Mobility Through Naming: Impact on DNS
ILNPv6: overview

Research Question

Principle

Hand-off

Additional Issues

Mobile Servers and Mobile Networks

Mobile IP Scenarios for ILNPv6

New DNS records

ILNPv6: use of DNS

Summary

Questions...
If DNS is used for ‘rendezvous’, in support of IP mobility, how might DNS be affected?
Concept of Operation

Do not name a Point of Attachment (PoA)

Do name a Point of Attachment (PoA)

As movement occurs:
Applications and users use FQDNS.

An IP (sub-)network – Locator
A node (host) – Identifier

Send Locator Update messages (LU) to correspondents.

(Re)send DNS + DNSec to update Locator value in DNS

Use DynDNS + DNSec to update Locator value in DNS

Existing sessions, ala IPV6 Binding Update (‘rendezvous’ for new sessions).
ILNPv6 packet format
<table>
<thead>
<tr>
<th>Correspondent node</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server (forward)</td>
<td>DNSH</td>
</tr>
<tr>
<td>DNS Server (reverse)</td>
<td>DNSR</td>
</tr>
<tr>
<td>Router serving MN</td>
<td>AR</td>
</tr>
<tr>
<td>Mobile node</td>
<td>MN</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>I</td>
<td>Identifier Record</td>
</tr>
<tr>
<td>L</td>
<td>Locator Record</td>
</tr>
<tr>
<td>PTRI</td>
<td>Reverse Identifier permits reverse lookup of FQDN, resolves to an FQDN, names a network using an Locator value for a host or network</td>
</tr>
<tr>
<td>PTRL</td>
<td>Reverse Locator permits reverse lookup of FQDN, including Relative Preference for network, including Relative Preference for a host</td>
</tr>
<tr>
<td>L</td>
<td>Locator Record</td>
</tr>
<tr>
<td>PTRI</td>
<td>Identifier Record</td>
</tr>
</tbody>
</table>
How might this affect use of DNS?

Correspondents use DNS to look-up current (sub-)network name at which the host is located. That is, 'rendezvous' is 'through DNS' rather than via additional agent(s)/server(s).

Hand-offs may be frequent (a few tens of seconds), so DNS record changes need to reflect new location in a timely manner. DNS records need lower TTL: same as the likely interval between hand-offs. Probably result in more DNS traffic overall.
Mobile IP scenarios for ILNPy6

- Mobile network
- Mobile server
- Mobile client (no servers)
- Fixed hosts and networks
Many connections from clients on single server.

When a server moves:
- Many servers, many updates.
- One Locator Update (LU) message per existing sessions.
- Single L record update per server.

Can be optimised for servers on the same network.

(Mobile network scenario)
Many connections to/from nodes in mobile network.

Many servers: many DNS + LU updates may be required.

Reduce DNS updates by using Site Border Router (SBR) + Locator Pointer (LP) record.

Stills need LU messages to update existing sessions.

LP record 'points to' an L record - contains a FQDN which resolves to an L record.

(ala MR in NEMO) + Locator Pointer (LP) record.
<table>
<thead>
<tr>
<th>Summary</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>DNS traffic little impact, but Locator Update traffic may be an issue</td>
</tr>
<tr>
<td>Robustness</td>
<td>Potentially improves system robustness</td>
</tr>
<tr>
<td>Deployability</td>
<td>Incremental deployability</td>
</tr>
<tr>
<td>Functions</td>
<td>ILNP easily integrated with other network</td>
</tr>
<tr>
<td>Integration</td>
<td>ILNP supports multi-layer approach in-</td>
</tr>
<tr>
<td>Link mobility</td>
<td>Packed</td>
</tr>
<tr>
<td>Scalability</td>
<td>Extra DNS traffic not likely to be significant</td>
</tr>
<tr>
<td>Authentication</td>
<td>No impact</td>
</tr>
<tr>
<td>Traffic</td>
<td>Date traffic may be an issue</td>
</tr>
<tr>
<td>ILNP</td>
<td>Ilp</td>
</tr>
</tbody>
</table>
Summary

ILNPv6:
- Names a (sub-)network and a node.
- Deployed IPv6 routers/backbones unchanged.
- Host IPv6 implementations require updating.
- Adds a few new DNS record types.
- Backwards compatible & Incrementally deployable.
- Secure Dynamic DNS Update (RFC-3007)
- DNS Security (RFC-4035)
- Secure Dynamic DNS Update (RFC-3007)

ILNPv6 uses DNS for 'rendezvous':
- Via widely available IETF standards:
  - Secure Dynamic DNS Update (RFC-3007)
  - DNS Security (RFC-4035)

Main impact in Mobile Server and Mobile Network scenarios:
- Increase in volume of DNS traffic when low TTL is used?

Scenarios:
- Increase in volume of DNS traffic when low TTL is used?

Mobile Server and Mobile Networks scenarios:
- Increase in volume of DNS traffic when low TTL is used?
Questions ...

Thank you!
http://ilnp.cs.st-andrews.ac.uk/
## Summary of DNS Impact

### Scenario

<table>
<thead>
<tr>
<th>Extra DNS access</th>
<th>Server movement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same as Client scenario</td>
<td>Simultaneous movement</td>
</tr>
<tr>
<td>Extra access to resolve L record(s)</td>
<td></td>
</tr>
<tr>
<td>Correspondent: If L^p record returned, extra access to L^p record host: extra access to update multiple L records, unless an L^p records is used, and then only a single extra access to update multiple L records</td>
<td></td>
</tr>
<tr>
<td>Client host: access for update of L record(s)</td>
<td></td>
</tr>
<tr>
<td>Fixed (correspondent: access for a multi-</td>
<td></td>
</tr>
<tr>
<td>Fixed homer site)</td>
<td></td>
</tr>
</tbody>
</table>

---

**Network**

**Server**

**Client**
Legacy applications

- Legacy IPv6 apps can be supported via Sockets API.
- Some legacy apps (e.g., FTP) might not work well and might need to fall back to 'pure IPv6'.
- Legacy IPv6 apps might not be able to use all of the ILNPv6 features.

Watch this space ... ;-(

Legacy applications
Initial DNS graphs – very drafty :-)  

DNS data collected at School of Computer Science, University of St Andrews. 

DNS requests for local targets only. 

3 weeks, towards the end of semester 2 (i.e. busy): 

Linux ncsd turned off on lab machines. 

Graphs show: 

- A and PTR requests for servers only 
- 600s bins 

Graphs show: 

- Linux ncsd turned off on lab machines. 
- Week 3: TTL = 30s 
- Week 2: TTL = 60s 
- Week 1: TTL = 1800s 

3 weeks, towards the end of semester 2 (i.e. busy): 

DNS requests for local targets only. 

University of St Andrews. 

DNS data collected at School of Computer Science,
Initial DNS graphs – very drafty :-) II

Days

Number of DNS requests

DNS requests, TTL=1800 (servers)

A

PTR

10 / 15

Initial DNS graphs – very drafty :-)

II
Number of DNS requests

Days

DNS requests, TTL=60 (servers)

A

PTR

20 / 15
Initial DNS graphs – very drafty :-) IV

Number of DNS requests

Days

DNS requests, TTL=30 (servers)

Initial DNS graphs – very drafty :-) IV
Simultaneous movement

Assume:

- 2 communicating hosts.
- No soft-hand off.
- 2 communicating hosts.
- Each host misses the other one’s Locator Update.
- LU sent on new connectivity (hand-off succeeds).
- Worst case, after timeout, kernel checks DNS, and uses new Locator(s) found there.
- Transport protocol could recover.
Use and generation of I values

- I values need to be unique in the context of Locator.
- This is required for ILNP to function.
- ILNPv6 does not require globally unique I values.
- ILNPv6 does not preclude globally unique I values.
- Would be an advantage for mobility.

- EUI-64 syntax uses bits from MAC addresses of any host interface.
- EUI-64 syntax has a Local/Global "scope bit".
- This follows existing IPv6 practices.

- I values always use the EUI-64 syntax/format.
- ILNPv6 does not require globally unique I values.
- This is required for ILNP to function.
- I values need to be unique in context of Locator.

- Could use dynamically generated I values (local bit).
- Could use cryptographically generated I values (local bit).
- High probability of being globally unique.