draft-ietf-hip-nat-traversal-03

IETF71 13.3.2007

Editor: Miika Komu <miika@iki.fi>

Marcelo Bagnulo <marcelo@bagnulo.net>

Thomas Henderson <thomas.r.henderson@boeing.com>

Ari Keränen <ari.keranen@nomadiclab.com>

Philip Matthews <philip_matthews@magma.ca>

Jan Melen <jan.melen@nomadiclab.com>

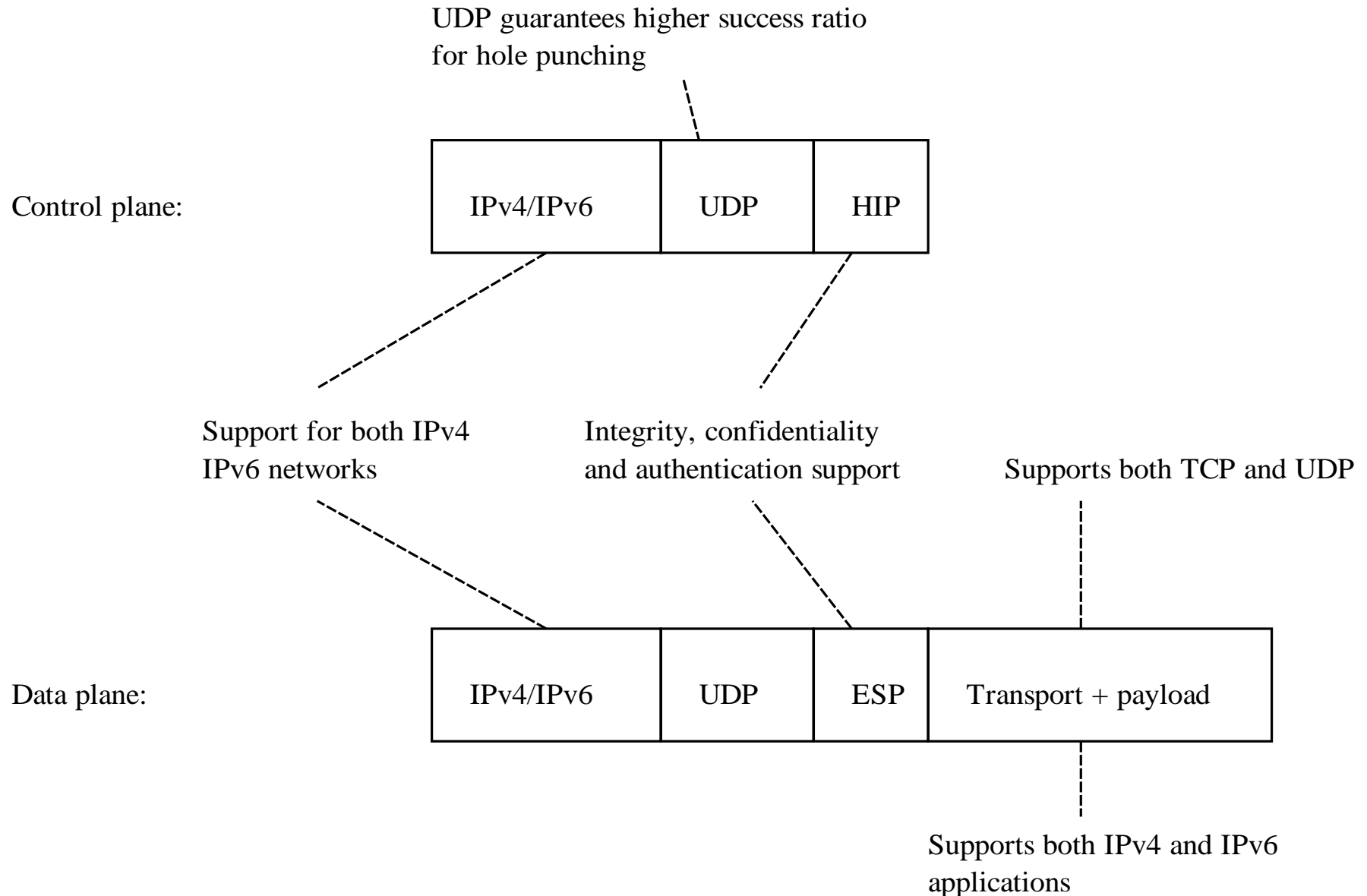Hannes Tschofenig <hannes.tschofenig@gmx.net>

Status of the Draft

- WG item

- Main change from previous version: uses STUN and TURN instead of HIP extensions

- More authors for the draft
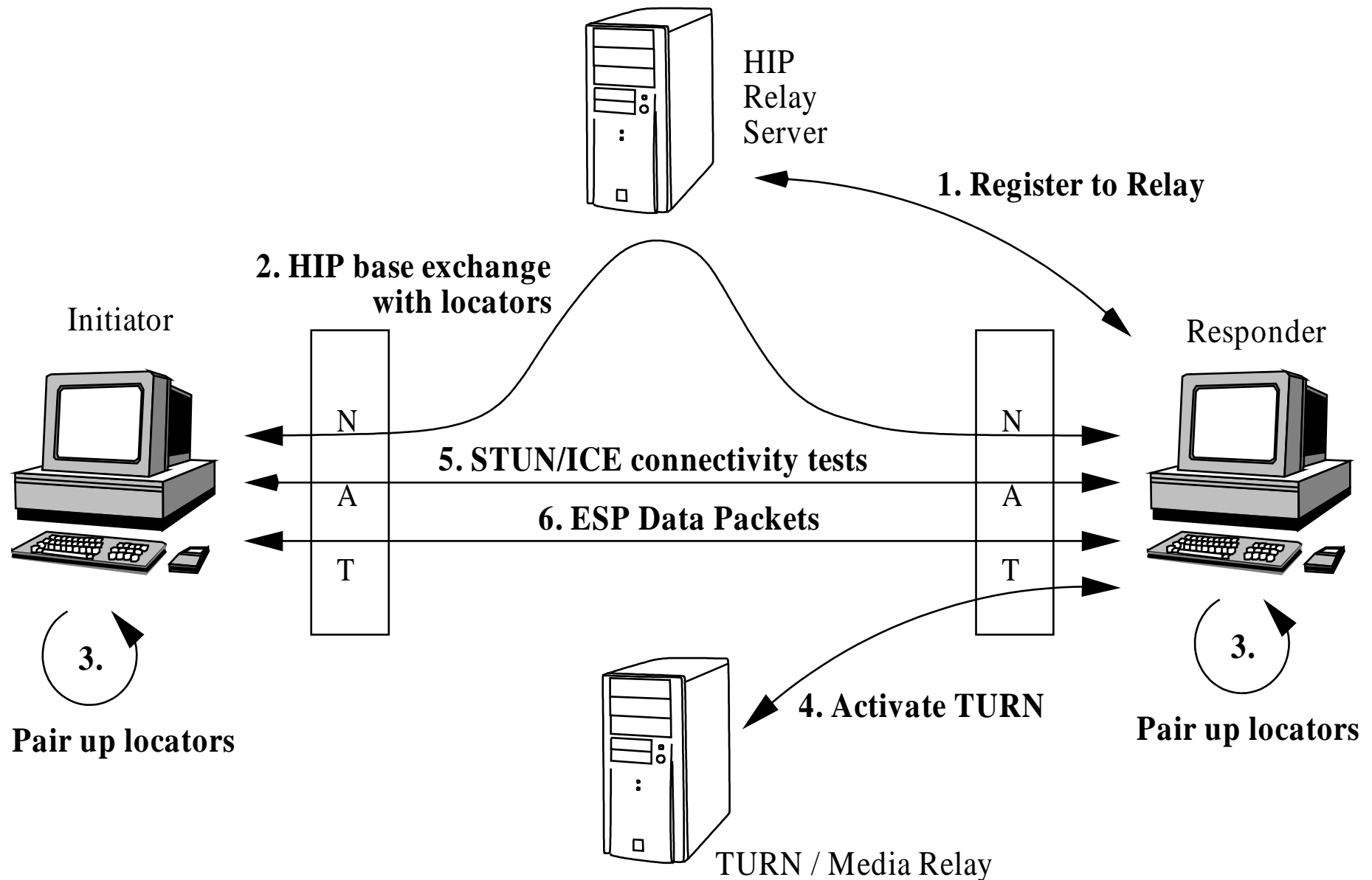 - Old authors acknowledged in contributors section

NAT Traversal using HIP

- Identity/locator split makes it possible to globally name hosts within private address realms

- Try to establish direct communications path between the end-hosts; fallback to relaying

- Both client and server applications can be located behind NAT devices

- Works also with (unmodified) legacy applications

- Reuses ICE/STUN protocol

Efficient, Secure and Universal Solution

UDP guarantees higher success ratio
for hole punching

Control plane:

IPv4/IPv6	UDP	HIP

Support for both IPv4
IPv6 networks

Integrity, confidentiality
and authentication support

Supports both TCP and UDP

Data plane:

IPv4/IPv6	UDP	ESP	Transport + payload

Supports both IPv4 and IPv6
applications

How Does It Work?

HIP
Relay
Server

1. Register to Relay

Initiator

Responder

2. HIP base exchange with locators

| N |
| A |
| T |

| N |
| A |
| T |

5. STUN/ICE connectivity tests

6. ESP Data Packets

3.

3.

Pair up locators

Pair up locators

4. Activate TURN

TURN / Media Relay

NAT Transform Parameter

- Consider a server (Responder) with a fixed, publicly reachable address

  – No need to run ICE connectivity checks

  – UDP encapsulation for ESP is enough

- Responder omits NAT transform parameter from the R1 packet

  – Initiator and Responder omit connectivity checks and use UDP encapsulation for ESP

- Notice: NAT transform is not "ICE lite"

STUN and ESP Demux Issue

- Demux issue: STUN and ESP messages arriving at the same UDP port (see RFC3948 and RFC3489bis)

- Alternative solutions:

  – Constrain SPI namespace in HIP daemon

  – STUN awareness in IPsec

  – 32-bits of zeroes in the beginning of STUN header

    - For all STUN packets

    - Only for HIP connectivity tests

Implementation Activities

- Ericsson implemented their own STUN/ICE implementation

- InfraHIP/HIPL in HIIT integrating to PJSIP implementation

- OpenHIP starting up implementation work

Design Team Goals for IETF72

- New version of NAT base draft

  - Integrate with draft-rosenberg-mmusic-ice-nonsip

  - Solve demuxing issues

  - More detailed descriptions for STUN, ICE and TURN usage

- New draft on mobility and multihoming for the next IETF

References

- http://www.ietf.org/internet-drafts/draft-ietf-hip-nat-traversal-03.txt

- ftp://ftp.rfc-editor.org/in-notes/rfc3948.txt

- http://www.ietf.org/internet-drafts/draft-ietf-mmusic-ice-19.txt

- http://www.ietf.org/internet-drafts/draft-ietf-behave-rfc3489bis-15.txt

- http://www.ietf.org/internet-drafts/draft-rosenberg-mmusic-ice-nonsip-00.txt