Implications of Identifier / Locator Split

Dr. Pekka Nikander
Ericsson Research Nomadic Lab

Presentation outline

- New requirements for TCP/IP
- Point Solution Plague
- Introduction to Identifier / Locator Split
- An example: Host Identity Protocol (HIP)
- Implications and outlook
- Summary

Presentation outline

- ☑ New requirements for TCP/IP
- □ Point Solution Plague
- □ Introduction to Identifier / Locator Split
- □ An example: Host Identity Protocol (HIP)
- □ Implications and outlook
- □ Summary

New requirements

- Huge growth
- Security
- Mobility
- Multi-homing and multi-access
- Address agility

Requirement: growth

- Lack of IPv4 addresses
    - NATs
        - Loss of end-to-end connectivity
- Routing instability
    - Classless routing
        - Loss of addressing flexibility

Requirements: Security

- DoS and DDoS protection
- Asymmetric attack/defence games
  - Raising the bar for attackers
  - E.g. opportunistic encryption
- Zero-configuration security
  - E.g. SSH leap of faith

Requirements: Mobility

- IP addresses determined by topology
  - Otherwise routing tables explode
- Mobile hosts change topological location
  - Their IP address must change
- IP address change breaks connectivity
  - Initial rendezvous; TCP connections

Reqs: Multi-homing

- Different types of multi-homing
  - Very large corporate multi-homing
  - Medium/large corporate multi-homing
  - SOHO multi-homing
  - Multi-access
- Latter three probably best addressed with multi-addressing

Requirements: Address agility generally

- Mobility requires address agility
- Multi-homing becomes easier with address agility
  - Can be solved by multi-addressing
- Network renumbering too hard today
  - Address agility would help

Presentation outline

- □ New requirements for TCP/IP
- ☑ Point Solution Plague
- □ Introduction to Identifier / Locator Split
- □ An example: Host Identity Protocol (HIP)
- □ Implications and outlook
- □ Summary

Point Solution Plague

- IETF has focused on separate solutions on the problems
  - Security: IPsec, TLS, SSH, ...
  - Mobility: MIPv4, MIPv6
  - Multi-homing: multi6 WG
- Integrated approaches starting to appear
  - mobike WG, btns BOF,

Why is this problematic?

- Solutions don’t integrate nicely
  - ⇨ Added complexity
    - ⇨ Brittleness
- Lots of code
  - MIPv4 + MIPv6 + IPsec + Teredo + ...
    = ~ 150000 lines of code
- “Fat” headers with lots of repetition

Presentation outline

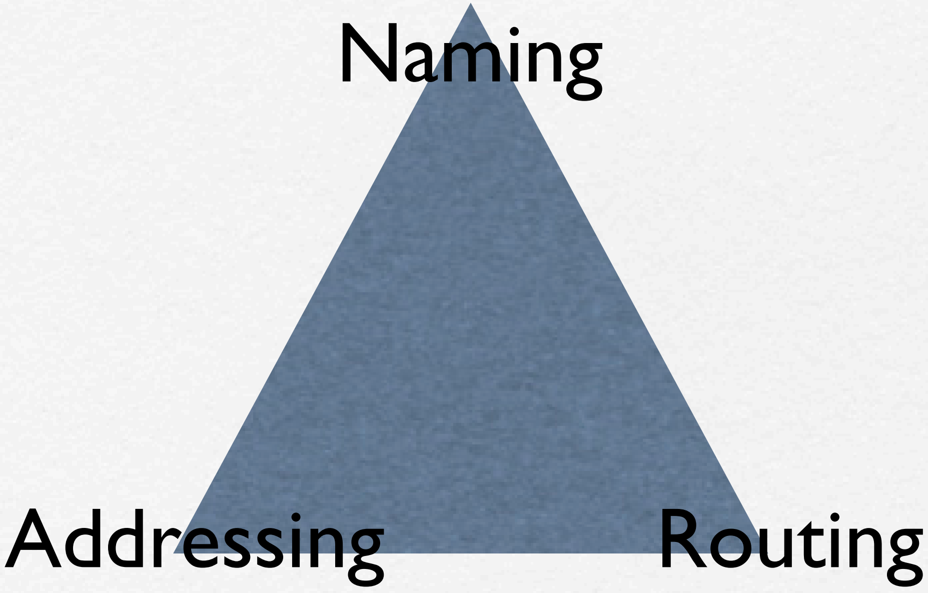
- □ New requirements for TCP/IP
- □ Point Solution Plague
- ☑ Introduction to Identifier / Locator Split
- □ An example: Host Identity Protocol (HIP)
- □ Implications and outlook
- □ Summary

Identifier / Locator Split

- Important issues in networking
- Current roles of IP addresses
  - Roles from networking point of view
- ID / Loc split idea
  - Network viewpoint

What is networking?

- How to refer to an entity?
- How to refer to a route to an entity?
- How to deliver packets to the entity?

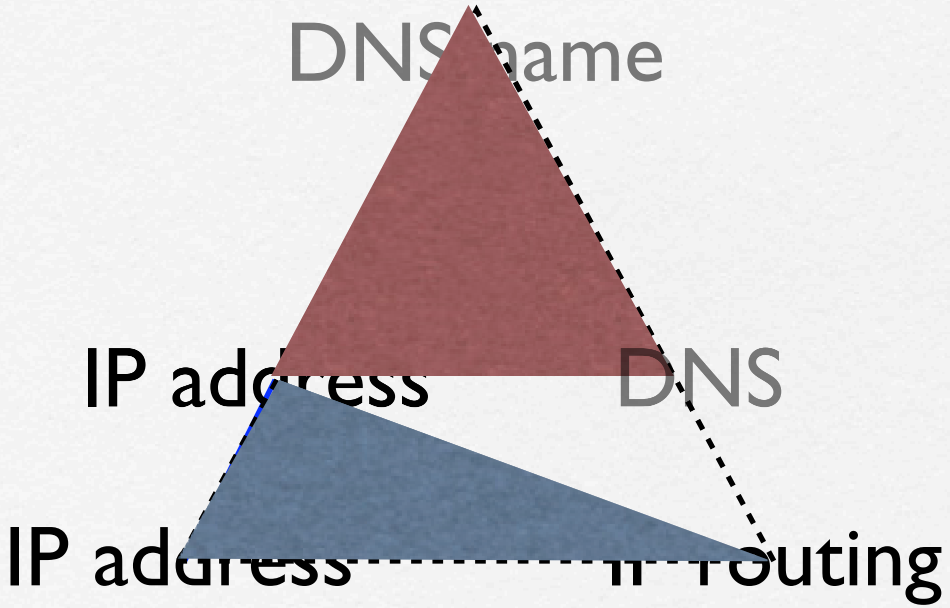


Roles of IP addresses

- Two roles combined:
  - End-point Identifiers
    - Names of interfaces on hosts
  - Locators
    - Names of topological locations
- This duality makes address agility hard

Current IP architecture

- □ IP addresses used for both naming and addressing
- □ DNS naming a separate and similar issue

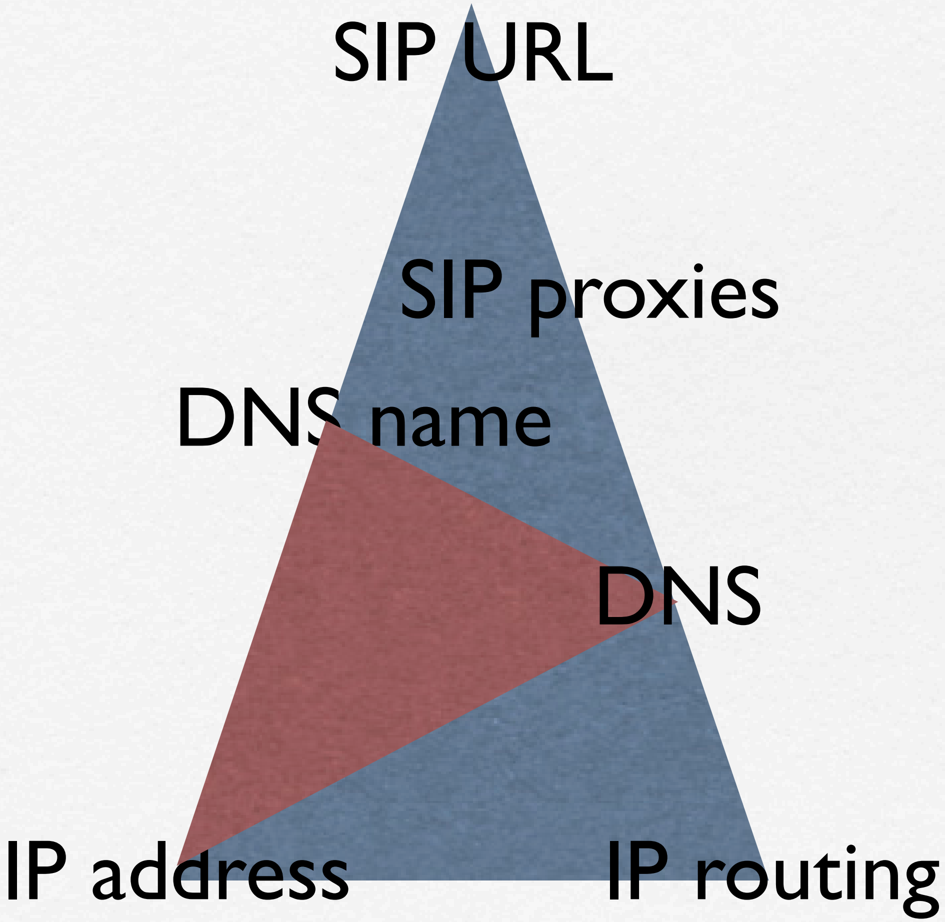


Identifier / Locator split

- Separate the roles of IP addresses
- Different approaches
  - Use appl layer names as identifiers
  - Use DNS names as identifiers
  - Introduce a new layer
  - Split IP addresses
  - Maybe others

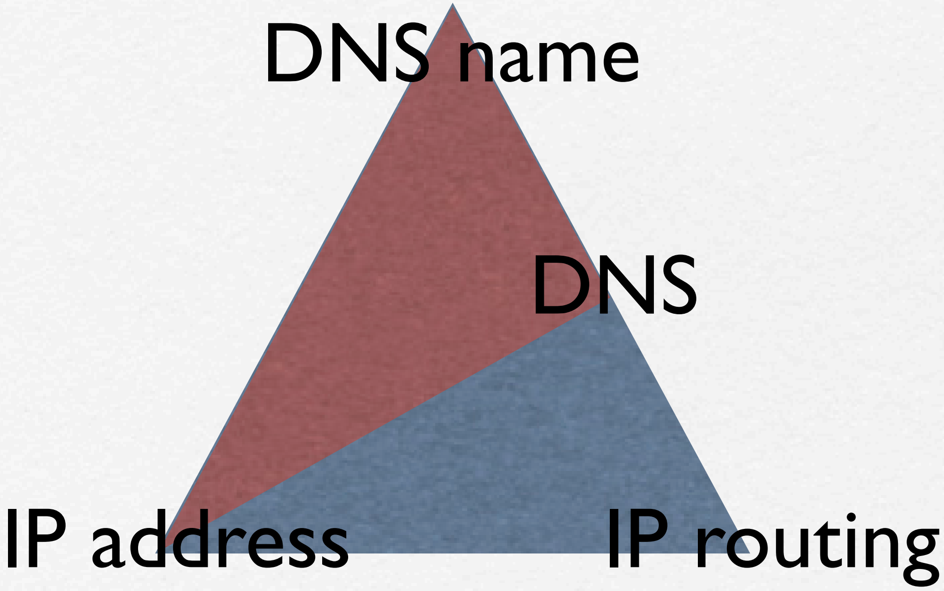
Appl layer identifiers

- Use some sort of application layer names for identifiers
- E.g. SIP URLs in IMS
- Ties end-to-end connectivity to the specific application
- Happening all the time



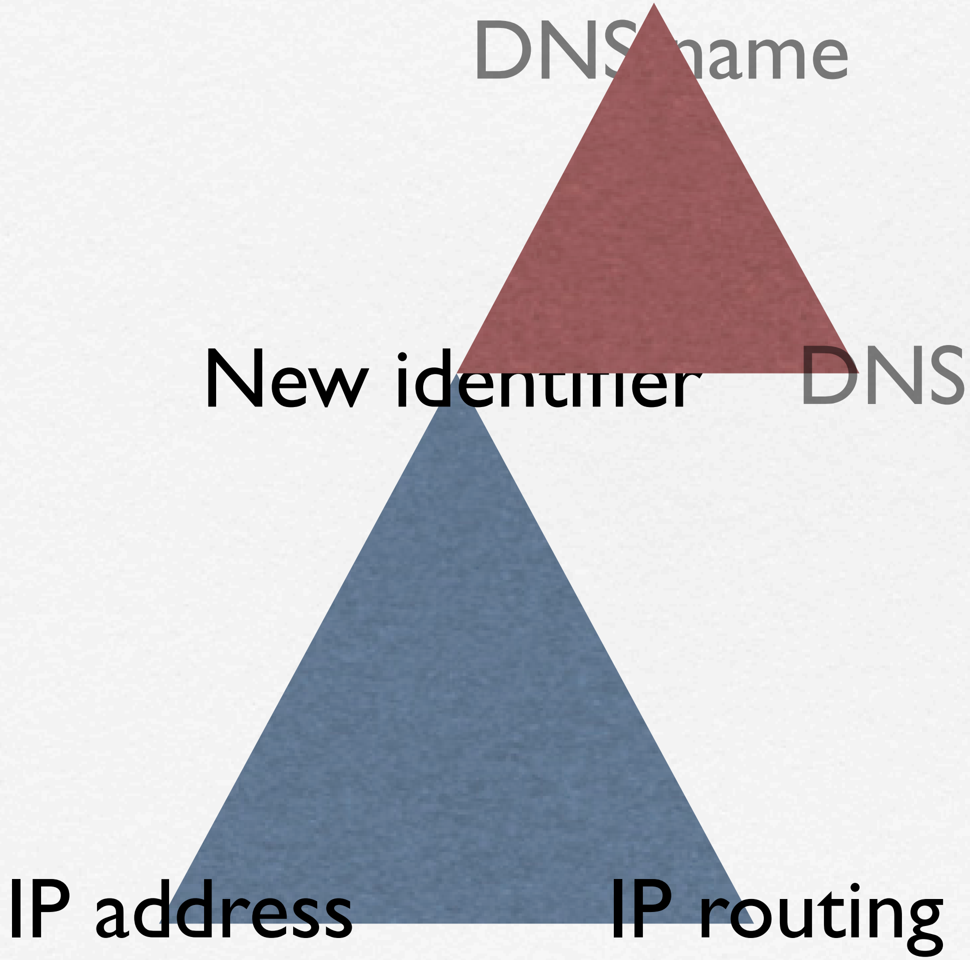
Push DNS down the stack

- ❑ Make DNS name the stable reference point
- ❑ Transmit DNS names, not IP addresses, as referrals (e.g. in FTP)
- ❑ Change the socket API to take DNS names?



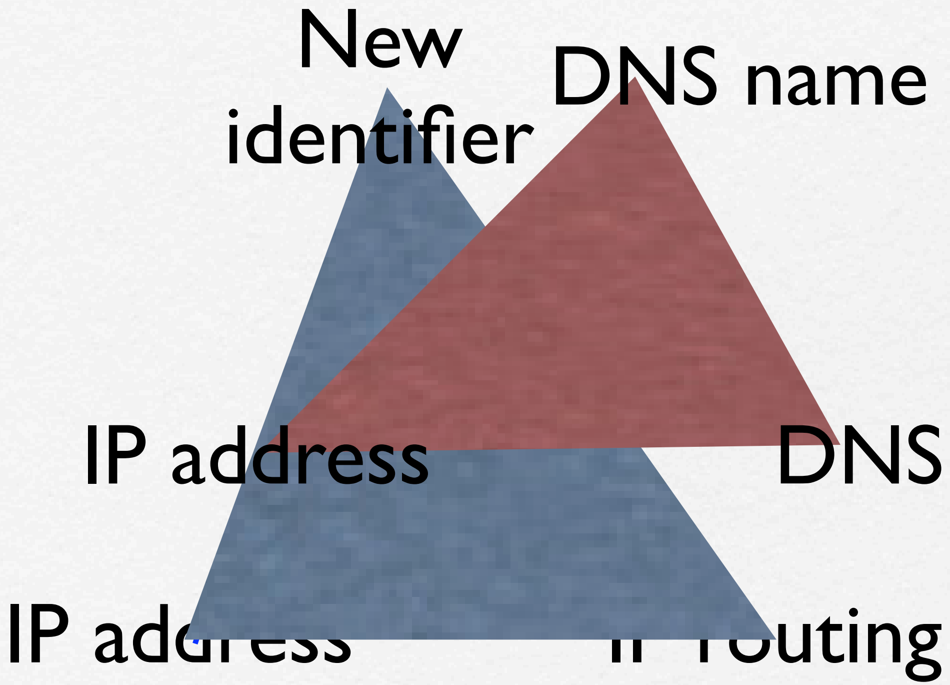
Introduce a new layer

- New identifiers at a new layer
- Introduces new security problems
  - Binding between the new identifiers and IP addresses



Split IP addresses

- □ Interface ID of IPv6 address *encodes* a new identifier
- □ DNS still resolves to an IP address
- □ API still uses IP addresses



ID / loc split summary

- Make host identification and addressing separate from each other
  - Allow addresses to be agile
- Different approaches
- Occam’s razor: Which one is simplest?
- Which one is least brittle?

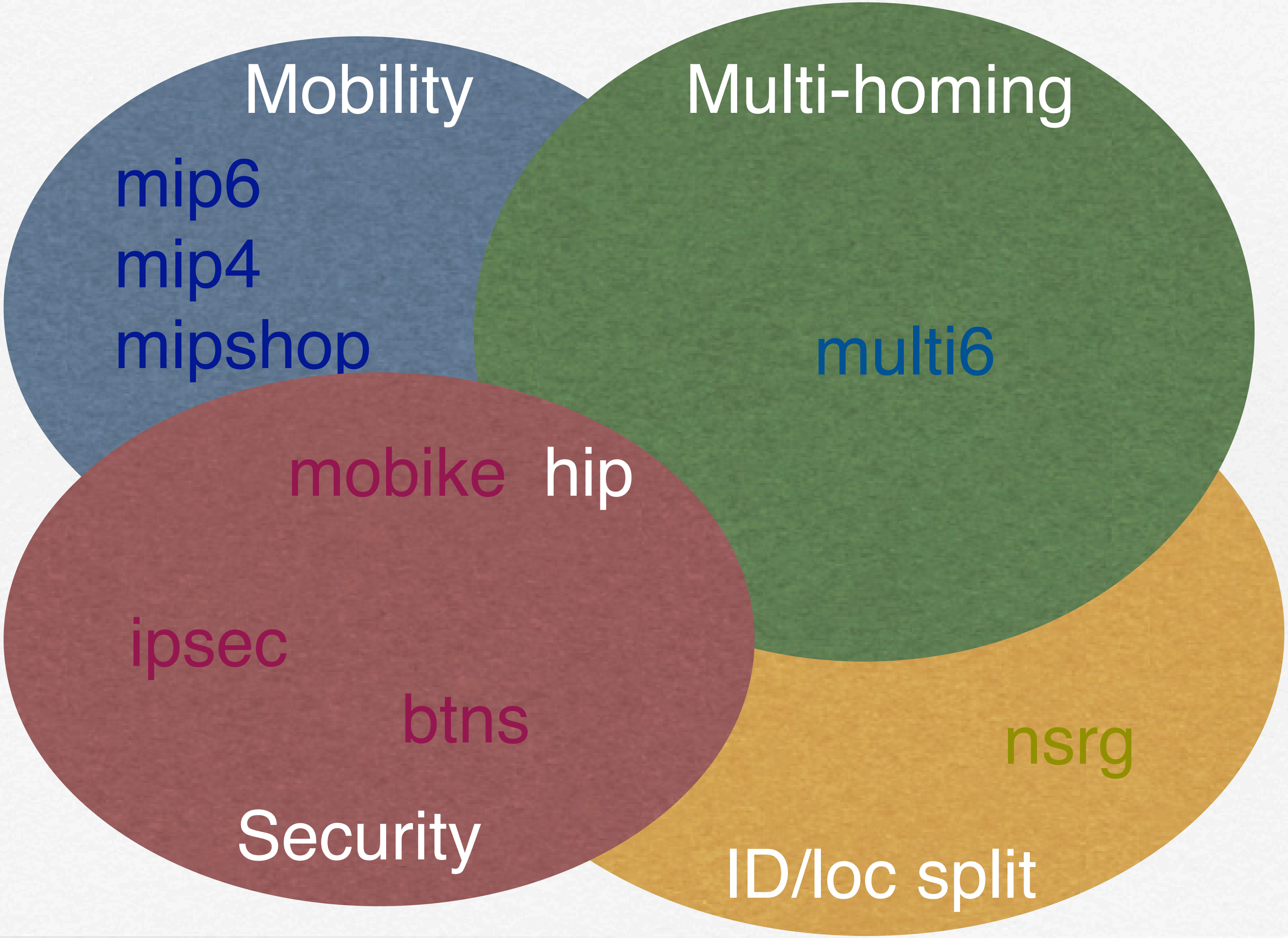
Presentation outline

- □ New requirements for TCP/IP
- □ Point Solution Plague
- □ Introduction to Identifier / Locator Split
- ☑ An example: Host Identity Protocol (HIP)
- □ Implications and outlook
- □ Summary

Host Identity Protocol

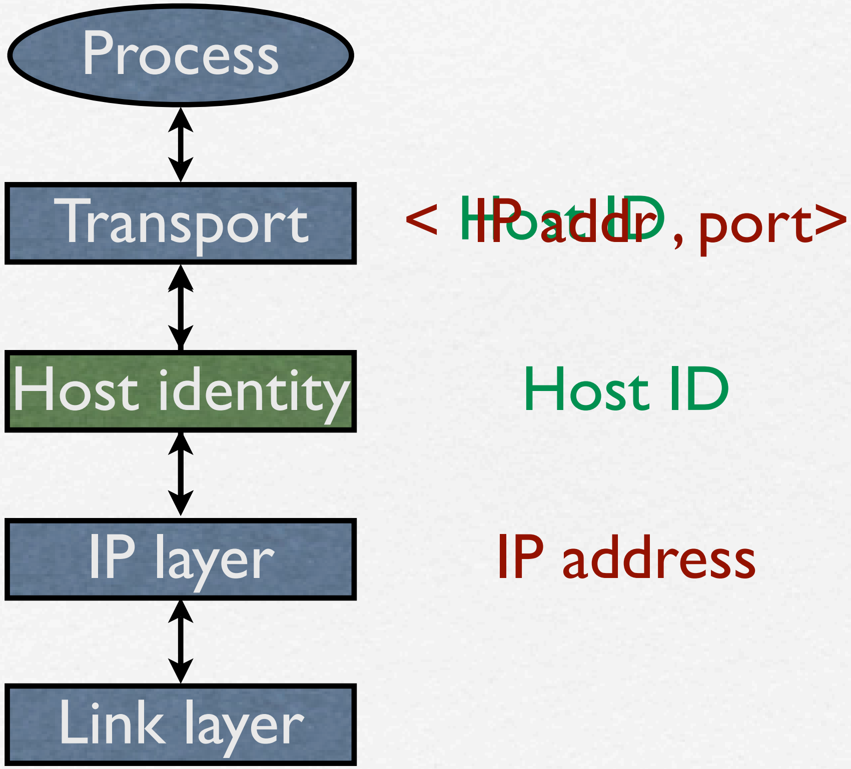
- Being standarised at the IETF
- Integrates mobility, multi-homing and security across IPv4 and IPv6
  - Much simpler than the point solutions combined (~ 15000 lines of code)
- Implements the identifier / locator split
- Separate protocols for control and data

Related IETF WGs and RGs

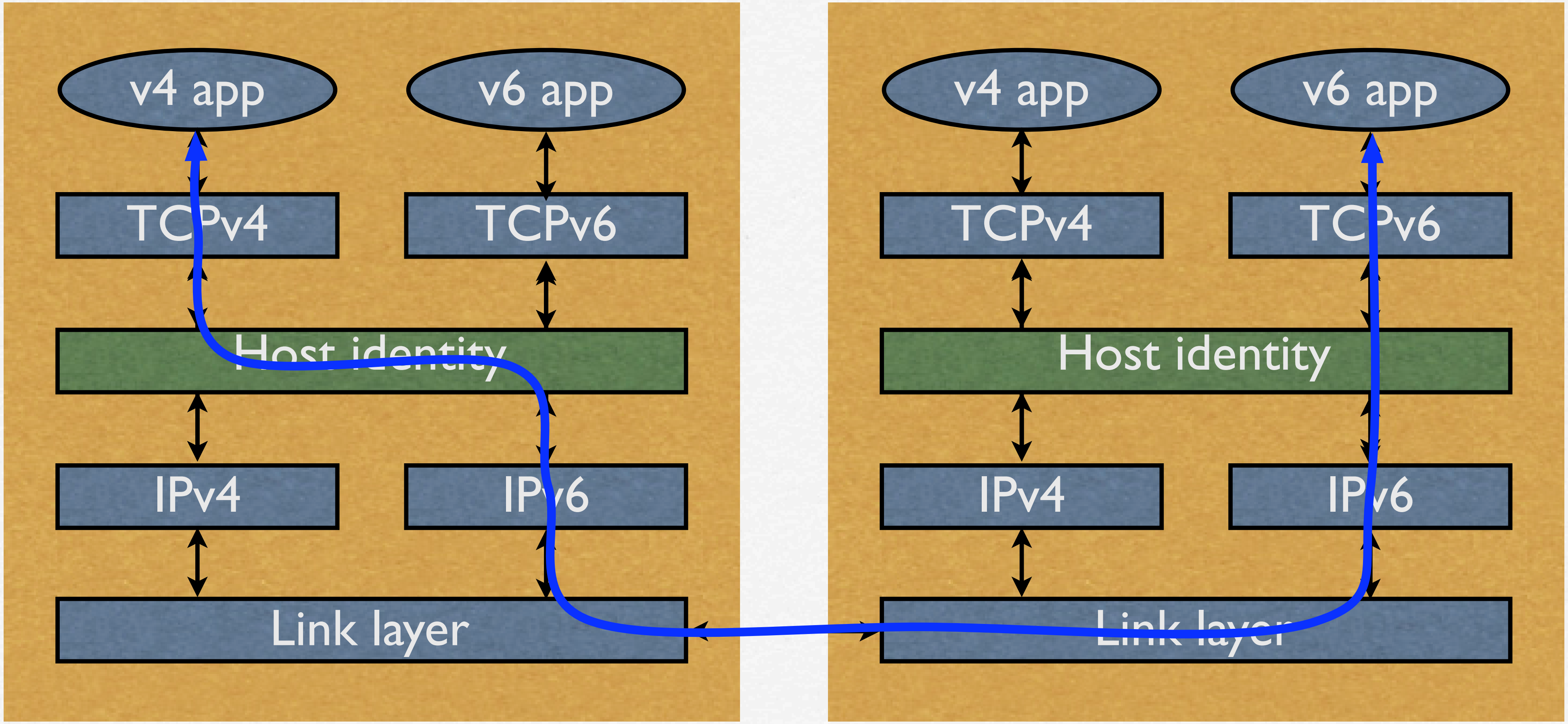


The HIP Idea

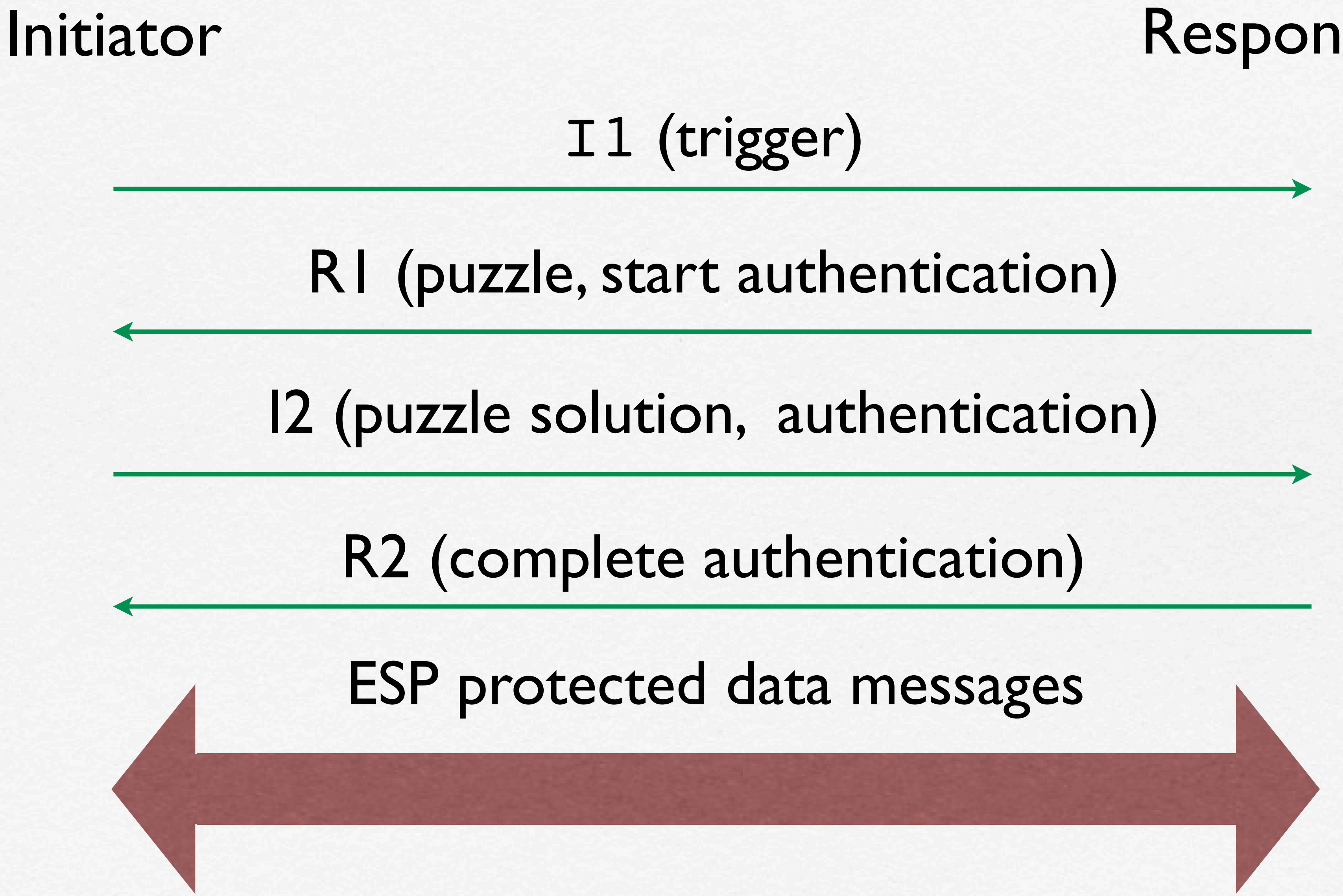
- □ A new Name Space of Host Identifiers (HI)
  - □ Public crypto keys!
- □ Sockets bound to HIs
  - □ not IP addresses



New “waist” for TCP/IP



Protocol overview



Initiator

Responder

I1 (trigger)

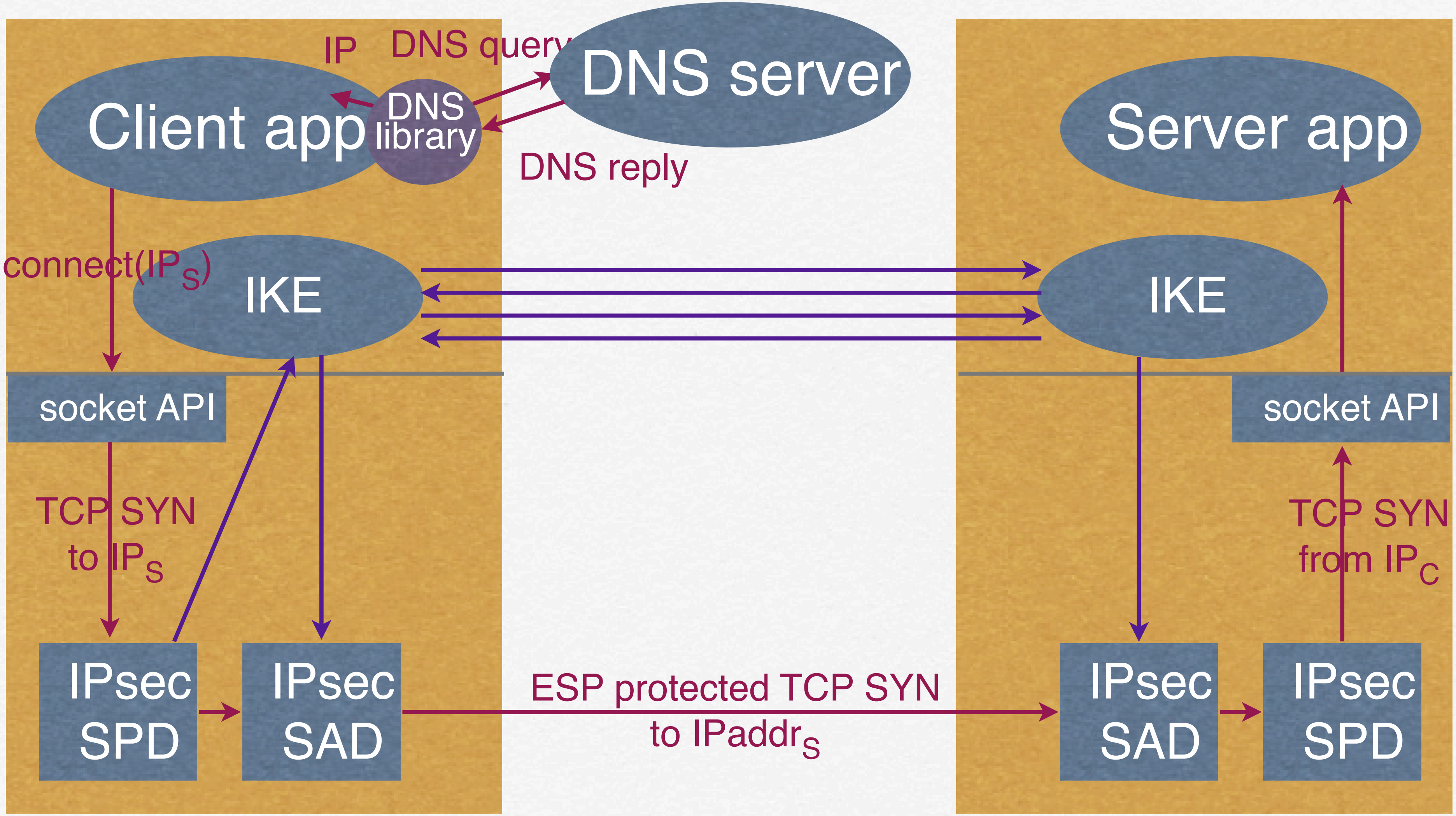
R1 (puzzle, start authentication)

I2 (puzzle solution, authentication)

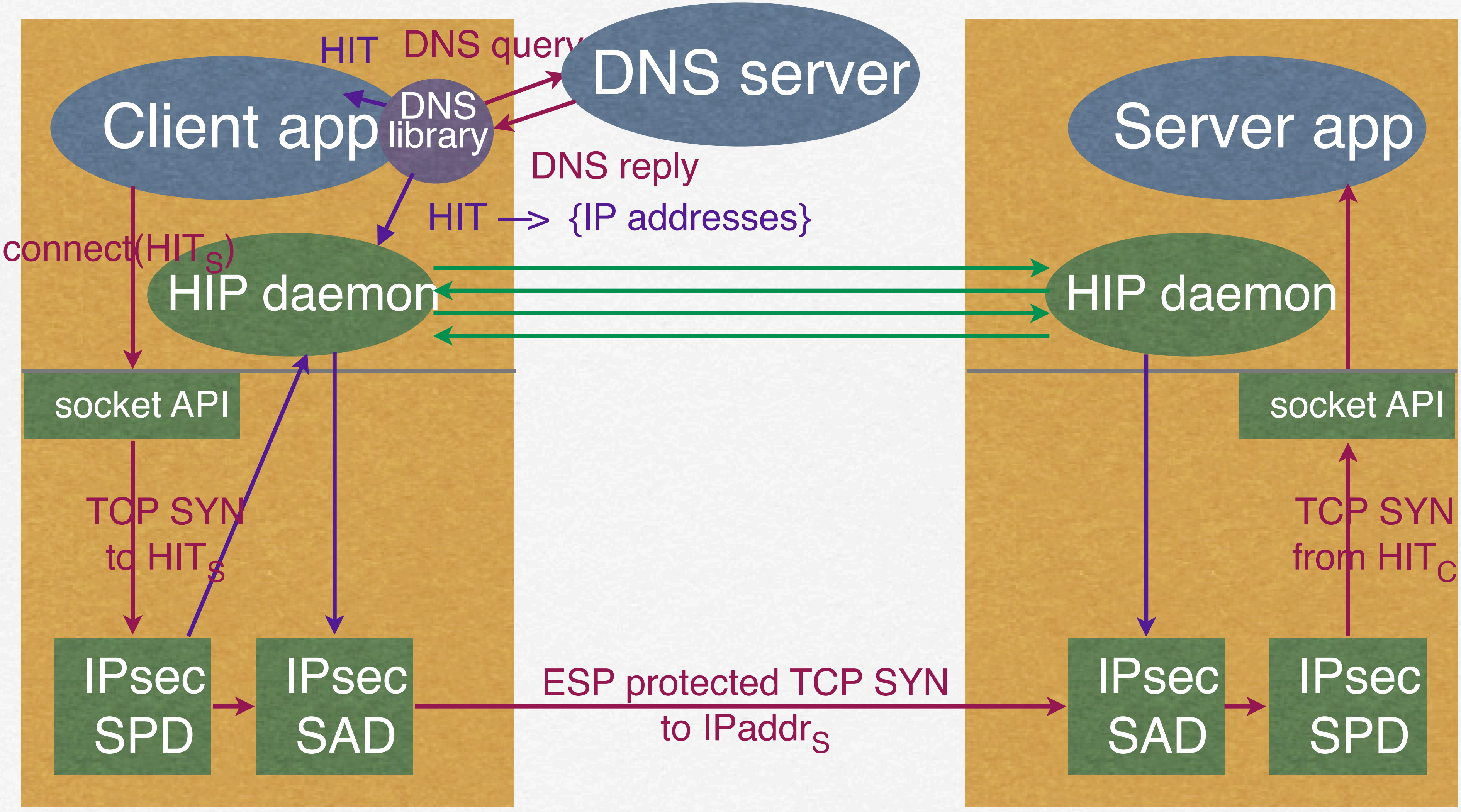
R2 (complete authentication)

ESP protected data messages

How it works today



One way to do HIP



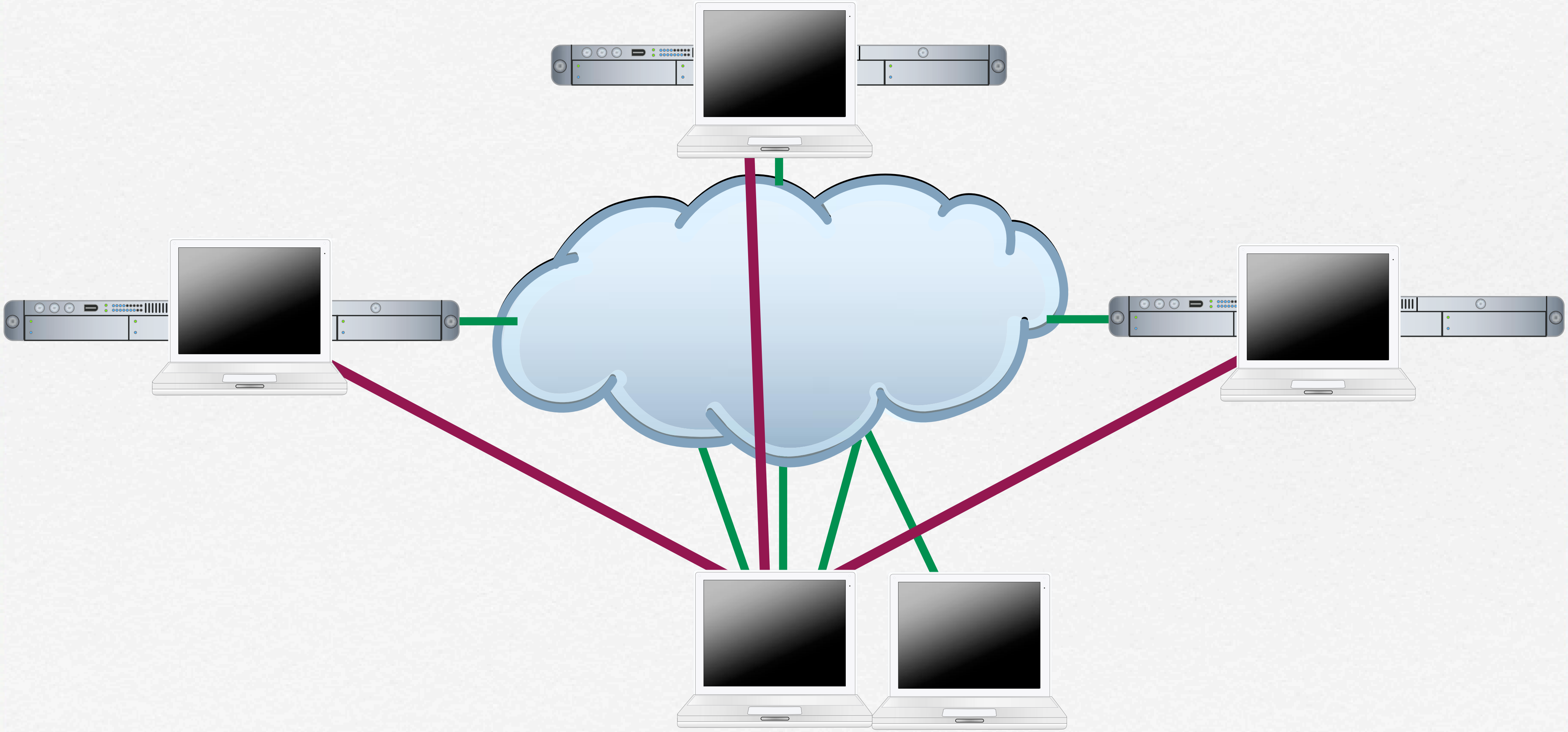
convert HITs to IP addresses

convert IP addresses to HITs

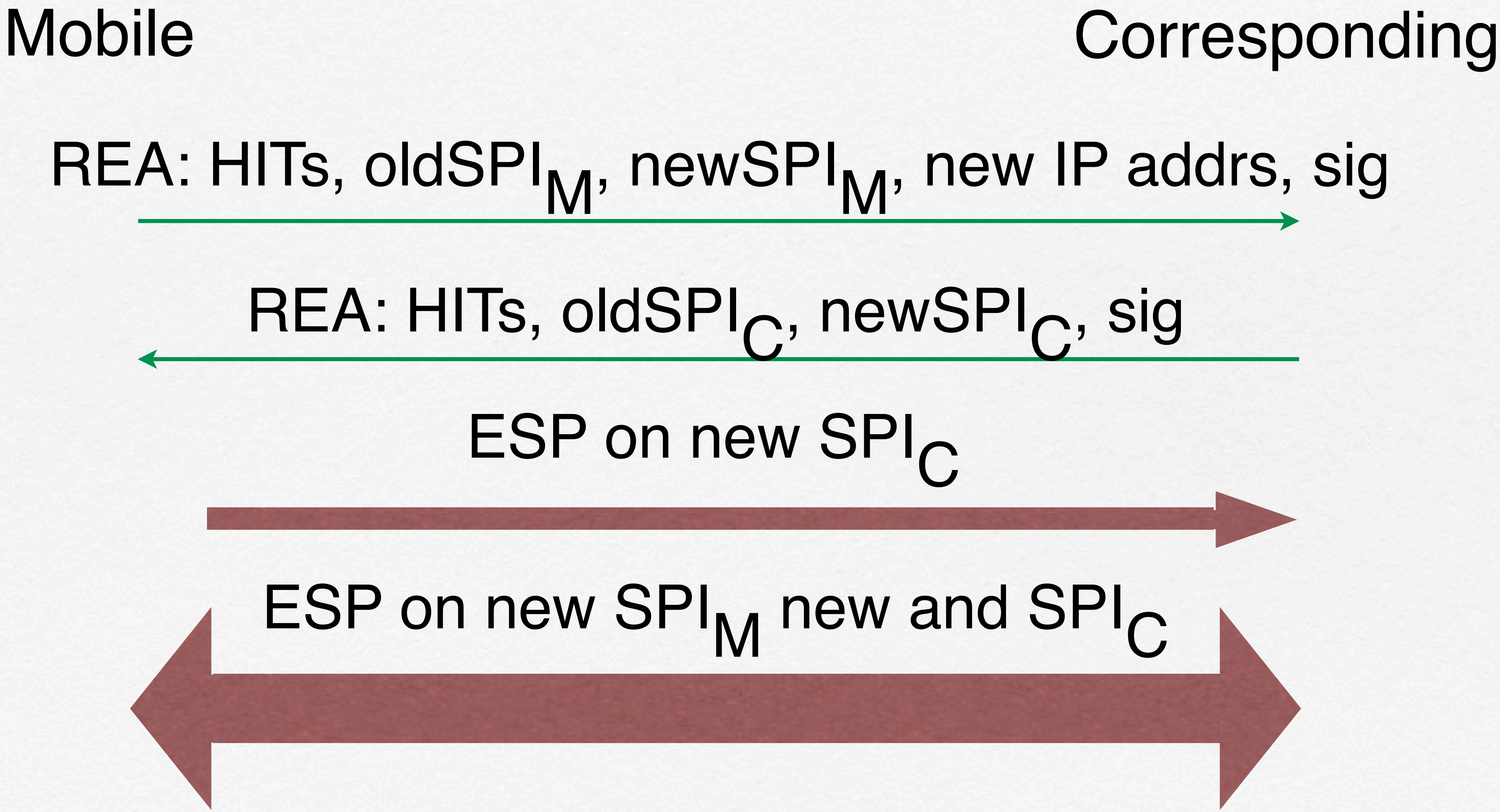
HIP Mobility & Multi-homing

- Mobility and multi-homing become duals of each other
  - Mobility: many addresses over time
  - Multi-homing: many addresses now
- Leads to a Virtual Interface Model
  - Real and virtual interfaces
  - Subsumes MIP “Home Agent” concept

Virtual Interface Model



Mobility protocol



Mobile

Corresponding

REA: HITs, oldSPI$_M$, newSPI$_M$, new IP addrs, sig

REA: HITs, oldSPI$_C$, newSPI$_C$, sig

ESP on new SPI$_C$

ESP on new SPI$_M$ new and SPI$_C$

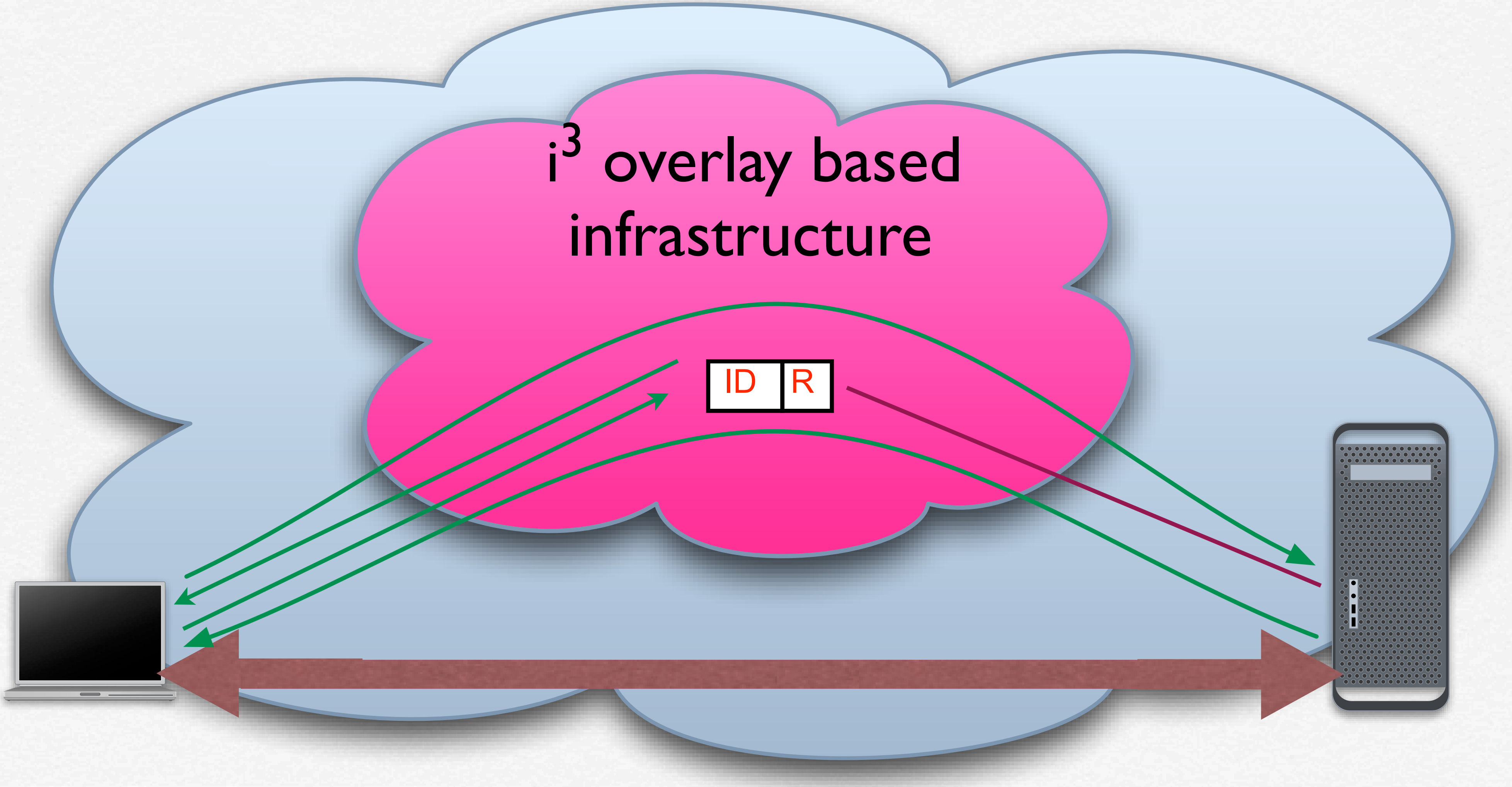
Infrastructure research

- HIs currently stored in the DNS
  - Retrieved with IP addresses
  - Does not work if you have only a HIT
- How to get data based on HIT only?
  - HITs look like random numbers
- Maybe use DHT based overlay like i^3

Distributed Hash Tables

- Distributed directory for flat data
- Several different ways to implement
- Each server maintains a partial map
- Overlay addresses for finding the server
- Resilience with parallel mappings
- Used to create overlay networks

How it might work



Presentation outline

- □ New requirements for TCP/IP
- □ Point Solution Plague
- □ Introduction to Identifier / Locator Split
- □ An example: Host Identity Protocol (HIP)
- ☑ Implications and outlook
- □ Summary

Basic implications

- IP layer mobility becomes easier
- Multi-address multi-homing gets easier
- New security problems emerge
- More freedom to routing
  - Better possibilities to re-consider division of information between addresses and routing table

HIP-slanted approach

- Solve the new security problems by having self-certified identifiers
  - No need for security infrastructure
- Provide handles to secure identifiers to upper layers for channel binding
- More research needed on rendezvous
  - Should use i^3 or something else?

HIP-slanted implications

- Restoration of end-to-end connectivity
- New end-point names
  - First class citizens
  - Application and DNS *independent*
  - Self certifying
- Layer 3.5 connectivity possible

Open research topics

- How to run large scale DHTs in practice?
  - Not for p2p but for infrastructure
- Security, performance, and dependability problems in DHTs
- New routing with agile addresses
- Architectural implications to other functions (e.g. congestion control)

Presentation outline

- □ New requirements for TCP/IP
- □ Point Solution Plague
- □ Introduction to Identifier / Locator Split
- □ An example: Host Identity Protocol (HIP)
- □ Implications and outlook
- ☑ Summary

Summary

- New requirements mandate some sort of identifier / locator split in the future
  - Real need to get end-to-end back
- Much controversy about the approach
  - Right now IMS strong in 3GPP / ETSI
  - HIP one possible future direction
- Lots of interesting open research topics