

Mobility as an Integrated Service Through the Use of Naming

Ran Atkinson, Extreme Networks
Saleem Bhatti, University of St Andrews
Steve Hailes, University College London



1. ILNPv6 - changing naming and addressing
2. Approach to mobility
3. Approach to multi-homing, NAT and security
4. Project status

Architectural Claim

If we provide a richer set of namespaces then the Internet Architecture can better support mobility, multi-homing, and other important capabilities:

- ▶ *provide broader set of namespaces than at present*
- ▶ *reduce/eliminate names with overloaded semantics*
- ▶ *provide crisp semantics for each type of name*

“Standing on the Shoulders of Giants”

- Computer Science is sometimes accused of blindly reinventing the wheel.
- We actively tried to avoid that, so credit to:
 - ▶ Dave Clark for (c.1995) email to a public IRTF list proposing to split the IP address into two pieces
 - ▶ Mike O’Dell for two early proposals (8+8, GSE)
 - IETF claimed these ideas were unworkable
 - ▶ IRTF Name Space RG (NSRG)
- We extended and enhanced those early ideas to address a broad set of issues with our comprehensive proposal.

ILNPv6

- We propose an alternative networking protocol derived from IPv6, which we call **ILNPv6**:
 - ▶ could be considered a set of enhancements to IPv6
 - ▶ provides full backwards compatibility with IPv6
 - ▶ provides full support for incremental deployment
 - ▶ IPv6 routers do not need to change
- **ILNPv6** splits the IPv6 address in half:
 - ▶ **Locator (L)**: 64-bit name for the subnetwork
 - ▶ **Identifier (I)**: 64-bit name for the host

Locators versus Identifiers

- **Locator (L):**
 - ▶ uses the existing “Routing Prefix” bits of an IPv6 address
 - ▶ names a single subnetwork (/48 allows subnetting)
 - ▶ **topologically significant, so the value of L changes as subnetwork connectivity changes**
 - ▶ only used for routing and forwarding
- **Identifier (I):**
 - ▶ uses the existing “Interface ID” bits of an IPv6 address
 - ▶ **names (physical/logical/virtual) host, not an interface**
 - ▶ remains constant even if connectivity/topology changes
 - ▶ uses IEEE EUI-64 syntax, which is the same as IPv6
 - MAC-based Identity is very probably globally unique
 - ▶ only used by transport-layer (and above) protocols

Use of Identifiers and Locators

- All ILNP nodes:
 - ▶ have 1 or more Identifiers at a time
 - ▶ only Identifiers used at Transport-Layer or above
 - ▶ have 1 or more Locators at a time
 - ▶ only Locators are used to route/forward packets
- An ILNP “node” might be:
 - ▶ a single physical machine,
 - ▶ a virtual machine,
 - ▶ or a distributed system.

Naming Comparison

Protocol Layer	IP	ILNP
Application	FQDN or IP address	FQDN
Transport	IP address (+ port number)	Identifier (+ port number)
Network	IP address	Locator
Link	MAC address	MAC address

1. ILNPv6 - changing naming and addressing
2. **Approach to mobility**
3. Approach to multi-homing, NAT and security
4. Project status

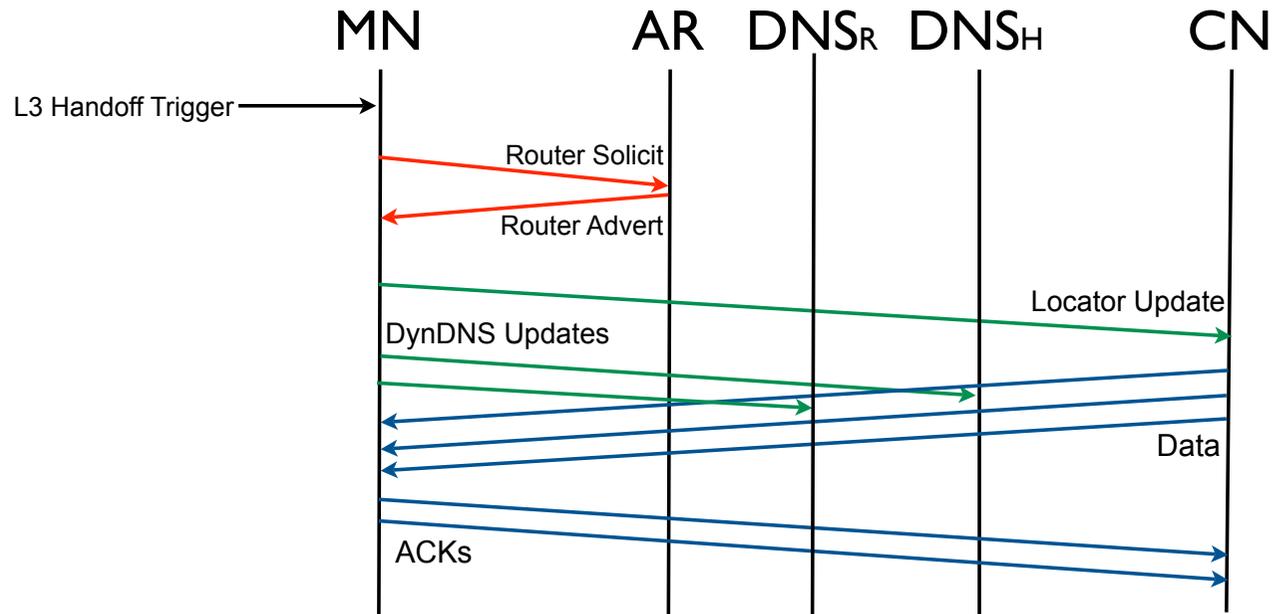
Naming and Mobility

- With MIP (v4 and v6), IP addresses retain their dual role, used for both **location** and **identity**:
 - ▶ overloaded semantics creates complexity, since all IP addresses are (potentially) topologically significant
- With ILNP, identity and location are separate:
 - ▶ **new Locator used as host moves**
 - reduces complexity: only Locator changes value
 - ▶ **constant Identifier as host moves**
 - agents not needed and triangle routing never occurs
 - ▶ **upper-layer state (e.g. TCP, UDP) only uses Identifier**

Mobility Implementation

- Implementation in correspondent node:
 - ▶ uses DNS to find MN's set of Identifiers and Locators
 - ▶ only uses Identifier(s) in transport-layer session state
 - ▶ uses Locator(s) only to forward/route packets
- Implementation in mobile node (MN):
 - ▶ accepts new sessions using currently valid I values
 - ▶ With ILNPv6, when the MN moves:
 - MN uses *ICMP Locator Update (LU)* to inform other nodes of revised set of Locators for the MN
 - LU can be authenticated via IP Security or new Nonce
 - MN uses *Secure Dynamic DNS Update* to revise its Locator(s) in its Authoritative DNS server
 - Already on the IETF standards-track as RFC-3007

ILNPv6 Network Handoff



MN	Mobile Node
AR	Router serving MN
DNS _R	DNS Server (reverse)
DNS _H	DNS Server (forward)
CN	Correspondent Node

1. ILNPv6 - changing naming and addressing
2. Approach to mobility
3. Approach to multi-homing, NAT and security
4. Project status

Multi-Homing with ILNP

- ILNP supports both forms of multi-homing
- *ICMP Locator Update* mechanism handles uplink changes (e.g. fibre cut/repair)
- ILNP reduces size of RIB in DFZ:
 - ▶ more-specific routing prefixes are no longer used for this
- In turn, this greatly helps with BGP scalability
- New DNS *Locator Aggregator (LP)* record enhances DNS scalability for site multi-homing
- **Also supports mobile networks**

ILNPv6: NAT Integration

- NAT/NAPT is here to stay:
 - ▶ many residential gateways use NAT or NAPT
 - ▶ often-requested feature for IPv6 routers is NAT/NAPT
- ILNPv6 reduces issues with NAT/NAPT:
 - ▶ upper-layer protocol state is bound to I only, never to L
 - ▶ only value of L changes as the NAT is traversed
 - ▶ so NAT function now invisible to upper-layer protocols
- ILNPv6 IPsec is not affected by NAT:
 - ▶ Security Association is bound to Identifiers, not Locators
 - ▶ ILNP AH covers Identifiers, but does not cover Locators
 - ▶ ILNP IPsec and NAT work fine together
 - special-case “IPsec NAT traversal” code is no longer needed

ILNP: Integrated Solution

- Mobility support is better integrated than MIPv4 or MIPv6:
 - ▶ mobility is native capability
 - ▶ mobility mechanisms are much simpler
 - ▶ authentication is practical to deploy
- Multi-homing and mobile network support improved over MIPv4 and MIPv6:
 - ▶ supports dynamic multi-homing for hosts and networks
 - ▶ multi-homing also integrated with mobility
 - ▶ routing scalability (BGP, DFZ RIB) is greatly improved
- NAT support is integrated
- IPsec support is integrated

1. Introduction - background and a claim
2. ILNPv6 - changing naming and addressing
3. Approach to mobility
4. Approach to multi-homing, NAT and security
5. Project status

ILNPv6: No Free Lunch

- No globally-routable network interface name:
 - ▶ potential impact on SNMP MIBs, e.g. to get interface counters from a particular interface
- A few legacy apps might remain problematic:
 - ▶ FTP is probably the worst case
 - FTP mis-uses the IP address as application-layer name
- DNS reliance is not new, but is more explicit:
 - ▶ at present, users perceive “DNS fault” as “network down”
 - ▶ ILNP creates no new DNS security issues
 - ▶ existing IETF standards for *DNS Security* and *Secure Dynamic DNS Update* work fine without alteration
 - already supported in BIND and other DNS servers

Next steps

- Demo implementation of ILNPv6 in BSD UNIX
 - ▶ which is in progress now
- Implementation will be used in experiments to test feasibility of ILNPv6:
 - ▶ verify backwards compatibility with IPv6 routers
 - ▶ wide area testing on UK SuperJANET connectivity between St Andrews (Scotland) and London (England)
 - ▶ later extend to international testing over IPv6 backbone
- Fine-tune ILNP design and implementation based on experimental results

Summary

- ILNP breaks the IP Address into separate Identifier & Locator values
- This enables native Mobility (without agents)
- Also, Security, NAT, and Multi-Homing are well integrated with Mobility
- Improvements in the Naming Architecture enable these simpler protocol approaches

Thank you!

- Contact information:

- ▶ Ran Atkinson rja@extremenetworks.com
- ▶ Saleem Bhatti saleem@cs.st-andrews.ac.uk
- ▶ Steve Hailes s.hailes@cs.ucl.ac.uk

Backup Slides



Security Considerations

- IP Security with ILNP:
 - ▶ can use IPsec AH and ESP for cryptographic protection
 - ▶ ILNP AH includes I values, but excludes L values
 - ▶ IPsec Security Association (SA) bound to value of I, not L
- New IPv6 Destination Option - Nonce:
 - ▶ contains clear-text 64-bit unpredictable nonce value
 - ▶ protects against off-path attacks on a session (child proof)
 - existing IP w/o IPsec is vulnerable to off-path attack
 - affordable, yet provides equivalent protection as today
 - ▶ primarily used to authenticate control traffic:
 - e.g. ICMP Locator Update (LU) message
- Existing IETF DNS Security can be used as-is

Mobile IP [1]

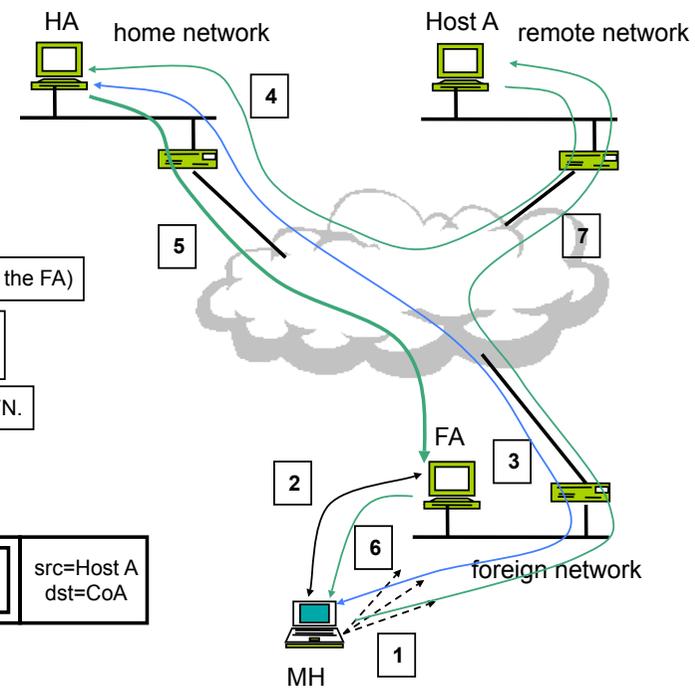
- Support mobile users without affecting others
- Transparency:
 - ▶ to upper layers
 - ▶ to remote end-systems
- IPv4 and IPv6:
 - ▶ IP address indicates **point of attachment to network**
- Movement of host means:
 - ▶ new IPv4 address?
 - ▶ update routing information?

Mobile IP [2]

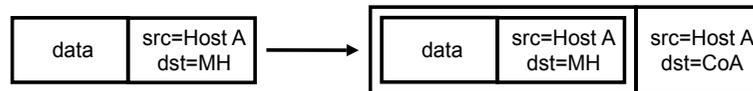
- Mobile host (MH):
 - ▶ **home address**, home network (HN), home agent (HA)
 - ▶ **care-of-address (CoA)**, foreign network (FN), foreign agent (FA)
- Communication:
 - ▶ HA sends packets to CoA: IP-in-IP encapsulation
 - ▶ HA must reply to ARP for MH
- CoA:
 - ▶ foreign agent
 - ▶ may be new IP address (co-located CoA)

Mobile IP [3]

- 1) MH arrives at FN, and locates FA (using agent advertisements from FA or by solicitation).
- 2) MH completes registration procedure with FA.
- 3) MH updates HA with its new CoA (i.e. the FA).
- 4) Host A now tries to contact MH. Packets for MH are intercepted by HA.
- 5) HA tunnels the packets from Host A to the CoA for MH (i.e. the FA)
- 6) The FA de-encapsulates the inner IP packet and transmits the packet locally to MH.
- 7) The packets from MH to Host A are sent directly from the FN.



IP-in-IP encapsulation



Mobile IP [4]

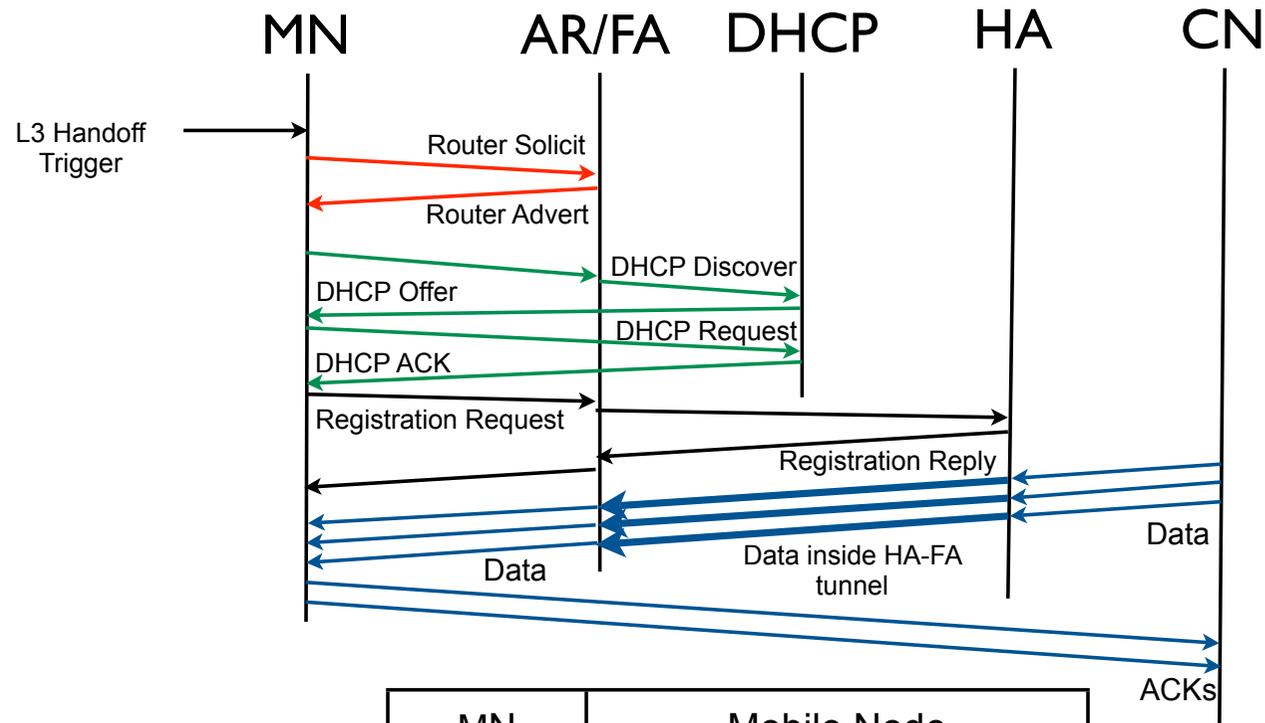
- ✓ Transparent to non-mobile hosts
- ✓ Does not break/change existing IP addressing and routing
- ✓ Can be introduced into the network as required (incrementally)
- ✓ Normal (unicast) routers do not need to be modified
- ✓ Does not affect DNS usage

- ✗ Complex architecture:
 - ▶ use of addresses
 - ▶ use of agents
- ✗ Asymmetric routing:
 - ▶ could be inefficient
 - ▶ QoS
 - ▶ higher layer protocol operation (e.g. TCP)
- ✗ Security:
 - ▶ firewalls configuration
 - ▶ authentication
 - ▶ end-to-end security
- ✗ Hand-off: FAs and FA/HA

Mobile IPv6

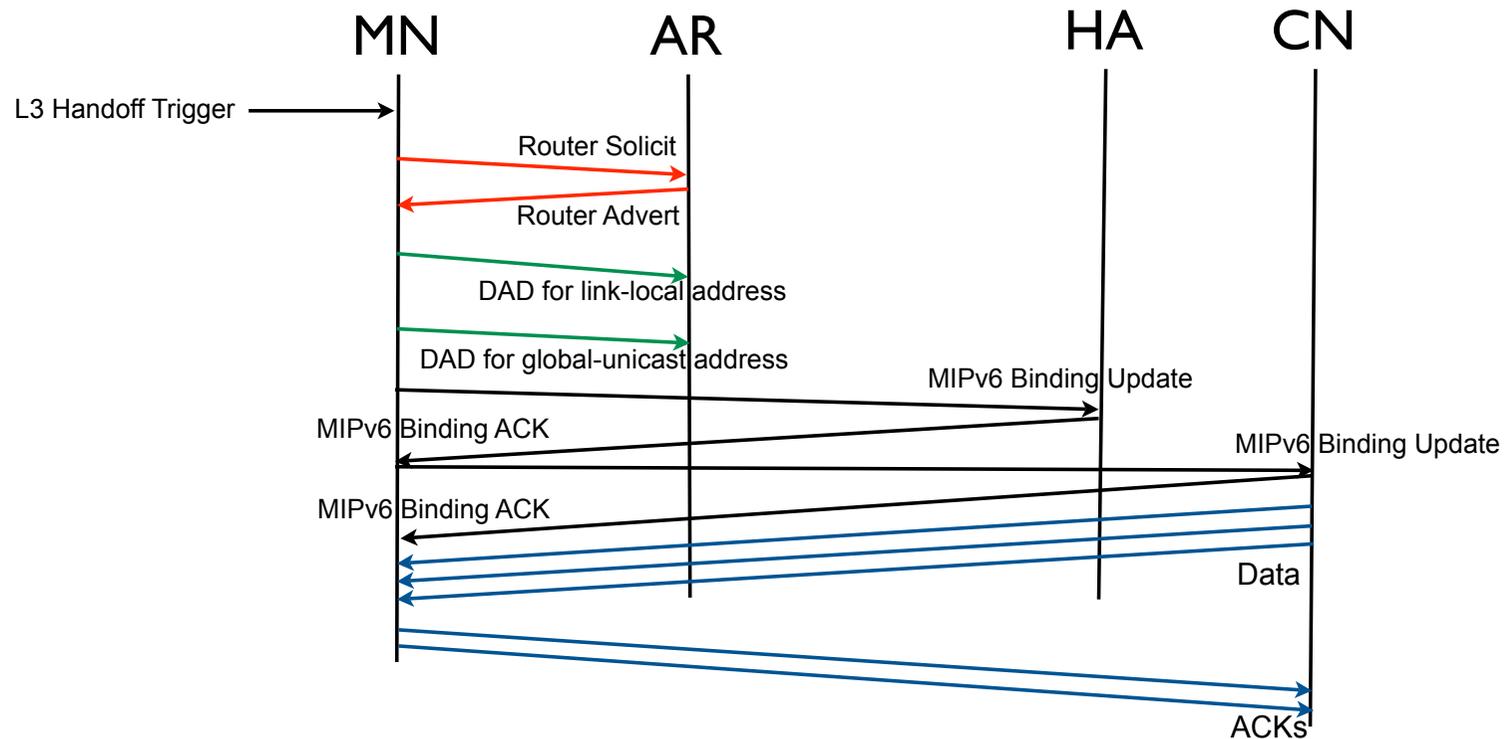
- Stateless address auto-configuration:
 - ▶ find an address (CoA) for use at the FN
- Neighbour discovery:
 - ▶ find default router
- No FA required to support mobility:
 - ▶ MH takes care of home address and foreign address
- Need dynamic DNS update support
- Route optimisation:
 - ▶ send CoA to remote end-system
- IPv6 Binding Update:
 - ▶ similar function to ILNIPv6 Locator Update
- Security (?):
 - ▶ authentication and privacy

MIPv4 Network Handoff



MN	Mobile Node
AR/FA	Router/Foreign Agent
DHCP	DHCP Server
HA	Home Agent
CN	Correspondent Node

MIPv6 Network Handoff



MN	Mobile Node
AR	Router serving MN
HA	Home Agent
CN	Correspondent Node

Multi-homing Today

- Site Multi-homing:
 - ▶ widely used today, growing in popularity
 - primary driver appears to be network availability
 - ▶ handled today by adding more-specific routing prefixes into the global routing table (DFZ RIB)
 - each multi-homed site adds 3 or more site-specific IP routing prefixes into BGP and the DFZ RIB.
 - ▶ creates significant BGP and DFZ RIB scaling issues
 - IRTF Routing RG is very concerned about scalability
- Host Multi-homing:
 - ▶ requires full-length prefix for each multi-homed node,
 - ▶ most ISPs filter out very long IP routing prefixes
 - ▶ not widely used today

Current Project Status

- Defined the ILNP protocol
- Defined DNS enhancements for ILNP:
 - ▶ collecting data on DNS to analyse possible impact
- Defined approaches to mobility, multi-homing, and NAT
- Identified and addressed potential security issues
- Addressed incremental deployment

Incremental Deployment

- ILNPv6 is a set of extensions to IPv6
- ILNPv6 requires no changes to IPv6 routing, IPv6 forwarding, or Neighbour Discovery (ND)
 - ▶ So no changes to IPv6 routers are needed !
- ILNPv6 enhances host TCP/IPv6 stacks
- How does a node know whether the remote node is ILNPv6 enabled or not?
 - ▶ ILNPv6 Nonce is present in received packet from remote node that is initiating a new UDP/TCP/SCTP session.
 - ▶ ILNPv6 DNS records (I, L) returned on DNS lookup, in addition to usual IPv6 (or IPv4) DNS records, when local node is initiating a new TCP/UDP/SCTP session.

Existing Mobility Approaches

- Mobile IPv4 (MIPv4):
 - ▶ not widely implemented or deployed at present
 - ▶ complex protocol: mobile node (MN), Home Agent (HA), Foreign Agent (FA)
 - ▶ numerous optional optimisations have been proposed
- Mobile IPv6 (MIPv6):
 - ▶ also not widely implemented or deployed at present
 - ▶ protocol similar to MIPv4
 - ▶ even more complex with numerous extensions proposed

DNS Locator Aggregator Record

- When an entire network moves together, there might be many L record updates for the DNS
- As a DNS storage and performance optimisation, we add the *Locator Aggregator (LP)* record:
 - ▶ LP record points to the FQDN associated with an L record
 - ▶ if DNS lookup yields and LP record, need to perform L record lookup using FQDN in LP record
 - ▶ FQDN/LP associated with a subnetwork, not a single host
 - ▶ LP record is one additional level of indirection :-)
- Operators can use a mix of L and LP records
- DNS Security works as usual

ILNPv6: DNS Enhancements

- New address records (for forward lookups):
 - ▶ I: Identifier(s), 64-bit unsigned value, EUI-64 syntax
 - ▶ L: Locator(s), 64-bit unsigned value, topological
- New pointer records (for reverse lookups):
 - ▶ PTRL: Authoritative DNS server for specified Locator
 - ▶ PTRI: FQDN for with specified I for a given L
 - ▶ (LP: DNS data optimisation - pointer to L record)
- Reverse look-up becomes 2-stage process:
 - ▶ 1: Use PTRL to find authoritative DNS server to query
 - ▶ 2: Use PTRI to find FQDN for specified I value
 - ▶ leverages ability to cache PTRL for longer time periods

DNS Enhancements

Name	DNS Type	Definition
Identifier	I	Names a Node
Locator	L	Names a subnet
Reverse Locator	PTRL	FQDN for the DNS Server responsible for subnet L
Reverse Identifier	PTRI	FQDN for the I that is present at subnet L
Locator Aggregator	LP	Forward pointer from FQDN to an L record

Network realms

- Much interest in non-IP edge networks:
 - ▶ e.g. sensor and actuator networks
- Would be useful to have session state across boundary of IP and non-IP network
- ILNP Identifier / Locator separation permits sufficient functional de-coupling:
 - ▶ Identifier could be maintained across boundary
 - ▶ Locator or even the network protocol could be different, enabled through use of an appropriate network layer gateway

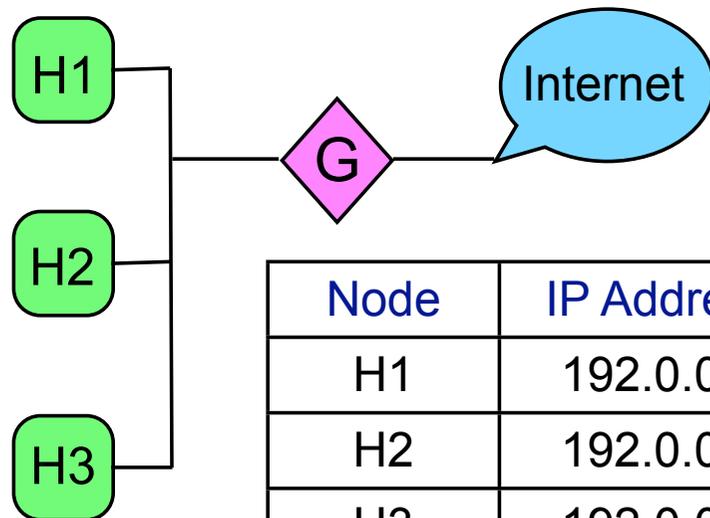
NAPT Basics

- Network Address & Port Translation (NAPT)
- Common variant on Network Address Translation (NAT)
 - ▶ often used to multiplex multiple hosts behind 1 public IP address
 - ▶ gateway/NAT device changes not only IP addresses (public vs private), but also changes TCP/UDP port numbers (public vs private).
- Question: Does NAPT break ILNP or not ?

NAPT: Rendezvous Issue

- Many sites deploy either NAT or NAPT for perceived security advantages:
 - ▶ primarily: remote nodes are blocked from initiating sessions with hosts inside the NAT/NAPT gateway.
 - ▶ this can affect some applications (e.g. VTC, VoIP).
 - ▶ ILNP does not change this “security” property, which is good for sites that deploy NAPT for this reason.
- Some sites might deploy NAT or NAPT to get IP address portability or to conserve IPv4 addresses:
 - ▶ neither issue exists in an IPv6/ILNPv6 context because of the much larger IPv6 address space & because ILNP handles renumbering/multi-homing natively.
 - ▶ so neither reason exists in an IPv6/ILNPv6 context.

NAPT Scenario



Node	IP Address	Port range
H1	192.0.0.2	5100-5199
H2	192.0.0.3	5200-5299
H3	192.0.0.4	5300-5399
G1	192.0.0.1	5400-5499
G1 (public)	3.1.2.3	-

- G1 uses its 1 public IP address to handle traffic to/from The Internet for itself and hosts H1, H2, & H3 behind G1.
- So, G1 is using NAPT and has different TCP/UDP port numbers in public versus on the private LAN segment.

NAPT does not break ILNP

- **IP:** with NAPT, sessions with H1, H2, H3, or G1 all will use the public IP address that belongs to G1
 - ▶ So, ICMP Locator Update messages for sessions to hosts H1, H2, H3 or gateway G1 will be sent to G1's public IP address.
 - ▶ So, *all* ICMP Locator Update messages from outside will naturally be sent to G1 by normal ILNP operation
- **ILNP:** when G1 sees a valid Locator Update message, G1 updates its NAPT lookup table with the new Locator(s)
 - ▶ G1 does not need to tell any interior host about the change.
- So, ILNP works with NAPT deployments:
 - ▶ Even with IPsec in use, because IPsec end-point will be G1

References

- R. Atkinson, S. Bhatti, S. Hailes
“Mobility as an Integrated Service Through the Use of Naming”
Proc. MobiArch2007 - 2nd ACM International Workshop on Mobility in the Evolving Internet Architecture , ACM SIGCOMM 2007 Conference, Kyoto, Japan . 27 August 2007
- R. Atkinson, S. Bhatti, S. Hailes
“A Proposal for Unifying Mobility with Multi-Homing, NAT, & Security”
Proc. MobiWAC2007 - 5th ACM International Workshop on Mobility Management and Wireless Access , MSWiM2007 - 10th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems), Crete, Greece . 22 October 2007.