

ASP Key Ideas

- Security Framework
- NAT Traversal
- Extensibility
- Usage Models
- Pluggable DHT
- Forwarding Layer
- Multiple P2P Networks

HIP-HOP

Breaks P2P layer into 3 parts; detailed proposal using HIP for Distrib Transport part. Take rest from other proposals?

	HIP-HOP	Others
Peer IDs	Special IPv6 addr with crypto	Bitstring (usually 160 bits)
Application API	Socket API	Some new API
Transport connections	End-to-end	Hop-by-hop
NAT traversal and mobility	At HIP layer	In each app

P2PP

- Pluggable DHT and non-DHT protocols
- Overlay maintenance
- Replication
 - publisher
 - Storage-node oriented
- NAT Traversal
- Simple and Extensible
- No DHT-mash up

RELOAD

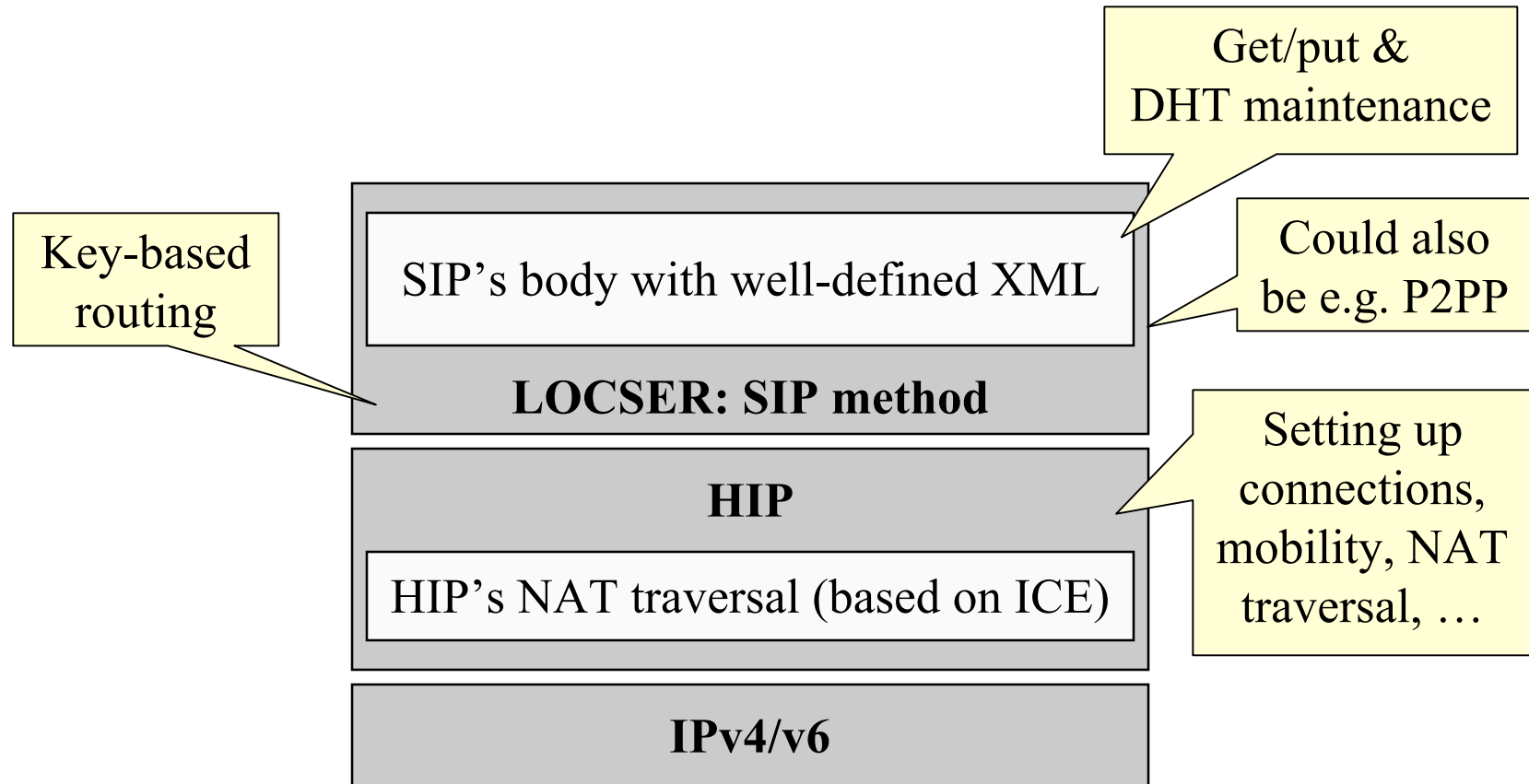
- Binary TLV messages
- Fixed routing header
- Pluggable DHT and security
- Security for overlay, resources, peers...
- Attributes use hierarchical, extendable types
- One-to-many resources annotated with parameters for types, etc.
- NAT Traversal: new RELOAD connections, tunnel or open for apps

LOC SER + HIP

`draft-hautakorpi-p2psip-peer-protocol-00.txt`
`draft-hautakorpi-p2psip-with-hip-00.txt`

**Jani.Hautakorpi@ericsson.com &
Joakim.Koskela@hiit.fi**

Overview



Highlights

- Benefits of HIP for P2PSIP:
 - Supports mobility (i.e. connections can survive the IP-address exchange)
 - Has an ICE-like NAT traversal mechanism
 - Supports leap-of-fait type of security
 - Can be used with different Peer Protocols (e.g. P2PP)
- Distinct design choices:
 - LOCSEER: Not generic, HIP: Generic
 - Overlay routing is done above the HIP layer
 - No changes to HIP, just a BCP document

XPP(-PCAN) Goodies

XPP

- **Session based** – Sessions are negotiated with SIP
- **NAT Traversal** – Due to simultaneous connections, ICE is only recommended and not mandated
- **Backed up by an open source implementation**
- **Very lightweight** – Small header and TLV options
- **Works for any DHT**

XPP-PCAN

- Trusted neighbors and passive approach
- Designed after an open source implementation