

NAT Traversal for HIP

HIP NAT Traversal Design Team

Hannes Tschofenig

Philip Matthews

Jan Melen

Marcelo Bagnulo

Miika Komu

Problem Description

- HIP over IP does not traverse NATs
- ESP over IP may not traverse NATs
- P2P NAT traversal
 - Both peers behind NAT boxes
 - Host Identities can be used for naming the hosts in private address realms

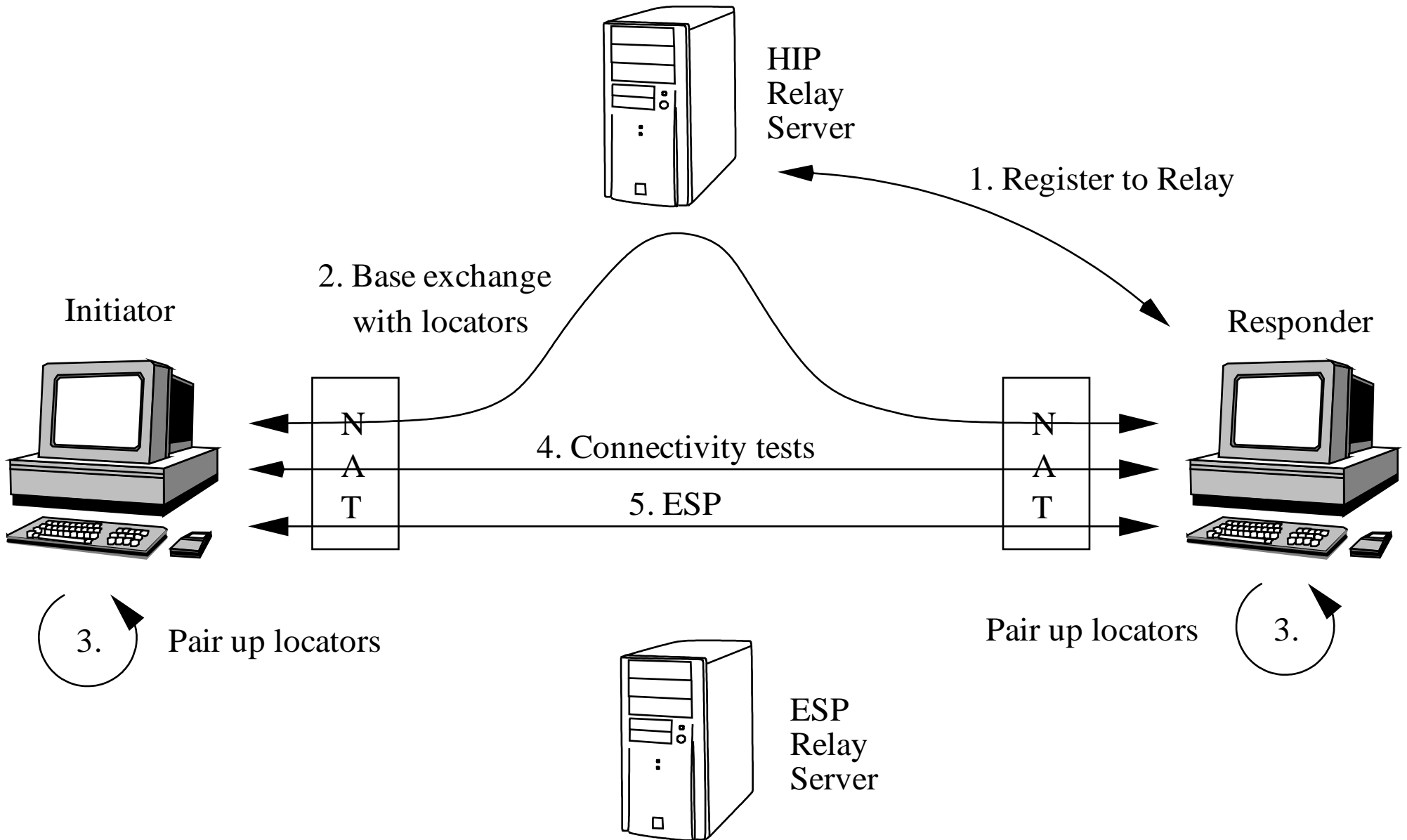
Problem Scope

- Cover the same issues as ICE
 - Candidate gathering, connectivity tests, etc
- Additional issues
 - Mobility and multihoming
- Try to find a direct path between two peers
 - Relaying of ESP still needed with some NAT boxes

Out of Scope Issues

- Compatibility with existing RVS is not top priority
- draft-ietf-hip-nat-traversal-01 is out of scope
 - Does not support ESP relays
 - Mobility support inadequate
 - Detecting if host is "behind" a NAT was a bad idea because it is not always reliable
- Fragmentation and MTU detection out of scope
 - Fragmentation problem is orthogonal to NAT traversal
- Address candidate gathering is a local issue

ICE-based Design Solution 1/2



ICE-based Design Solution 2/2

- Carrying of address candidates ("offer/answer")
 - Relayed through a forwarding middlebox (Relay)
 - TURN does not work for this
 - HIP-based Relay service will be used
- Connectivity tests
 - Single format for failure detection, NAT keepalives and connectivity tests
 - We could use STUN or HIP
 - No strong consensus yet within design team

Packet Format, Ports and Demuxing

- Control and data plane format as in [RFC3948]
 - HIP and ESP use same port (fate sharing)
 - HIP port is different from IKE
- Demux either on port or SPI (policy issue)
 - Allow different implementation techniques
 - SPI for IPsec-aware NAT boxes
 - Non-ESP dataplanes
 - Possibility to reuse TURN

STUN-based Connectivity Tests

- Base exchange with HIP, connectivity tests and keepalives using STUN
- Possibility to..
 - reuse existing STUN servers
 - reuse STUN/ICE implementations
- Requires extensions to STUN (HIT replaces password, etc) are required

HIP-based Connectivity Tests

- Single protocol for base exchange, mobility, connectivity tests and keepalives
 - Inherits security properties of HIP (public-key signatures)
- Requires new extensions to HIP
- Compatible with RFC 3948 (ESP over UDP)
- ADs of Transport and RAI areas in favour of this approach

References

1. draft-ietf-behave-rfc3489bis-13
2. draft-ietf-mmusic-ice-19
3. draft-ietf-hip-nat-traversal-02
4. draft-manyfolks-hip-sturn-01
5. draft-tschofenig-hip-ice-00
6. RFC 3949