

draft-ietf-sip-identity-02

Jeremy George

June 16, 2004

Abstract

“The existing security mechanisms in the Session Initiation Protocol are inadequate for cryptographically assuring the identity of the end users that originate SIP requests and responses, especially in an interdomain context. This document recommends practices and conventions for identifying end users in SIP messages, and proposes a way to distribute cryptographically secure authenticated identities.”

Abstract

So, that last slide boils down to a first step toward preventing forged From: addresses in an effort to minimize spam. A key in the model is that it does not require previous association or a trust relationship.

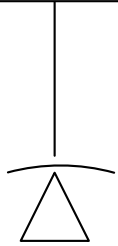
Two new SIP headers

Identity: digest encryption of To/From addr, Call-id, SIP-Date, Contact addr and the message-body.

Identity-info: HTTPS URI or SIPS URI to a resource containing the certificate of the authentication service.

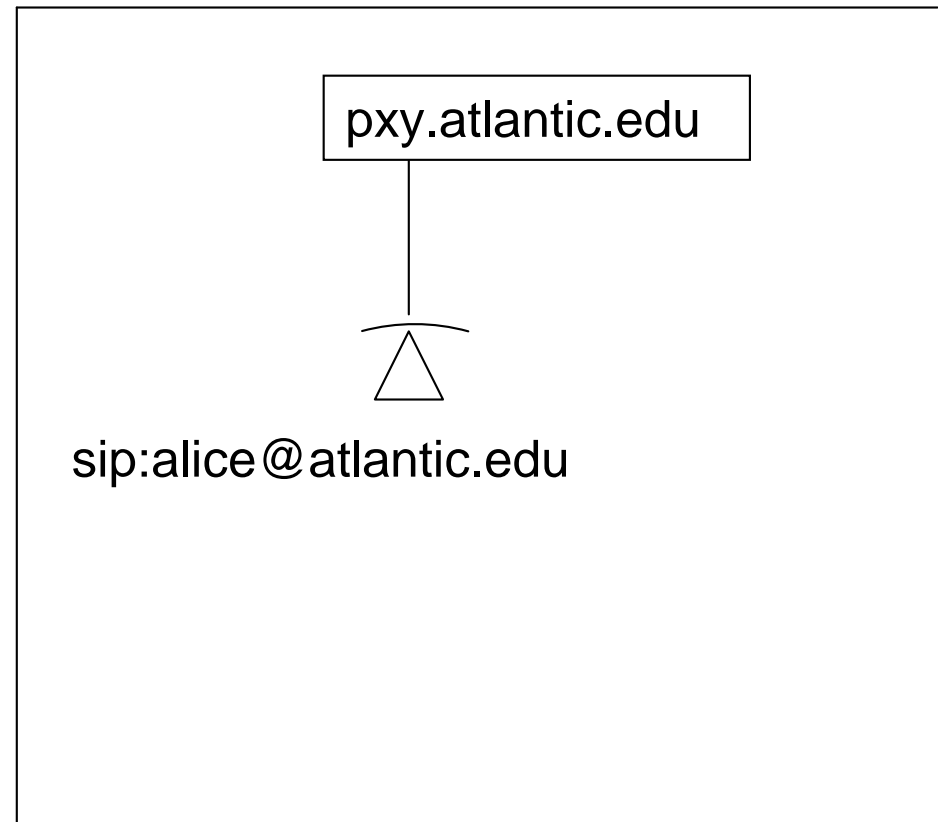
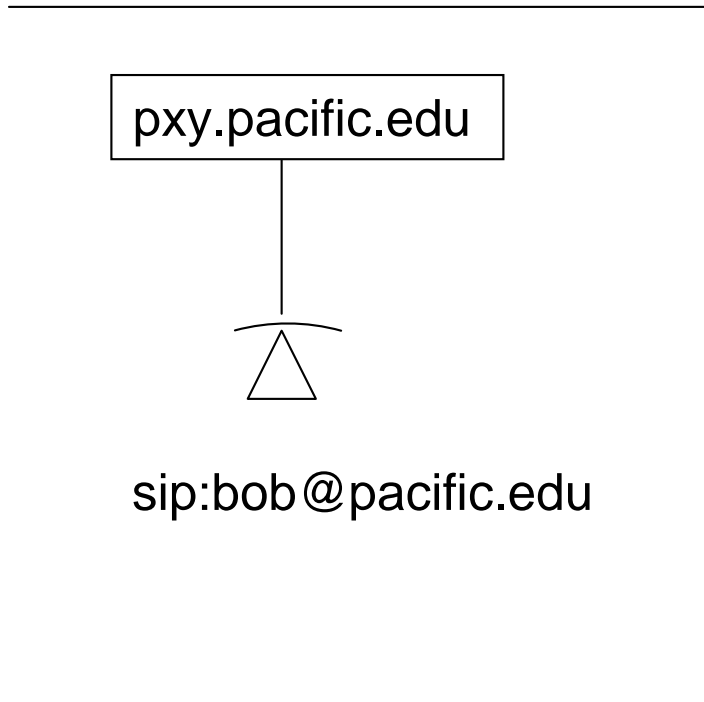
Call Flow

pxy.pacific.edu

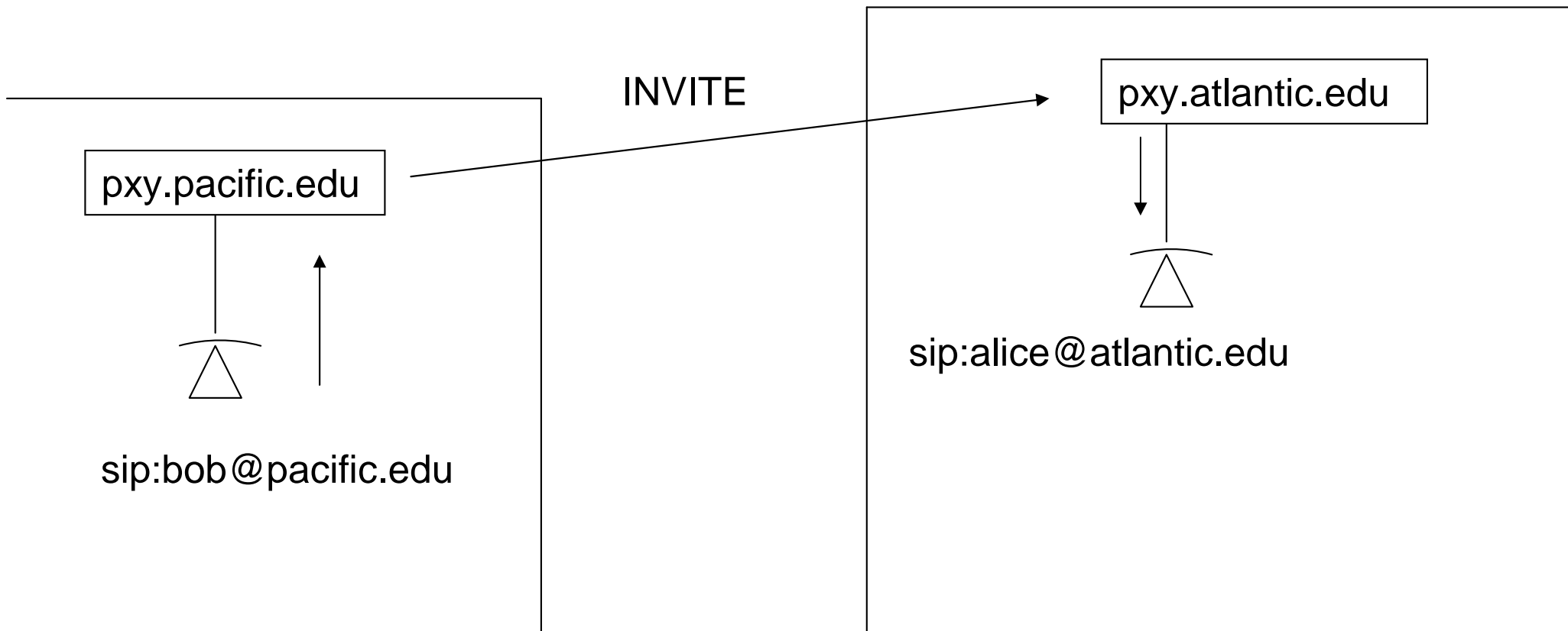


sip:bob@pacific.edu

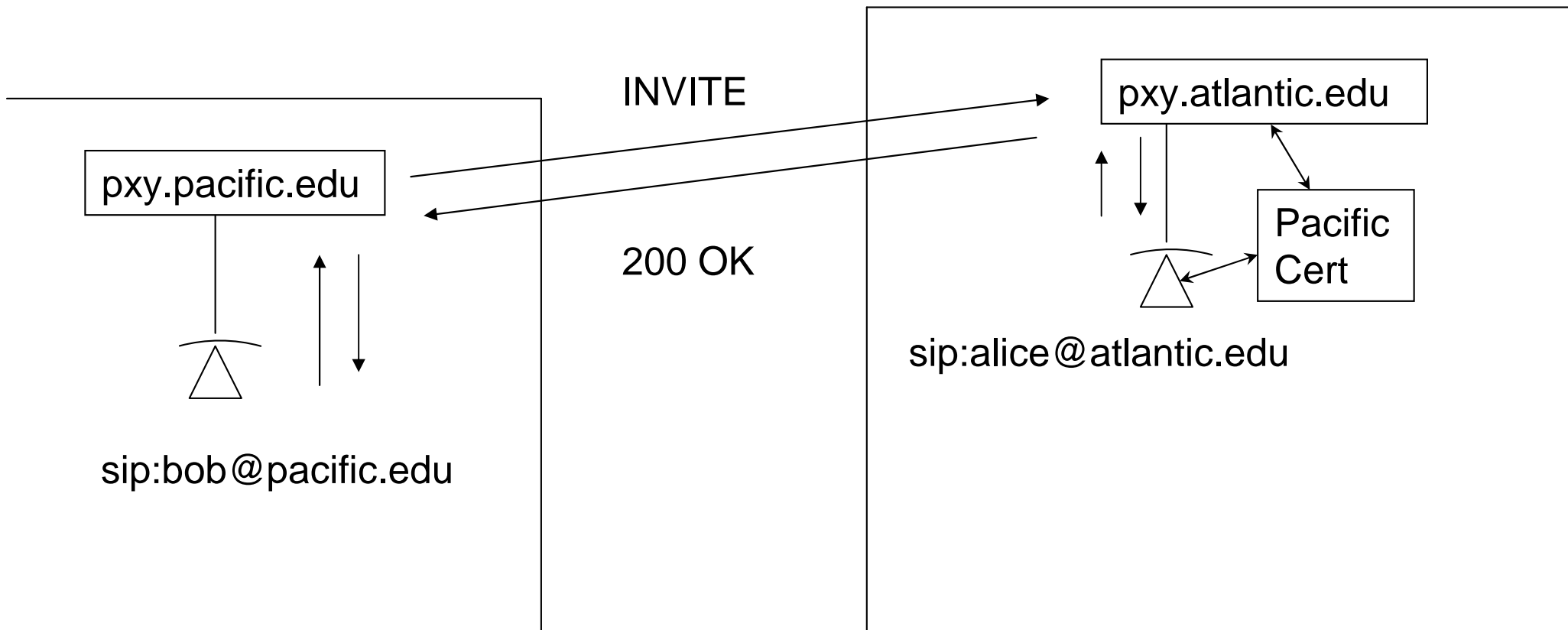
Call Flow



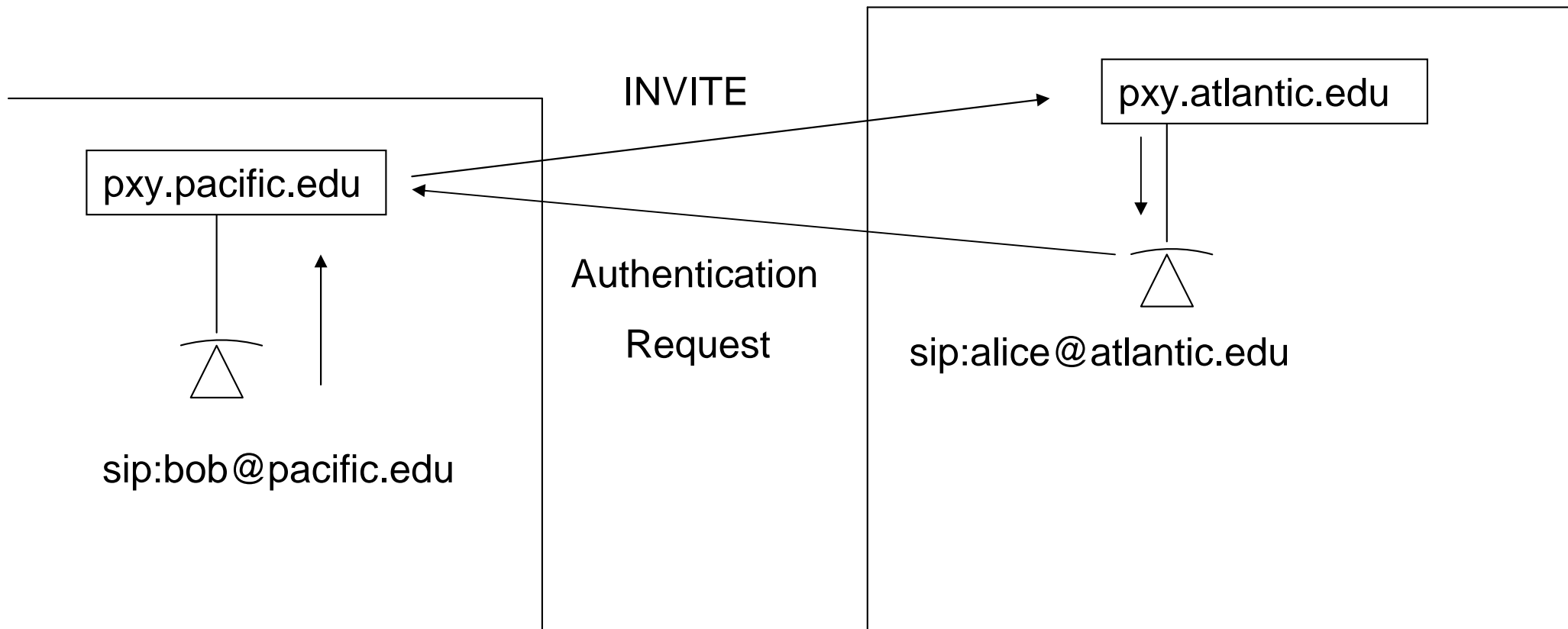
Call Flow



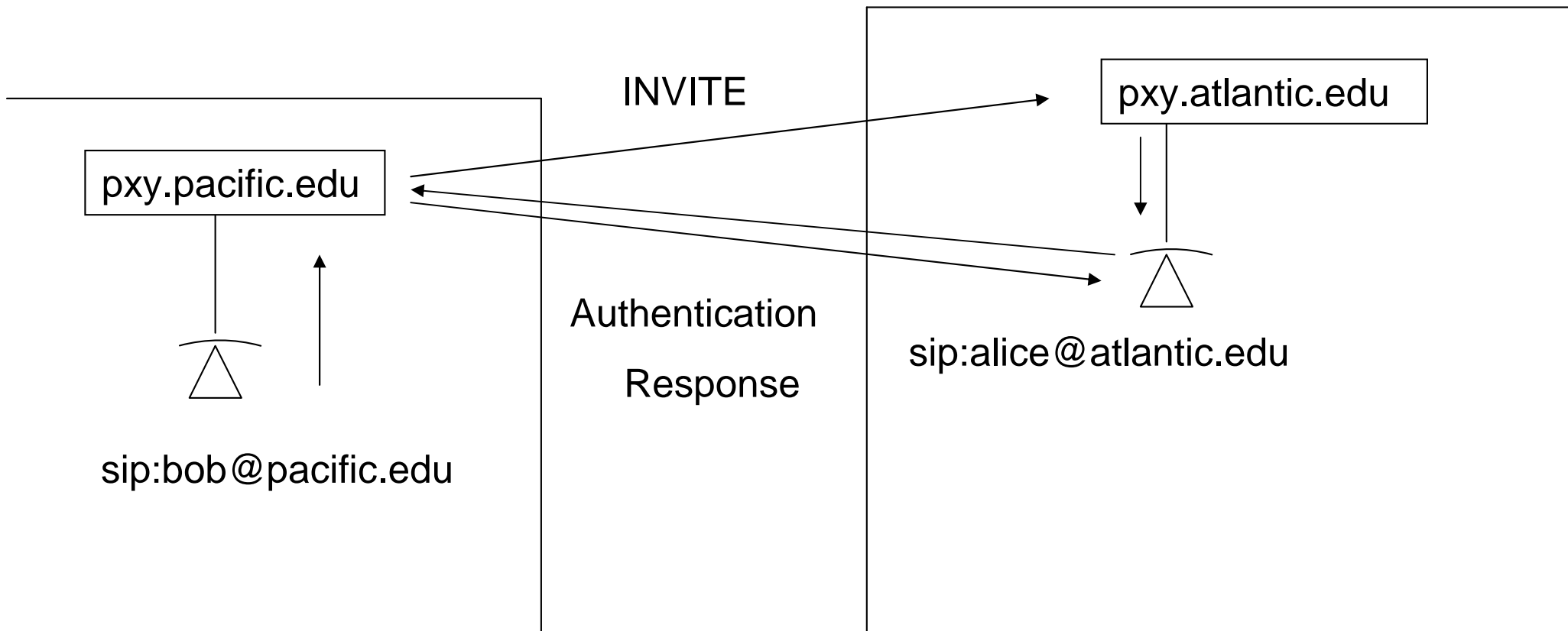
Call Flow



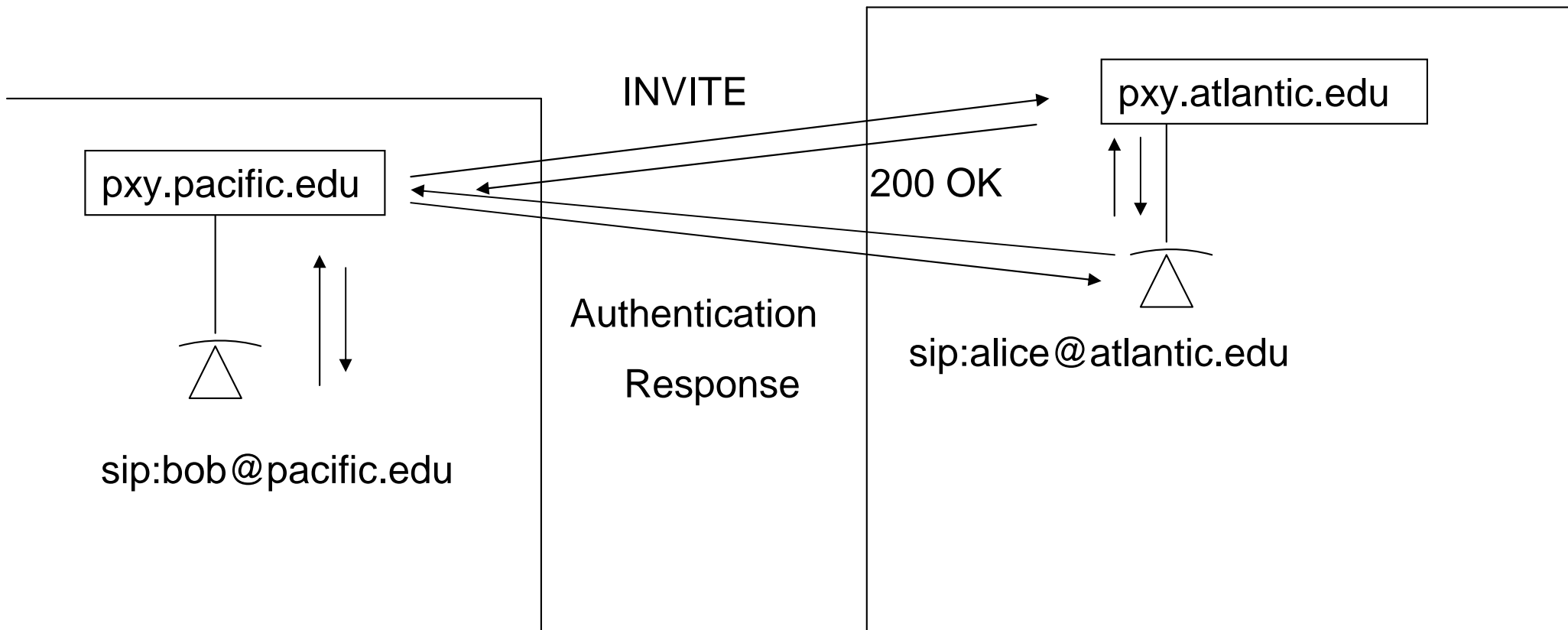
Call Flow



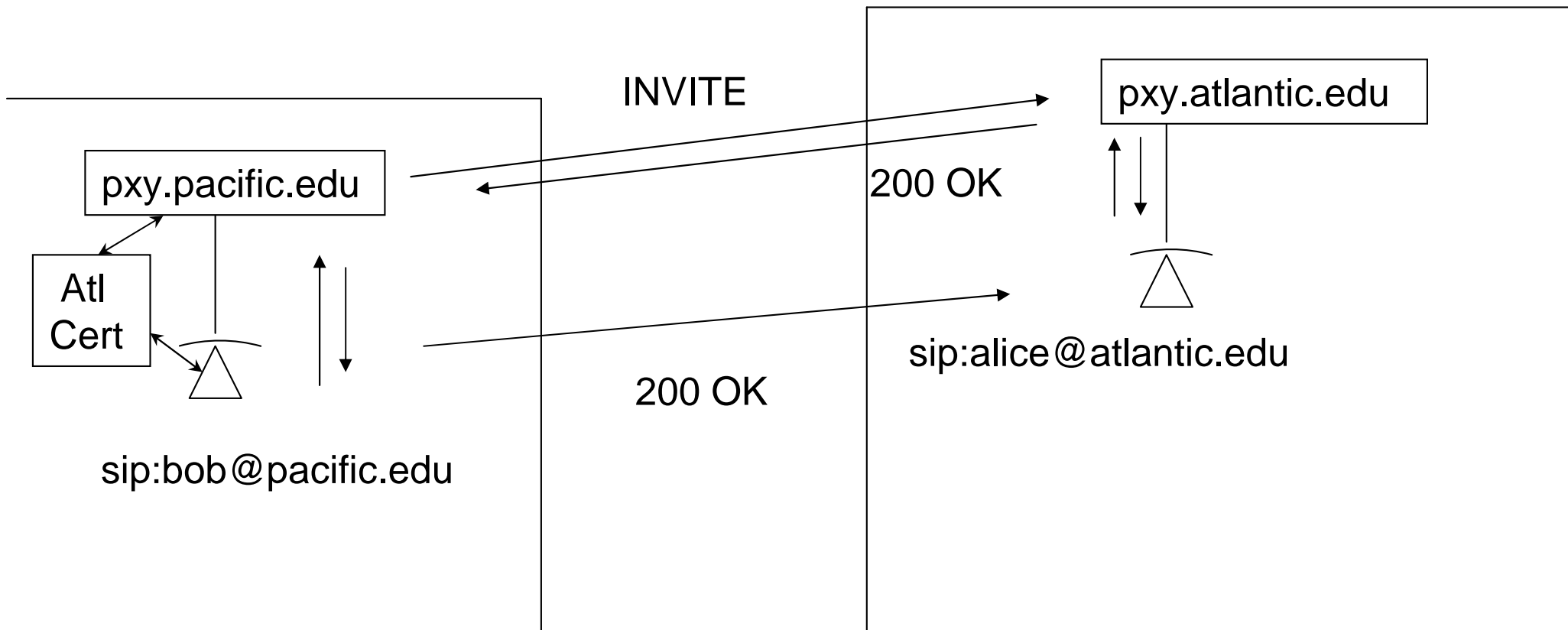
Call Flow



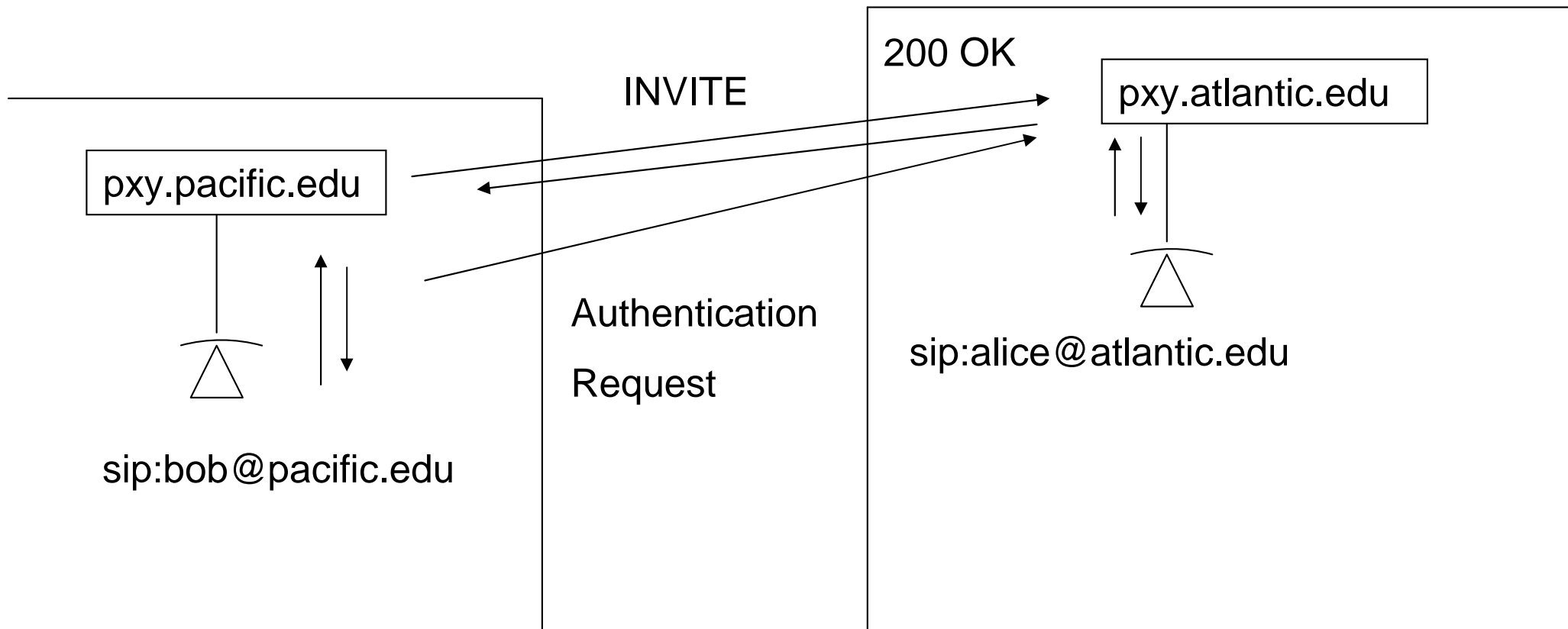
Call Flow



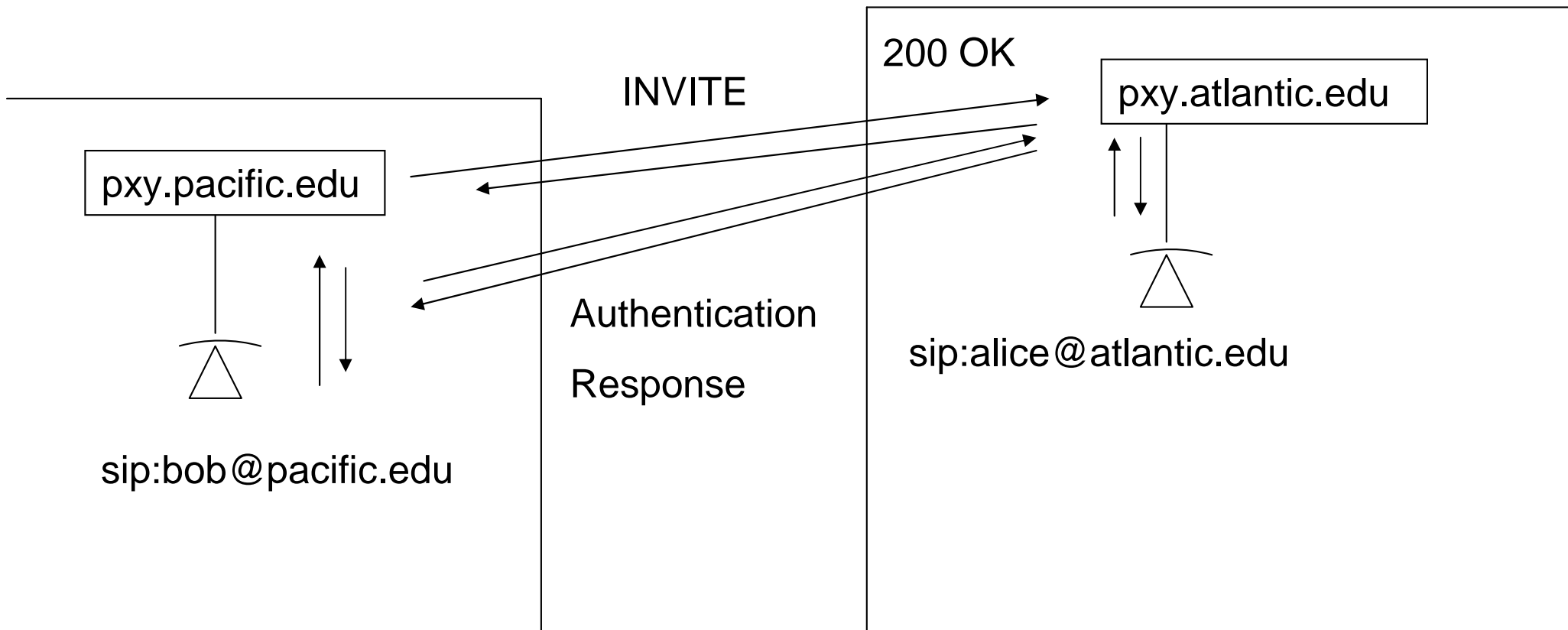
Call Flow



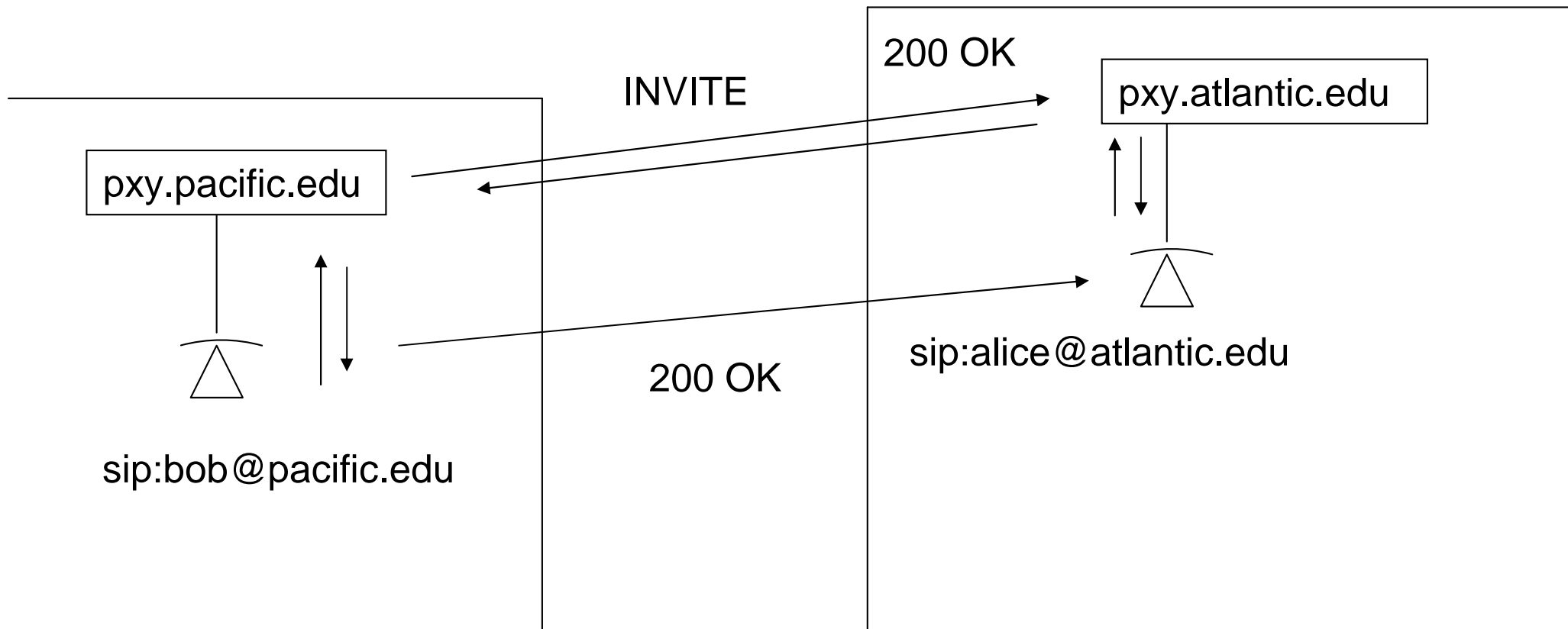
Call Flow



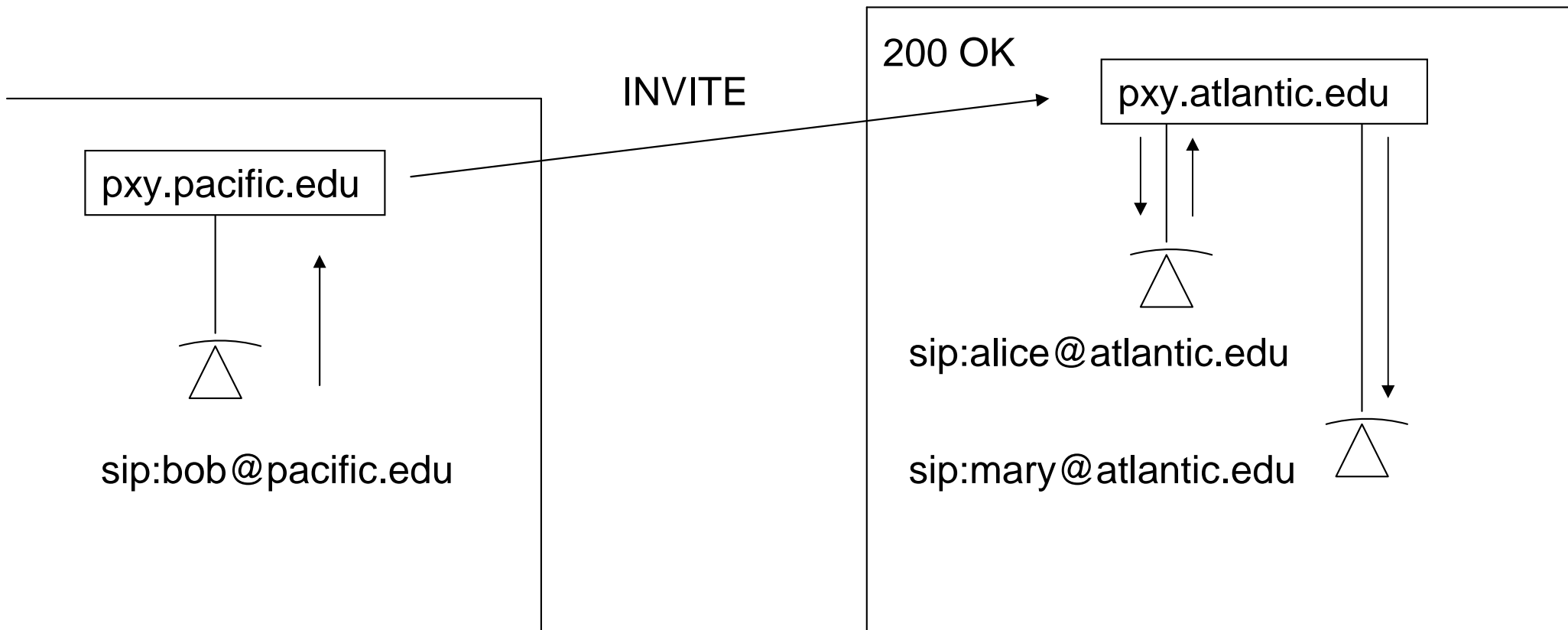
Call Flow



Call Flow

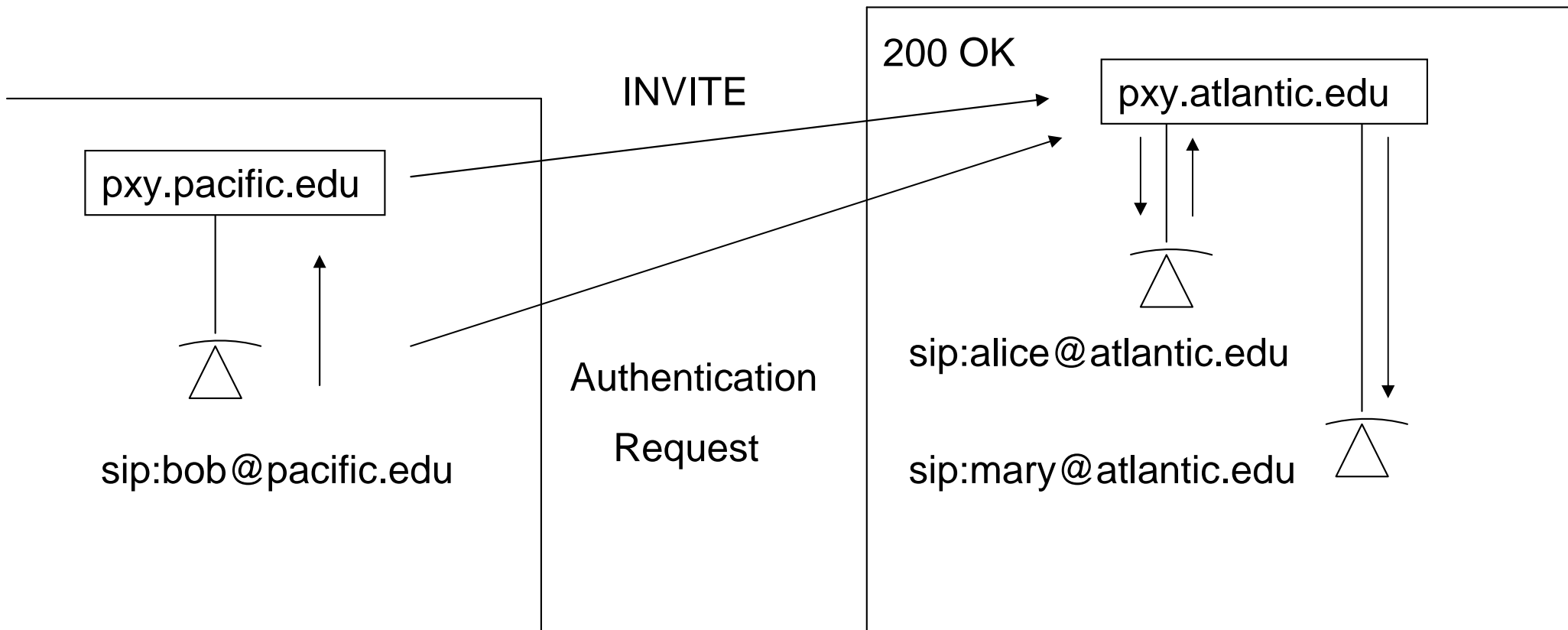


Call Flow

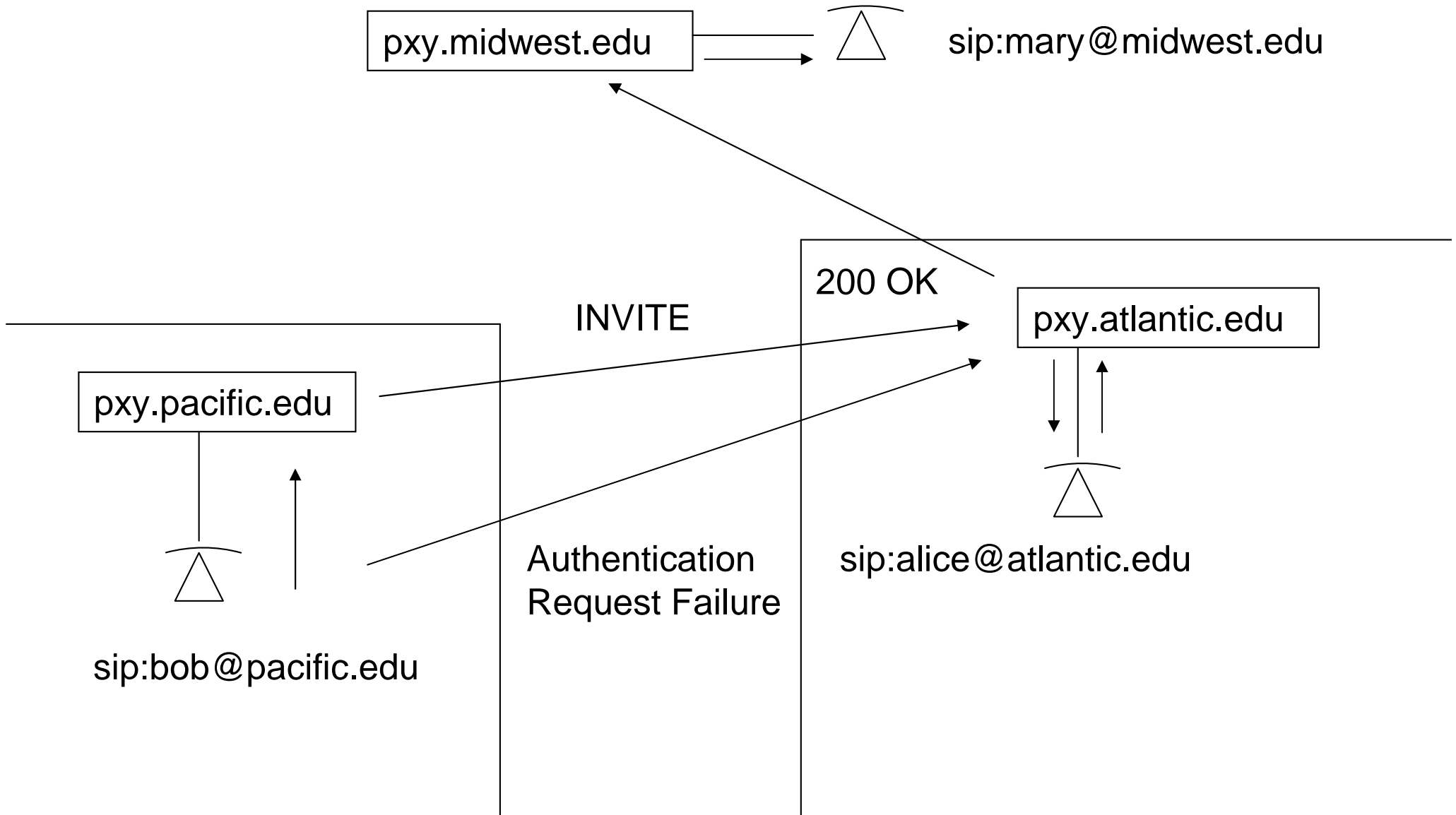


Call Flow

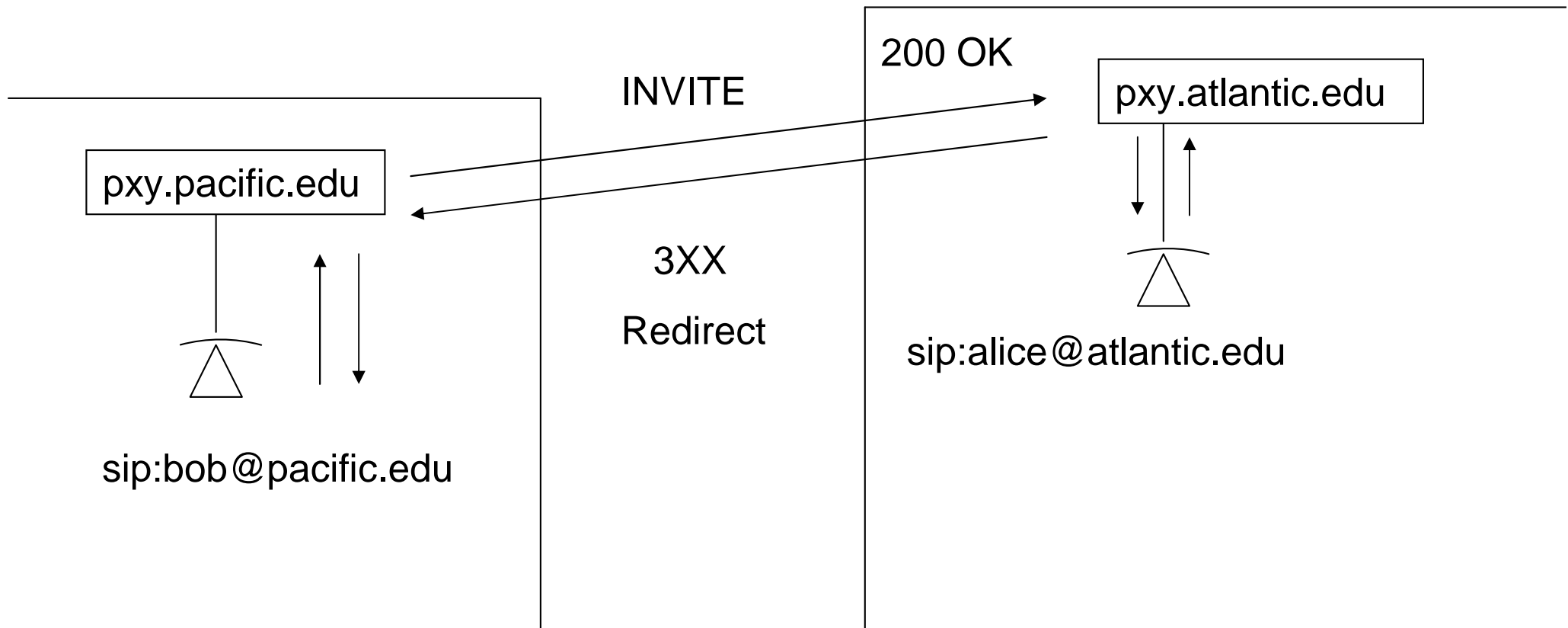
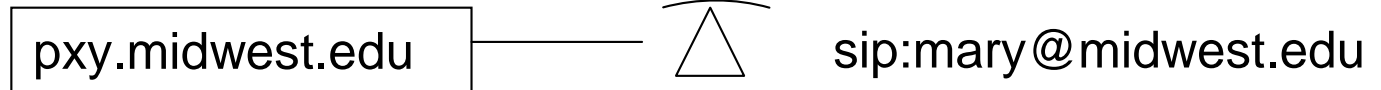
Keeping in mind that the TO: field does not change during forwarding, the authentication request will fail because the TO: field does not match the AOR of the callee. This is known as the “response identity problem.” As long as the forward stays within the original callee’s domain the callee’s proxy can handle the problem with additional code.



Call Flow



Call Flow



Call Flow

