Design features vs. potential benefits of id / loc separation

Internet area meeting, Thu 23 2007
IETF 68, Prague
Pekka Nikander
Presentation outline

• Design features
  • Deployment scenarios
  • Implementation loci
  • Identifier structure and properties
  • Resolution models
• Obvious benefits
• Potential benefits
• Conclusions
Design features

- Deployment scenarios
- Implementation loci
- Identifier structure and properties
- Resolution models
Deployment scenarios
(stolen from the LISP draft)

• S1: identifiers fully conventionally routable
• S1.5: identifiers routable over another infra
  • e.g. IPv6 identifiers vs. IPv4 locators
• S2: identifier–locator mapping from the DNS
• S3: advanced: new id-based routing / query infra
  • e.g. based on compact name-independent routing, such as [Abraham et al 2004].
Implementation loci

- Architectural
- Vertical locus
  1. Within app / library
  2. In IP stack proper
  3. Below IP
- Reflects primary, designed trust model

- Implementational
- Horizontal locus
  1. Within host
  2. First hop router
  3. Site border router
  4. ISP
  5. Tier 1 ISP
- Reflects deployment
  • incl. trust model there
Identifiers: Structure and Properties

- Structure: hierarchical / flat / other
- Uniqueness: statistical / managed
- API backwards compatibility:
  - IPv4 / IPv6 / both
- Routability: global / local / none
- Security: self-authenticating / not
Resolution models

Query based

ID mapping infrastructure

Initiator (client)  Responder (server)

ID-routing based

ID routing infrastructure

Initiator (client)  Responder (server)
Presentation outline

• Design features
  • Deployment scenarios
  • Implementation loci
  • Identifier structure and properties
  • Resolution models
• Obvious benefits
• Potential benefits
• Summary
Obvious benefits
(not included in the comparison matrices)

• Stable identifiers for everyone
• No need for provider independent locators
• More freedom to change ISPs
• Some NAT problems maybe alleviated
• ... depends on details; see next slides
Potential benefits

• Eases pressure on the locator routing table
• Helps traffic engineering and site multi-homing
• Provides end-node mobility and multi-access
• Provides sub-network mobility
• Provides interoperability between IPv4 and IPv6
• Makes middle boxes “first class citizens”
• Supports delegable application-level naming
• Provides for DoS and/or DDoS protection
Background for the next slide
(see the additional slides)

- Early evaluation of some solution proposals vs. the potential benefits
- Extraction of a number design options and considering them vs. the potential benefits
- Some recorded in additional slides
  - Too much to cover here
  - Too subjective at this point of time
- Going to be opened up in draft-nikander-ram-ilse-XX.txt
Summary

• More features further down the road
  • Purely network-based solutions tend to limit what is possible in terms of overall features
• Surved above-IP approaches limit RIB / TE benefits
• Two distinct communities
  1. Jack-up / “routing” focus
  2. ID-loc split / “mobility” focus
• A social or technical contrast?
• Is one solution possible? Do we need two separate ones?
Additional slides
(for reference)
One possible solution architecture

Host identifiers
- ORCHID or CGA

In-site locators
- (IPv4 or) IPv6

Core locators

Net-based mapping

Mapping 1
- IPv4 (or IPv6)

Mapping 2
- (IPv4 or) IPv6

Locidefier?

Privacy?

Security?

Host mobility

Host multi-homing

Site renumbering

Site multi-homing

Mapping 1

Coordination?
Trust models

- Whom to trust?
- Host owning a problem?
- Choice between ISPs?
- Recall: vertical vs. horizontal locus quite independent
- You can delegate…
- Real question: the designed, built-in trust model
- Deployment model can wait; flexibility there
## Correlation matrices: notation

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implemented*</td>
<td></td>
</tr>
<tr>
<td>Designed but not implemented</td>
<td></td>
</tr>
<tr>
<td>Loose specification exists</td>
<td></td>
</tr>
<tr>
<td>Back-of-the-envelope design exists</td>
<td></td>
</tr>
<tr>
<td>Thought to be possible; no design exists</td>
<td></td>
</tr>
<tr>
<td>Orthogonal or mutually neutral issues</td>
<td></td>
</tr>
<tr>
<td>Not analysed; open interactions</td>
<td></td>
</tr>
<tr>
<td>Incompatible; suspect architectural conflict</td>
<td></td>
</tr>
</tbody>
</table>

* the icon is a running imp
<table>
<thead>
<tr>
<th>A</th>
<th>C</th>
<th>Deployment</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Resol.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Self-authenticating identifiers</td>
<td>Both IPv4 and IPv6 representation</td>
<td>Conv. routable identifiers</td>
<td>1.5 DNS-based id-&gt;loc lookup</td>
<td>3 New mapping mechanism</td>
</tr>
<tr>
<td></td>
<td>At hosts At site border Deeper in network</td>
<td>Above IP At ~IP Below IP</td>
<td>Query-based ID-routing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>1.5 2 3</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>TE</td>
<td>1</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Mobility and multi-homing</td>
<td>1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>Mobile subnetworks</td>
<td>1</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>IPv[46] interop</td>
<td>1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>1st class middlebox</td>
<td>1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>Delegative names</td>
<td>1</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>1 1 1</td>
</tr>
<tr>
<td>DoS resistance</td>
<td>1</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

This slide is subjective and contains mistakes
<table>
<thead>
<tr>
<th></th>
<th>LISP</th>
<th>PASH</th>
<th>SHIM6</th>
<th>Unmodified HIP</th>
<th>Plain jack-up (e.g. MPLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RT</strong></td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃 / 🍃</td>
<td>🍃</td>
</tr>
<tr>
<td><strong>TE</strong></td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>Mobility and multi-homing</td>
<td>🍃</td>
<td>✉️</td>
<td>✉️ &amp;</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>Mobile subnetworks</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>IPv[46] interop</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; class middlebox</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>Delegative names</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>DoS resistance</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
</tbody>
</table>