Host Identity Protocol BOF

Monday, Nov 10th 2003
58th IETF, Minneapolis

David Ward, Cisco Systems
Pekka Nikander, Ericsson Research Nomadiclab

Introduction to the BOF

- (Agenda bashing next slide)
- This is the Host Identity Protocol BOF (hipbof)
- BOF goals
  - Introduce the current status of HIP
  - Discuss forming a working group
- Proposed WG charter
  - Complete work on HIP base protocol
  - Allow HIP experimentation in a wide scale

Agenda bashing

Intro and agenda bashing	5 min	Chairs
Introduction to HIP	20 min	Pekka Nikander
Introduction to live demo	5 min	Pekka Nikander
Live demonstration	20 min	Demo team
Potential Applications at Boeing	5 min	Steven Venema
Current status	15 min	Chairs
Charter discussion	70 min	All
Summary and next steps	10 min	Chairs & ADs

Introduction to HIP

Pekka Nikander
Ericsson Research Nomadiclab

Presentation outline

- A Brief History of HIP
- Some architectural background
- Related WGs
- HIP in a Nutshell
- Draft status
- Implementation status
- Summary

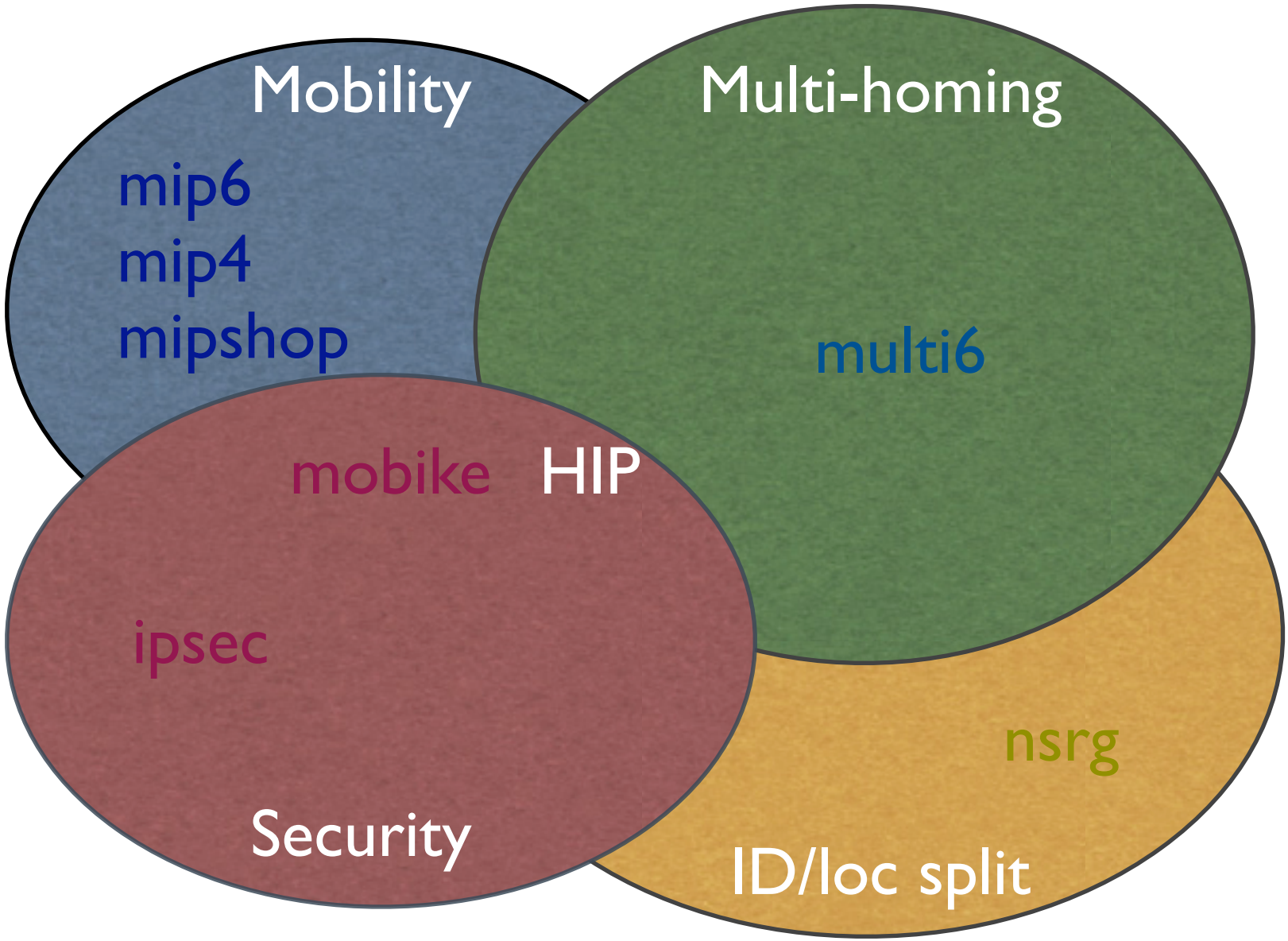
A Brief History of HIP

- Discussed briefly at 47th IETF
- Two earlier BOFs: 50th and 51st IETFs
  - No working group formed back then
- Development has happened next to the IETF
  - Active developer community
  - Five interoperating implementations
- HIP base protocol more or less ready
  - More work needed on infrastructure issues

Some architectural background

- IP addresses serve the dual role of being
  - End-point Identifiers
    - Names of network interfaces on hosts
  - Locators
    - Names of naming topological locations
- This duality makes many things hard
- IRTF Name Space Research Group (nsrg) studied the issue without reaching consensus

Related WGs and RGs

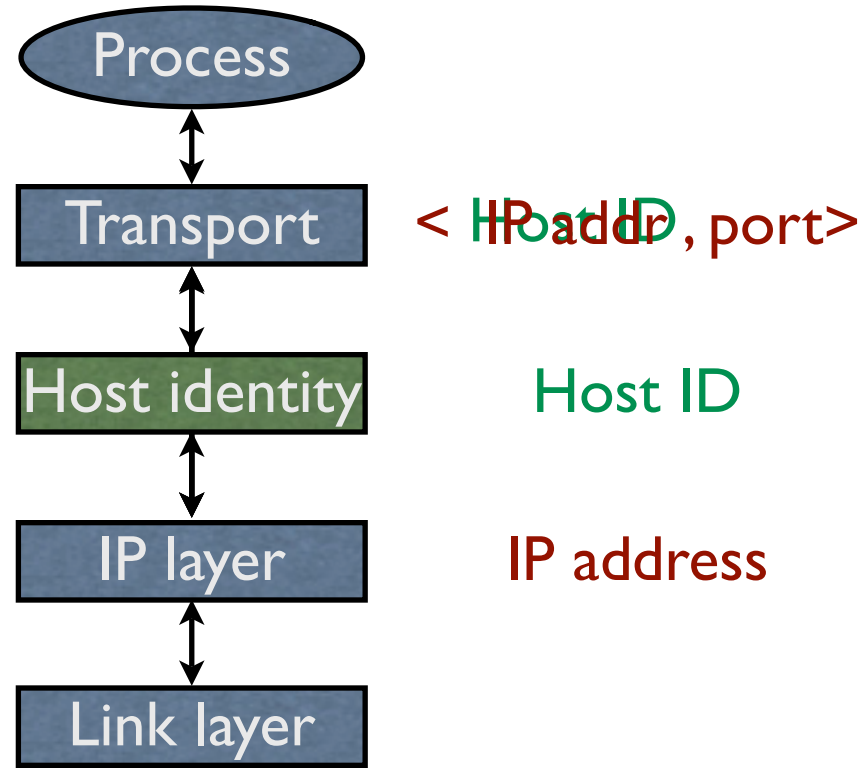


HIP in a Nutshell

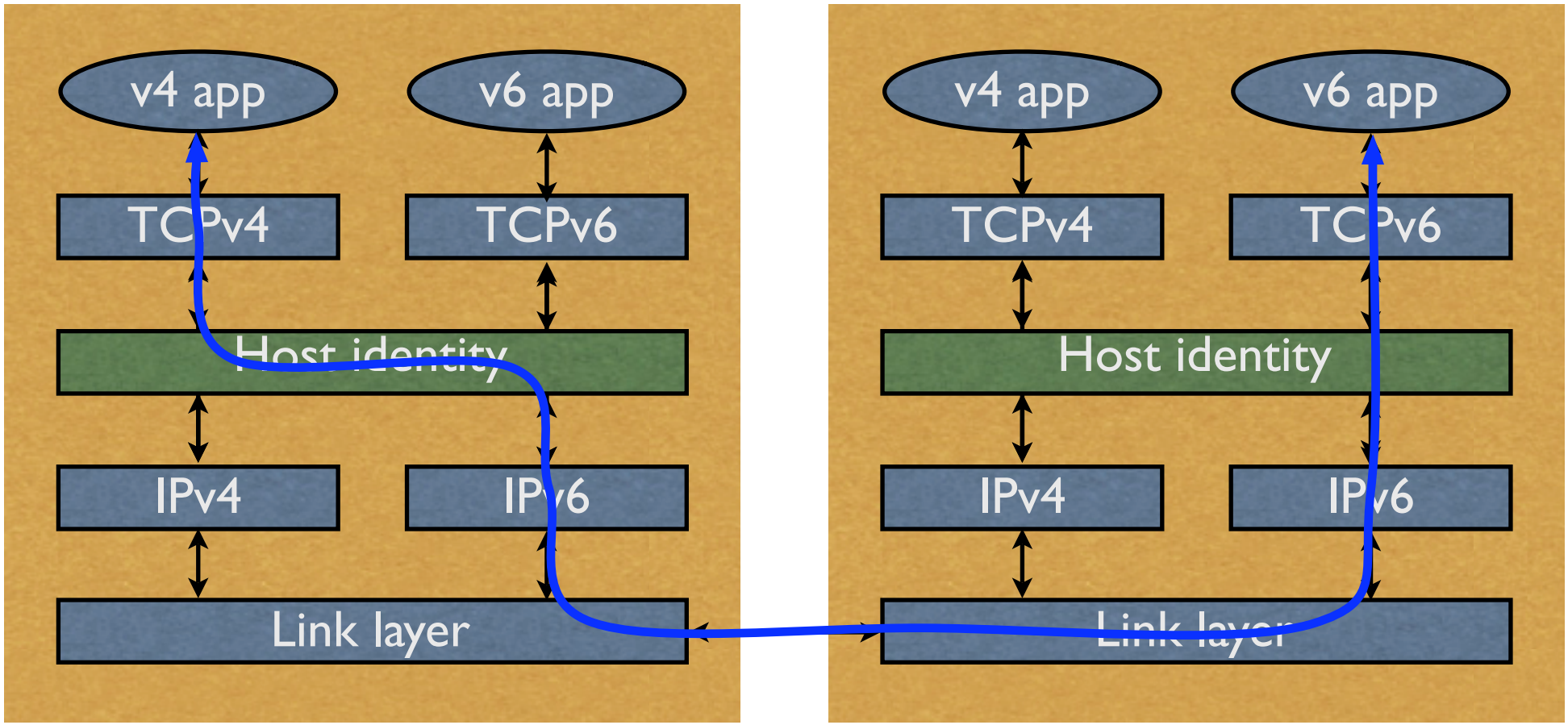
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host IPsec ESP
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-address multi-homing, IPv4/v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport
  - Introduces cryptographic Host Identifiers

The Idea

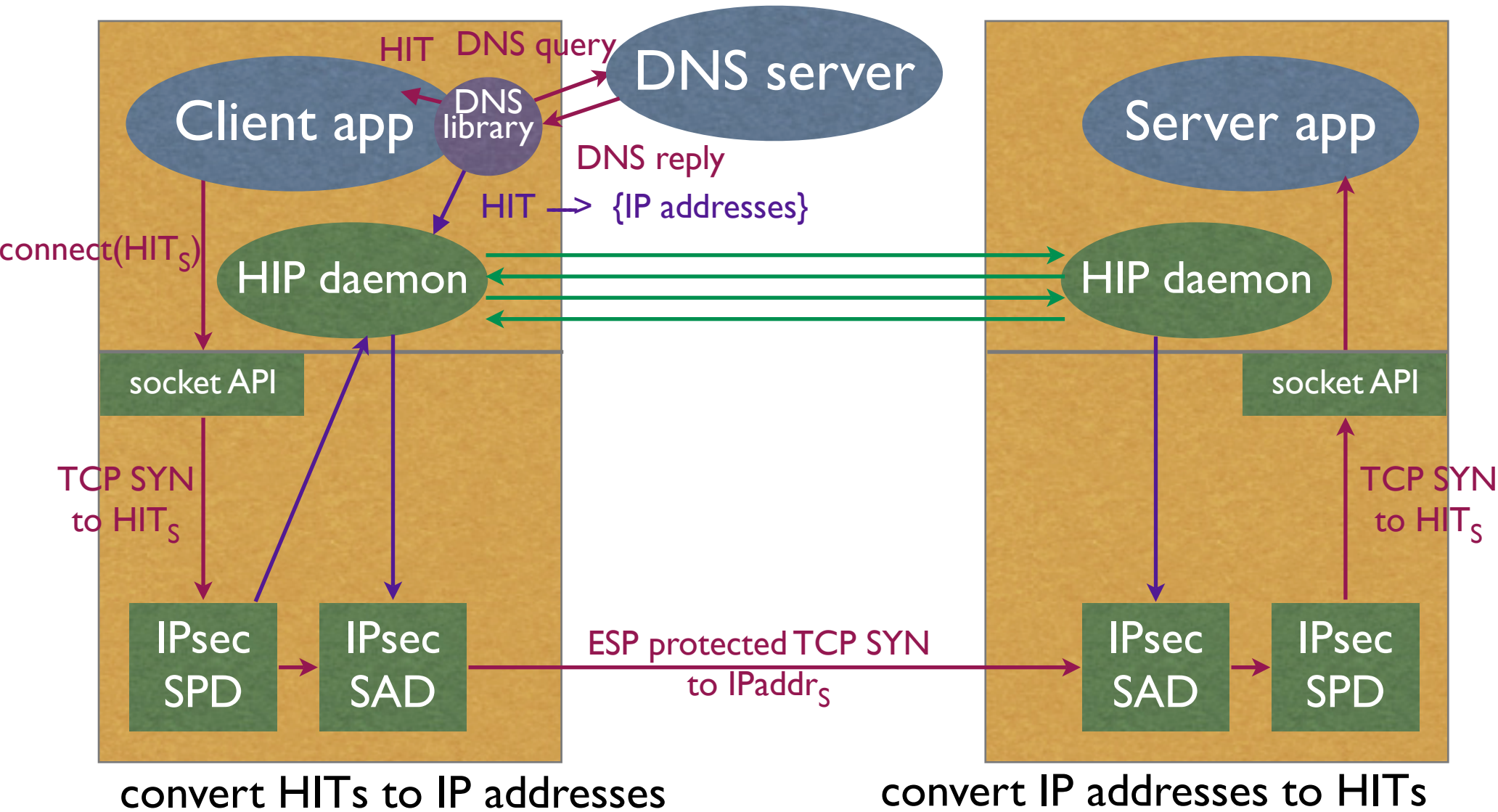
- A new Name Space of Host Identifiers (HI)
  - Public crypto keys!
  - Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



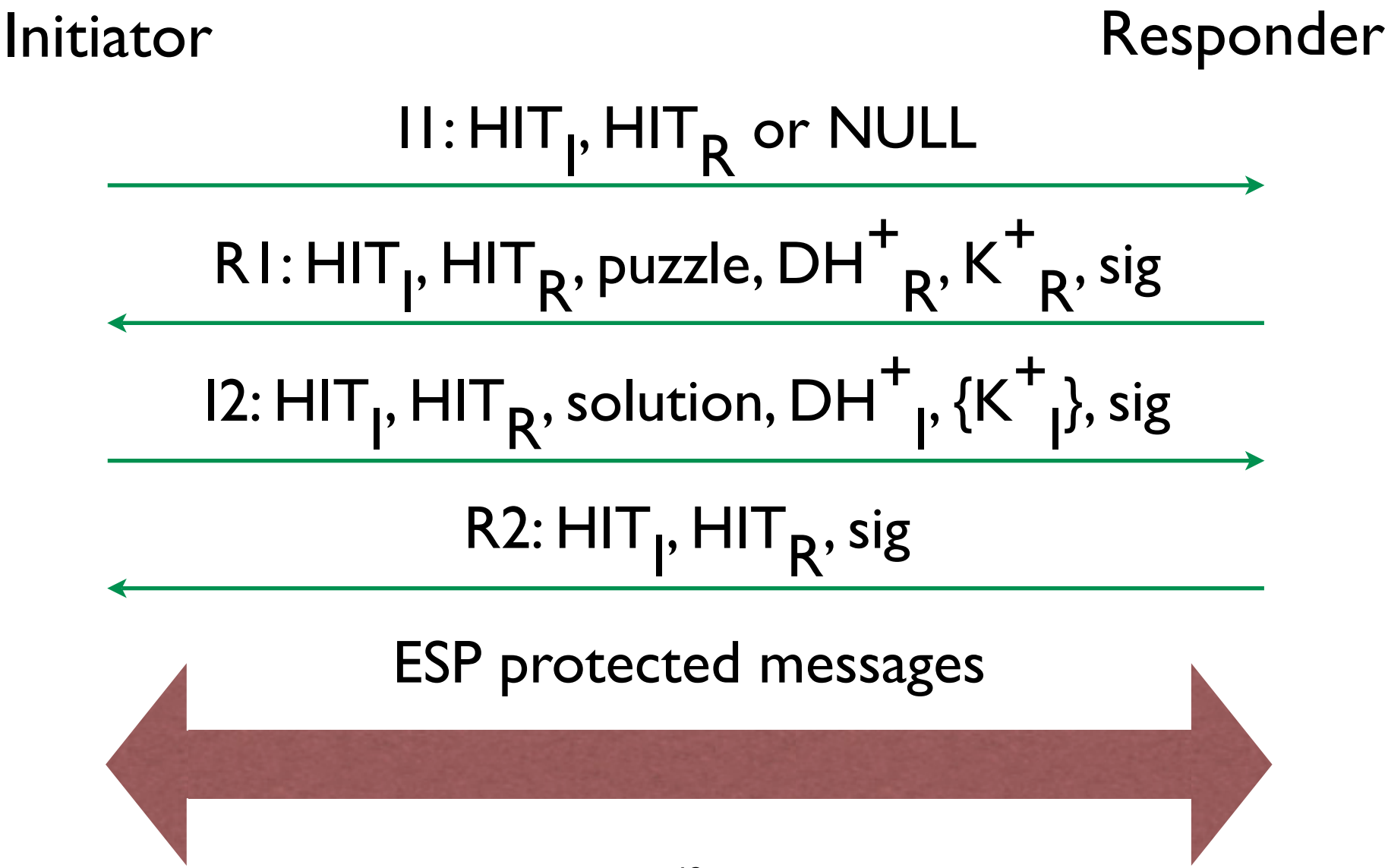
HIP as the new waist of TCP/IP



One way to implement HIP



Protocol overview



Internet drafts

- draft-moskowitz-hip-arch-05
  - architecture – sent to RFC editor
- draft-moskowitz-hip-08
  - base protocol – almost ready
- draft-nikander-hip-mm-00
  - mobility & multi-homing – needs work
- draft-nikander-esp-beet-mode-00
  - IPsec ESP extensions

Implementation status

- Five publicly known implementations
  - Boeing Phantom Works, Linux, IPv4 only
  - Ericsson Research Nomadiclab, FreeBSD
  - Helsinki University of Technology, Linux IPv6
  - Andrew McGregor, Python user level
  - Sun Labs Grenoble, Solaris?
- Fourth interop testing going on here in MPS

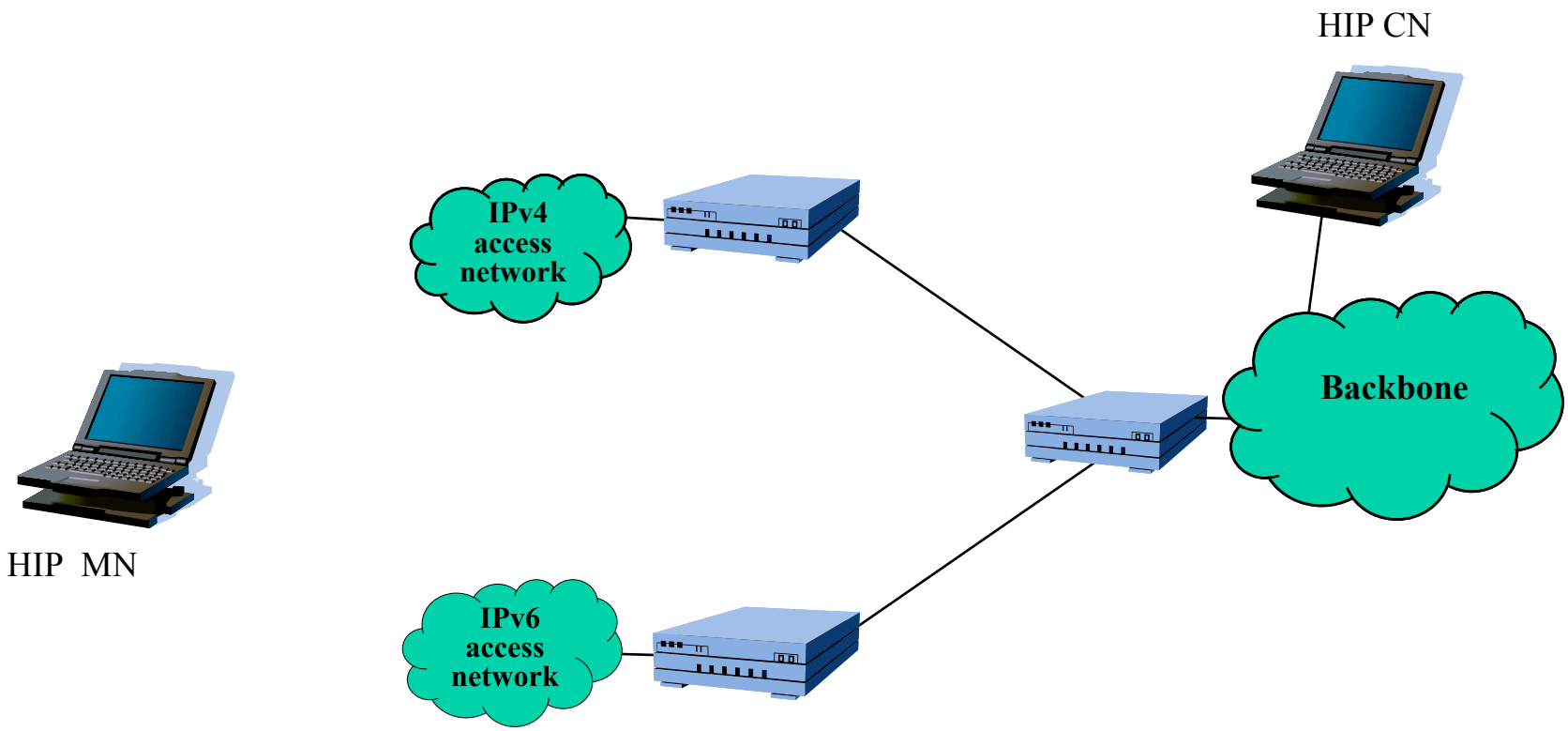
Summary

- New cryptographic name space
  - Hosts identified with public keys
- Integrates security, mobility, multi-homing
- Initial ideas at the IETF in late 1999
- Five interoperating implementations
- Base specifications start to be mature
  - Architecture draft at RFC editor

Demonstration

Jeff Ahrenholtz, Miika Komu, Mika Kousa, Jan Melen,
Jukka Ylitalo, and Jorma Wall

Demo network structure



Mechanisms demonstrated

- HIP base exchange
  - between Ericsson and HUT implementations
  - ethereal & tcpdump, 3des encryption
- Mobility & application interoperability
  - IPv4 telnet connecting to IPv6 telnet server
  - from IPv4 to IPv6 and back

Current status

Chairs

Status overview

- Architecture draft at the RFC Editor
  - To be published as an Informational RFC
- Base protocol specification closing completion
  - Resolving last open issues, based on interops
- Proposal for ESP extensions (BEET mode)
  - Complete draft; easier HIP implementation
- More work needed on infrastructure issues
  - Multi-addressing, DNS interactions, NAT traversal, rendezvous / proxy

Architecture specification

- draft-moskowitz-hip-arch-05.txt
- Submitted to the RFC Editor on Oct 27th
- Intended to be published as Informational
- Reasons for such early submission
  - Create a snapshot of current thinking
  - Create a starting point for the proposed WG

Base protocol specification

- draft-moskowitz-hip-08.txt
- First complete, fully specified version
- Open issues
  - Appendix containing packet examples
  - Exact bit formats for extension capability
  - Clarification on ESP SA key generation
  - Clarification on D-H key material generation
  - Small bug in state machine description

IPsec ESP extensions

- draft-nikander-esp-beet-mode-00.txt
  - Also discussed at ipsec wg and mobike bof
- Bound End-to-End Tunnel mode
- Transport mode processing with limited tunnel mode semantics
  - Fixed inner addresses, no address ranges
- Translates inner addresses (HITs) to outer addresses on output and back on input

Multi-addressing

- draft-nikander-hip-mm-00.txt
- Security analysis and protocol goals ok
- Proposed solution needs to be reworked
  - Needs better SA handling to take care of different QoS properties of different paths
  - Packet formats must be updated to match the newly added extension capability

DNS interactions

- No drafts yet
- Need a method to store HIs or HITs
- Minimum level: Store HIT in an AAAA like RR
- Better: Store HI in an IPSECKEY like RR
- Maybe: DNS updates secured with HIP

NAT traversal

- No drafts yet
- Work must be aligned with multi-addressing
- Basic idea: Let NATs learn SPIs from HIP messages, setting up SPI based NAT (SPINAT)

Rendezvous / proxy server

- No drafts yet
- Rendezvous server allows fast / simultaneous mobility
  - Dynamic DNS updates are not fast enough
- Proxy allows a HIP host to use multi-addressing when communicating with a non-HIP host
- Functionality fairly similar; a proxy can easily function as a rendezvous server, too

Charter discussion

Please do remember to identify yourself
at the microphone!

Proposed charter items

1. Complete base protocol specification
2. Define ESP extensions (BEET mode)
3. Complete the basic mobility and multi-homing
4. DNS interactions
5. NAT traversal
6. Rendezvous and proxy servers
7. Optionally a DHT based search mechanism
8. *Application guideline: how apps see HIP*
9. *Implementation report*
10. *MIB*

REMEMBER TO IDENTIFY YOURSELF AT MICROPHONE

Next steps

Chairs and ADs

http://honor.trusecure.com/pipermail/hipsec/