On Host Identity Protocol

Miika Komu <miika@iki.fi>
Data Communications Software Group
Dep. of Computer Science and Engineering
School of Science
Aalto University

17.10.2011

Table of Contents

- Introduction
- Naming and Layering
- Control Plane
- Data Plane

Introduction

Motivation

- Why do I need screen for IRC session?
- Why Youtube video stops when I switch from 3G to WLAN?
- Why do I need to pinhole my NAT box to reach my home server?
- Why do I use SSH instead of telnet?
- Why do we have NFSv4?
- Why do we passwords for WLAN?

Identity-Locator Split

- Identity-locator split separates the “who” from “where”
  - Application and transport layer sees the “who”
  - Network layer sees “where”
- Benefits of id-loc split
  - Realized e.g. in HIP, LISP, SHIM6
  - Isolates upper layers from network changes
  - Useful for mobile devices
- Disadvantage: indirection introduces complexity

Benefits of Host Identity Protocol

- Protects and/or authenticates application data
  - IPsec or S-RTP can be used
- IPv4 applications can talk to IPv6 apps
- Mobility and multihoming for transport layer
  - Works in IPv4 and IPv6 networks
- End-to-end NAT traversal
  - Connect to home server without pinholing
- Backwards compatible
  - TCP, UDP, IPv4, IPv6, ICMP(v6)

Drawbacks of Host Identity Protocol

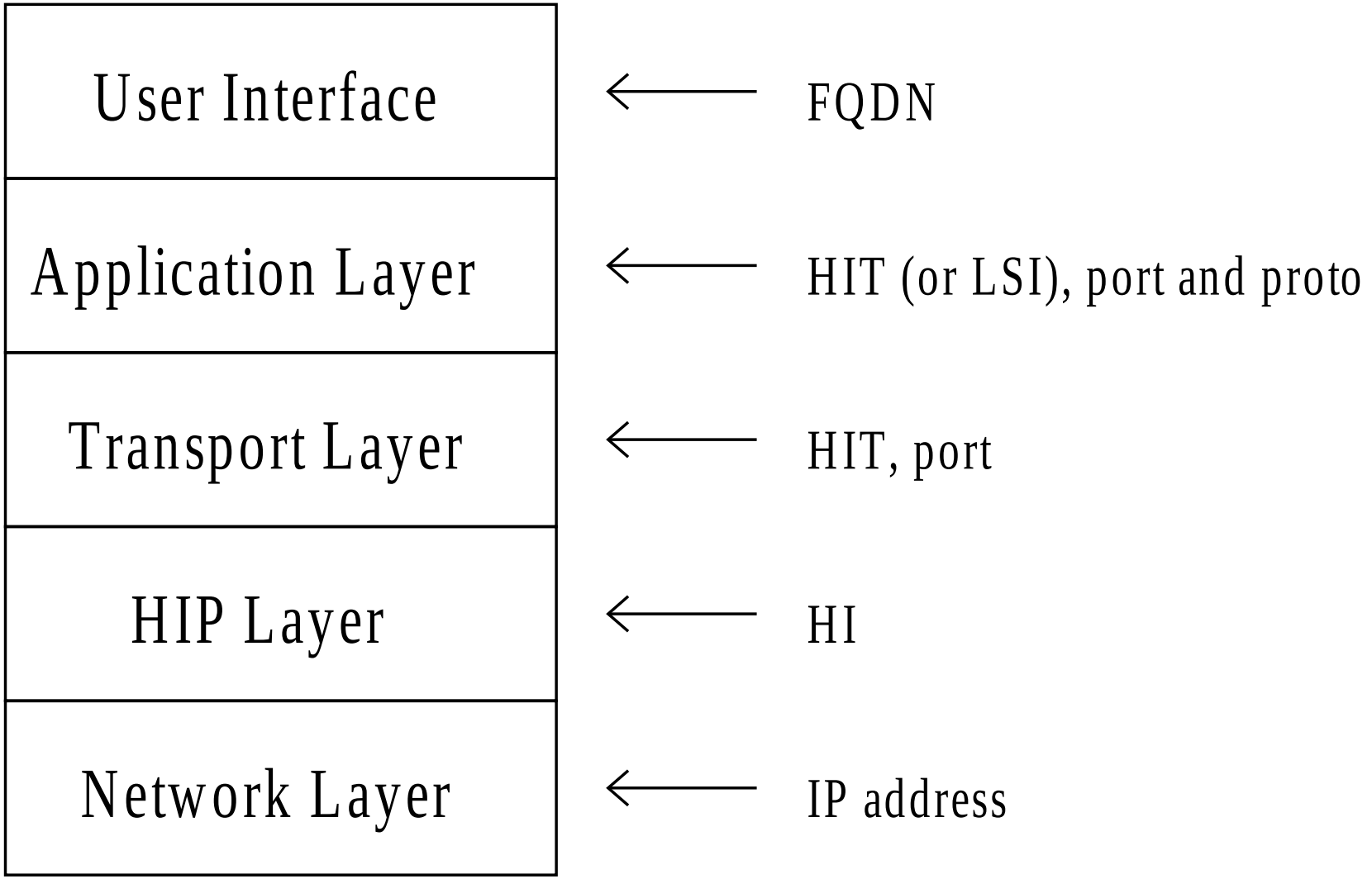
- Additional complexity
  - New layer of indirection
  - New namespace to manage (e.g. reverse look up)
- Security is transparent
  - How does application or user know when connection is secured?
- TCP is still the bottleneck
  - Suspending of laptop for hours disconnects TCP
- Is it too late?
  - Generic architecture
  - Specific solutions exist (MobileIP, VPN, SSH, etc)

HIP Standardization

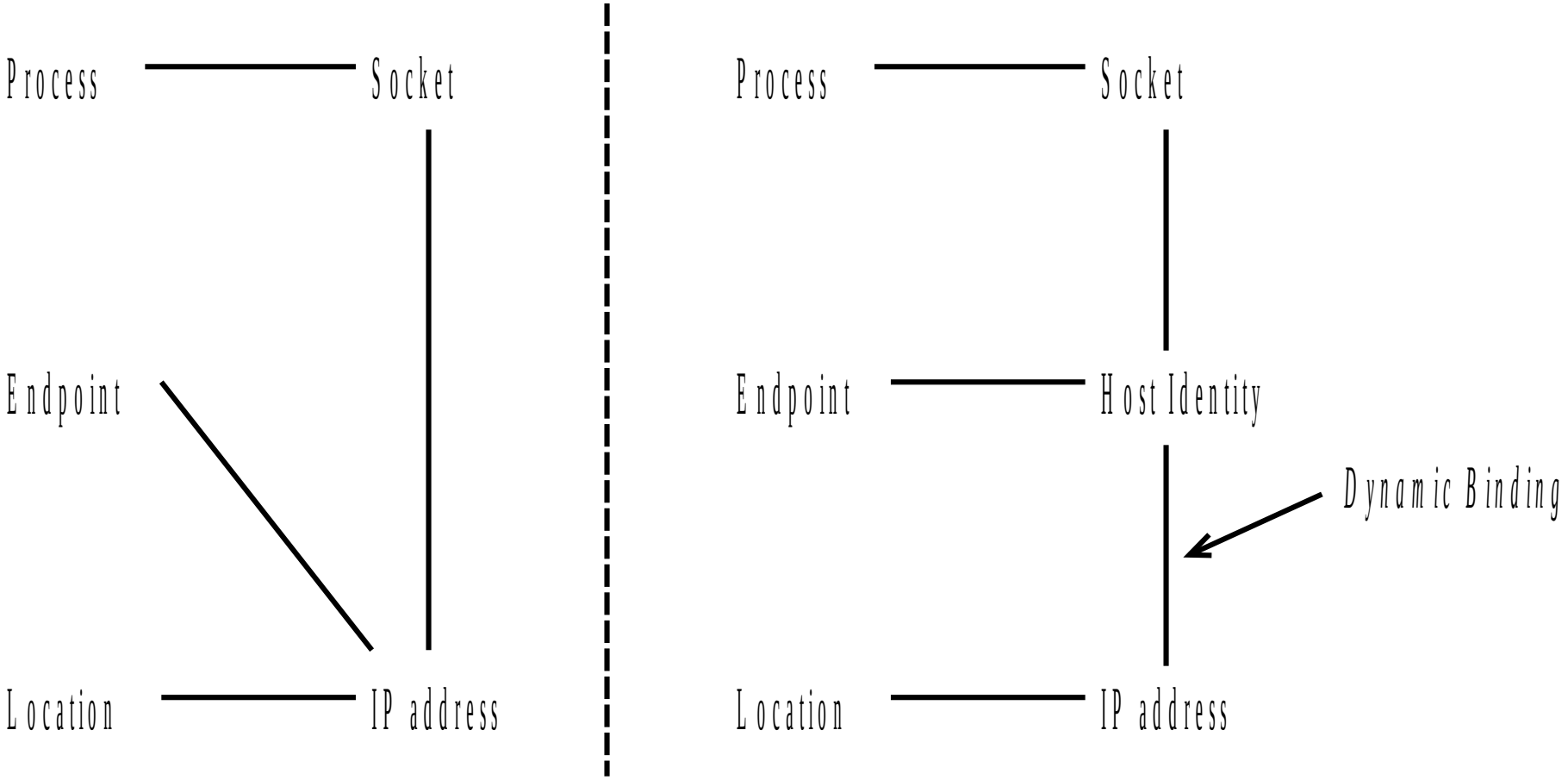
- Work split to two working groups
  - Internet Engineering Task Force (IETF)
  - Internet Research Task Force (IRTF)
- RFC5201-5201, RFC4423, RFC5338
  - Experimental track
  - Moving to standards track (see “bis” drafts)
- Major change in RFC5201
  - Cryptoagility

Naming and Layering

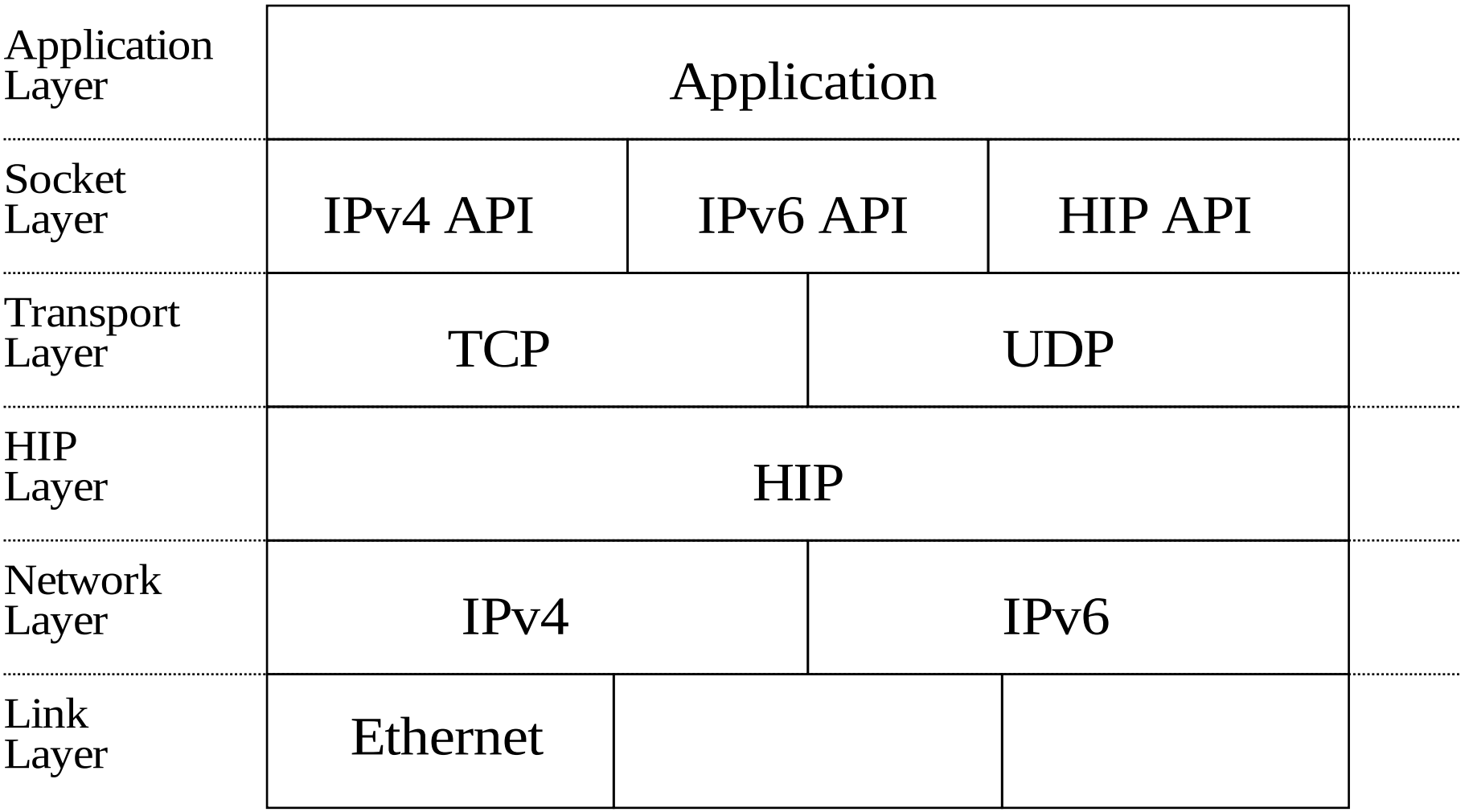
Layering in Naming in HIP



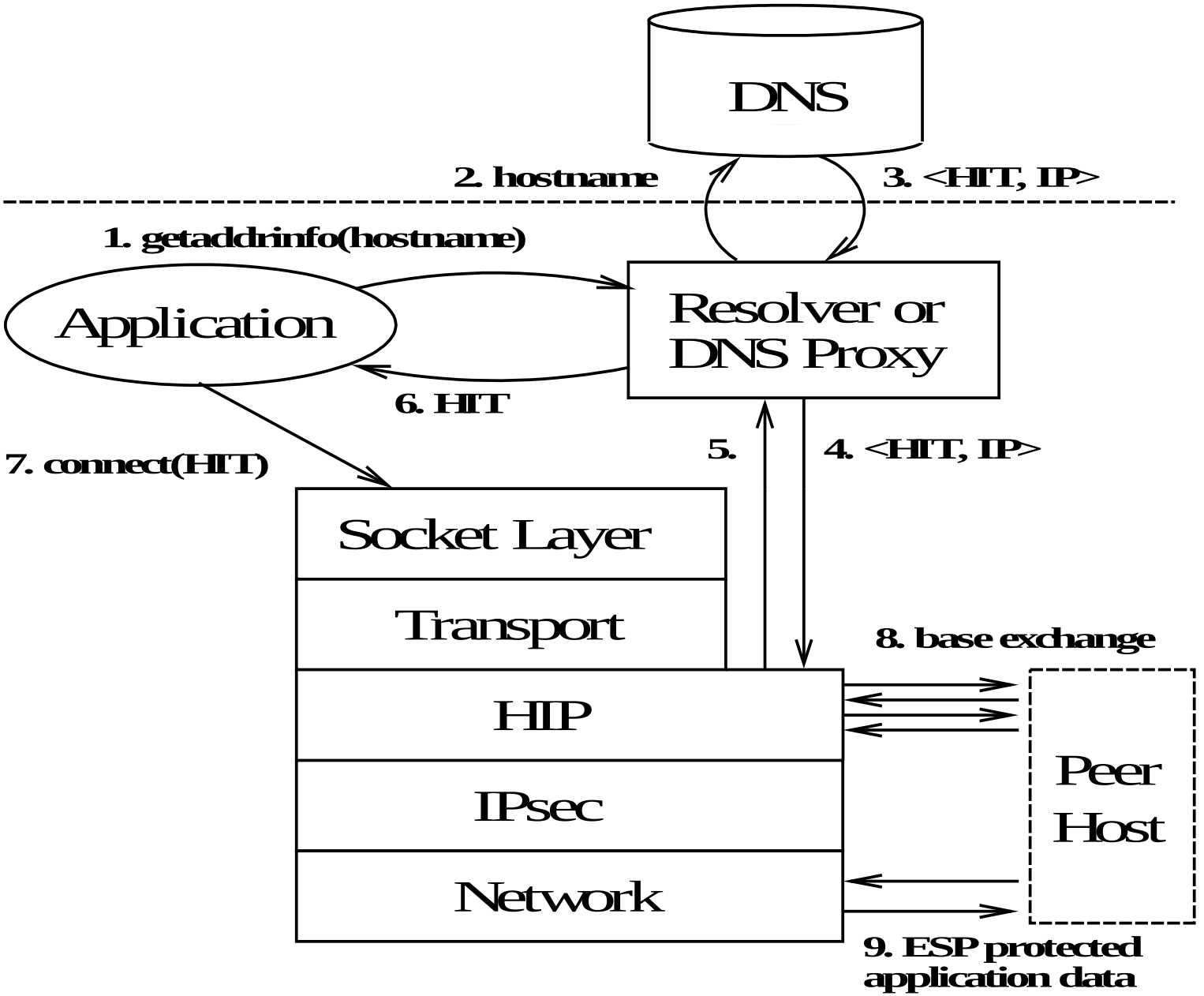
Non-HIP vs. HIP Socket Bindings



APIs


Application Layer
Application
Socket Layer
IPv4 API
IPv6 API
HIP API
Transport Layer
TCP
UDP
HIP Layer
HIP
Network Layer
IPv4
IPv6
Link Layer
Ethernet

Client-Side Name Look Up Example

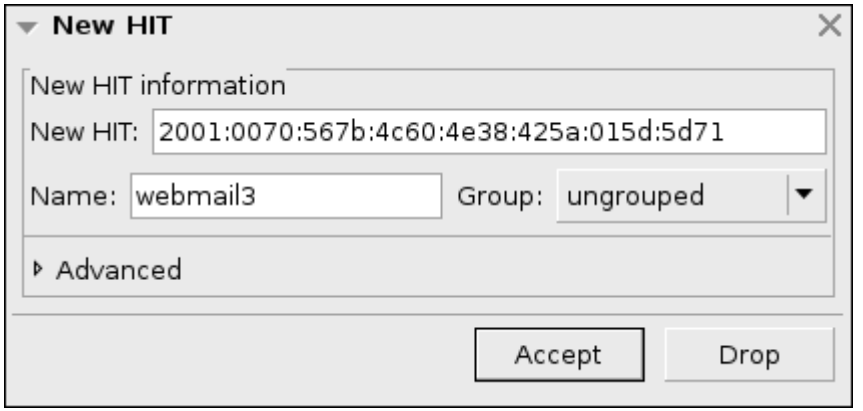


Implemeting Name Translation

- #1 LD_PRELOAD getaddrinfo()
- #2 Local DNS Proxy
  - #2a Snoop DNS requests with iptables
  - #2b Substitute nameserver in /etc/resolv.conf
- #3 No changes to DNS interaction
  - Implement lower in the stack (opp. mode)
  - Implemented in a router (HIP proxy)

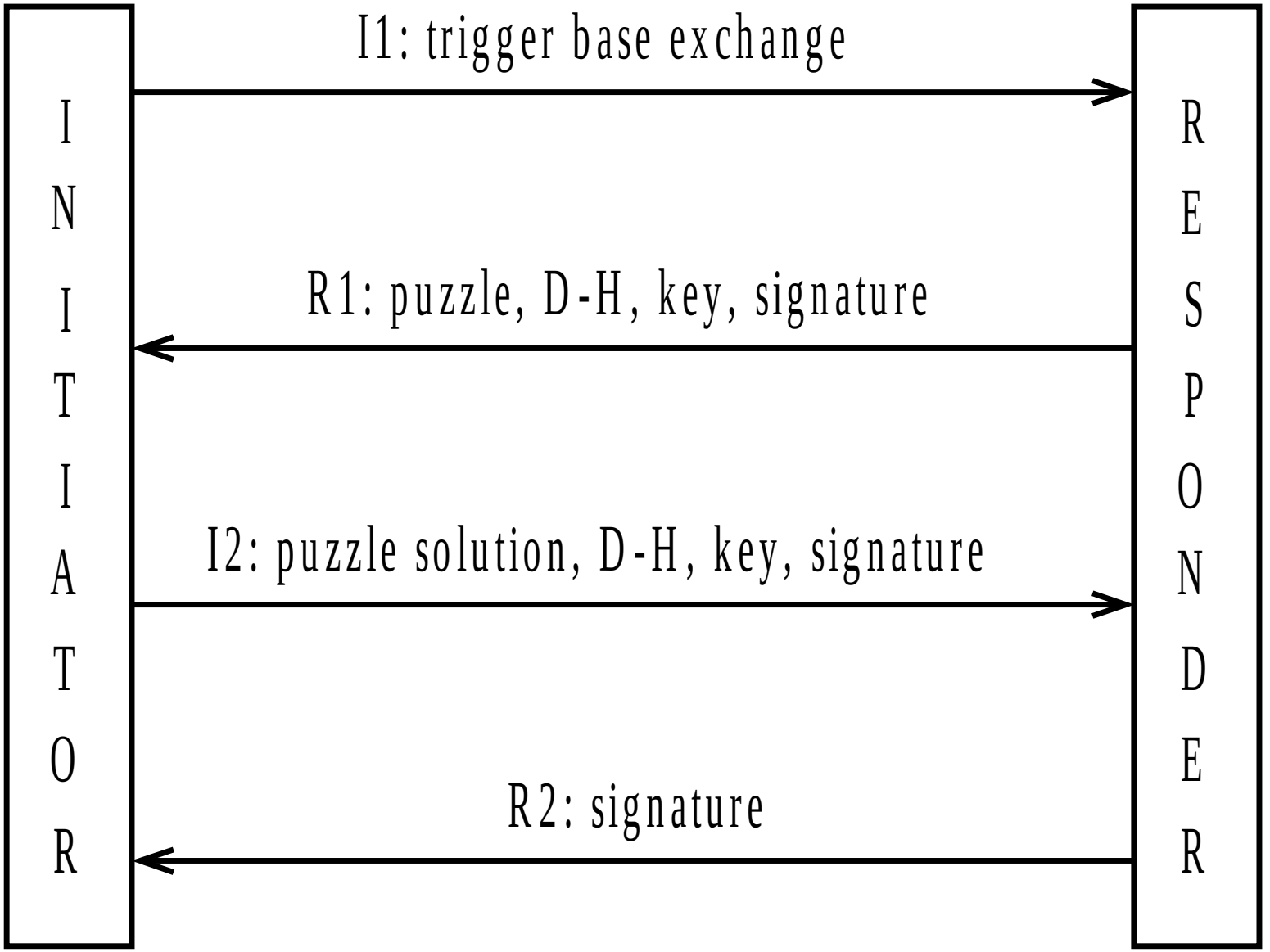
GUI / End-user Firewall

- An optional GUI can be used for managing all collecting HITs
  - HIP is visible to the user (but not application)
- The GUI can prompt the user to accept incoming or outgoing connections
  - Similar to end-user firewalls
- Screenshot from HIPL



Control Plane

The Base Exchange

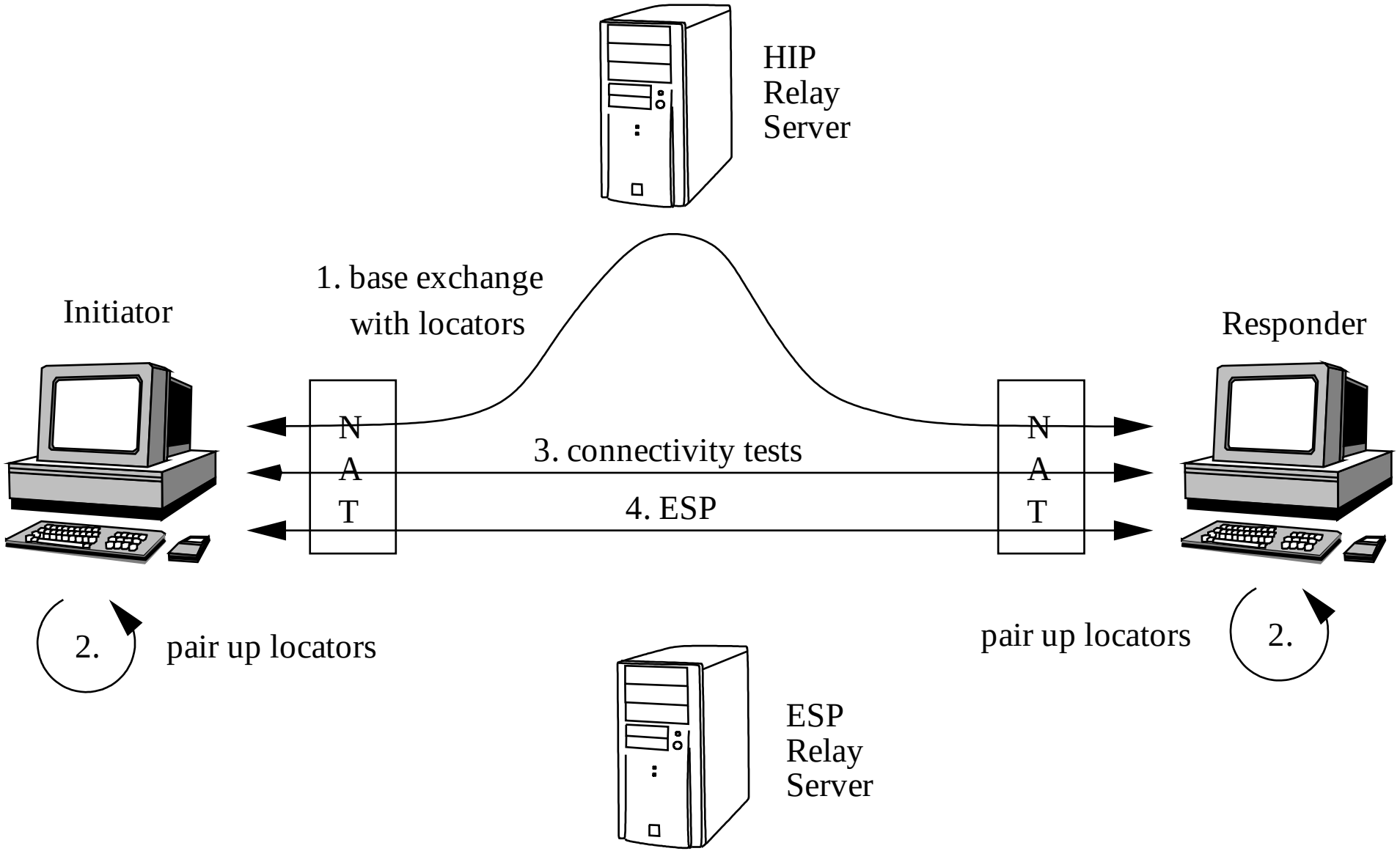


Opportunistic Mode

- I1 sent to an unknown HIT
- Less secure than normal HIP
  - “Leap of faith” (like in SSH)
  - Subsequent connections can be cached
- Does not require public keys in DNS
- Convenient for
  - Service registration
  - HIP-aware applications
  - HIP “anycast”
- Problematic for NAT traversal

Handover (UPDATE)

Native NAT Traversal using HIP



Native NAT Traversal vs. Teredo

- Teredo pros
  - Plenty of free Teredo servers available
  - No changes to the HIP implementation
- Teredo cons
  - Servers that do “full relay” cost
  - Teredo requires an IPv6 application (without HIP)
  - In windows, a socket option in the app
  - Patented by Microsoft

IPv4-IPv6 Interoperability

- At the network layer
  - Identity-locator split hides the underlying access technology from applications
  - Cross-family handovers from IPv4 to IPv6 and vice versa are trivial (not available in MobileIP)
- At the application layer
  - HITs for applications requesting IPv6
  - LSIs for applications requesting IPv4
  - IPv4 apps can talk with IPv6 apps!

Data Plane

HIP and IPsec

- Currently BEET mode ESP is the default
  - HIP supports negotiating others (e.g S-RTP)
  - Implemented in the Linux and BSD kernel
  - Linux and Windows can use userspace impl.
- Public-key protected data plane (hiccups)
  - Avoids the base exchange and use of IPsec
  - Data protected with public-key signatures
  - Switch to IPsec by sending an R1

HIP Proxy

- Proxy support on an intermediary host
  - No changes at client and/or server side
  - Similar to VPN gateways
- Can be implemented on different layers
  - ARP level proxy (see Tofino security product)
  - IP level proxy (supported by several HIP s/w)
  - HTTP proxy (HIP between the client and proxy)
- Can use different naming or routing methods
  - Normal or opportunistic mode
  - Normal IP routing or overlays (e.g. Tofino)

Cool HIP Extensions

- HIP is too fat?
  - RFID version of HIP
  - HIP Diet Exchange
- PISA Wifi Sharing
  - Authenticates people sharing WLANs with HIP
- Mobile proxy
  - Handover delegation to a middlebox
- HIP-based Virtual Private LAN service
  - Connects transparently separate networks

Questions?

Miika Komu <miika@iki.fi>

Documentation and software for HIPL:
http://hipl.hiit.fi/

Interested in contributing? Contact us:
https://launchpad.net/hipl

Other two HIP implementations:
http://www.openhip.org/
http://www.hip4inter.net/

Literature 1/3

- RFC5201-5206
- RFC4423, Host Identity Protocol Architecture, Moskowitz et al, May 2006
- RFC5338: Using the Host Identity Protocol with Legacy Applications, Henderson et al, Sep 2008
- Integrating Mobility, Multi-homing and Security in a HIP way, Pekka Nikander et al, Feb 2003
- Using DNS as an Access Protocol for Mapping Identifiers to Locators, Ponomarev et al, November 2007
- RCF6317: Basic Socket Interface Extensions to Host Identity Protocol, Komu et al, Jul 2011

Literature 2/3

- Overview and Comparison Criteria for Host Identity Protocol and Related Technologies, Koponen et al, Feb 2005
- Leap-of-faith security is Enough for IP mobility, Komu et al, Jan 2009
- HIP-based Virtual Private LAN, Henderson et al, Sep 2011
- Enterprise Network Packet Filtering for Mobile Cryptographic Identities, Janne Lindqvist et al, June 2007
- Native NAT Traversal Mode for HIP, Keränen et al, Jan 2011
- Host Identity Protocol (HIP), Connectivity, Mobility, Multihoming, Security and Privacy over IPv4 and IPv6 Networks, Nikander et al, 2010

Literature 3/3

- Secure and Efficient IPv4/IPv6 Handovers using Host-based Identifier-Locator Split, Varjonen et al, September 2009
- RFC6078: HIP Immediate Carriage and Conveyance of Upper-Layer Protocol Signaling (hiccups), Nikander et al, Jan 2011
- Host Identity Protocol Proxy, Salmela et al, Nov 2007
- Backwards Compatibility Experimentation with Host Identity Protocol and Legacy Software and Networks, master thesis, Finez, Dec 2008
- HIP Support for RFIDs, Urien et al, Nov 2010
- HIP Diet Exchange, Moskowitz, Jan 2011
- HIP-based Mobile Proxy, Melen et al, Aug 2009