

Introduction to HIP

DoCoMo Labs USA

Pekka Nikander

Ericsson Research Nomadiclab & Helsinki Institute for Information Technolog

Outline

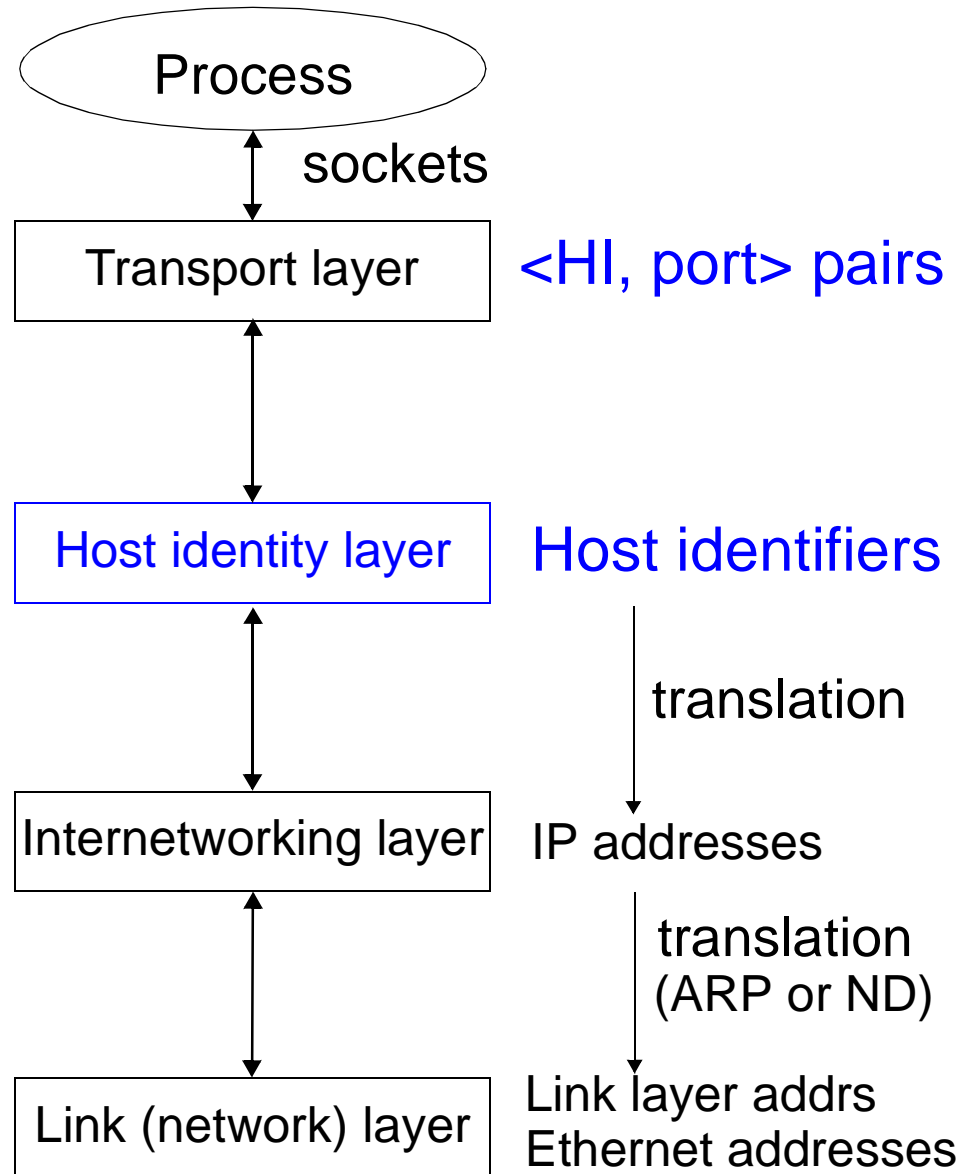
- Introduction
- The Basic Idea of HIP
 - Bindings, Conceptual model
- End-host Mobility & Multi-homing
 - End-Host Mobility & Multi-Homing Models
 - Conceptual model for mobility & multi-homing
 - A Virtual Interface Model
 - Components in the Architecture
- HIP for Monets
 - Basic delegation, Delegation to Mobile Router
- Summary

Introduction

- Once upon a time computers were big and bulky ...
 - ... and now I usually carry five computers with me.
- Once upon a time Internet connectivity was a luxury ...
 - ... but in a few more years it will be ubiquitous.
- Internet addresses still are *addresses* (locators) ...
 - ... but today they work poorly as end-point *identifiers*.
- Since Mobile IP(v6) is such a gross hack ...
 - (and I know since I was in the security desing team)
 - ... maybe it is a time to rethink everything.
- Host Identity Payload (HIP) is a concrete attempt to rethink the architecture — we may be right, we may be wrong, but we try, and hopefully we learn.

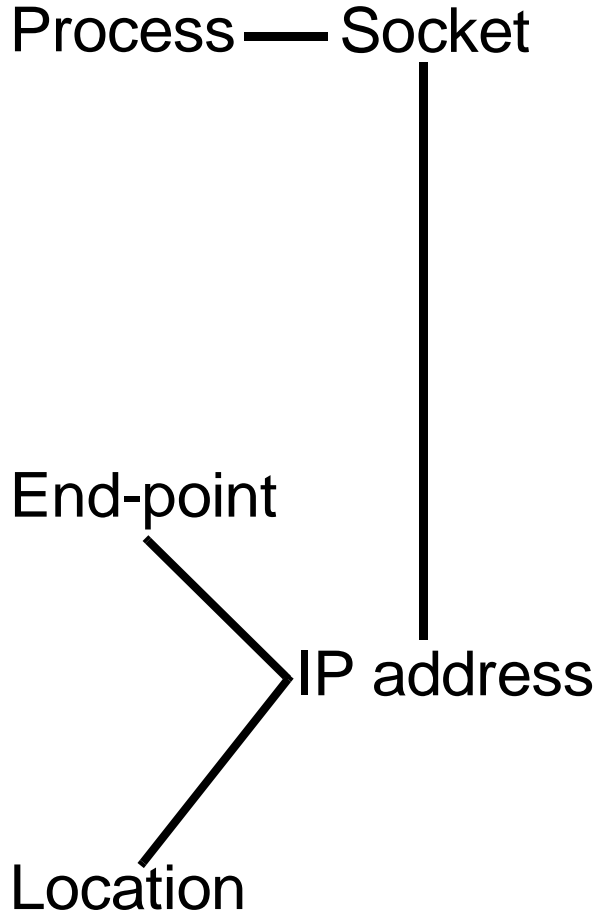
The Basic Idea of HIP

- A new layer
- A new Name Space: Host Identifiers
 - Public keys!
 - Represented as hash values, Host ID Tags (HIT)
- Sockets bound to the Host IDs, not IP addresses
- HIs translated to IP addresses transparently in the kernel

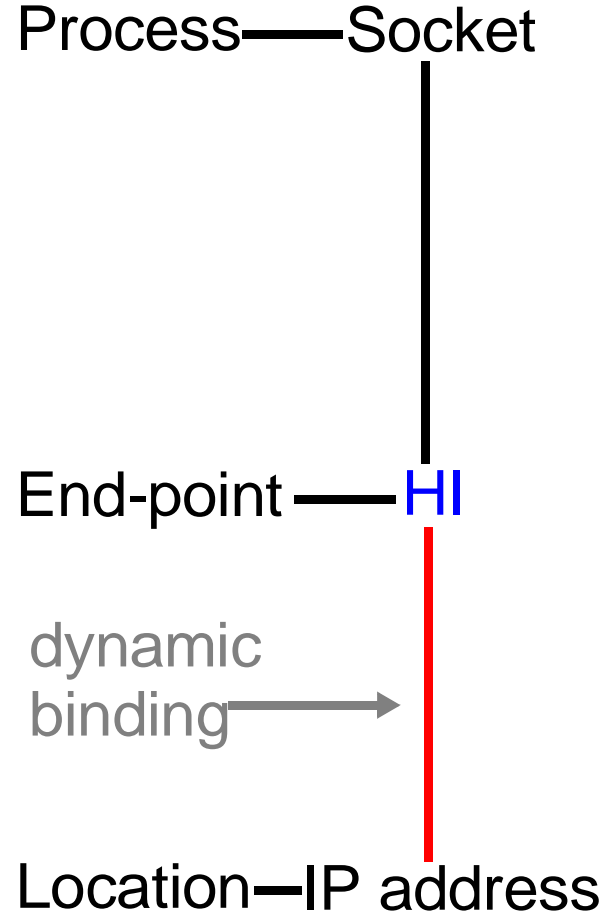


Bindings

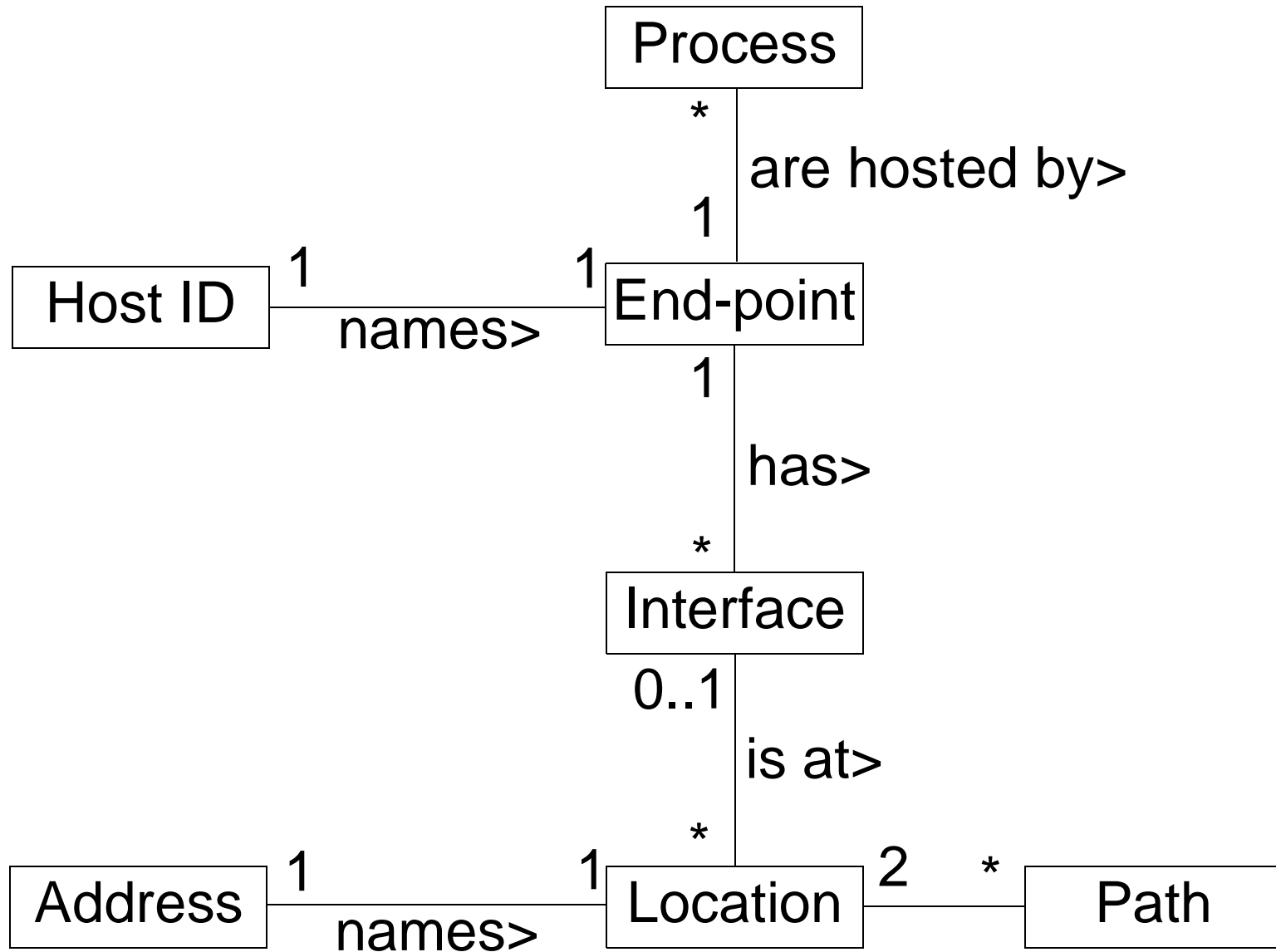
Bindings in the
current architecture



Bindings in the
new architecture



Conceptual model



End-host Mobility & Multi-homing

- HIP seems to solve end-host mobility and multi-homing problems almost trivially
- Mobility and multi-homing become *duals* of each other
 - A mobile host has multiple addresses *serially*
 - A multi-homed host has multiple addresses *parallelly*
- Also easy to explain the difference between
 - process mobility (migration) and node mobility
 - end-host multi-homing and site multi-homing
- The thinking can be *folded* into a *Virtual Interface Model*
- Resulting *Architecture* is relatively small and beautiful

The diagram illustrates a network topology. A central cloud-like shape is labeled "Topologically slowly changing internetwork". Several rectangular boxes are connected to this central network. Two boxes at the top are labeled "Mobile hosts". Two boxes at the top right are labeled "Points-of-attachment". A box at the bottom left is labeled "A host in transit". Arrows indicate connections and movement: one arrow points from "Mobile hosts" to a box, another from "Points-of-attachment" to a box, and a third from "A host in transit" to a box. The boxes are connected to the central network by lines.

Points-of-attachment

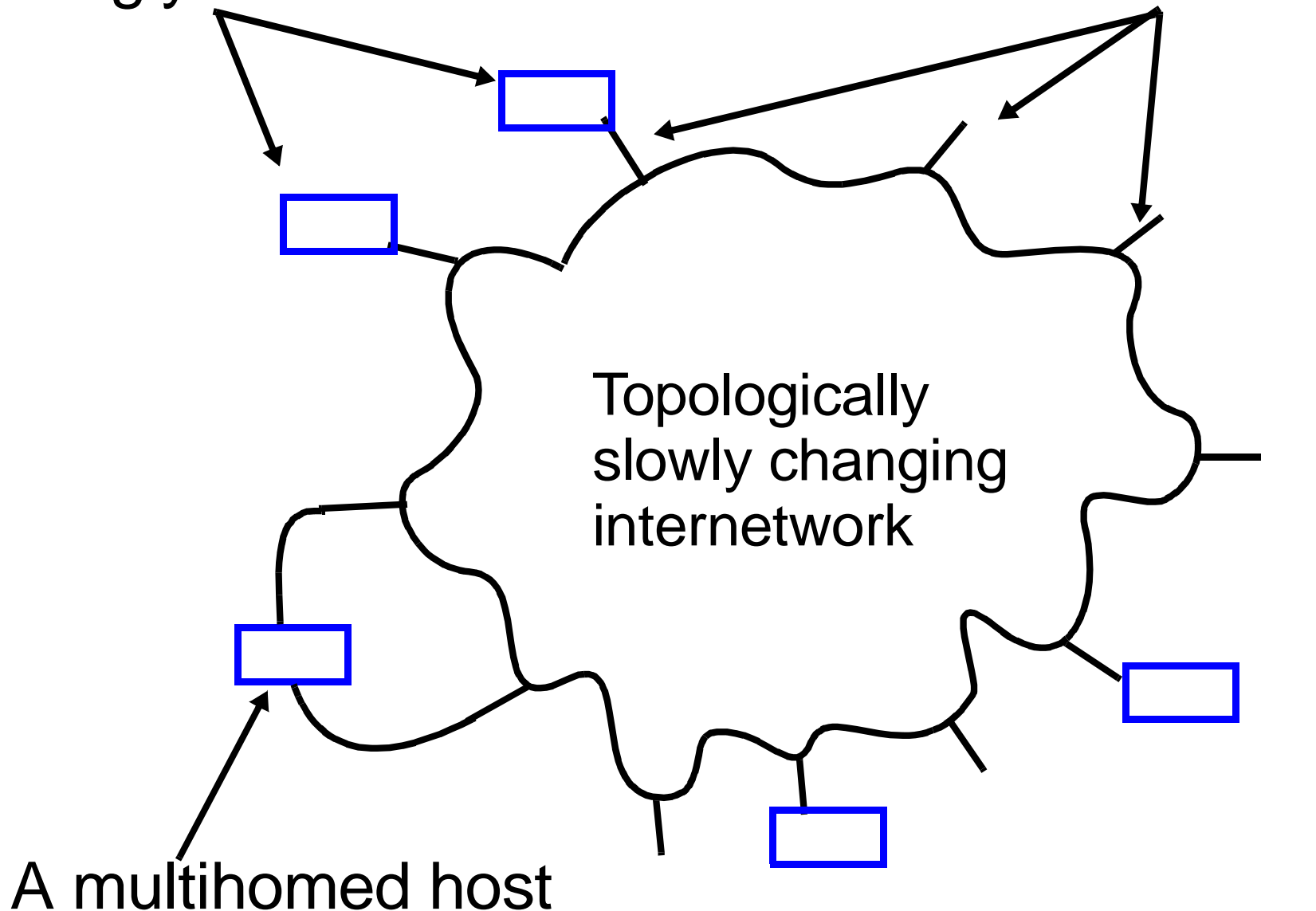
Topologically slowly changing internetwork

A host in transit

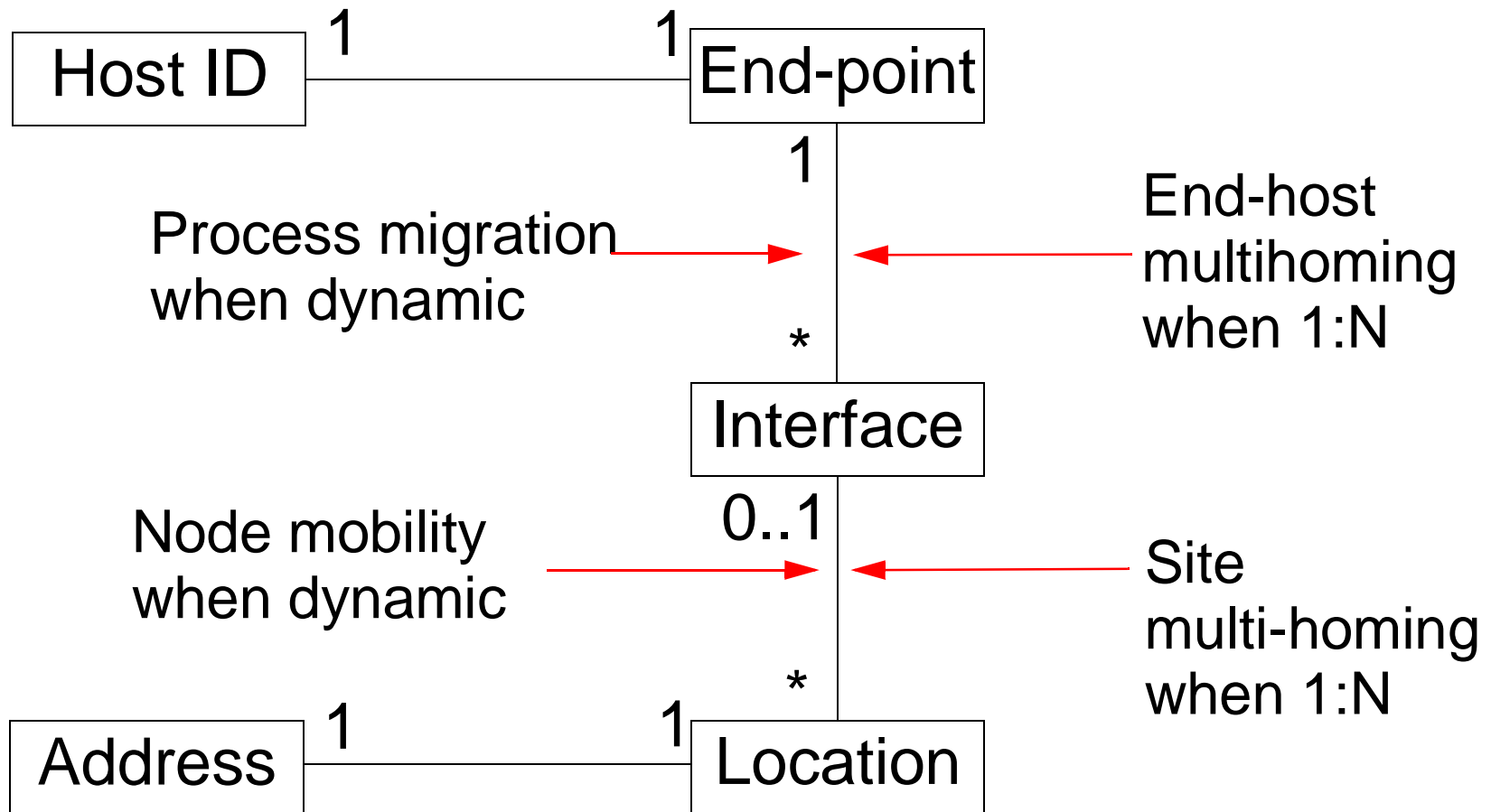
End-host Multi-Homing model

Singly-homed hosts

Points of attachment



Conceptual model

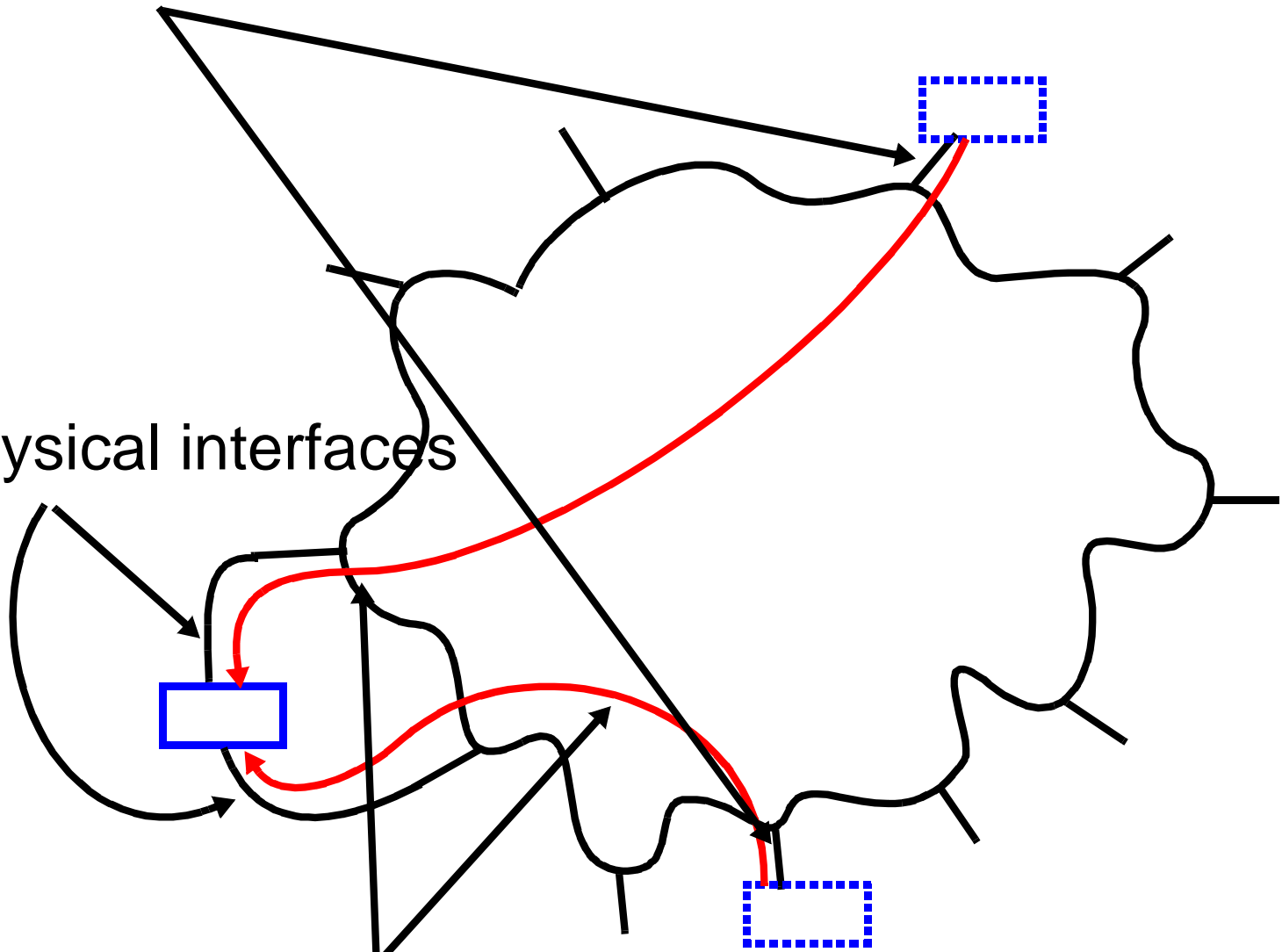


A Virtual Interface Model

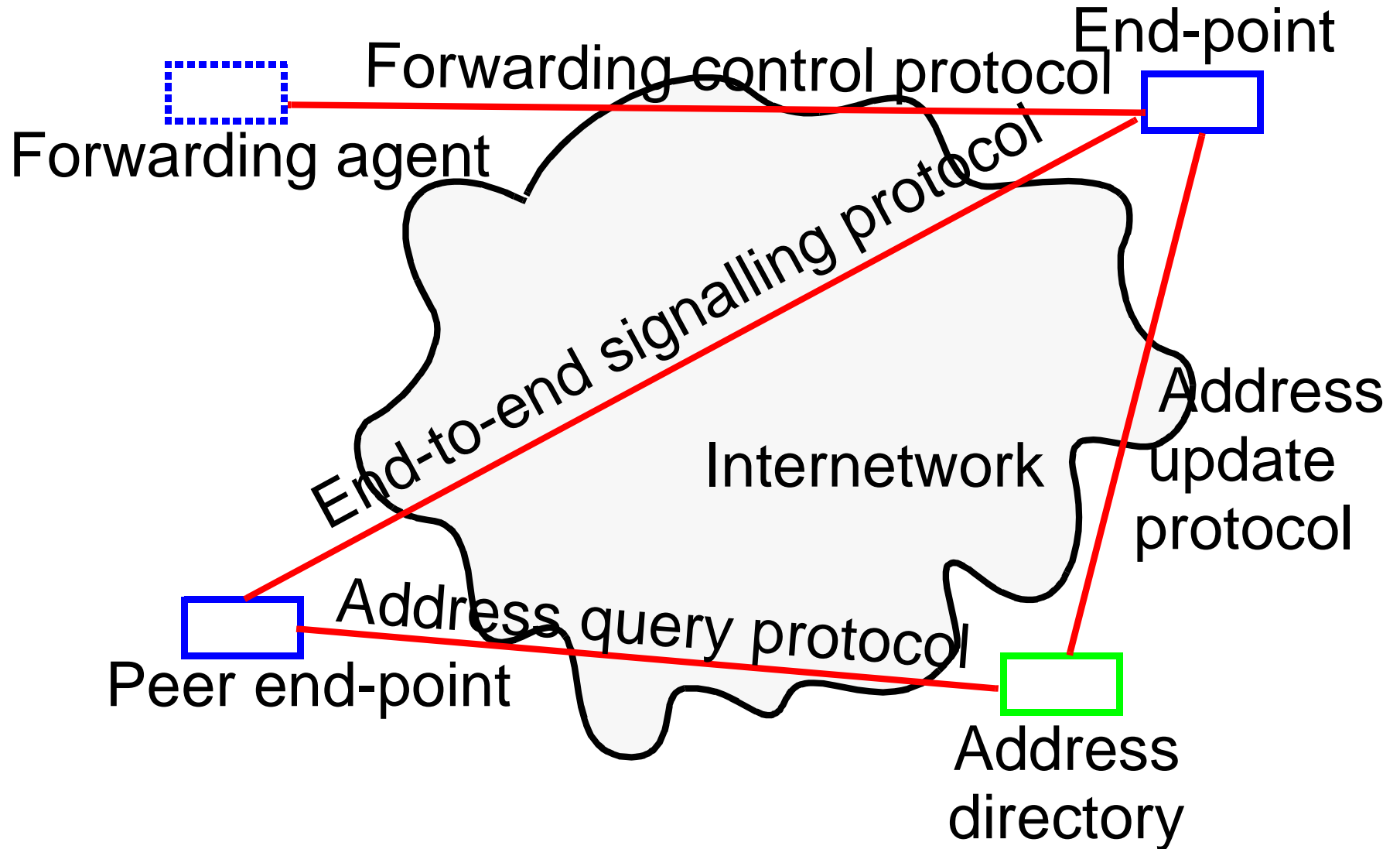
Virtual interfaces

Physical interfaces

Forwarding paths



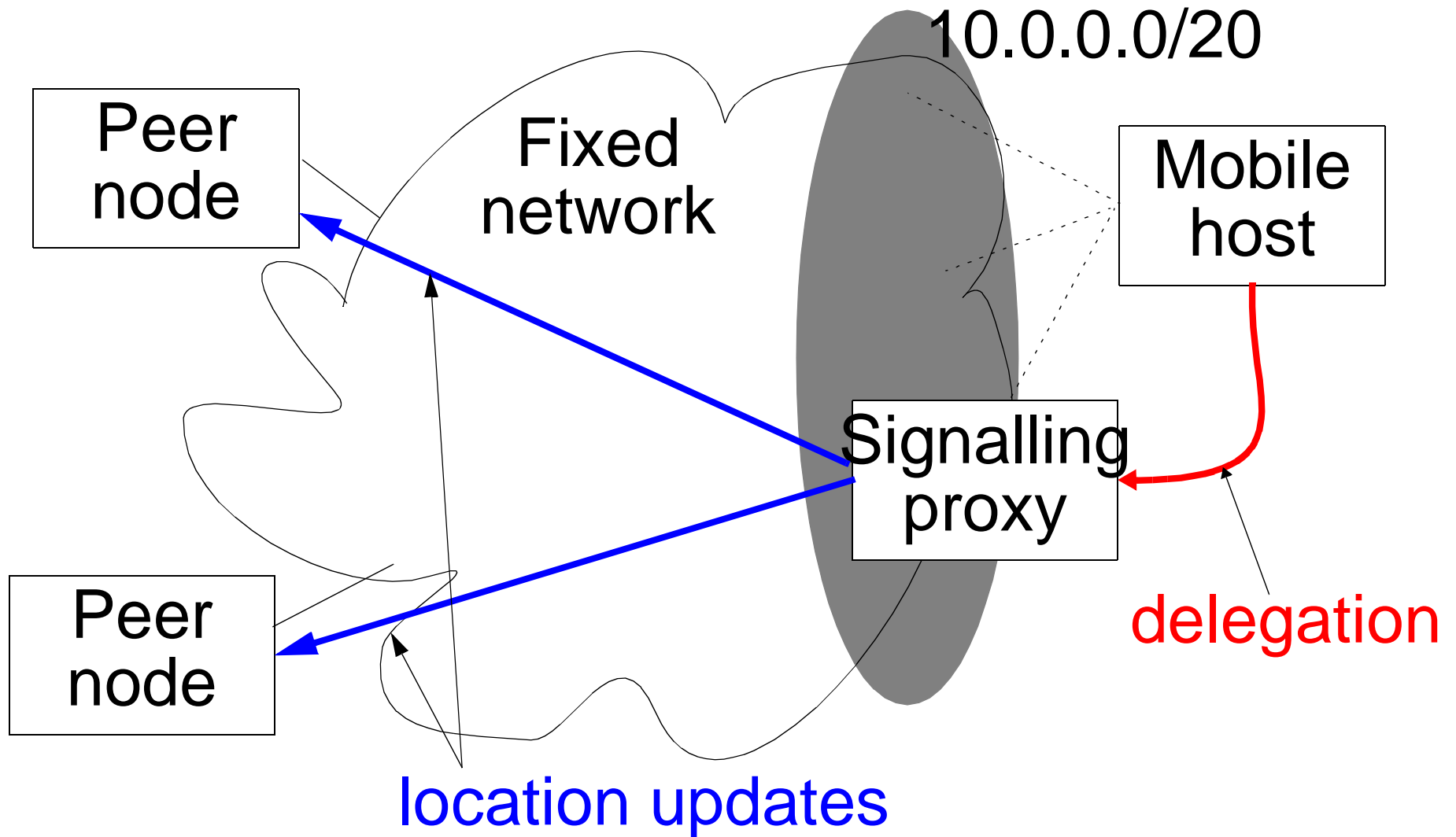
Components in the Architecture



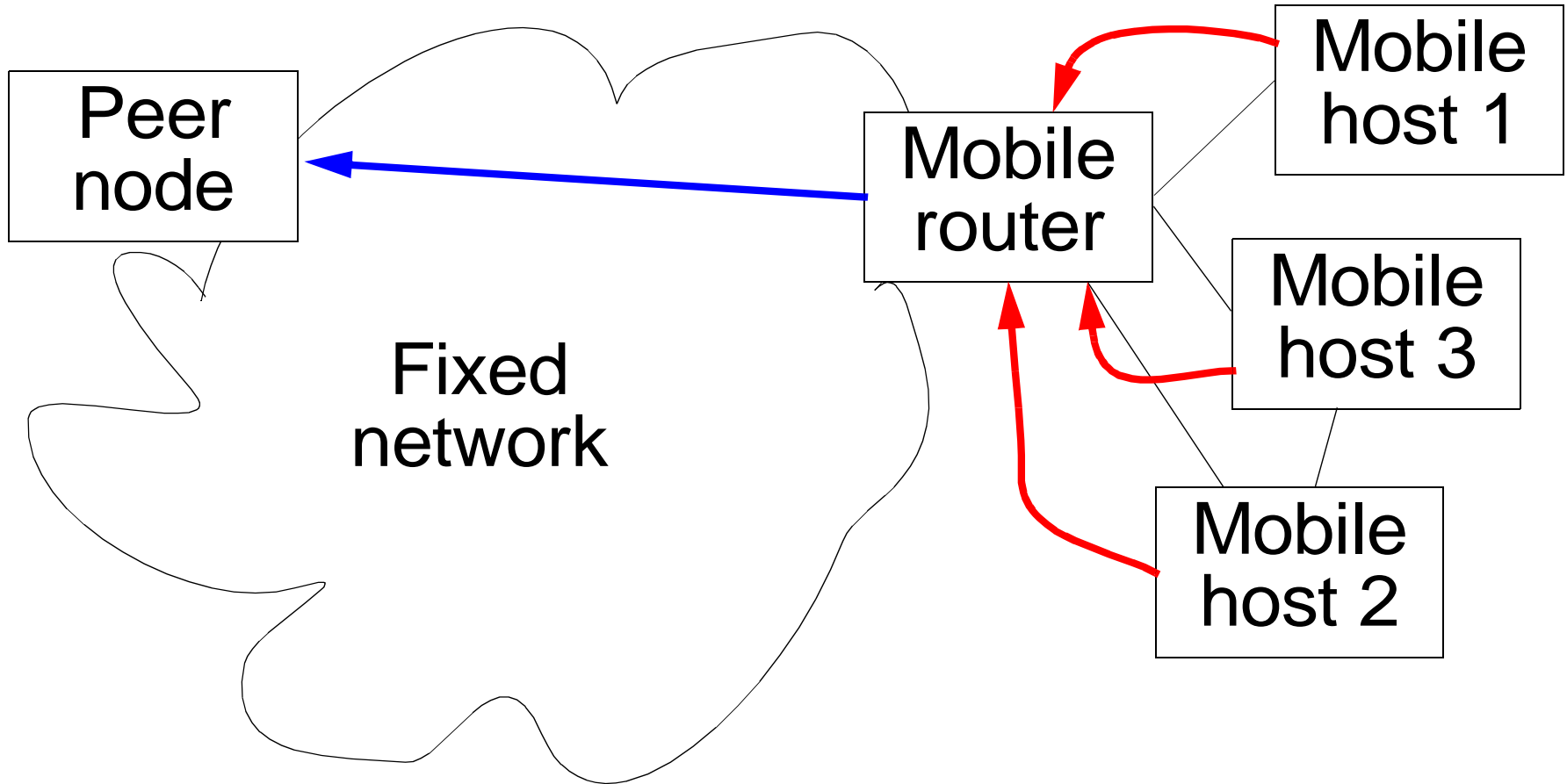
HIP for Monets

- Basic idea: Delegate right to send location updates
 - Remember, HI is a public key
- Use authorization certificates
 - SPKI, Keynote 2 or even PKIX
- The HI owner signs a certificate, delegating the right to send location updates on its behalf, to another HI
 - (HI_{Alice} , HI_{Bob} , right to send location updates)

Basic delegation



Delegation to Mobile Router



Summary

- A concrete, down-to-earth attempt to "fix" the Internet
 - Deployment can start at end-points
 - No changes required to routers
 - Can be made to work with firewalls relatively easily
 - Supports NAT, but requires HIP-capable NAT boxes
 - Backward compatibility can be provided with proxies
- Seems to solve almost trivially
 - end-host mobility
 - end-host multi-homing
- Provides components for
 - site multi-homing
 - monets