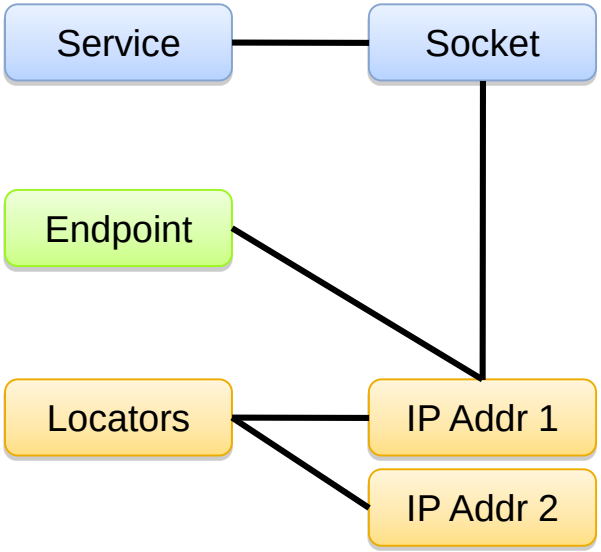
Introduction to Host Identity Protocol

Andrei Gurtov

LINKÖPING UNIVERSITY

Today's Internet Infrastructure and Protocols



Current Internet uses the TCP/IP stack

- Developed for non-mobile, single-homed hosts
  - *Dual role of IP addresses: identify and locate end-hosts*
- Offers no security mechanisms
  - *End-hosts cannot prove their identities*
  - *No data confidentiality and integrity protection*

Additional protocols extend specific IP functionality

- Mobility support: Mobile IP, …
  - *Requires additional infrastructure elements (see next slide)*
- Security: IPsec, ...
  - *Requires session setup → e.g. with IKE protocol*

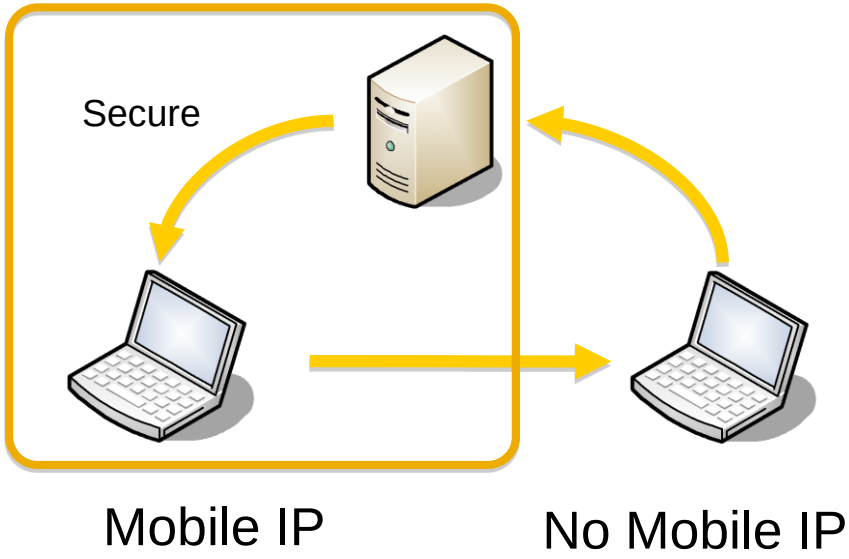
HIP vs. Mobile IP in a Nutshell

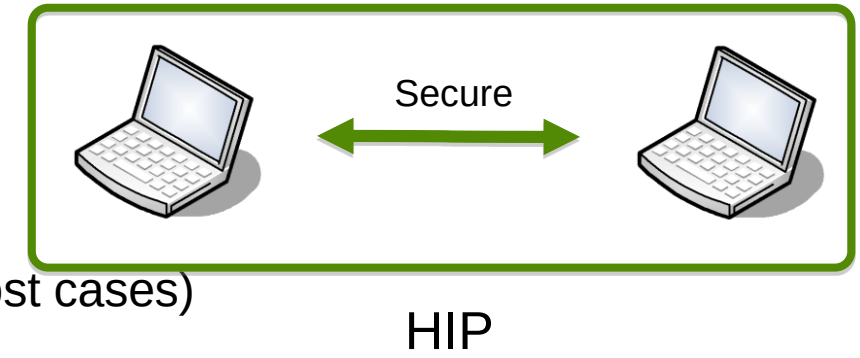
Mobile IP

- Home agent as fixed point
- Support for un-modified correspondent node
- Indirect mobility management
- Triangular routing
- Infrastructure support (FA, HA)

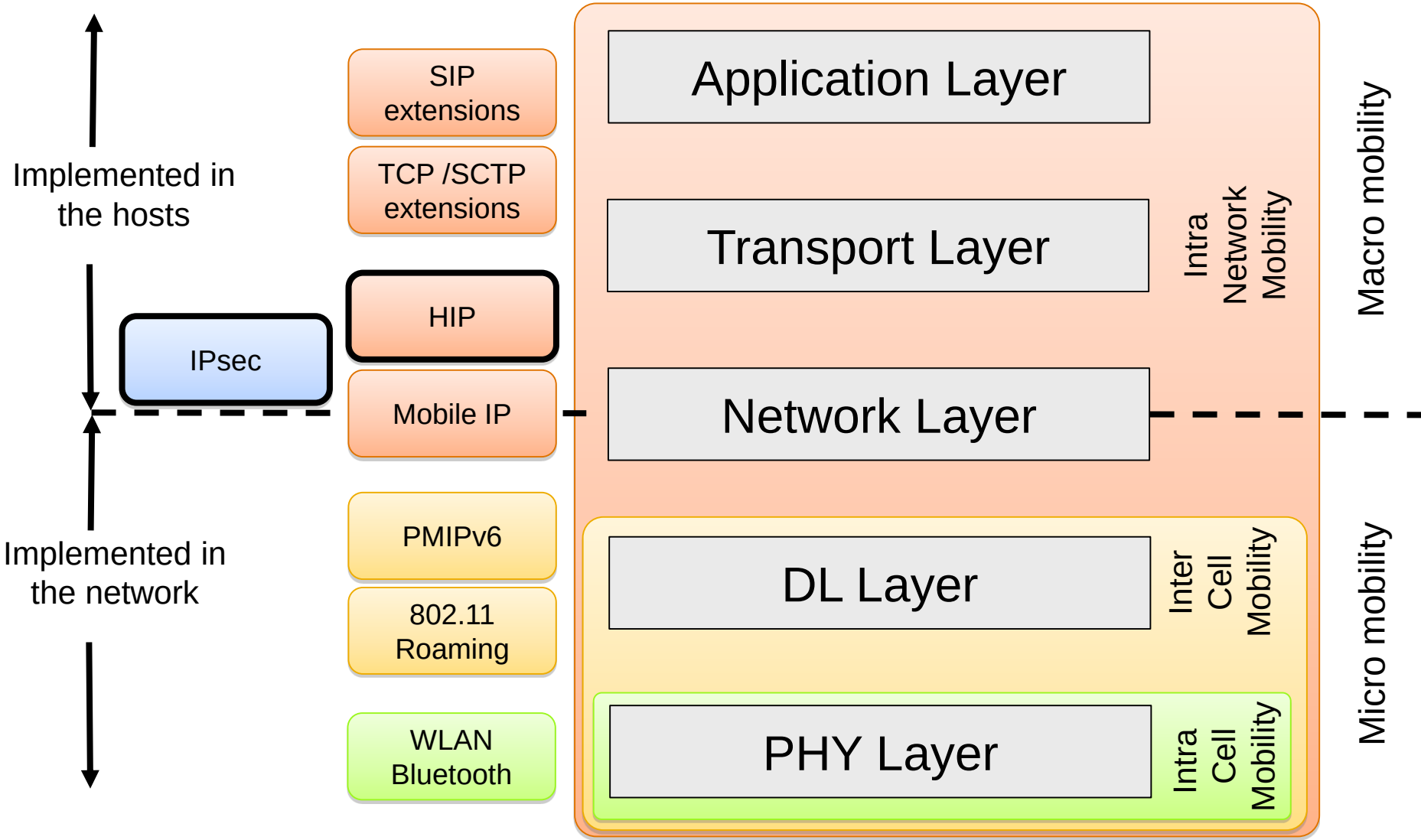
Host Identity Protocol

- End-to-end associations
- HIP-aware end-hosts
- Direct mobility management
- Authentication
- End-to-end security
- No infrastructure support needed (in most cases)

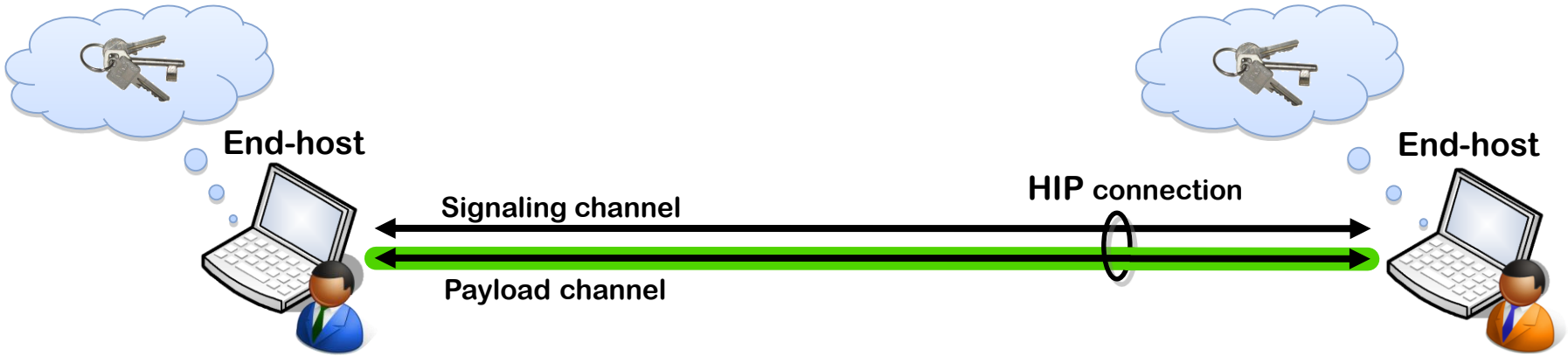




Mobility in the Network Stack



Host Identity Protocol (HIP)



Signaling and key-exchange protocol

- Separate control and payload channel
- Allows use of security services → e.g. IPsec payload channel
- Similar to Internet Key Exchange (IKE)

Introduces new namespace

- Namespace is cryptographic in nature
- Provides support for mobility and multi homing

Cryptographic Namespace

Host authentication is essential when supporting mobility and multi homing

- End-hosts have to verify they still talk to the same peer
- State changes at middleboxes may be required

Self-generated public and private key-pair provides the host identity (HI) in HIP

- RSA by default, DSA also supported in HIP specification
- Length of the public key - 512, 1024 or 2048 bits
- Abstraction required for use in network stack due to large and variable size of the public key

→Two additional forms of host identities: HIT and LSI

Globally Unique and Locally Unique Identifiers

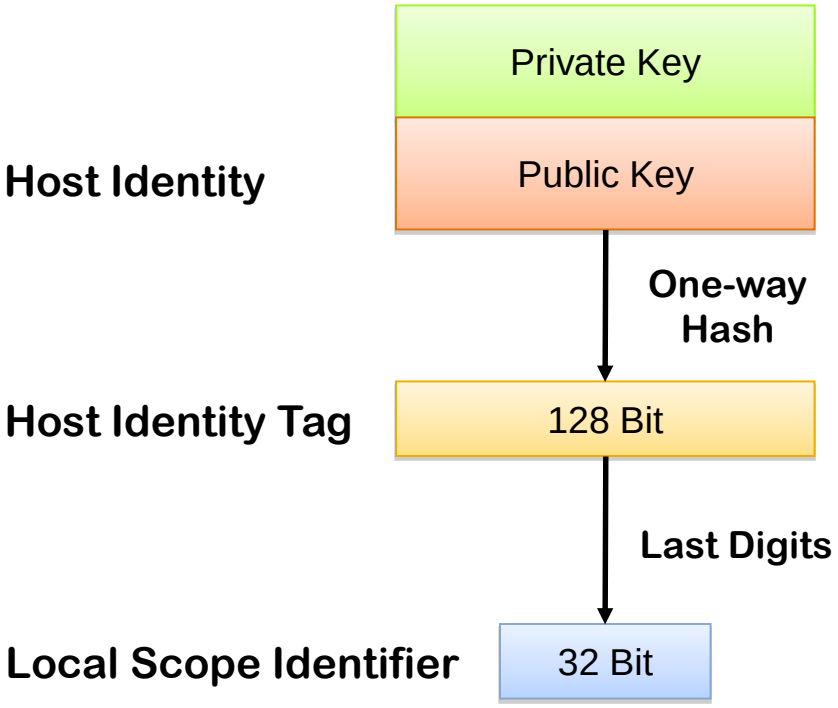
Host Identity Tag (HIT)

- Compatible with IPv6 address
- Statistically unique
- Probability of collisions is negligible

Local Scope Identity (LSI)

- Compatible with IPv4 address
- Probability of collisions is significant

→Restricted to local scope

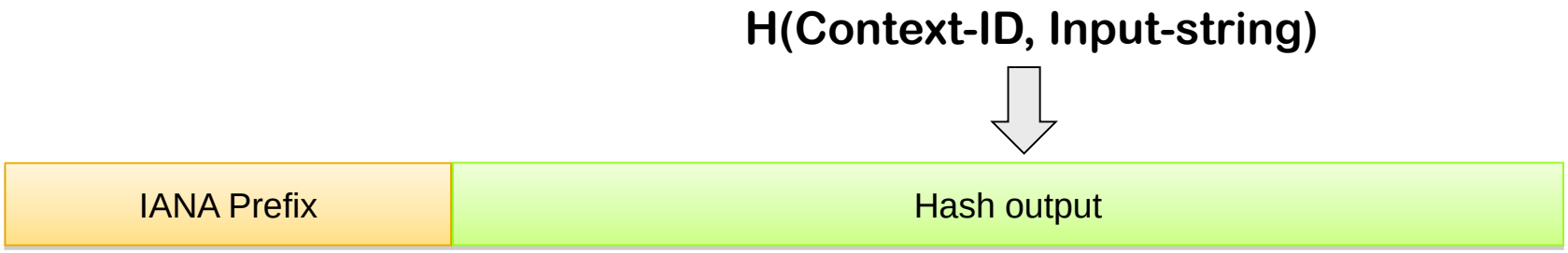


Computation of a HIT

HIT generation follows the Overlay Routable Cryptographic Hash ID (ORCHID) method

Components of a HIT

- Not routable IPv6 prefix assigned by IANA (2001:0010::/28)
- 100-bit string extracted from SHA1 hash over 128-bit context ID and input string
  - *Context ID – randomly chosen value for HIP*
  - *Input string must be statistically unique (here: public key)*



Identifier / Locator split

Major problem in the original Internet architecture:

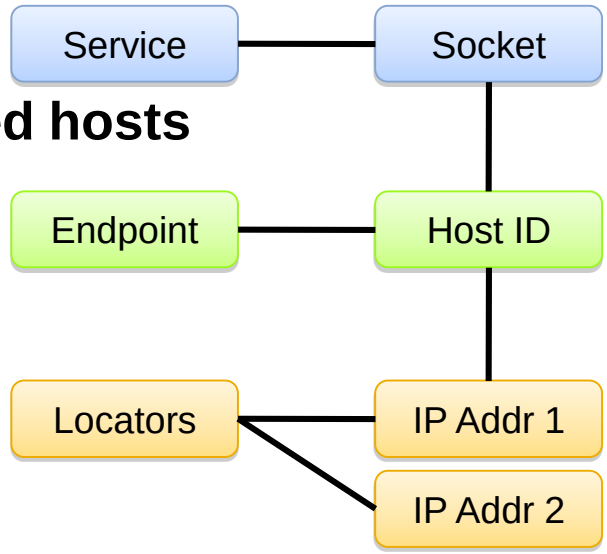
- Tight coupling between networking and transport layers (e.g. TCP checksum calculation)
- Mobility breaks transport layer connections

Separation of location and identity of networked hosts

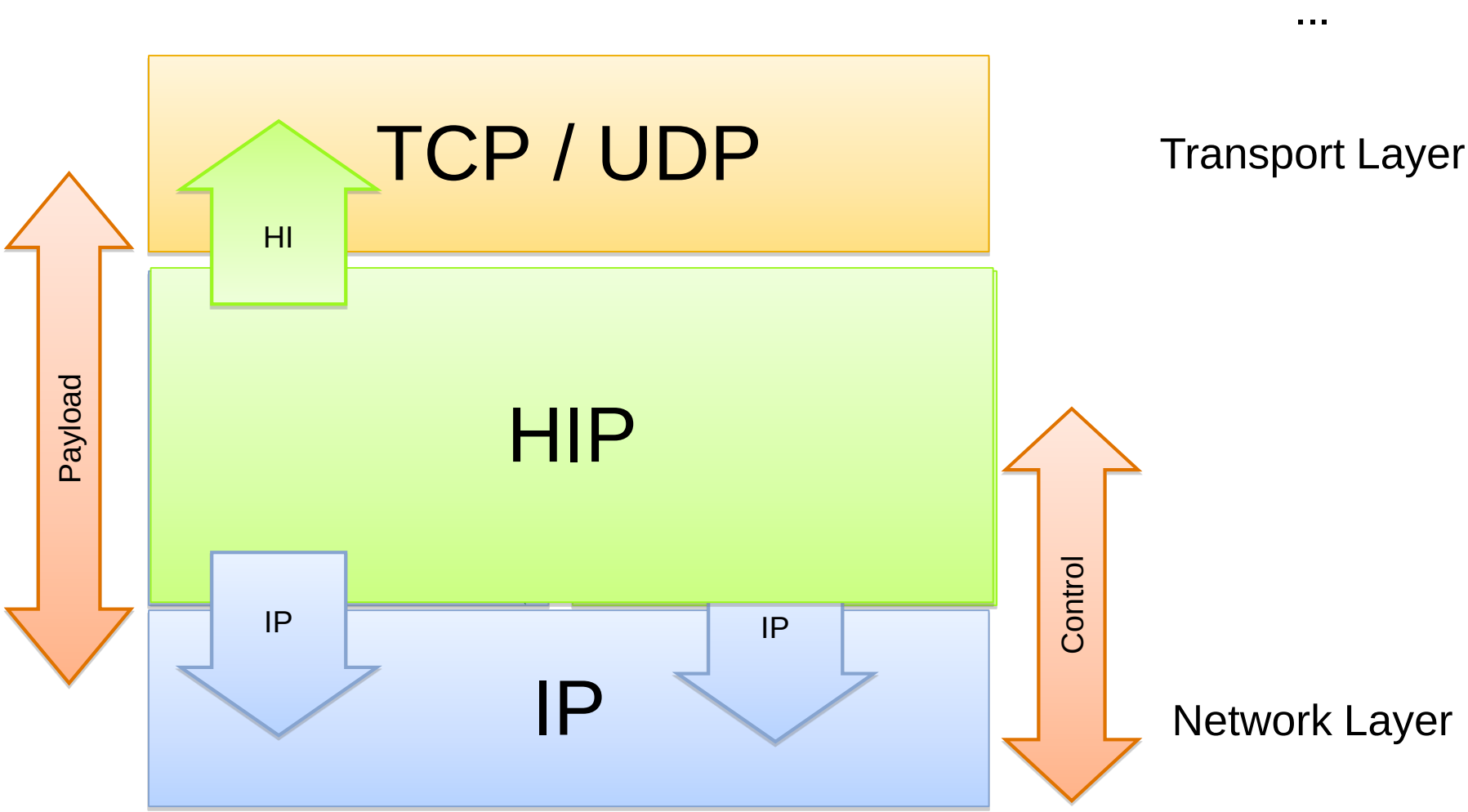
- HIP replaces role of IP as identifier
- IPv4 and IPv6 run underneath HIP
- Transport protocols bind to His

Benefit

- Applications see stable identity instead of a locator
- Routing decisions still based on locator
  - *No changes to core infrastructure required*



HIP in the Communication Stack



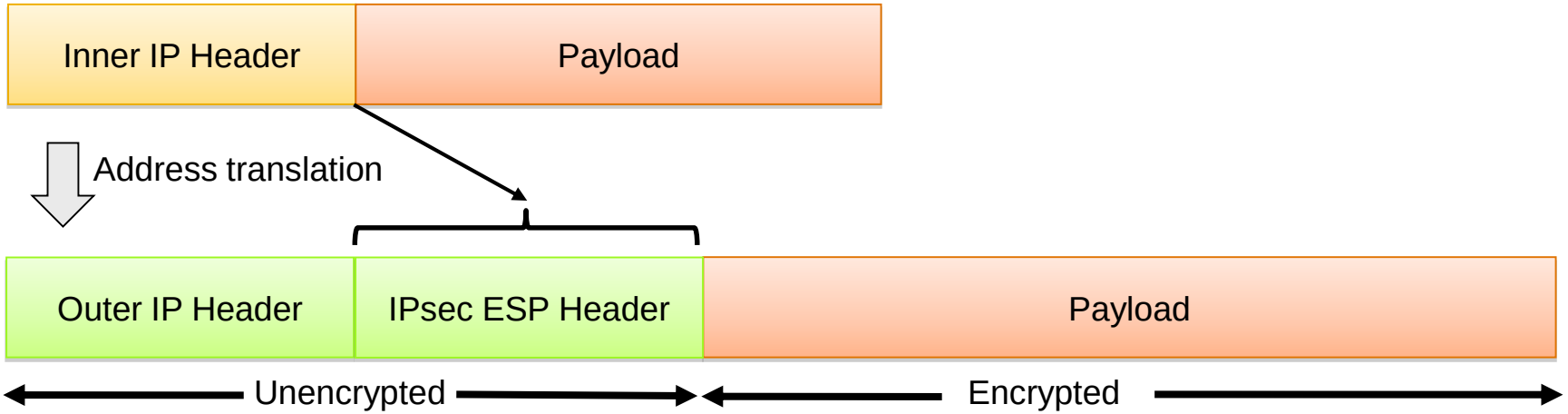
IPsec BEET mode with ESP

New IPsec mode introduced with HIP

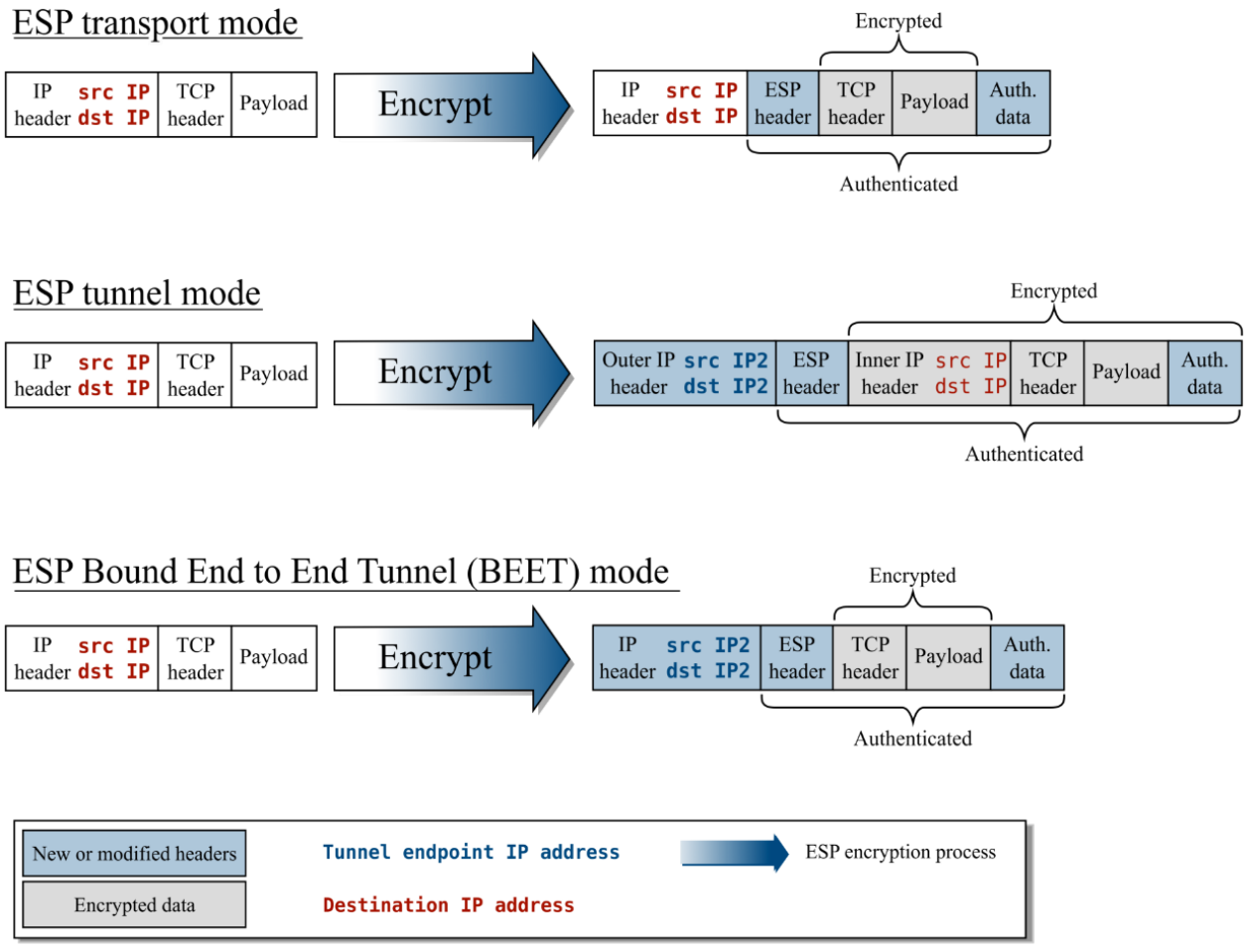
- Signaling of SPIs and stable host IDs affords header compression
- Syntactics of transport mode and semantics of tunnel mode
  - *HIP namespace denotes addresses of local network*

Address translation defined by HIP

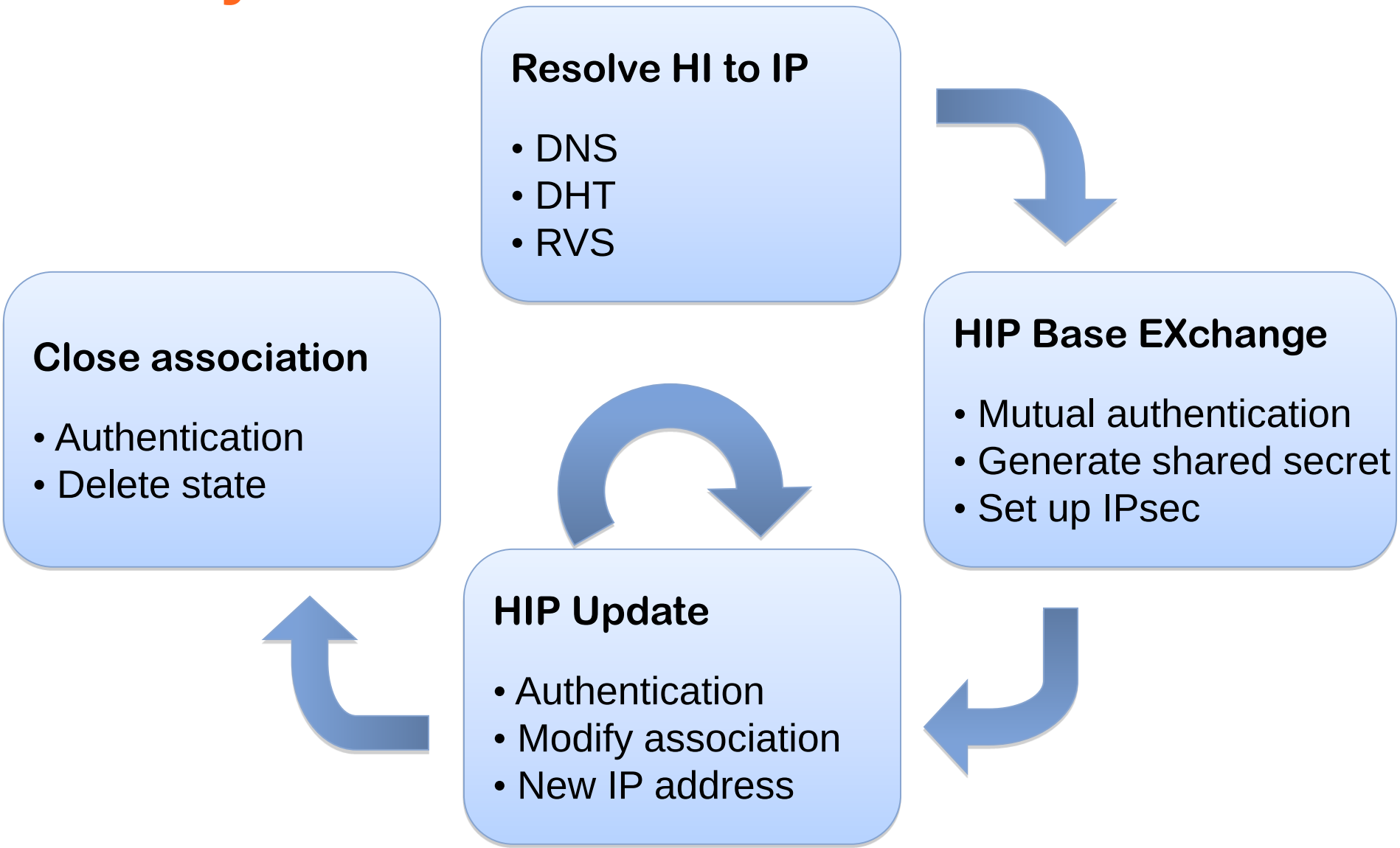
- Inner header: HIP host ID
- Outer header: routable IP address → visible on the wire



IPsec Modes with ESP Header – Overview



Lifecycle of a HIP Association



DNS Extension

Why name resolution?

3 different name spaces

- Users require some kind of human-readable representation
- With HIP, applications work on HIs or HITs
- HIP layer needs knowledge about HI ←→ IP mappings for address translation step in the stack

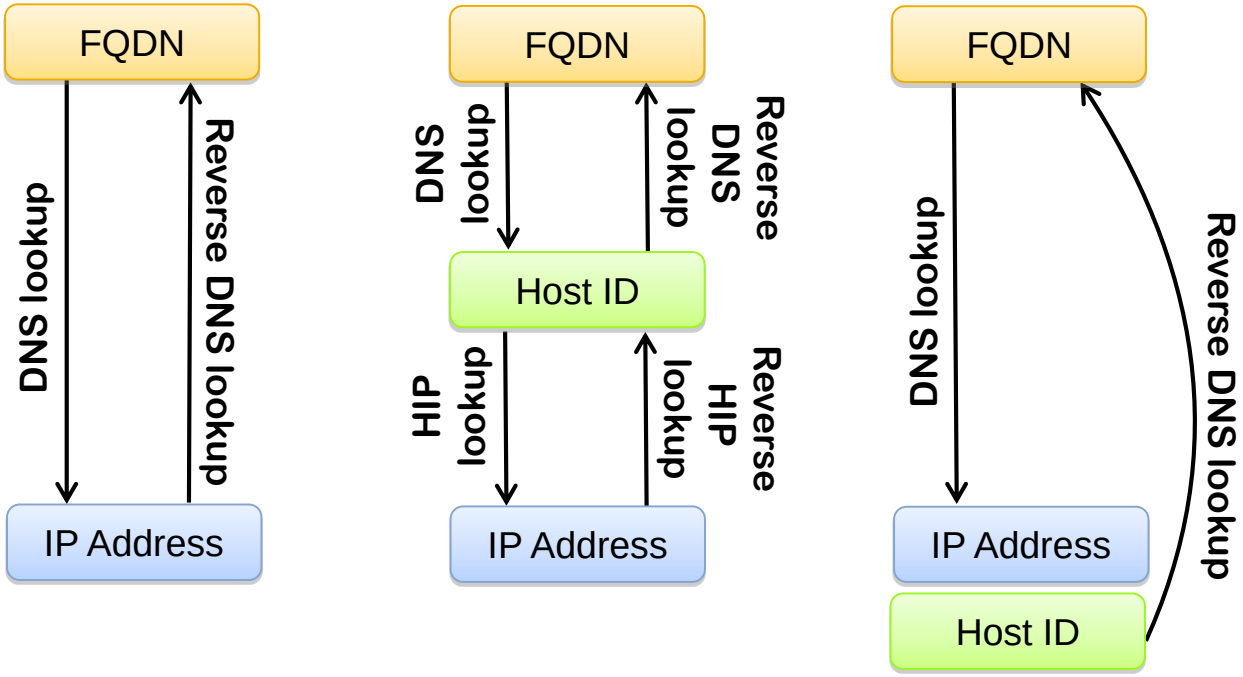
Different a priori knowledge before lookup

- Domain name or HI/HIT
- IP → opportunistic mode (not covered here)

Possible lookup architectures

- Usage of overlays (e.g. Distributed Hash Tables (DHT))
- Integration with DNS

Name resolution mechanisms



(1) (2) (3)

(1) DNS resolution in the current Internet

(2) Logical resolution for HIP

(3) Resolution proposed in HIP DNS extension

Rendezvous Server

RVS provides host with a stable IP address

- Comparable to Home Agent of Mobile IP

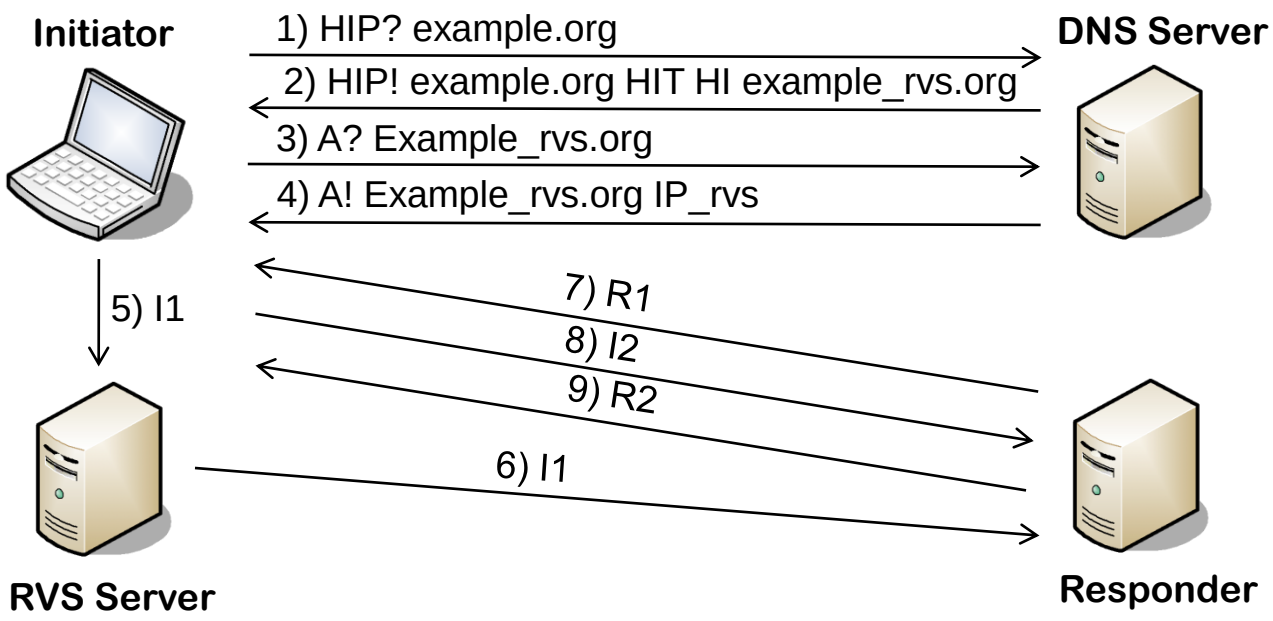
Integration of RVS with name resolution

- HIP RR from DNS stores pointer to responsible RVS
- Mobile host registers with RVS
- Mobile host updates its registration with RVS after mobility event

2-step address lookup

- HIP Initiator first queries a HIP RR from DNS
- Returns IP address of the Responder or its RVS
- If RVS, additional address lookup

HIP Name Resolution with RVS



1–4) Initiator obtains IP address of RVS from DNS

5) HIP BEX initiated with the mobile host through the RVS

6) RVS relays the I1 packet to the mobile host

7–9) HIP BEX continues between the two end-hosts

Base Protocol

HIP Control Packets

End-hosts transmit control packets on signaling channel

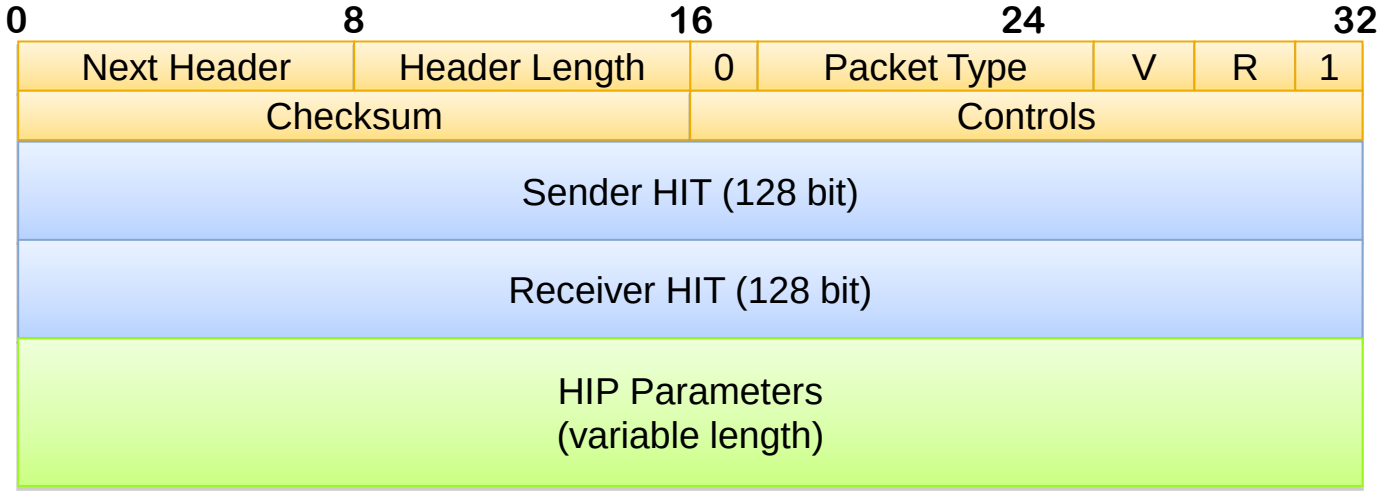
HIP control packets provide…

- Current HIT-IP mappings
- Verifiable identities of communicating end-hosts
- Keying material required for setup of security mechanisms
- Replay and DoS protection

Definition of HIP control packets

- Added behind IPv4 header or as IPv6 extension header
- HIP protocol number is 139
- Common HIP header defined for all HIP control messages

HIP Control Message Format



Next Header: set to “no next header”

Header Length: length of the HIP Header and HIP parameters in 8-byte units

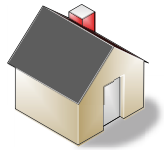
- excluding the first 8 bytes

Packet Type: indicates the HIP packet type

HIP Version: current version is 1

HIP Handshake

Mobile Host
(Initiator)



Remote Host
(Responder)

I1: Handshake request

R1: Host Identity, {Diffie-Hellman}, Sig

Shared key

I2: Host Identity, {Diffie-Hellman}, IPSec Info, HMAC, Sig

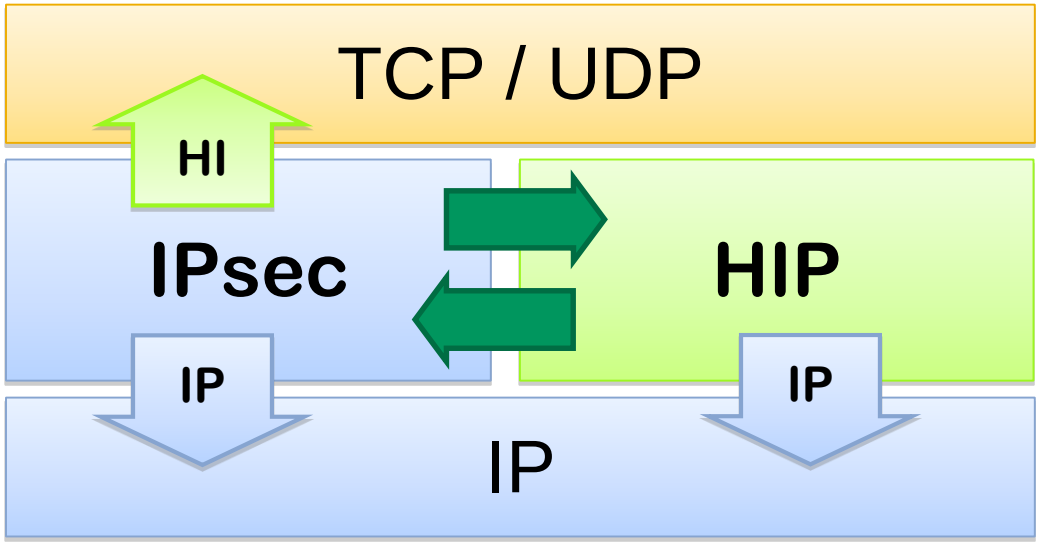
R2: IPsec Info, HMAC, Sig

Shared key

IPsec tunnel

Mobility

Recap: Network Stack supporting HIP



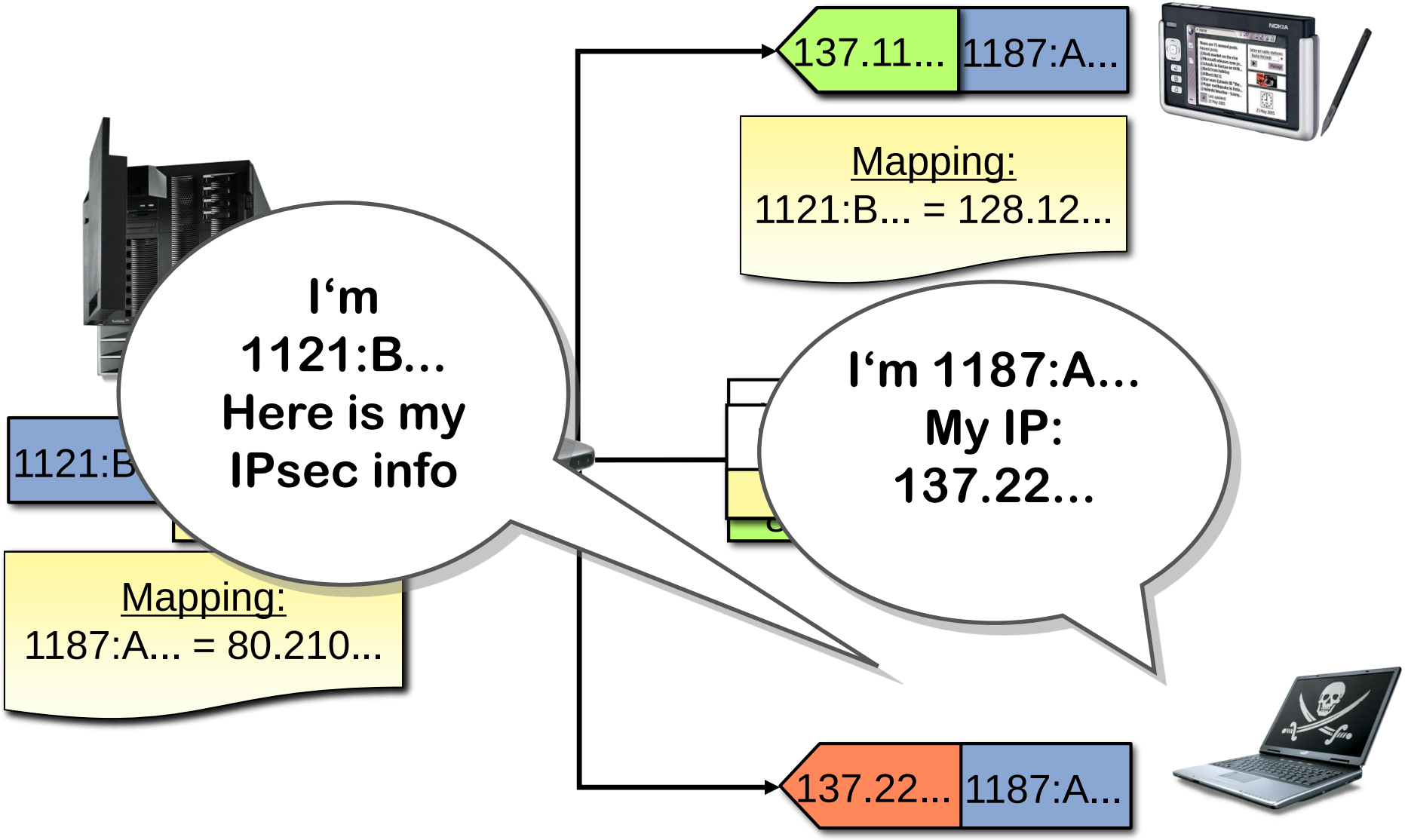
Applications bound to (stable) HITs

- New points of network attachment do not influence this binding
- Allows to handle mobility transparently for transport layer

HIP layer maps HITs to routable IPs

→Mobility event requires update of mapping information at peer host

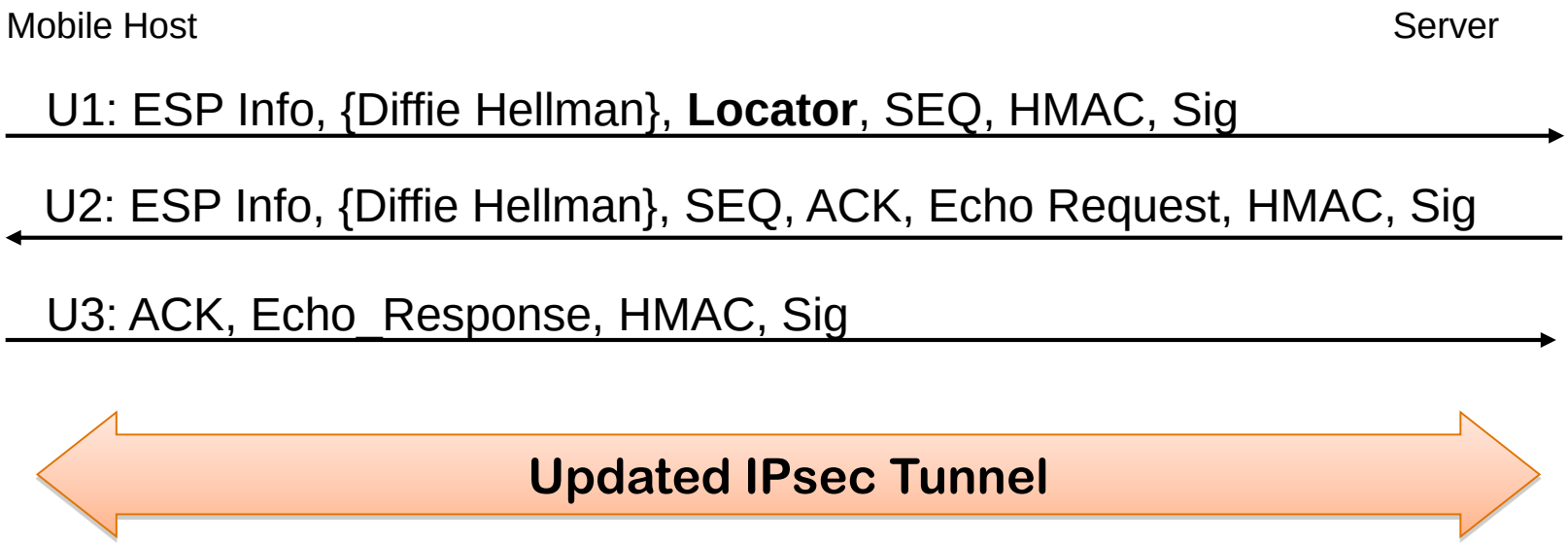
HIP Mobility in a Nutshell



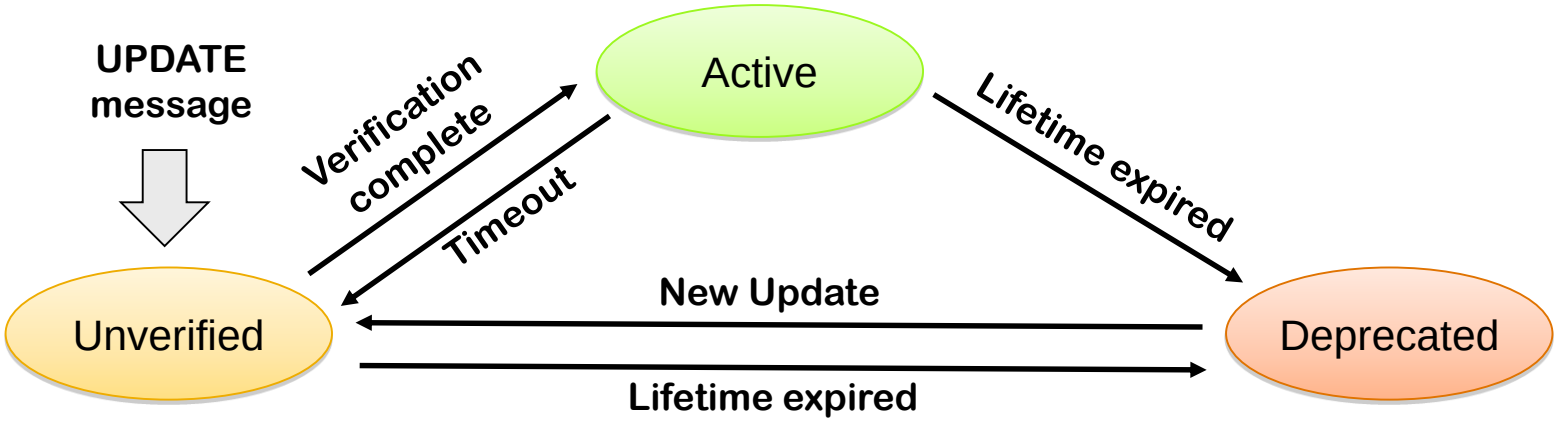
Mobility signaling

Similar message exchange for...

- IPsec rekeying
- Multi homing (*see next chapter*)



Three States of a Locator



UNVERIFIED - address reachability not tested yet

ACTIVE - address is valid and has not expired

DEPRECATED – expired originally valid locator

No transition from DEPRECATED to ACTIVE

- Requires another address reachability verification

Multi Homing

Multi Homing as Extension of Mobility

Typical multi homing scenario

- Host connected through 2 or more interfaces

Handling of multi homing in HIP corresponds to mobility signaling

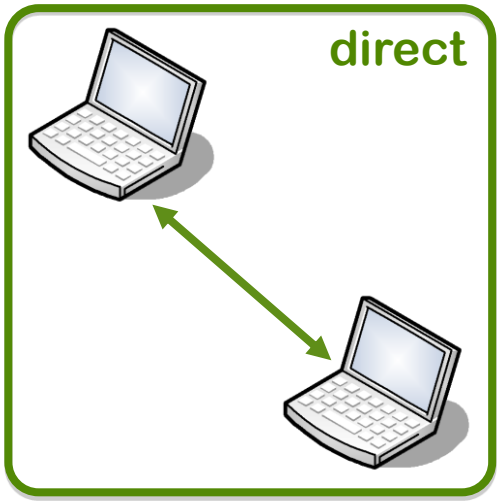
- Multi-homed host informs peer of further addresses with additional Locator parameters in UPDATE message
- Peer runs reachability check for all advertised locators
- Possibility to set new preferred locator → data is sent here

Multi-homed host can also send locator during BEX

- IP addresses used during BEX are preferred locators by default
- Verification of host reachability is necessary as well

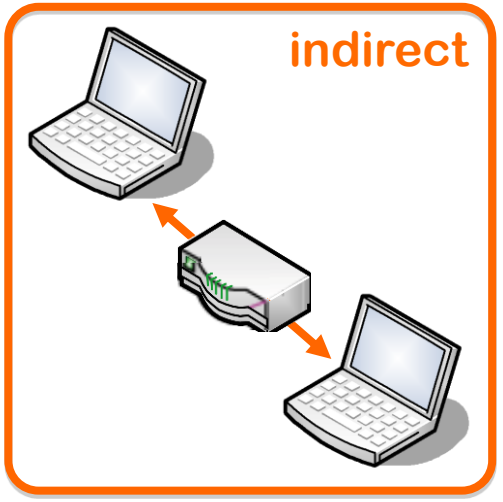
NAT Traversal

Infrastructure Elements in the Internet



Original Internet architecture

- Intelligence expected to be located at end-hosts
- Network is „dumb“ → best effort packet delivery
- Packet header inspection up to layer 3
- Packet not modified in transit



Emergence of middleboxes

- Intelligence at the edges of the network
- NAT: compensation for lack of IPv4 addresses
- Firewall: prevention of attacks, access control
- QoS and Proxy: data delivery performance

Legacy Middleboxes and HIP

Strong (theoretical) advantage of HIP architecture

- Ability to function without changes to existing IP routers

BUT: Middleboxes can affect HIP packet delivery

- Support only limited set of protocols (often TCP and UDP over IPv4)
  - *E.g. NAPT requires port information*
- Restrictive firewall rules may prevent HIP traffic

→Requirement to engineer support for legacy middlebox traversal

Legacy Middleboxes and IPsec

Similar problem with IPsec

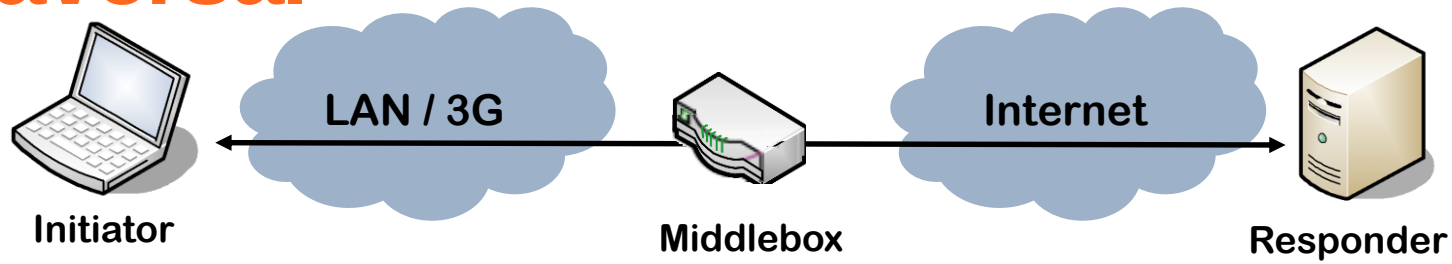
- Does not provide port information either

Some NATs offer VPN pass-through feature

- Attempt to learn SPIs in both direction
- Setup SPI ←→ IP mappings

BUT: all on-path middleboxes need to support pass-through

HIP Strategy for Legacy Middlebox Traversal



First step – UDP encapsulation for HIP control and payload packets

- UDP understood by majority of middleboxes (MB)
- Port information allows MB to multiplex and demultiplex traffic
- Sufficient if only Initiator behind NAT

Deficiencies of UDP encapsulation

- Header overhead
- Does not help if Responder or both end-hosts are located behind NAT

HIP Proxy

HIP-support for Legacy Clients

HIP requires both end-hosts to support it

HIP does not need support of core network

- Unlike IPv6

Additional infrastructure element to support legacy clients (HIP Proxy)

- HIP Proxy poses as end-point of the HIP connection
- One end-hosts of a connection can remain HIP-unaware
- Allows incremental deployment of HIP

HIP Proxy helps to obtain HIP benefits in 2 scenarios

- Legacy host contacting a HIP-aware peer
- HIP-aware host contacting a legacy peer

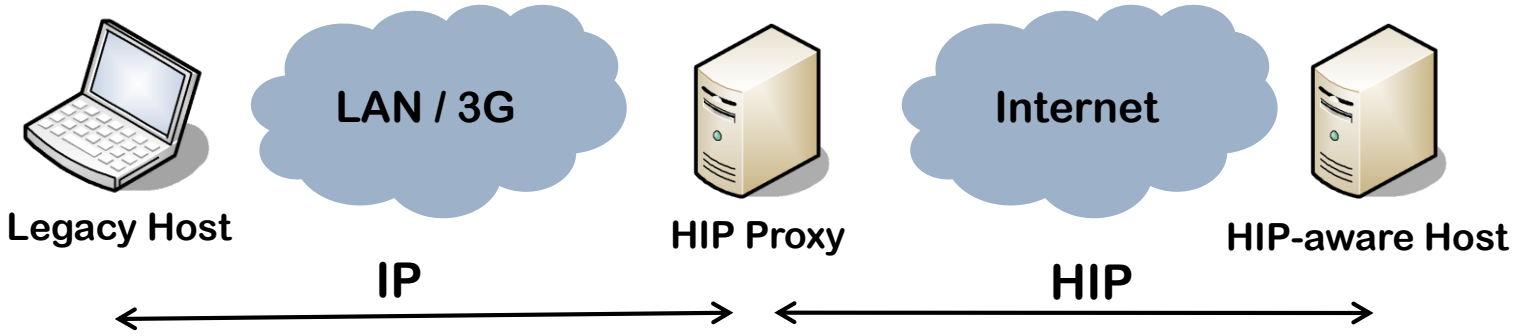
Legacy Contacting Host

HIP Proxy terminates HIP-connection with HIP-aware host

- Provides secure data transmission in the Internet
- Still unprotected traffic between legacy host and HIP Proxy

Setup does not add mobility and multi homing support

- Requires upgrade to end-to-end HIP awareness



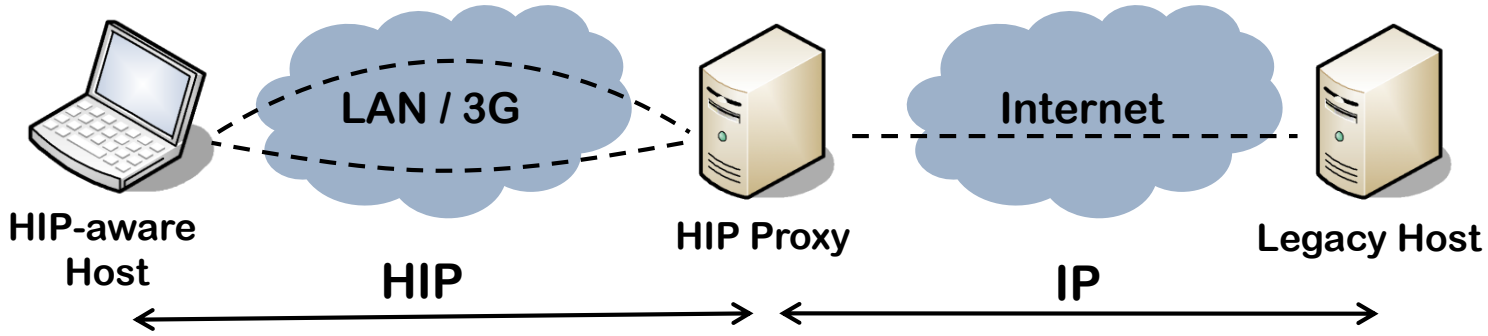
Legacy Peer Host

Advantages of using a HIP Proxy

- Traffic protection on the path between the mobile hosts and the proxy
- Mobility and Multi homing for HIP-aware host is provided in LAN

Example

- Mobile host uses WLAN for Internet access
- Mobile host can connect to a HIP proxy in the network
- All air traffic is encrypted
- Moving between different WLAN networks behind proxy is possible



Certificates

Certificates Exchange on HIP Control Channel

HIP namespace builds upon public keys

- Certificates allow to leverage this namespace further
- Centralized control over end-hosts
- Offline verification possible

End-hosts send certificates in a special parameter during HIP BEX or in UPDATE messages

- Certificate follows the Simple Public Key Infrastructure (SPKI) format

Scenario: HIP-aware Firewall

HIP allows firewalls to permit access based on host ID

Without certificates the firewall ACL has to include the HI or HIT of each permitted end-host

Certificates simplify the authentication process for HIP-aware firewalls

- Firewall trusts and stores the public key of Certificate Authority (CA)
- Authentication of HIP hosts during BEX and UPDATE based on HI and corresponding certificate transferred on control channel
- HIs of end-hosts can be purged from the memory after connection teardown

Certificate Lifetimes

HIs can be compromised or hosts can behave maliciously

The lifetime of a certificate determines the validity time span

- No further authorization when lifetime has ended

Tradeoffs for short lifetimes

- HIP host has to frequently apply for new certificates
- Reduction of the need for a Certificate Revocation Lists (CRL)

Standardization Status of HIPv2

HIP Working Group

- **http://datatracker.ietf.org/wg/hip/charter/**

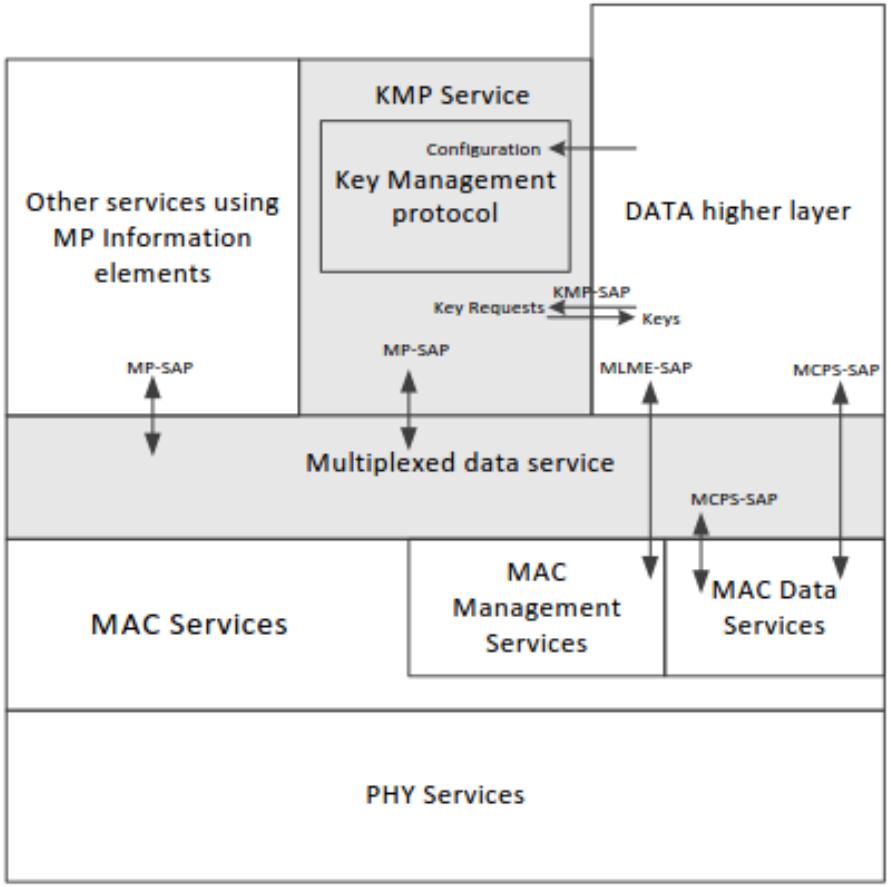
Approved by Internet Engineering Task Force as Proposed Standards in 2015

- **RFC7401, Host Identity Protocol Version 2 (HIPv2)**
- **RFC7402, Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)**
- **RFC7343, An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)**

New in HIP v2

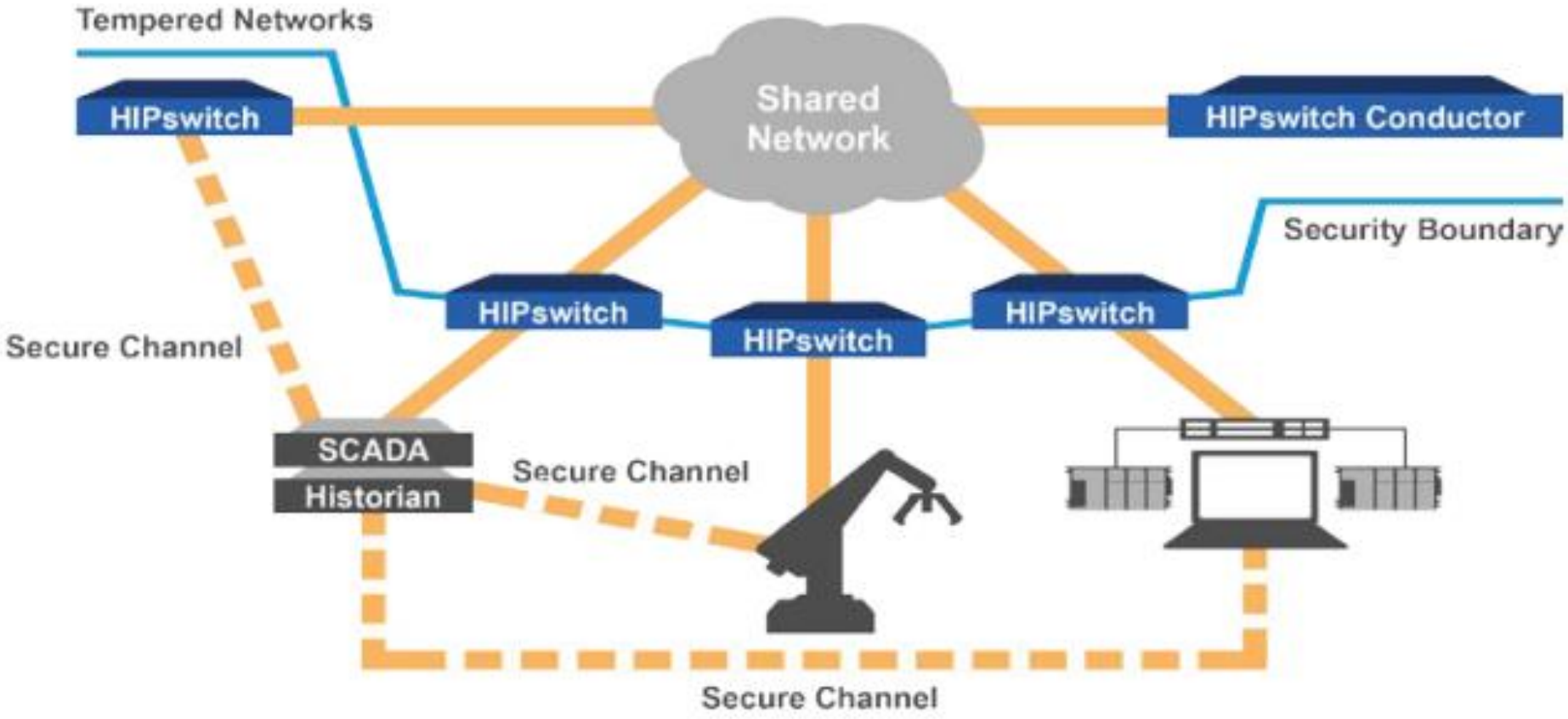
The main technical changes are the inclusion of additional cryptographic agility features, and an update of the mandatory and optional algorithms, including Elliptic Curve support via the Elliptic Curve DSA (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) algorithms. The mandatory cryptographic algorithm implementations have been updated, such as replacing HMAC-SHA-1 with HMAC-SHA-256 and the RSA/SHA-1 signature algorithm with RSASSA-PSS, and adding ECDSA to RSA as mandatory public key types. This version of HIP is also aligned with the ORCHID revision

IEEE 802.15.9 Key Management Protocol



KMP	KMP ID value
802.1X/MKA	1
HIP	2
IKEv2	3
PANA	4
Dragonfly	5
802.11/4WH	6
802.11/GKH	7
Reserved for future use	8 - 254
Vendor-Specific	255

Tempered Networks - Architecture



Tempered Networks – Bump in a Wire

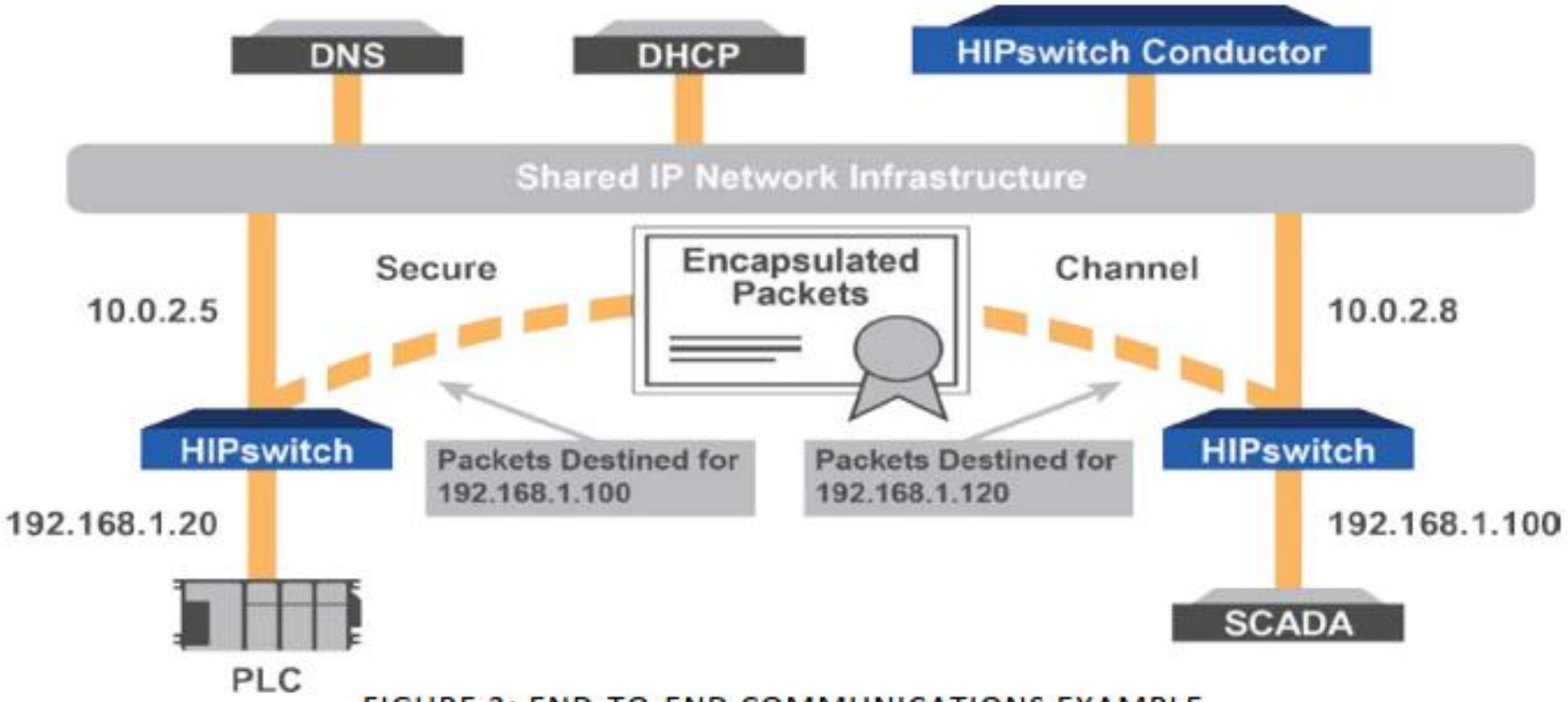
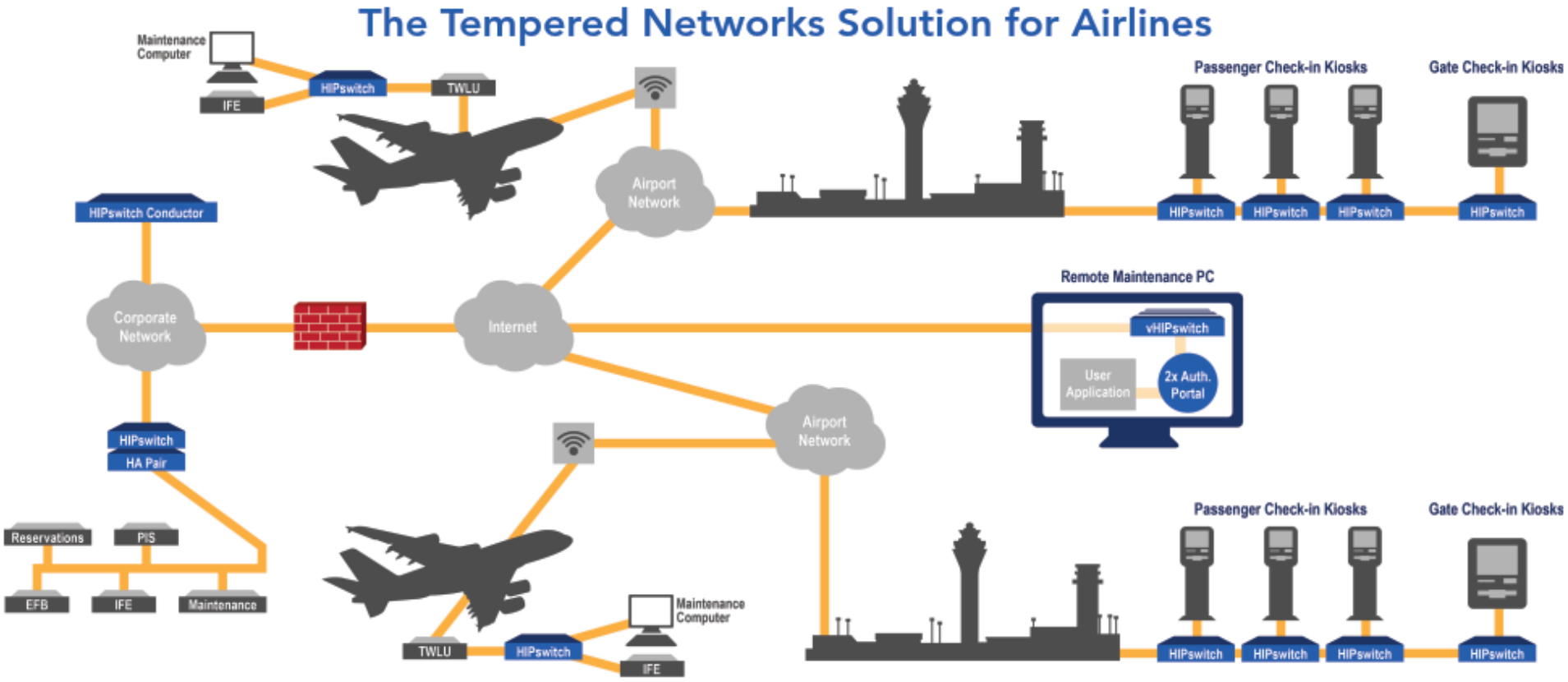


FIGURE 2: END-TO-END COMMUNICATIONS EXAMPLE

Tempered Networks- Airlines



EFB: Electric Flight Bag | TWLU: Terminal Wireless Lan Unit | PIS: Passenger Info System | IFE: Inflight Entertainment Management System