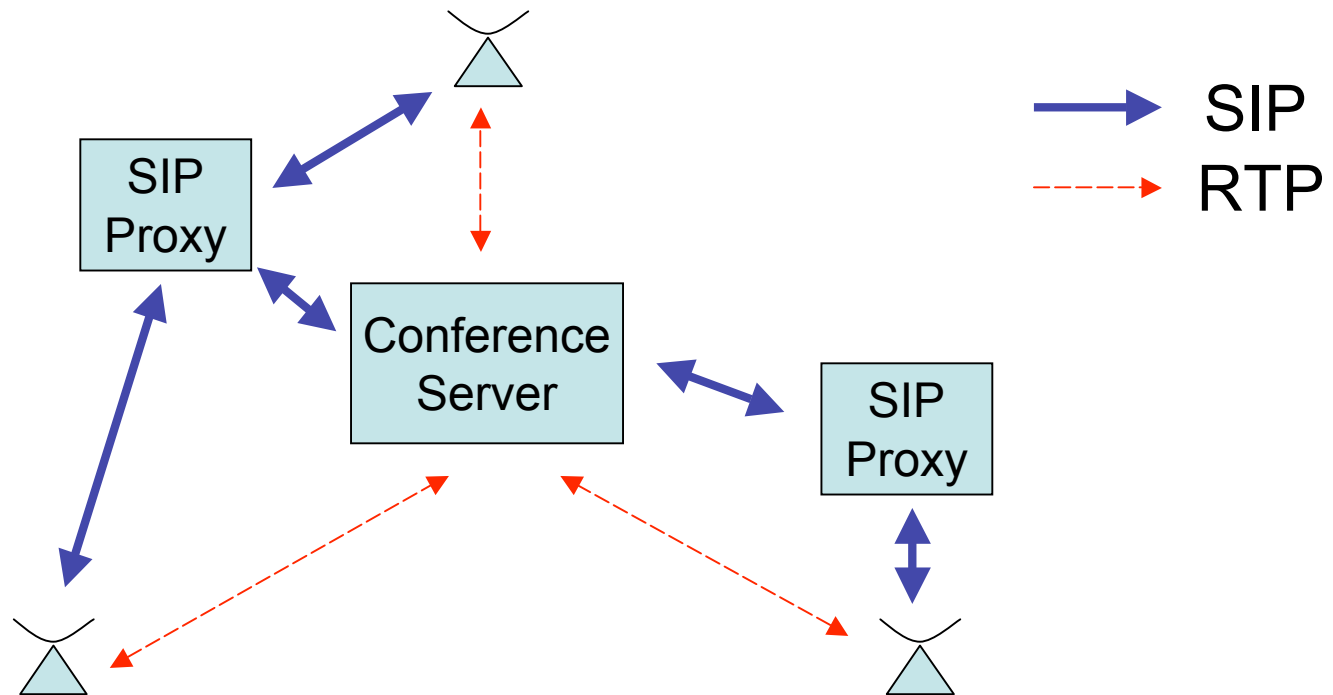
# Ecosystem Members

Voice Mail / IVR systems



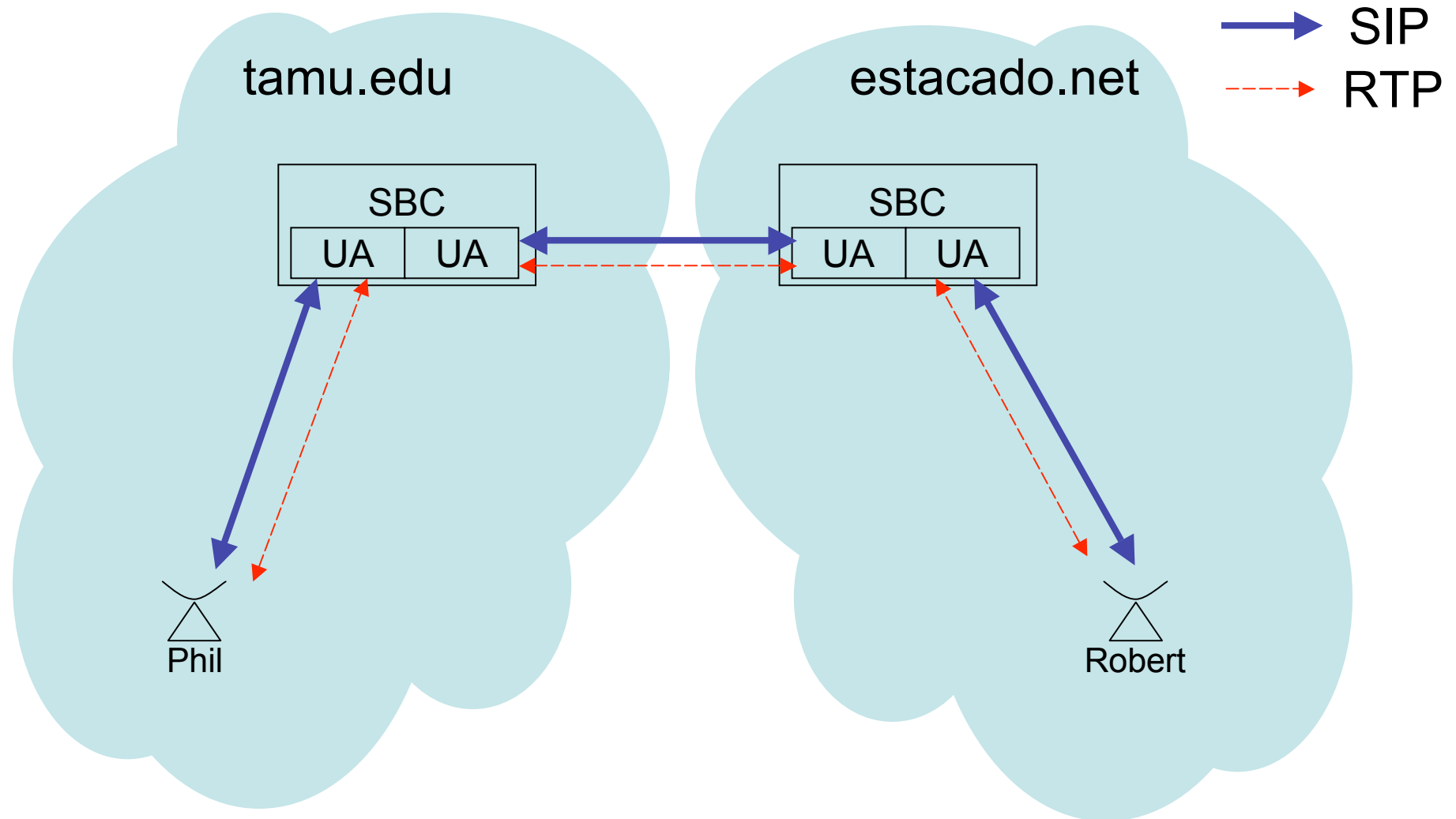
# Ecosystem Members

## Conference Servers

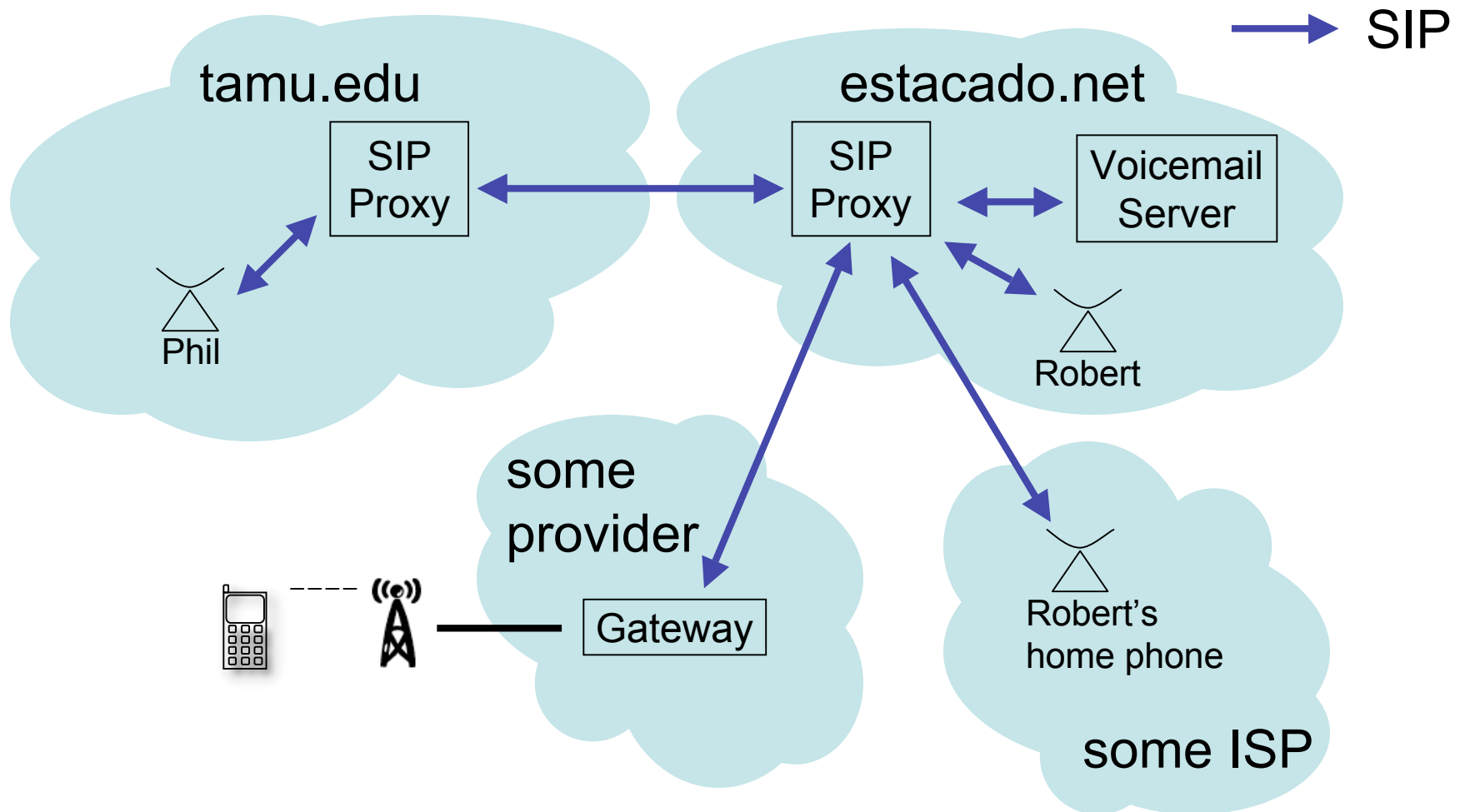


# Ecosystem Members

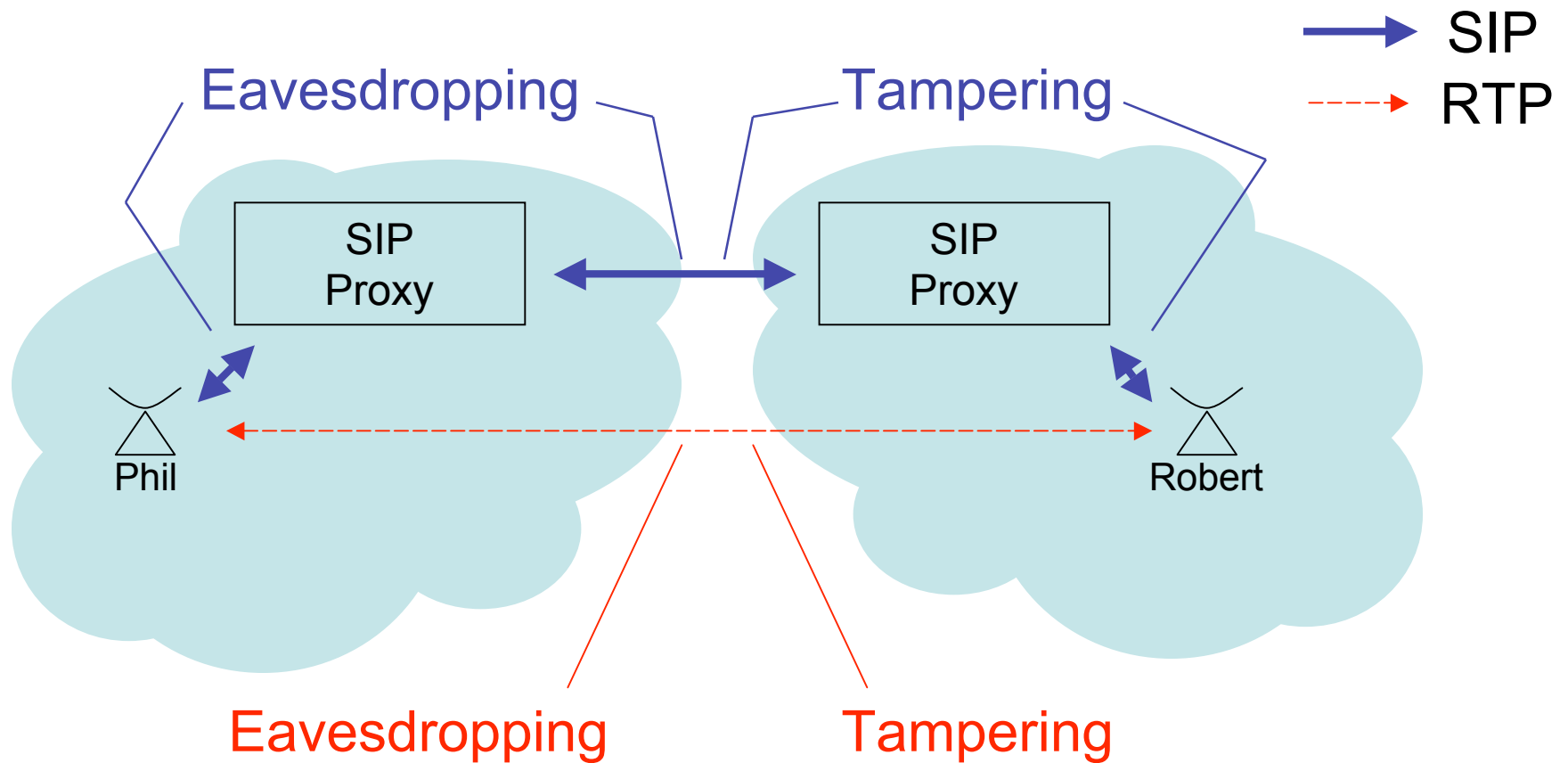
## Session Border Controllers



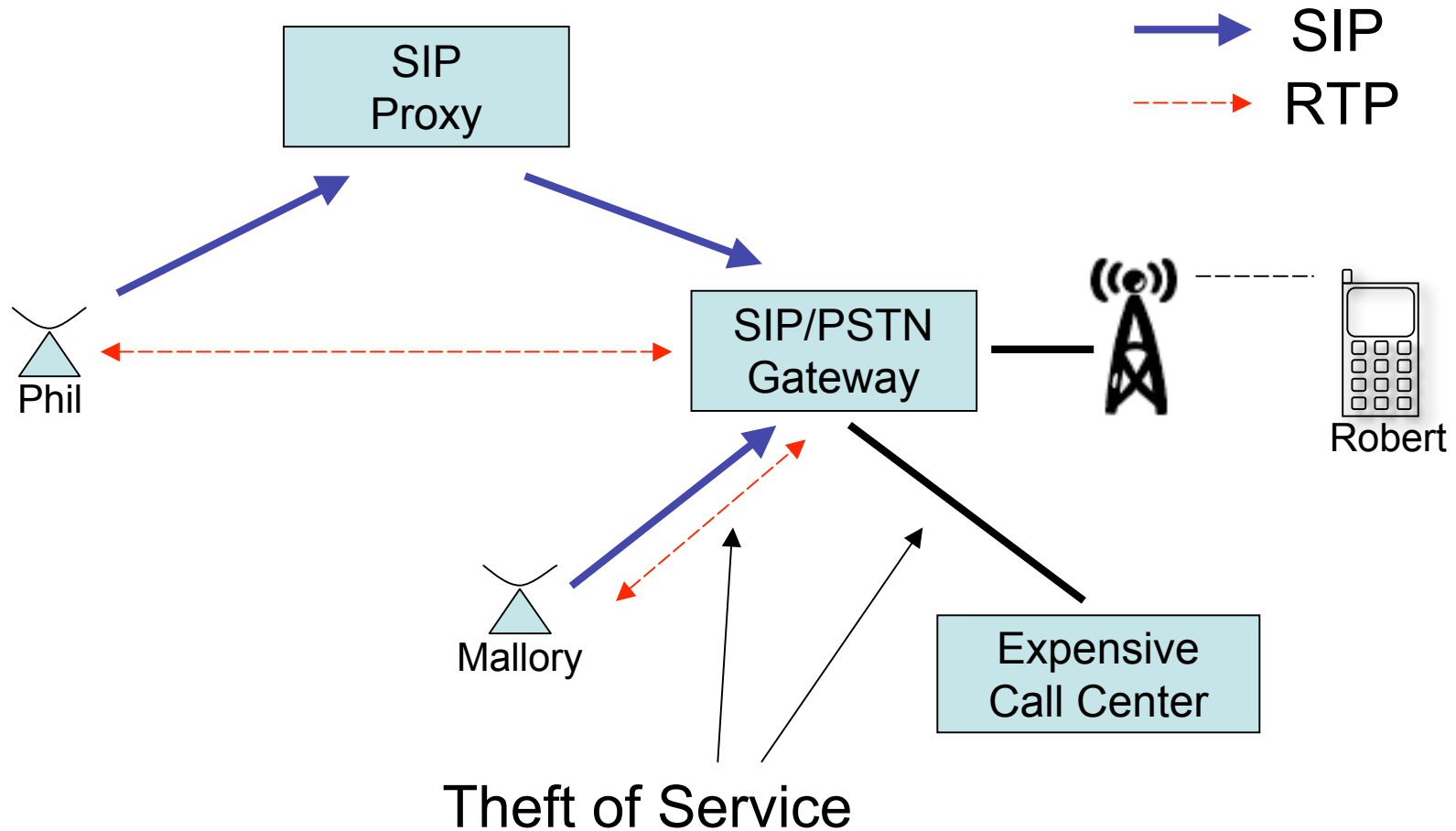
# Forking



# Threats



# Threats



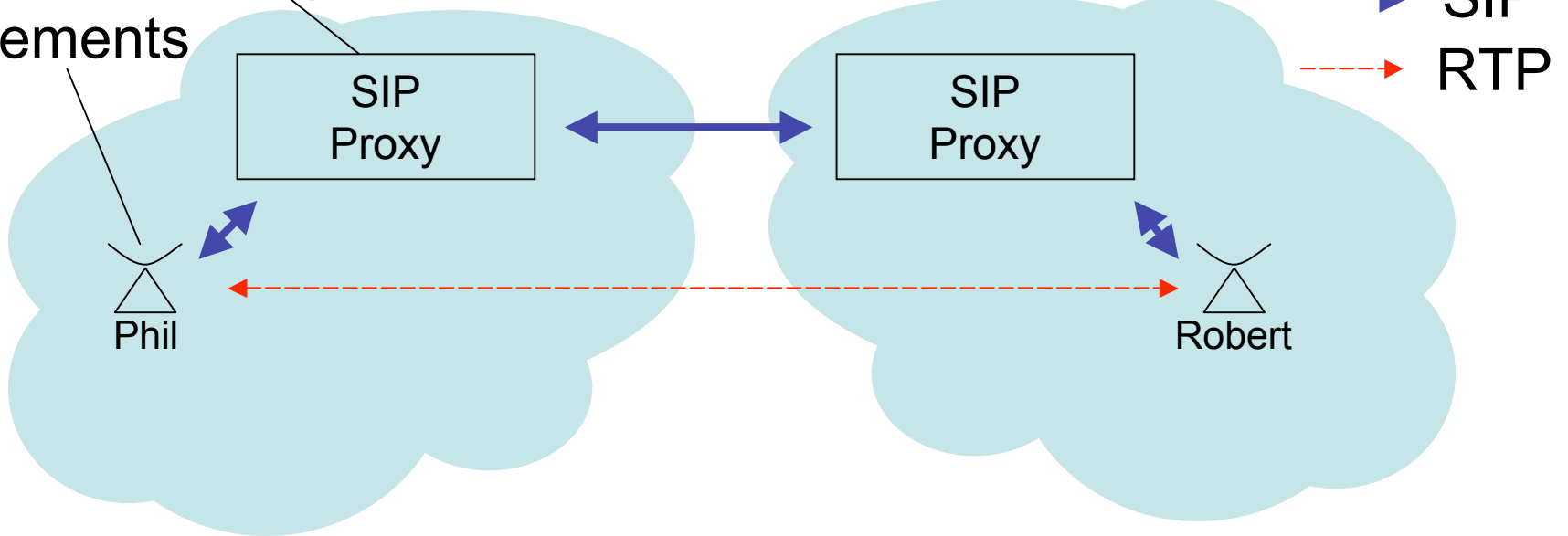
# Threats

Weak storage of credentials  
 Poor interoperability  
 Unsafe networking code

lead to

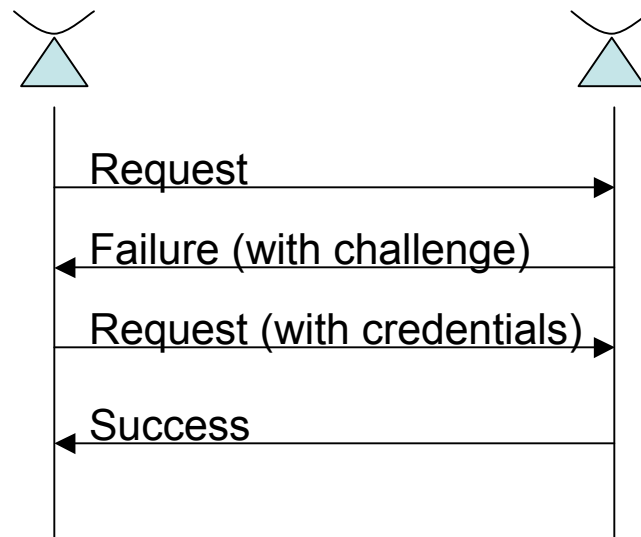
Identity theft  
 Hijacking of service  
 Denial of service

Compromising  
 elements



# Protecting the Signaling: DIGEST

- Similar to HTTP digest: password based
  - WWW-Authenticate, Authorization
  - Proxy-Authenticate, Proxy-Authorization

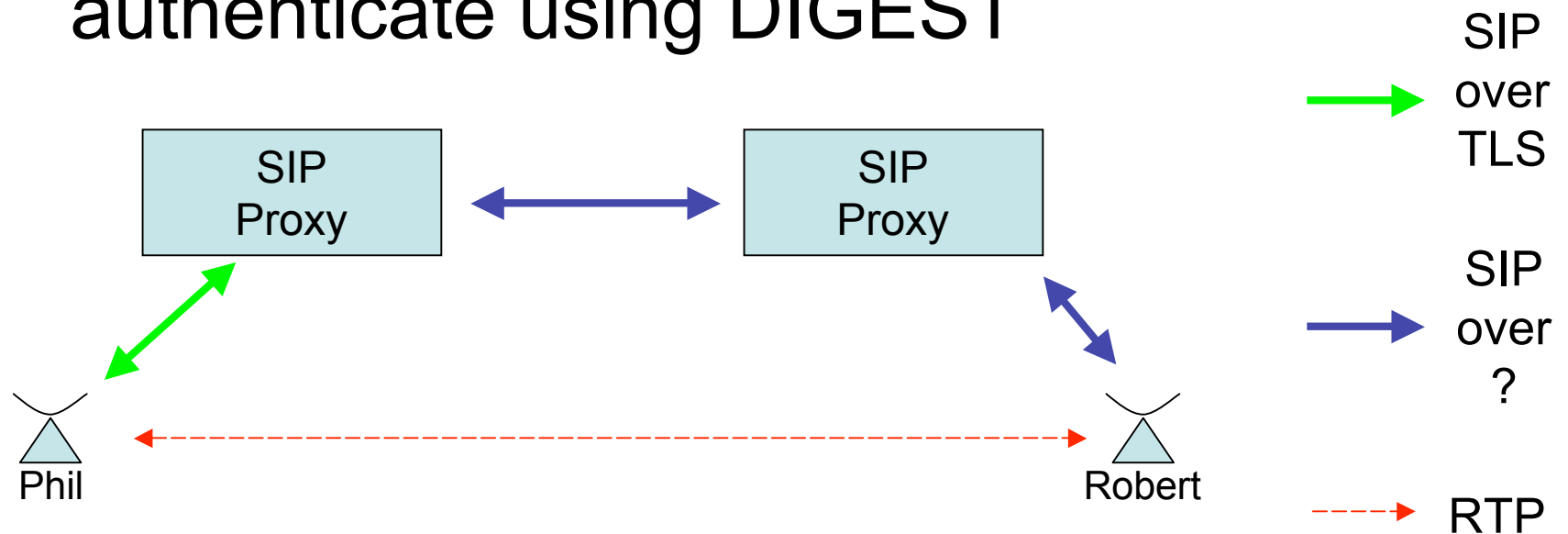


# Problems with DIGEST

- Hash is weak
- Authenticating a request to more than one element is problematic
  - Leaks hash to elements in the path
  - Not well implemented
- In practice, DIGEST is only good for authenticating to the first hop

# Protecting the Signaling: TLS

- Hop-by-hop transport security
- Typically, endpoints enter into a server-auth relationship with a server and authenticate using DIGEST



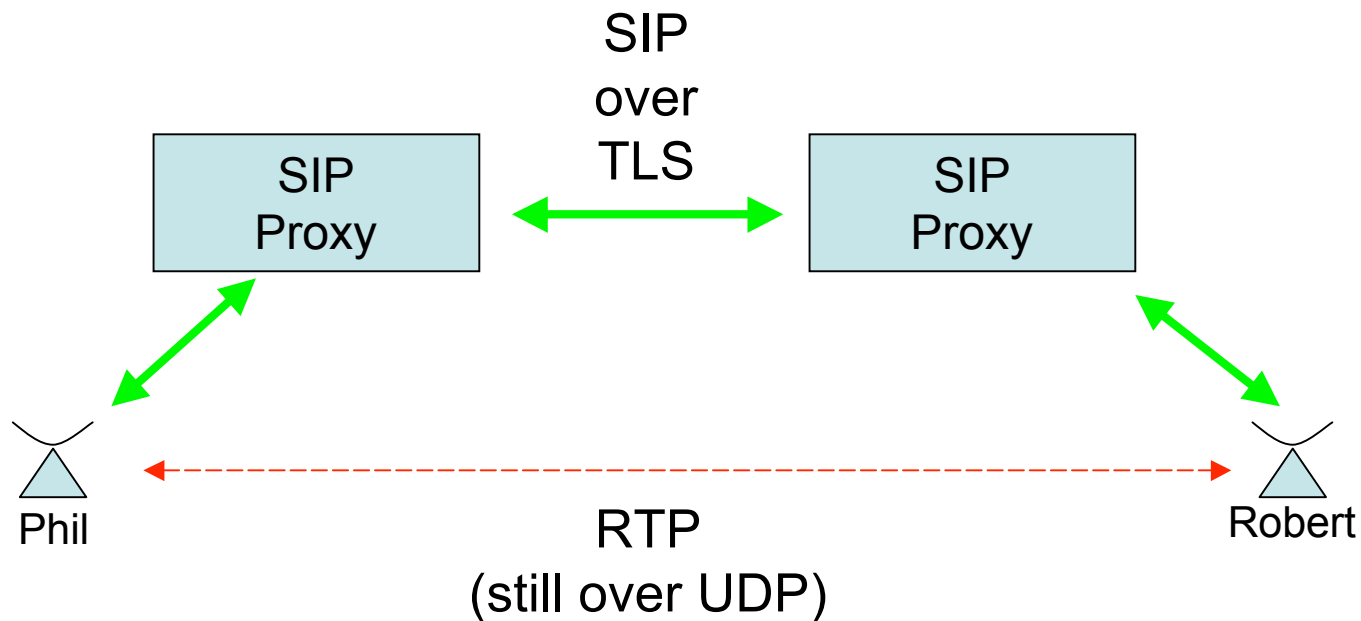
# Problems with TLS

- Key distribution makes mutual authentication impractical (so far)
- Only protects one hop - no assurances of what happens beyond that hop

# Protecting the Signaling: sips

- “Secure” sip, like https is to http
- Proxies receiving a sips request are required to forward only on secure transports (weakened in private domains)
- Not as strong as https - no way to tell if a proxy doesn't conform to the requirement

# Protecting the Signaling: sips



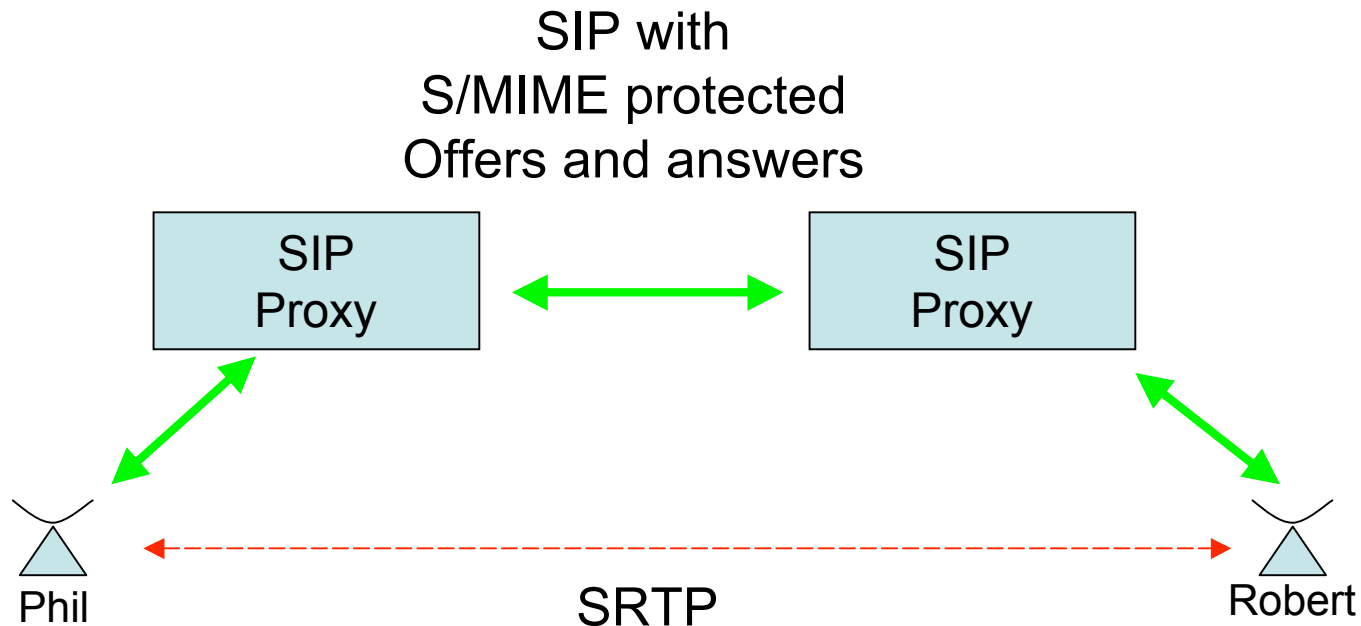
# Protecting the Signaling: S/MIME

- Provides end-to-end integrity protection and encryption of the body and parts of the message header
- Suffers from same key distribution issue hindering mutual-auth TLS

# Protecting the Media: SRTP

- Encrypts individual media packets using a symmetric session key.
- Session key must be securely exchanged - current recommendation is to use S/MIME in the signaling.

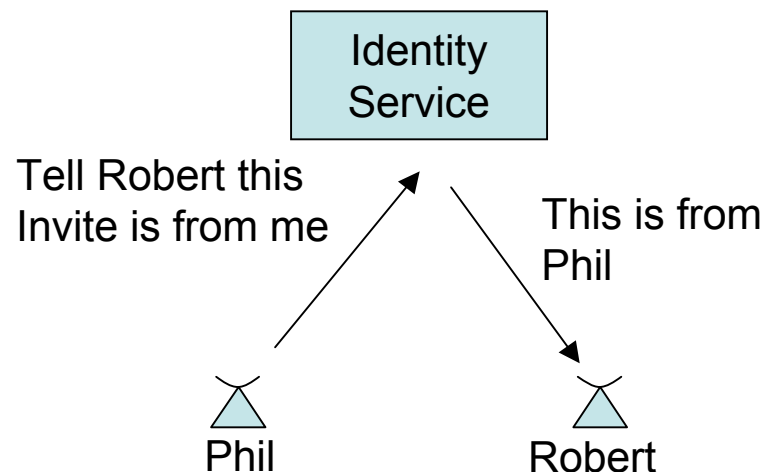
# Protecting the Media: SRTP



The *payload* of individual RTP over UDP packets is encrypted with symmetric keys exchanged in the protected offer and answer

# Improving Protection SIP Identity

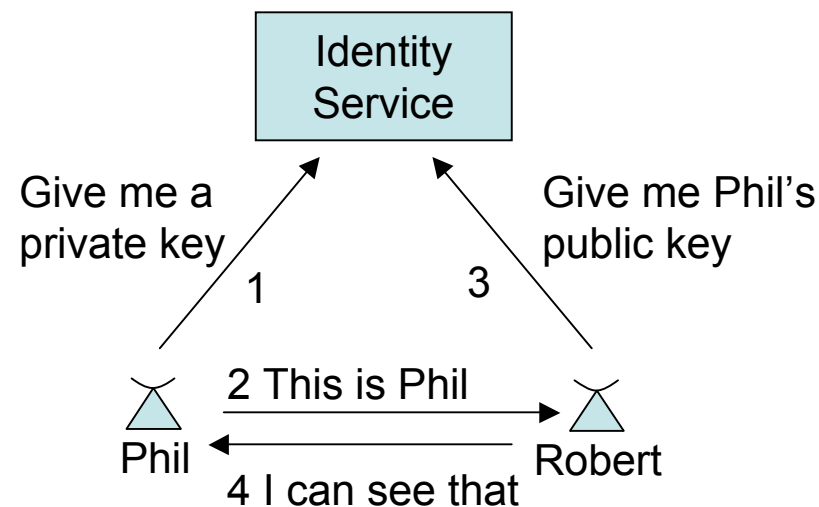
- Allows a service with a certificate signed by a trusted root to say “I’ve verified this message came from this particular identity”



# Improving Protection

## Certificates and Credentials

- Uses SIP-Events (Subscribe/Notify) to distribute keys
- Compelling solution to the key distribution and revocation problems



# Compromising elements


- Implementations are often brittle
  - Postel's maxim is not intuitive to the average developer
  - There is never enough interoperability testing
- Mallory can leverage this brittleness to
  - Induce bad behavior from an element
  - Cause an element to reveal sensitive information
  - Cause an element to stop functioning
- Solution: Send all implementations to the SIP Forum's SIPIT interoperability events

# SIPIT

- Weeklong tests twice a year
- Hundreds of implementations
- Held around the globe
  - SIPIT 15: Aug 2004 - Taipei
  - SIPIT 16: Apr 2005 - Banff
  - SIPIT 17: Sep 2005 - Stockholm
- <http://www.sipit.net>



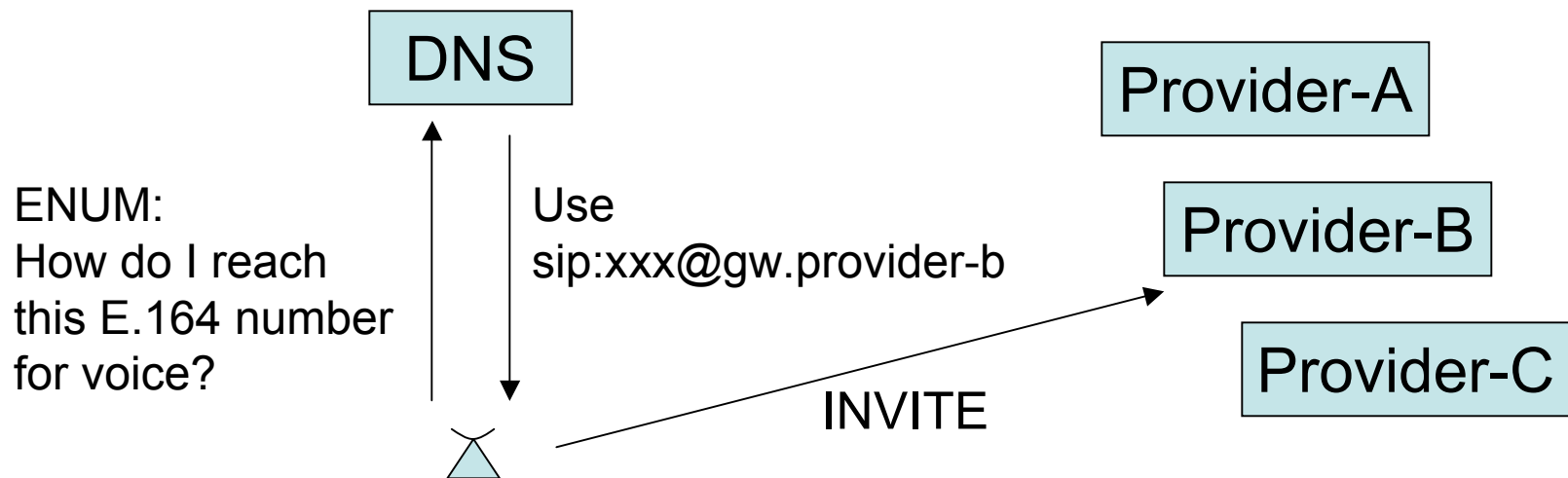
# More test tools

- OULU/Codenomicon tests for buffer-overflow, unexpected character, and other robustness weaknesses
- SIPPING Torture test messages
- SIP Forum Test Framework hosted at the the SIPfoundry

<http://www.sipfoundry.org>

# Compromising infrastructure

- SIP routing is particularly vulnerable to attacks on DNS
- Most implementations are very sensitive to DNS performance



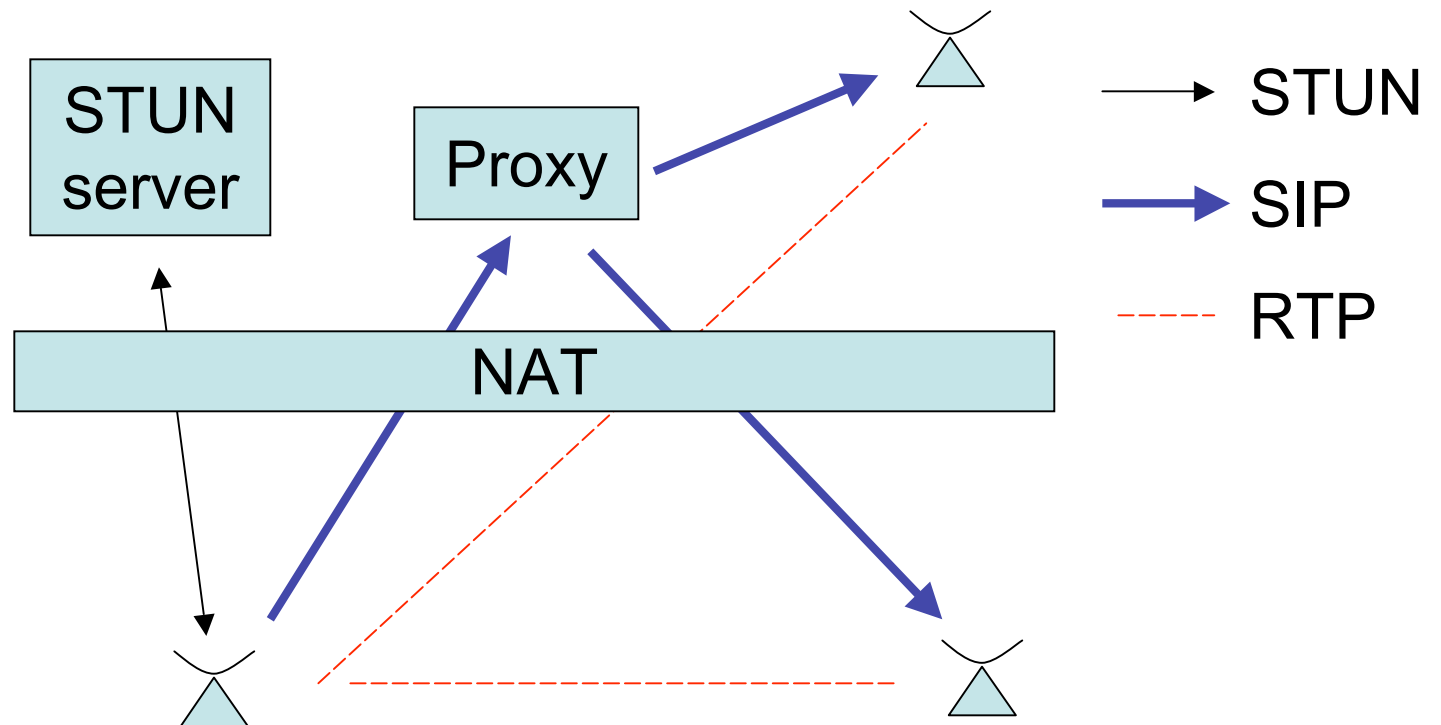
# Firewalls and NATs

- SIP carries IP addresses in headers and in offer/answer bodies
- RTP sessions negotiated with SIP are directly end-to-end using ephemeral UDP ports
- Firewalls often don't allow unsolicited incoming requests

# STUN and ICE

- Simple Traversal of UDP Nats allows endpoints to discover their “public” address
- The Interactive Connectivity Framework allows endpoints to offer all addresses it can discover (public or private) as alternatives for communication.

# STUN and ICE



# Connection Reuse

- Endpoints behind a NAT/Firewall nail up a TCP or TLS connection to a server in the public Internet
- Incoming requests make it through the firewall by coming down that connection
- Great for SIP only scenarios like presence/messaging, but doesn't solve getting RTP over UDP through a Firewall

# Additional Information

- [www.ietf.org](http://www.ietf.org)
  - SIP, SIPPING, SIMPLE working groups
- [www.softarmor.com](http://www.softarmor.com)
- [www.sipfoundry.org](http://www.sipfoundry.org)
- [www.sipit.net](http://www.sipit.net)

# Information Resource

Robert Sparks  
VP Research and Development  
Estacado Systems

RjS@estacado.net