InfraHIP

Helsinki-Rutgers Workshop
1.6.2007
Miika Komu <miika@iki.fi>
Helsinki Institute for Information Technology (HIIT)

What is My Problem?

- When I move my laptop from home to office, my ssh connections break.
- I want to access my home NFS filesystem automatically and securely from everywhere. I want to keep others out.
- My parents are bugging me with annoying questions on their Windows. I want to remotely login to their machine through their double NATted ADSL line to fix their problem. I cannot touch the NAT of ISP.

Solutions for My Problems

- Different protocols for different problems
  - Mobility: MobileIPv4, MobileIPv6, SCTP
  - Secure File systems: SFS, NFSv3 over IKE+IPsec, NFSv4
  - NAT traversal: ICE for SIP, application specific hacks (usually in games)
- Why not a single solution to all of my problems instead of “short-term” fixes?

Potential Benefits of A Single Solution

- Software reuse
  - Single protocol to handle network authentication, integrity, privacy and mobility
- Robustness
  - One proper NAT traversal implementation works better than 1000 application-specific hacks
- Usability
  - Zero-conf mobility like with GSM phones
  - Unified format for network access control identifiers

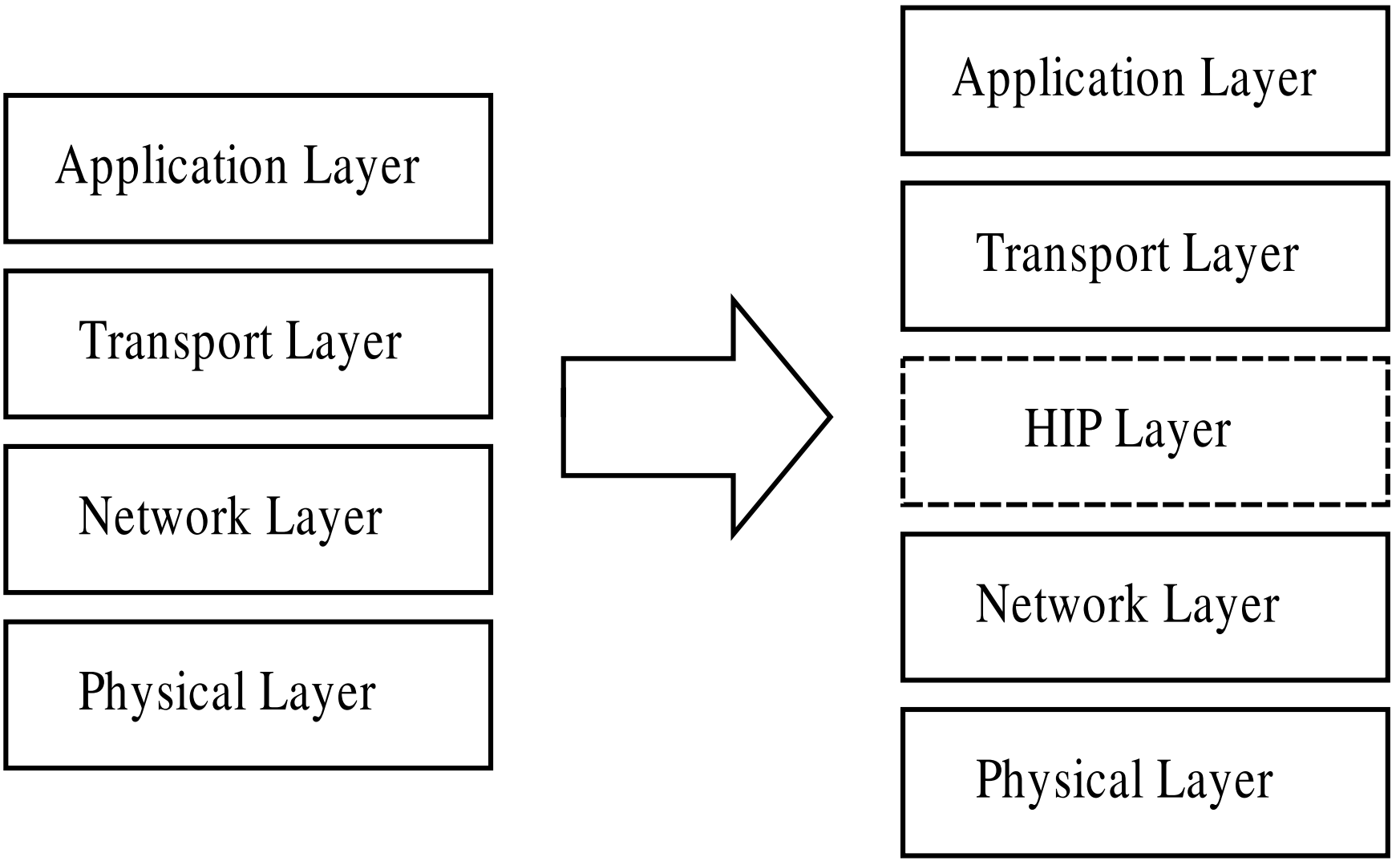
Deployment Costs

- End-host solution
  - Application layer: port all applications
  - Lower layer approach: costs more to develop but may not require changes to apps
- Middlebox solution
  - No changes to end-hosts, but introduces a dependency to infrastructure
  - May not realize all benefits, such as end-to-end security

A Solution to the Problems: Host Identity Protocol (HIP)

- Public key based host authentication
  - Public keys are exposed to applications
  - Can be used for access control at the application or lower layers
- End-host mobility and multihoming
  - Transparent to applications
- End-to-end encryption and integrity protection using IPsec
- NAT traversal and privacy extensions

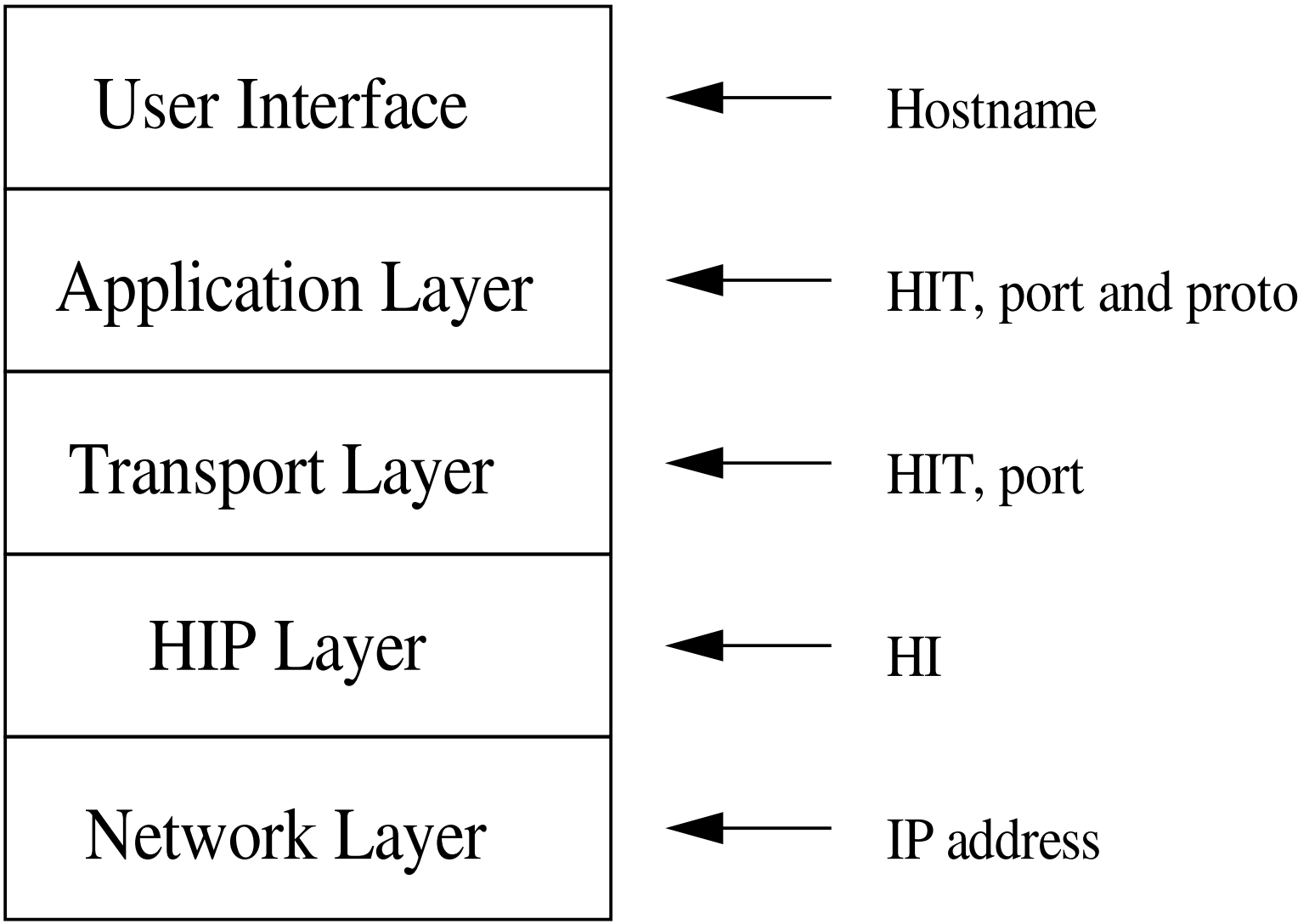
HIP Layering Architecture



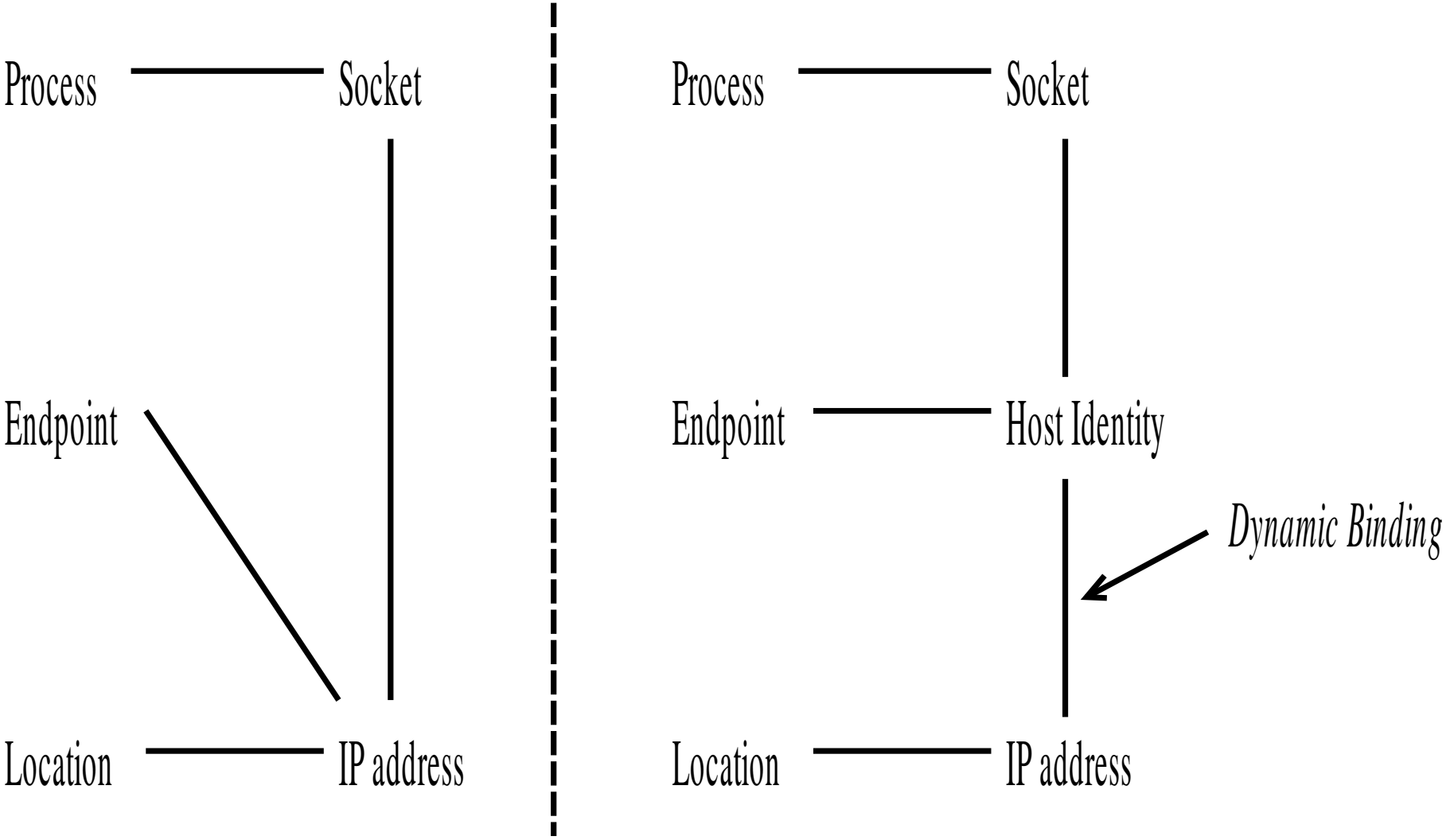
HIP Related Identifier Types

- Host Identifier = HI = public key
  - Currently standardized algos: RSA and DSA
- Legacy application identifiers
  - Host Identity Tag = HIT
    - prefix | hash(HI) = size of IPv6 address
  - Local Scope Identifier = LSI
    - IPv4-sized HIT (valid only on the local host)
- Locator = a routable IPv4 or IPv6 address

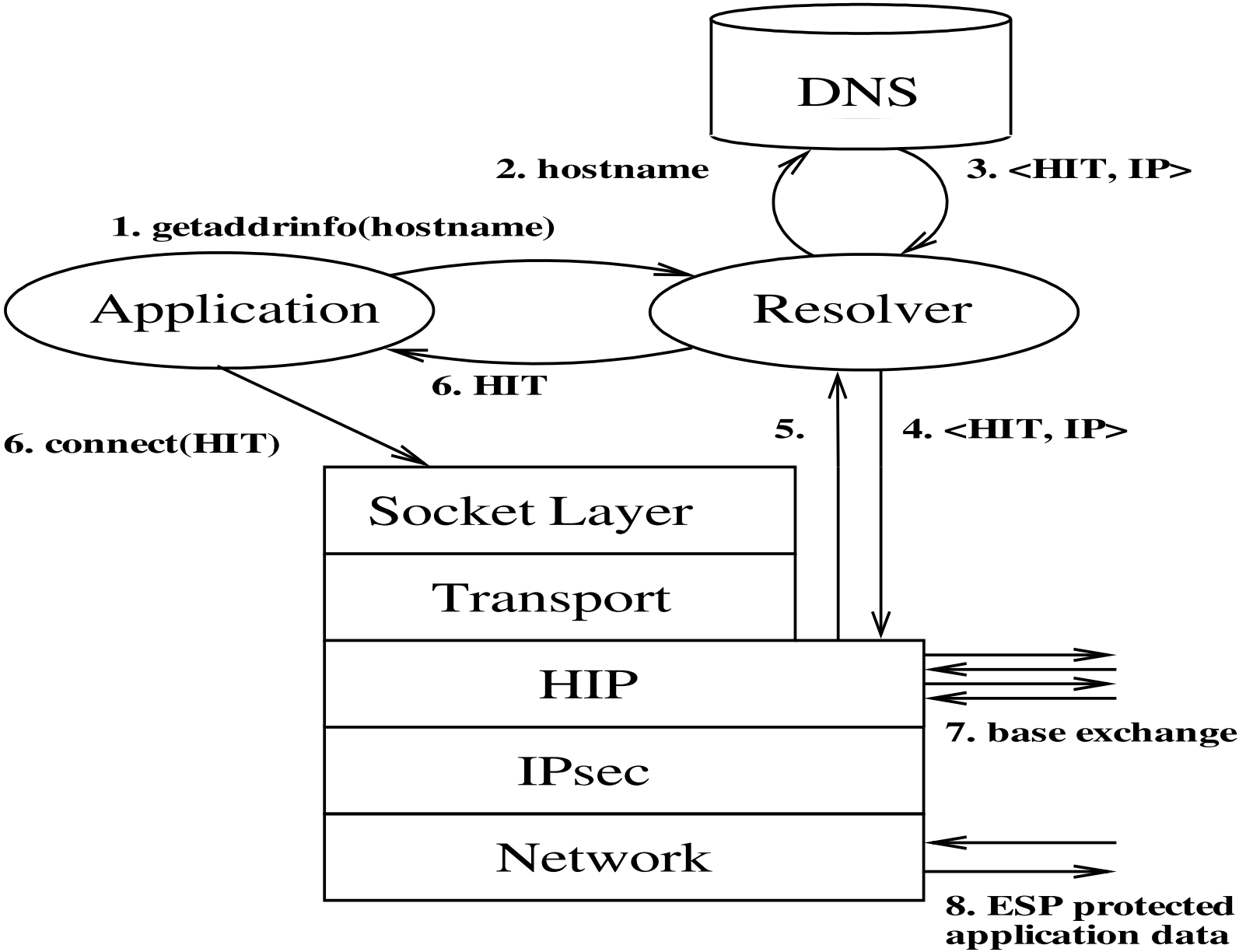
HIP Naming Architecture



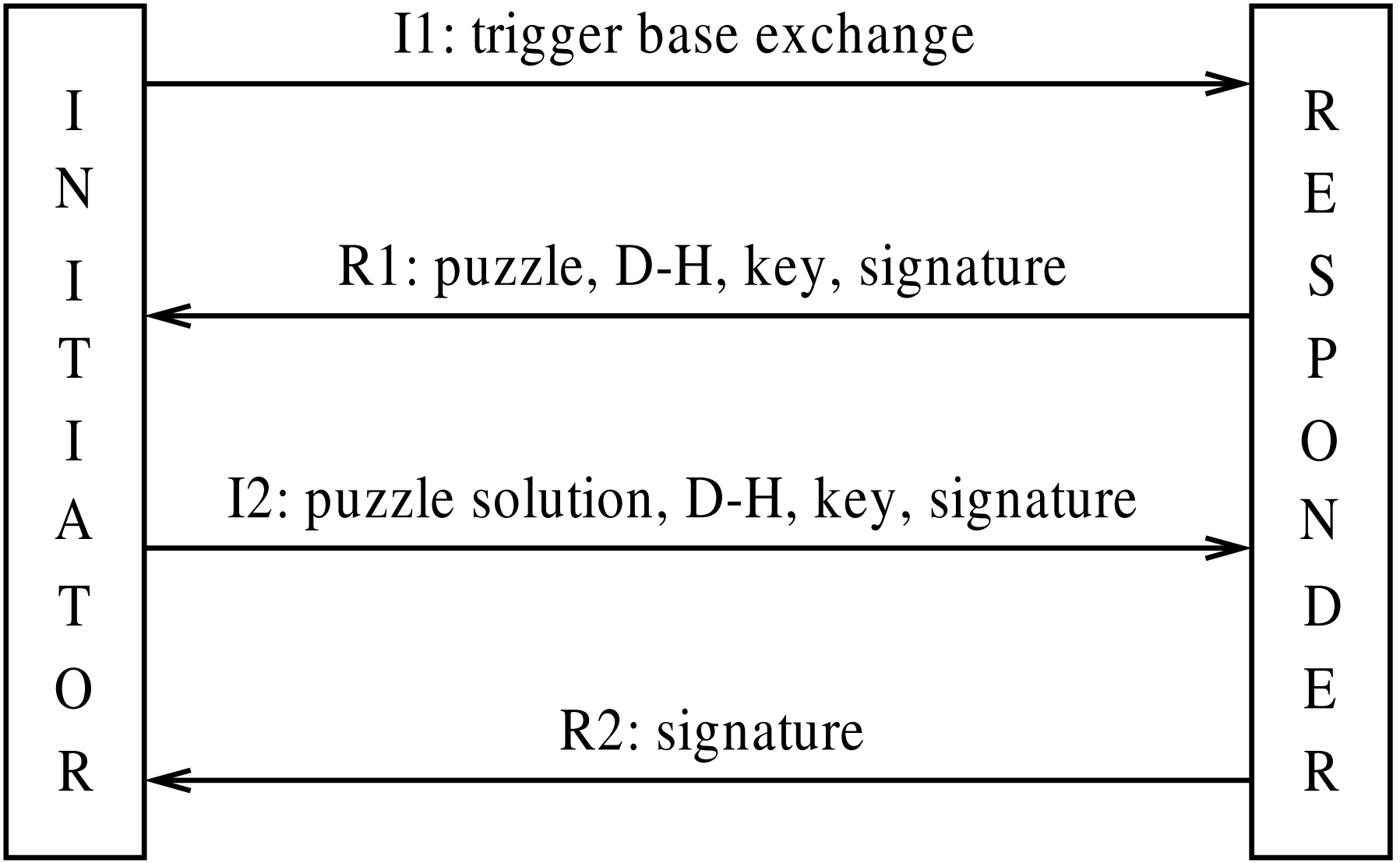
IP-based vs. HIP-based Socket Bindings



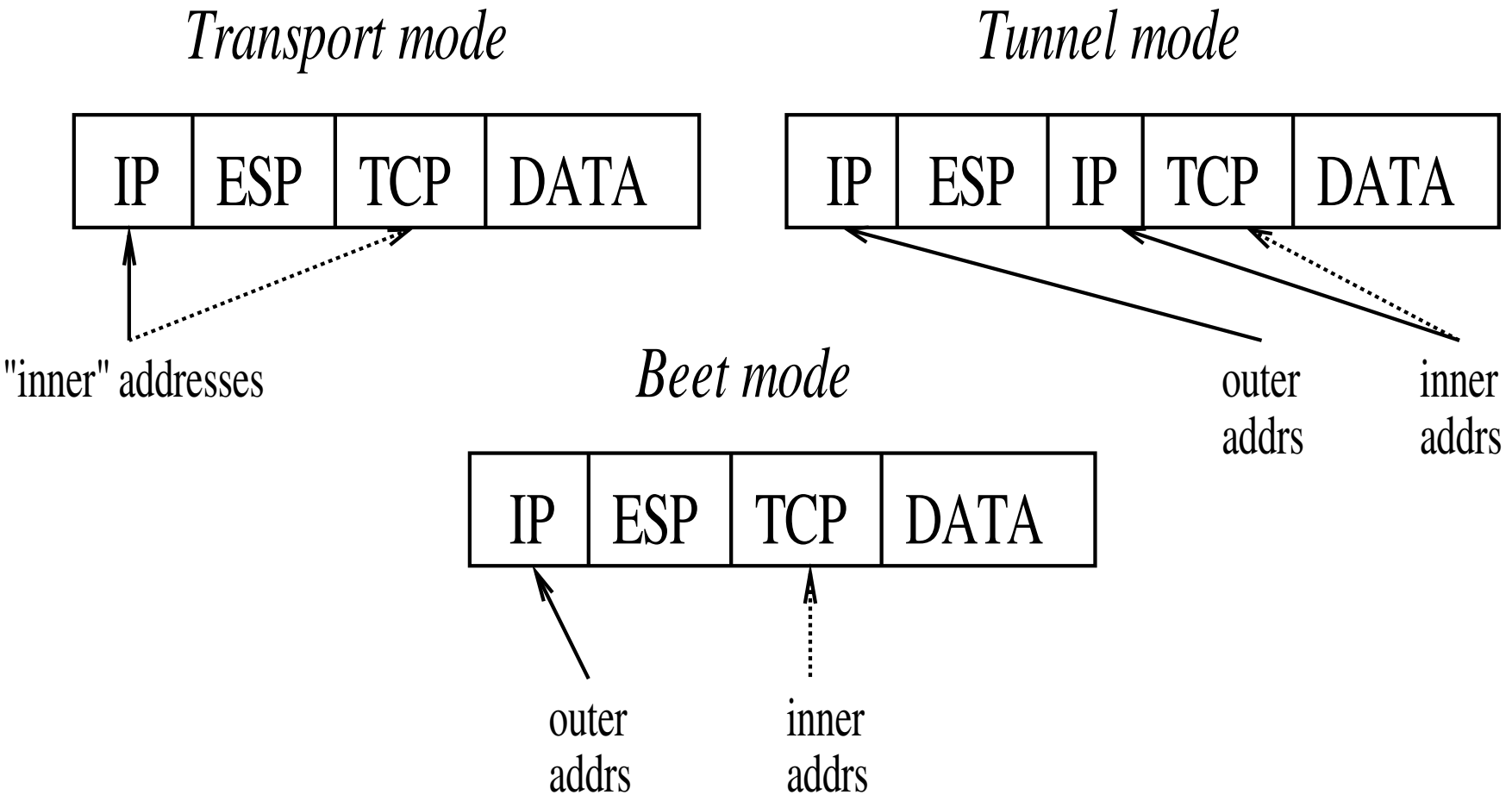
How Does HIP Work?



Base Exchange



Bound End-to-End Tunnel (BEET) IPsec ESP Mode vs. Other IPsec Modes



HIP vs. TLS

- TLS: IP(TCP(TLS(encrypted(data))))
  - NAT traversal works because NAT boxes support TCP
  - Attacks against TCP protocol (remember SYN cookies).
  - Reveals the port numbers (good and bad)
- ESP: IP(ESP(encrypted(TCP + data)))
  - Works also with UDP (e.g. NFS)
  - May work with some new NAT boxes
  - Usually requires extra UDP encapsulation which decreases MTU

HIP Mobility and Multihoming

- When a host moves, it updates its peer directly of its new location
- The peer sends a challenge and the host sends a response
  - Called the “return routability check”
  - Acknowledges the new location and protection against reflection/flooding attacks
- What if both hosts move at the same time?
  - They lose contact with each other

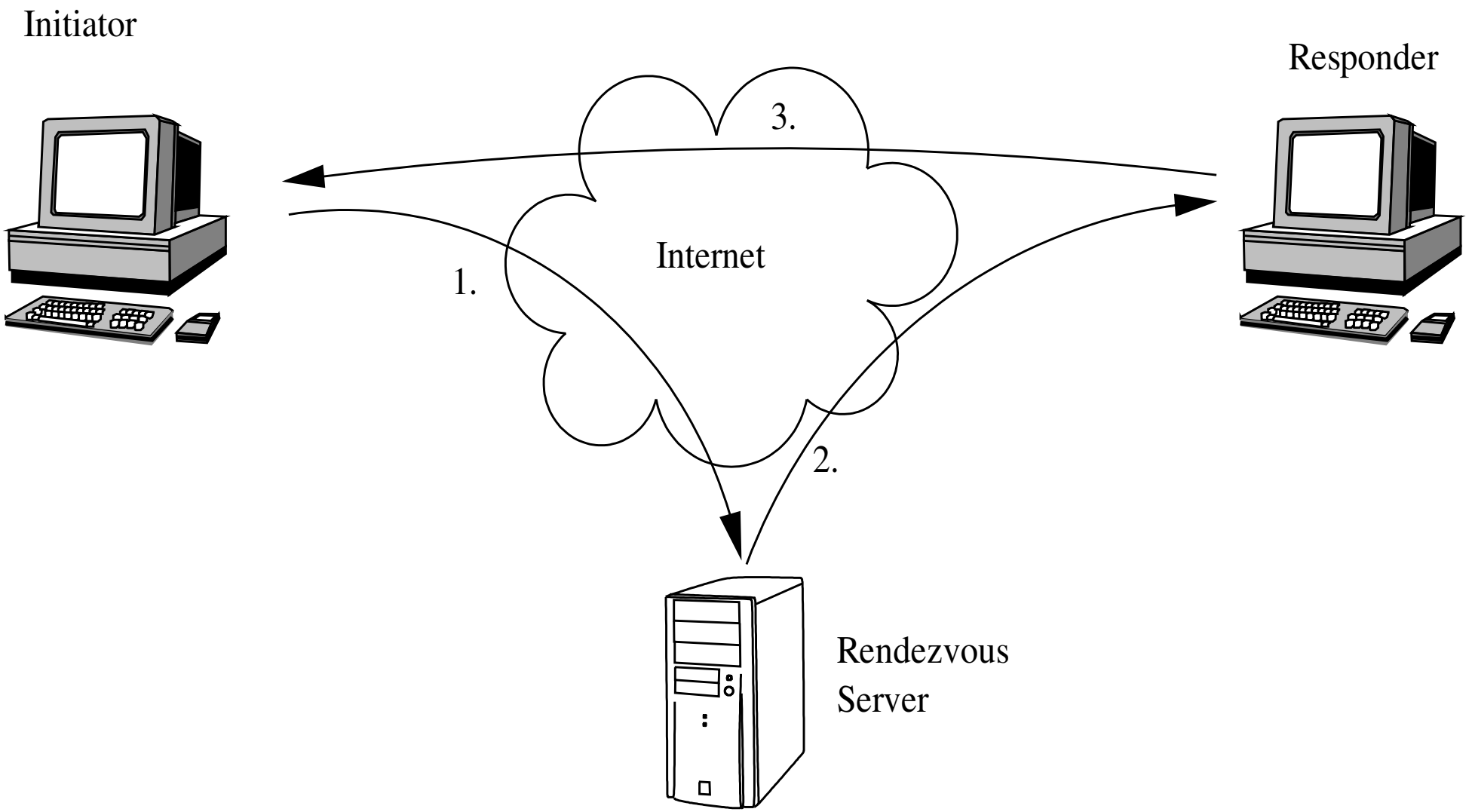
Rendezvous Server (RVS) 1/3

- Rendezvous server has a stable IP address
  - A host can use it as a contact point with a mobile for peer
  - Both for initial contact and “double jump”
- When Responder changes its location, it updates the RVS of its new location
- Configuration using DNS:
  - Hostname of peer
  - Host Identifier of peer
  - IP address of the RVS

Rendezvous Server 2/3

- Only the first packet is relayed!
  - Responder responds directly to Initiator
- RVS cannot be used to flood other hosts
  - Responder has to register to RVS
  - Registration is like a normal base exchange but with some extra parameters
  - RVS can enforce public-key based access control

Rendezvous Server 3/3



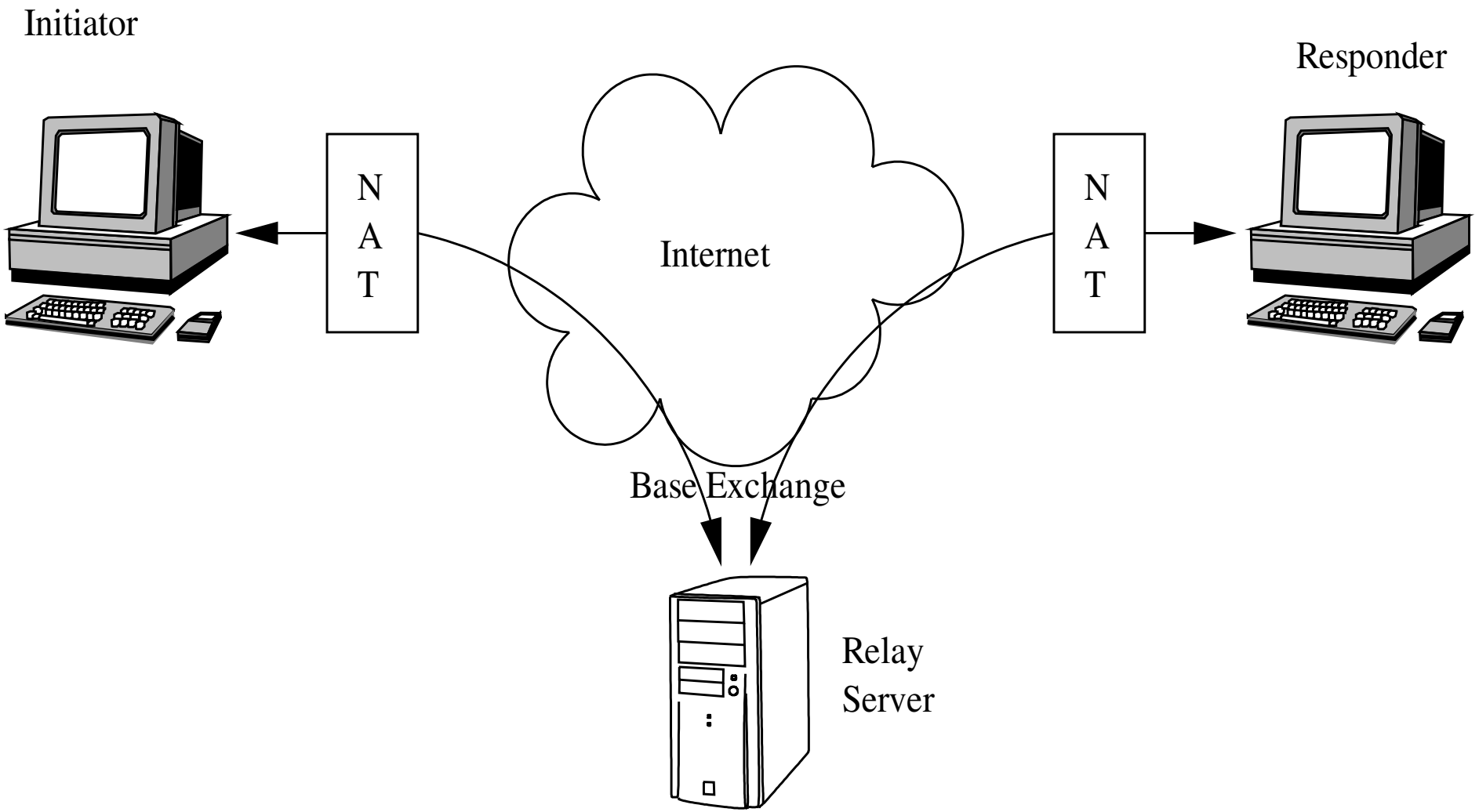
NAT Traversal with HIP

- End-to-end NAT traversal
  - Both the Initiator and Responder can be located behind NATs
  - End-hosts uniquely identifiable using HITs in private address realms
- Works with legacy NATs and requires no configuration of NAT devices

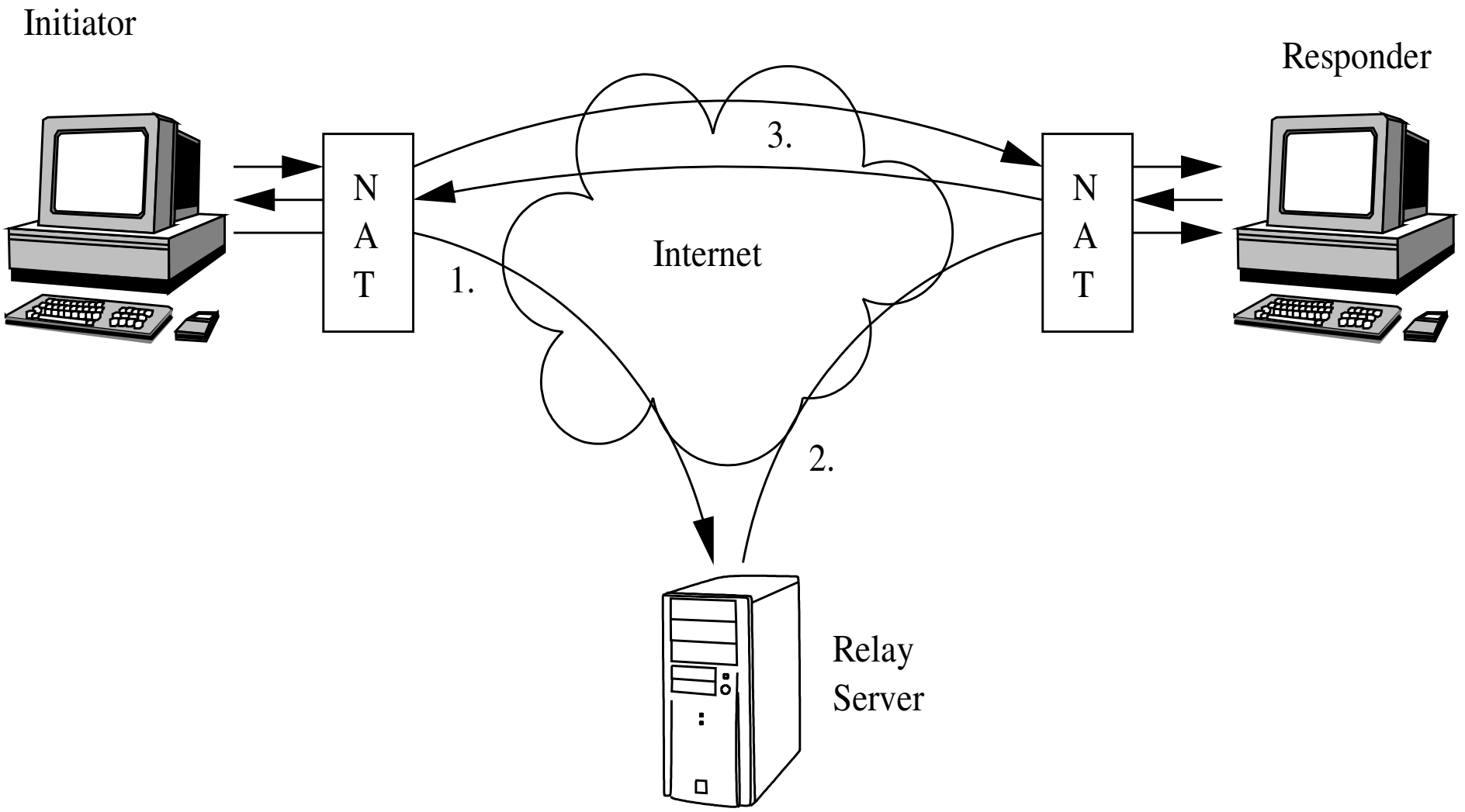
ICE Style Approach with NATs

- End-hosts exchange their locators
- Hosts test connectivity between locator pairs (tests also firewalls)
  - Prefer IPv6 locators
  - Detect when hosts are behind the same NAT
  - Prefer a direct end-to-end path
  - Relaying of ESP traffic if nothing else works
- Works also with multihomed hosts!
  - RTT measurement for selecting fastest iface

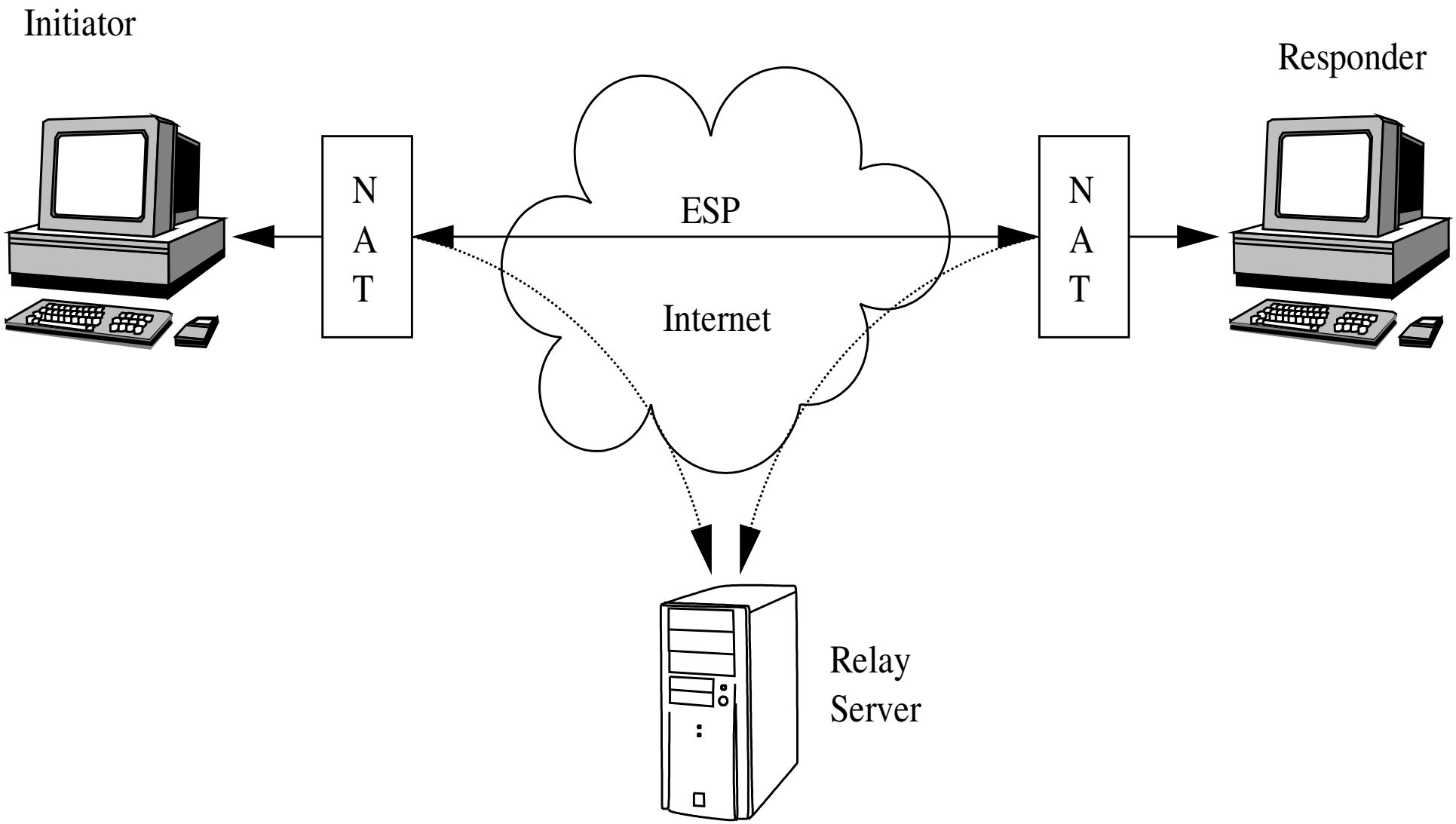
NAT Traversal: Base Exchange



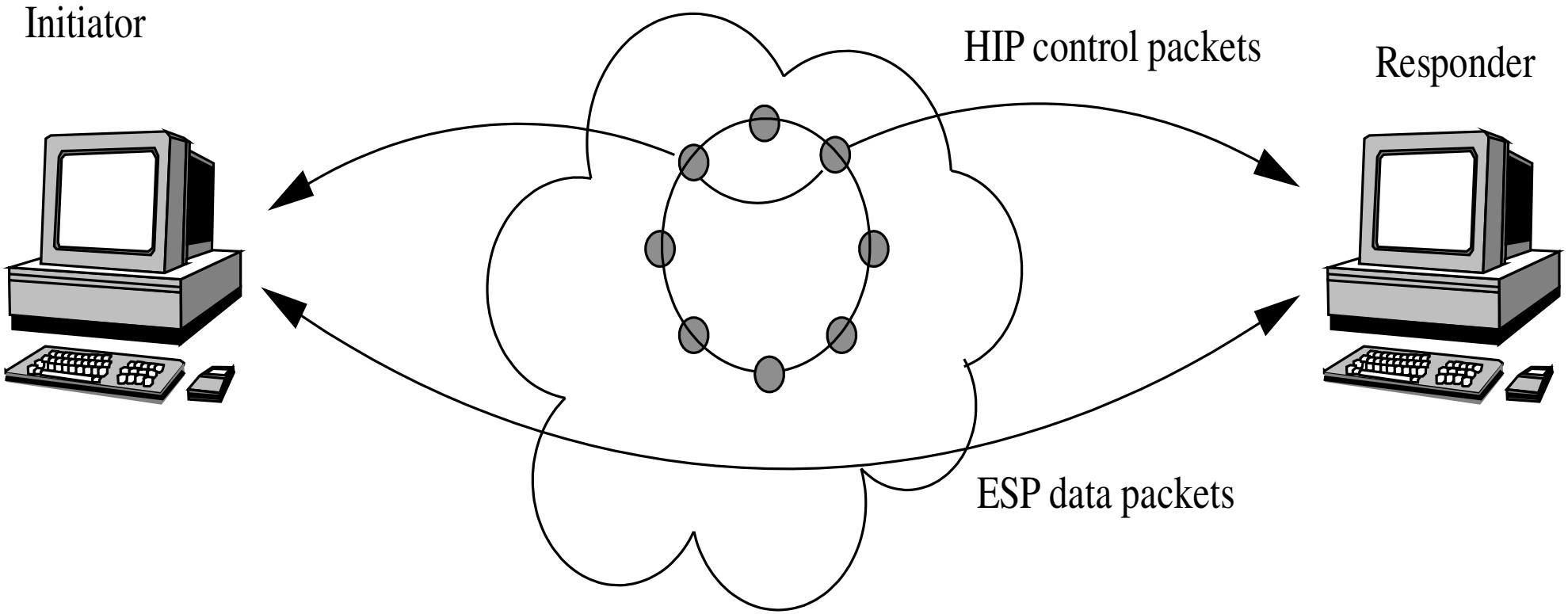
NAT Traversal: Connectivity Tests



NAT Traversal: Data Transfer



HIP + i3 = Hi3



HIP Implementations 1/2

- Ericsson
  - Main platform: FreeBSD
  - Used in Ambient Networks
  - Ericsson Open Source Licence
- Boeing (OpenHIP)
  - Platforms: Linux, Windows, MAC
  - Userspace IPsec
  - GPL licence

HIP Implementations 2/2

- HIP for Linux (HIPL), InfraHIP project / HIIT
  - Platforms: Linux, Nokia Tablet (Symbian port work in progress)
  - Actively maintained, used by various researchers
  - GPL licence
  - Supports several extensions: GUI, NAT traversal, HIP-firewall, rendezvous server, opportunistic mode, privacy, light-weight hip

InfraHIP II

- Deploy!
  - Supporting infrastructure (rvs and relay servers) to planetlab and test servers
  - Test varying network applications, report problems and solutions to the problems to IETF
- Couple of extensions
  - TCP extensions
  - “Advanced” opportunistic mode

Back to the Original Problems

- Yes, my SSH connections survive when I move my laptop from home to office
- Yes, I can access my NFS mounted share from everywhere. The NFSv3 traffic is authenticated by HIP and encrypted with IPsec. HIP firewall keeps others out.
- Yes, I can remotely access my parents Windows machine through ISP and ADSL NAT boxes.

Thank you!
Questions?

http://infrahip.hiit.fi/