Host Identity Protocol
InfraHIP Experimentation

Miika Komu <miika@iki.fi>
Helsinki Institute for Information Technology
26.11.2007

Host Identity Protocol for Linux (HIPL)

- Linux-oriented, open source implementation of HIP
  - Nokia Tablets are also supported
  - Symbian support work-in-progress
- Supports several protocol extensions
  - Base exchange, mobility, RVS, different APIs, etc
  - Includes kernel-based BEET IPsec mode
- Two other active projects at Ericsson and Boeing

HIPL Implementation History 1/3

- Started as a student project in 2001 (four students)
- Continued 2002 in HIIT in Fuego-Core, InfraHIP and InfraHIP II projects by two of the students
- Implementation efforts and interoperability tests detailed provided feedback to the IETF drafts
  - Interoperability tests with IndraNet, Ericsson and Boeing

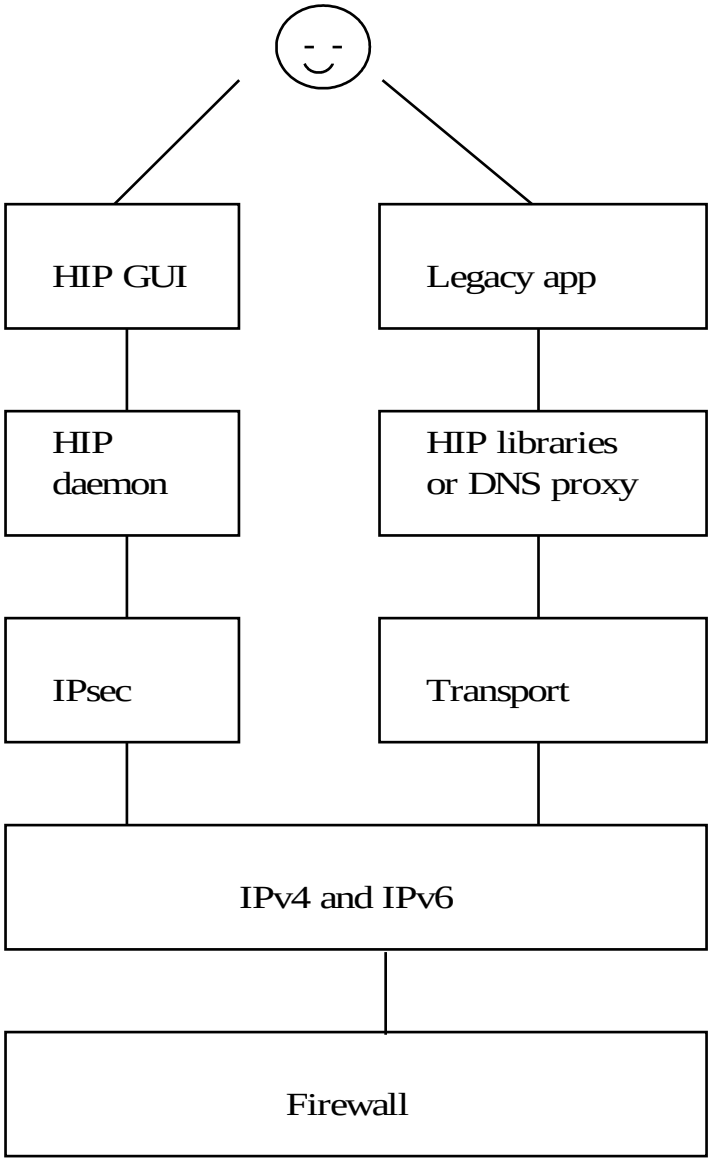
HIPL Implementation History 2/3

- Started as kernelspace-oriented implementation
  - Asymmetric crypto was done using a userspace daemon
  - BEET was implemented as a hack to Linux IPsec
- Ported asymmetric crypto to the linux kernel
  - (Nowadays there is RSA support in linux kernel)
- Moved everything (except BEET) to userspace
  - Linux networking maintainers rejected our huge kernel patch

HIPL Implementation History 3/3

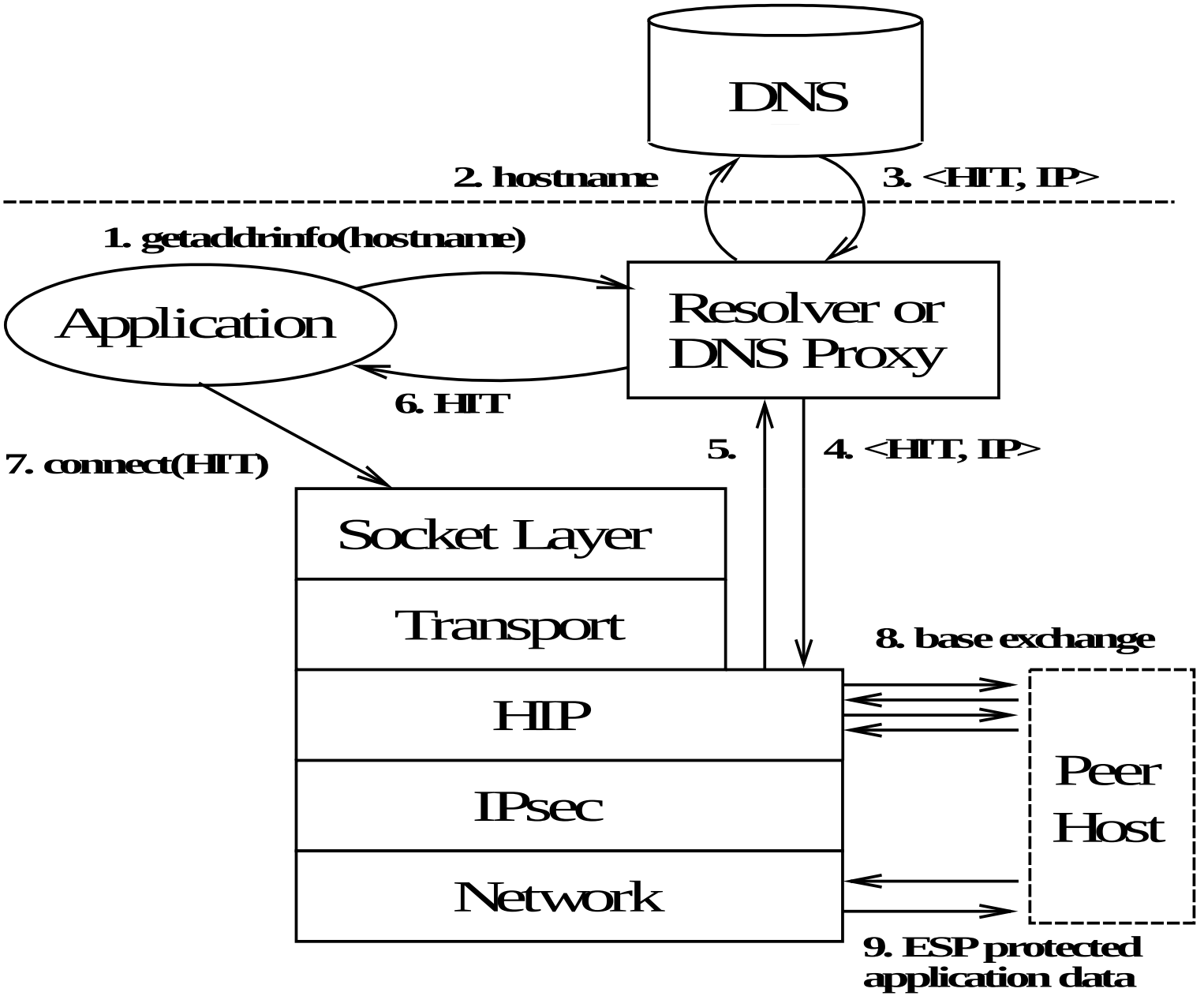
- Half of the BEET patch was accepted to the official 2.6.19 linux kernel
  - The rest of the patches received multiple comments which we have been fixing
  - 2.6.24 will have an unified IPv4/IPv6 handling for IPsec – need to revise BEET patch again
- HIP implementation has been moving from an research prototype towards an open source product

HIPL Implementation Architecture



- GUI notifies user for new host associations
- HIP daemon implements HIP control plane and controls IPsec
- Libraries / DNS proxy look-up HITs and convert HITs to IP addresses
- Both GUI and firewall can block connections

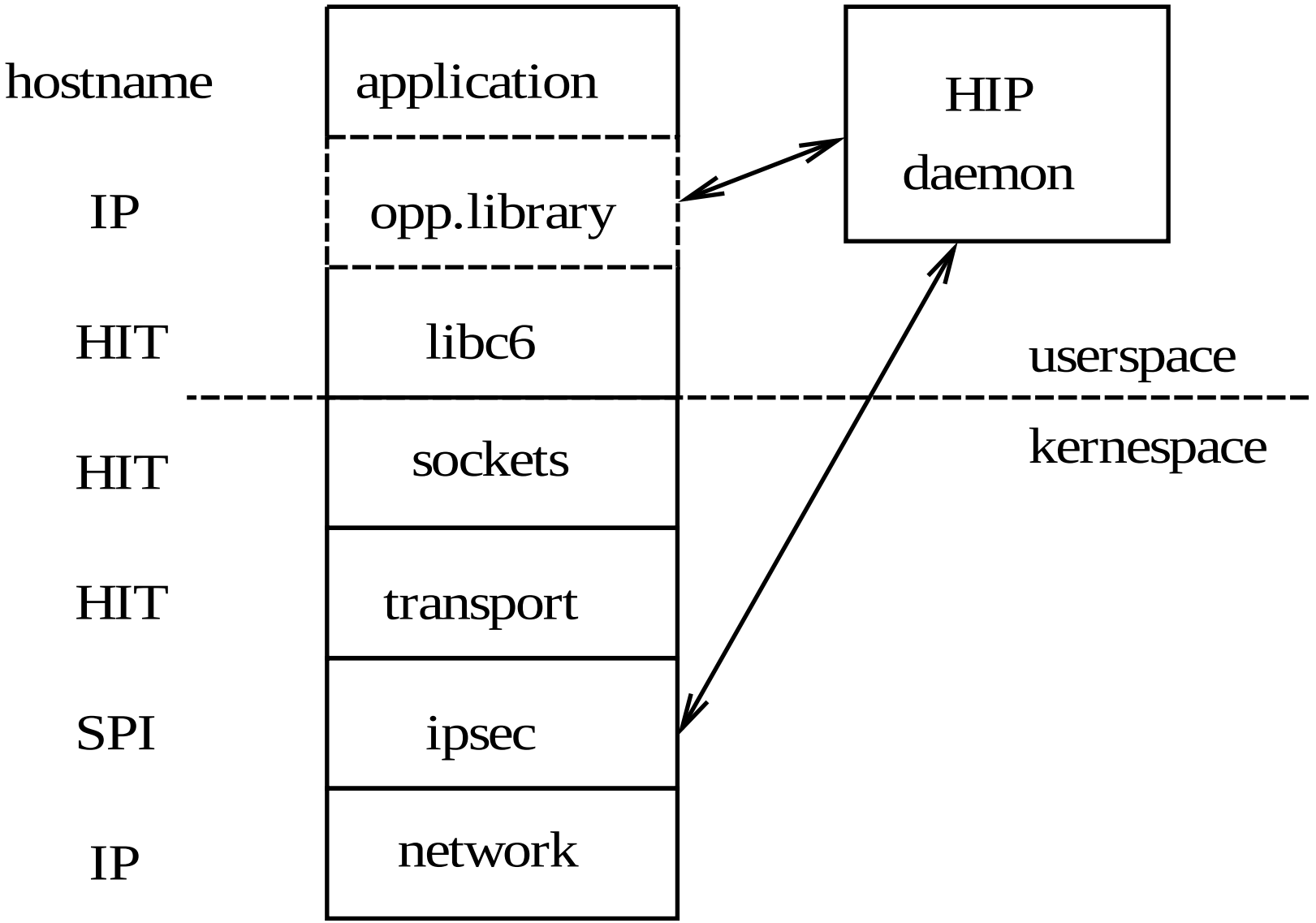
HIP-based Connection Example



Opportunistic Mode 1/3

- How to support HIP without (DNS) look-up infrastructure support in early HIP deployments?
  - Opportunistic mode establishes a connection to an unknown HIT
- What id to use in connect(id), sendto(id) calls?
  - Alternative 1: “pseudo-HIT”
  - Alternative 2: IP address (implemented)
  - Alternative 3: wildcard (standardized)

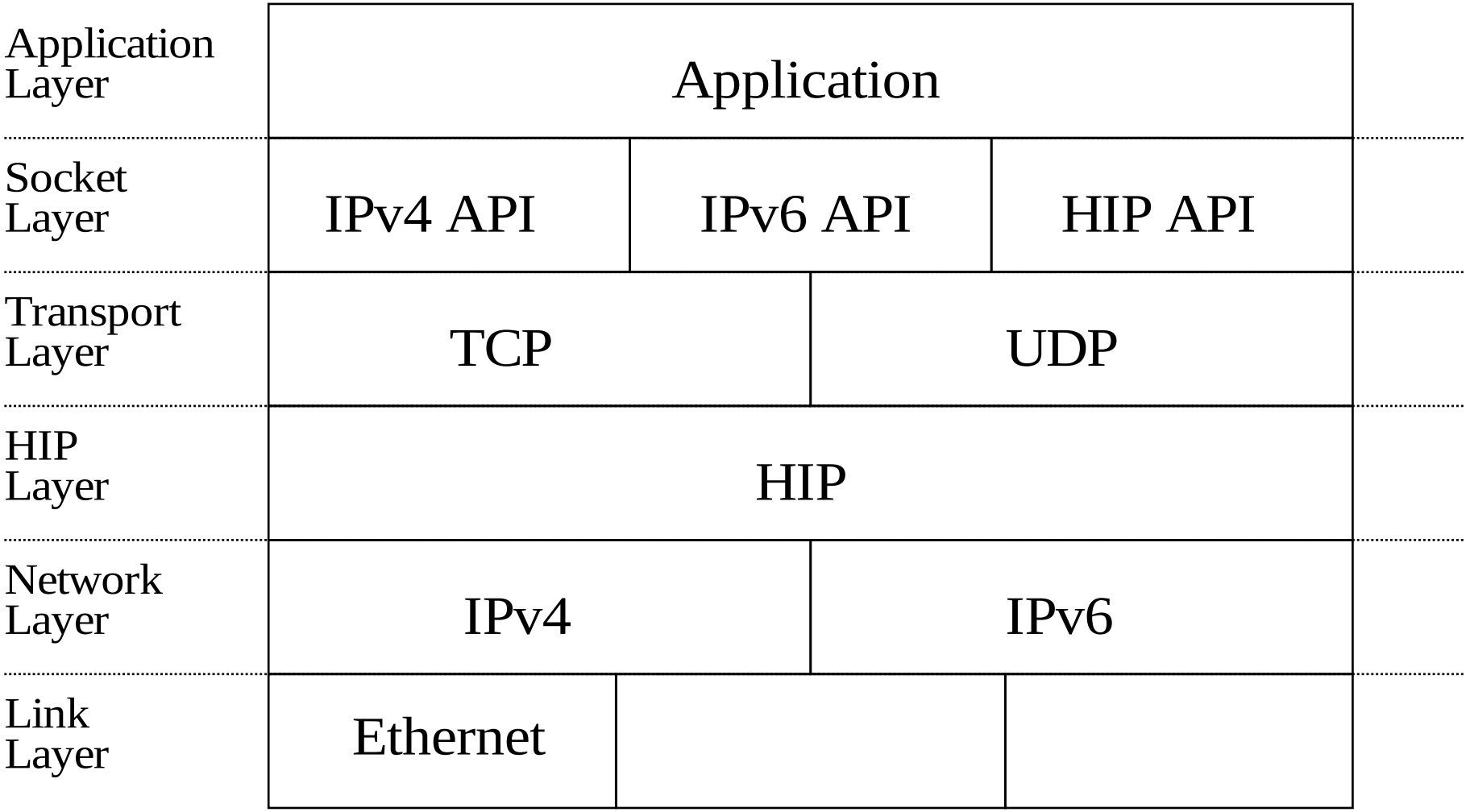
Opportunistic Mode 2/3



Opportunistic Mode 3/3

- Opportunistic mode hack: I1 is a TCP option
- Benefit: faster fallback to TCP/IP when peer does not supports HIP
- Drawback: works only for TCP, not UDP
- Implementation is work in progress

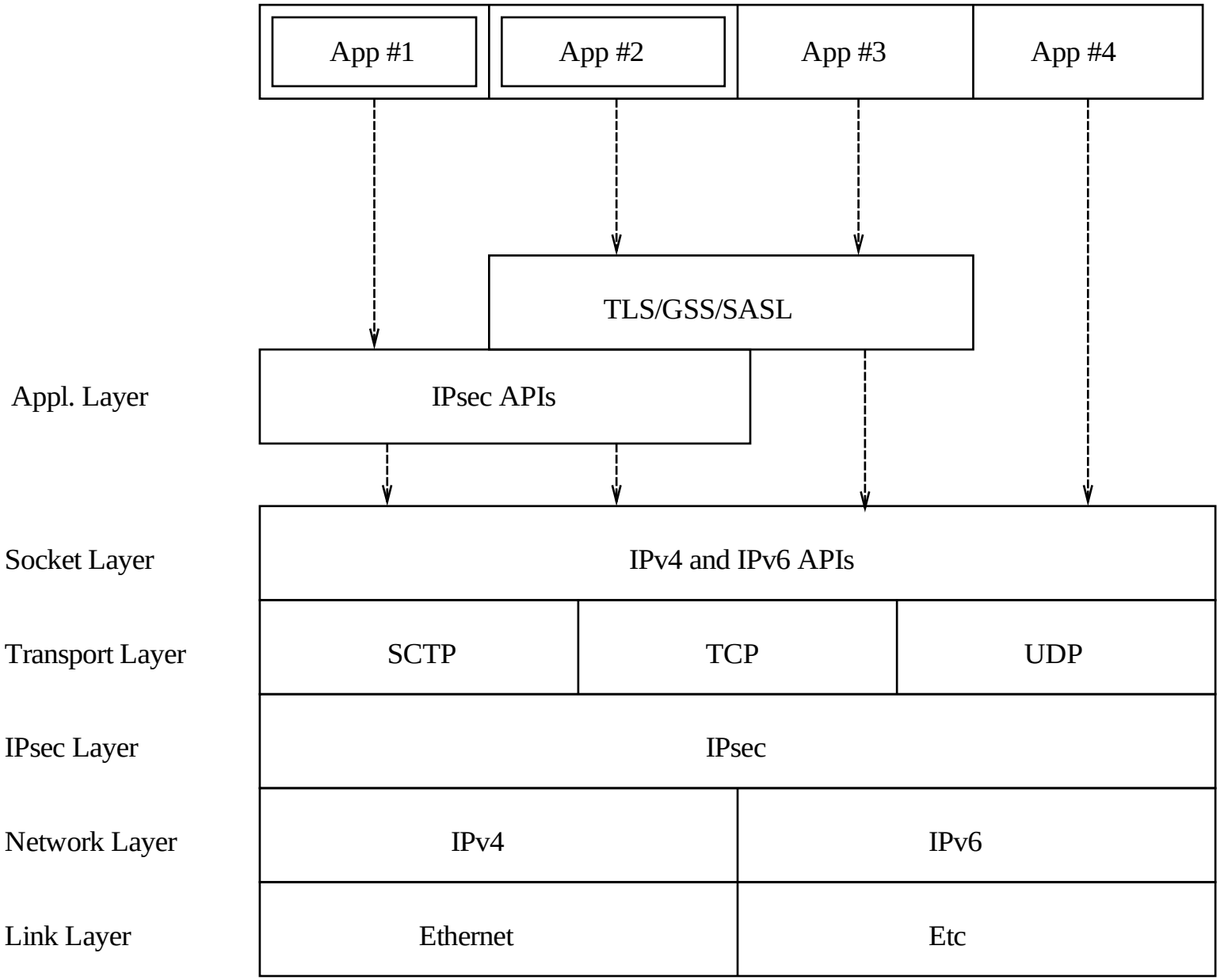
Native APIs for HIP



TLS Differences to IPsec

- TLS has wider deployment (HTTPS)
- TLS-over-TCP passes through NAT boxes
- TLS does protect the TCP port numbers
- TLS-over-TCP has automatic MTU discovery
- TLS-over-TCP is more prone to e.g. RST attacks
- DTLS works with UDP
- TLS requires to modify the application
  - Both a burden and also the key to TLS success?

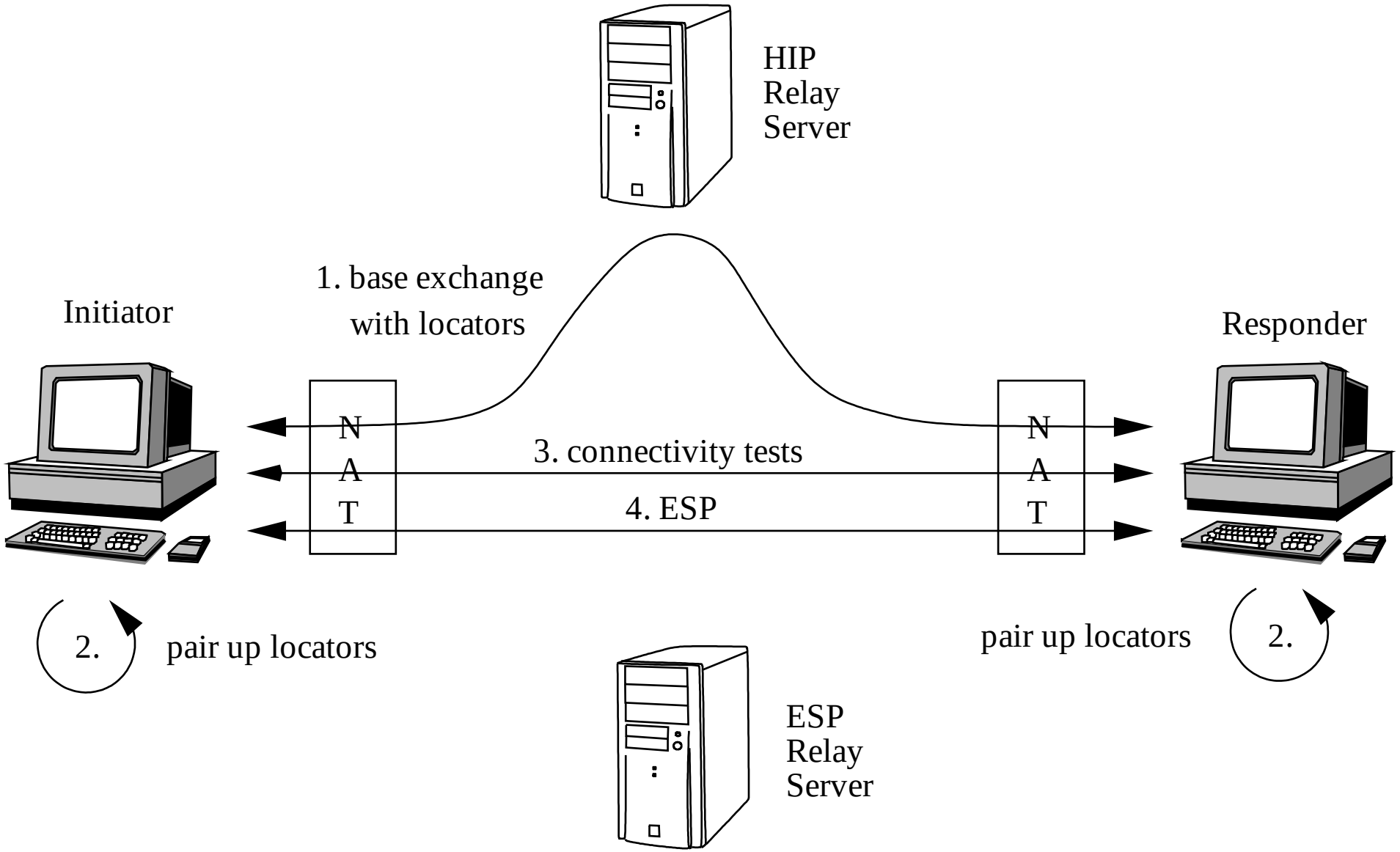
BTNS APIs


App #1
App #2
App #3
App #4
TLS/GSS/SASL
Appl. Layer
IPsec APIs
Socket Layer
IPv4 and IPv6 APIs
Transport Layer
SCTP
TCP
UDP
IPsec Layer
IPsec
Network Layer
IPv4
IPv6
Link Layer
Ethernet
Etc

DNS vs. OpenDHT

- DNS is quite rigid and difficult to configure
- Is there any alternative to DNS?
- OpenDHT/Bamboo is more flexible and open
- Problems in Bamboo:
  - Unstable and unmaintained
  - Performance problems
- DNS seems to be a better long-term alternative

HIP NAT Traversal



Protocol State in HIP

- Base exchange (mirrored state machine)
  - Initiator has to create state
  - R1 packets are stateless (or fixed state)
  - RVS and NAT relay are stateless towards Initiator
  - Firewalls and other HIP-aware middleboxes may add nonces to the HIP control messages
- Mobility updates (asymmetric state machine)
  - Mobile node assumes the address of corresponder works
  - Corresponding node creates state and verifies

Mobility Management

- Locators in base exchange
- Interfamily handovers
- Handovers with long disconnectivity create problems with TCP timeouts
  - TCP user timeout option
- Simultaneous multiaccess
  - Which outbound security association to use?

Misc Implementation Fun

- Retransmissions
  - Different mechanism for base exhange and update
  - Choosing optimal retransmission timeout can be tricky (slow ADSL lines, slow WLAN authentication)
- HIP loopback
- Broadcasting of I1s
- Simultaneous initiators
- Userspace IPsec

Questions?

Miika Komu <miika@iki.fi>
http://infrahip.hiit.fi/

References 1/2

- RFC4423, Host Identity Protocol Architecture, Robert Moskowitz et al, May 2006
- Host Identity Protocol, Robert Moskowitz et al, October 2007, work in progress
- End-host Mobility and Multihoming with Host Identity Protocol, Thomas Henderson, March 2007, work in progress
- Using the Host Identity Protocol with Legacy Applications, Thomas Henderson et al, Nov 2007, work in progress
- Native Application Programming Interfaces for Host Identity Protocol, Miika Komu, Nov 2007, work in progress

References 2/2

- Integrating Mobility, Multi-homing and Security in a HIP way, Pekka Nikander et al, Feb 2003
- Opportunistic Security of Host Identity Protocol, Bing Zhou, master thesis, July 2006
- Enterprise Network Packet Filtering for Mobile Cryptographic Identities, Janne Lindqvist et al, June 2007
- Establishing Host Identity Protocol Opportunistic Mode with TCP option, Janne Lindqvist, March 2006, expired internet draft
- Host Identity Protocol Domain Name System Extensions, Pekka Nikander et al, Apr 2007, work in progress