A Reference Model for Autonomic Networking

draft-ietf-anima-reference-model-01.txt

95th IETF, 4 Apr 2016
Michael Behringer, Brian Carpenter, Toerless Eckert, Laurent Ciavaglia, Bing Liu, Jefferson Nobre, John Strassner
Reference Model – High Level View

Autonomic Networking Infrastructure:
- GRASP
- Bootstrap
- ACP
- Naming
- Addressing
- Discovery

Network with autonomic functions

ASAs deployed as needed
Base infra: Every node must support

Autonomic Function A
- ASA
- ASA
- ASA
- ASA
- ASA
- ASA
- ASA
- ASA

Registrar
- ASA

Autonomic Function B
- ASA
- ASA

Node 1
- ASA

Node 2
- ASA

Node 3
- ASA

Node 4
- ASA

Node 5
- ASA

Domain ID
- Pre-set ID

Domain ID
- Pre-set ID

Domain ID
- Pre-set ID

Domain ID
- Pre-set ID

Domain ID
- Pre-set ID
Naming Section

- Naming section updated
  - each autonomic device should be assigned a name.
  - Requirements are 1) uniqueness, 2) consistency, 3) autonomic
  - “It is recommended that the names are generated by the autonomic nodes themselves.” \(\rightarrow\) Needs more thinking
Changes from draft-behringer-anima-reference-model-04

Addressing Section

• The proposed addressing schemes are now in ACP draft (as per chair’s request)
• → Pointing to ACP draft
Changes from draft-behringer-anima-reference-model-04

Other Changes

• Re-ordered sections in section 4 (ANI)
• For each section, now pointing to the relevant draft.
• Included text on MASA
• Included text on sub-domains, cross-domain.
• Intent section changed;
  – needs more updates from recent discussion; editorial
• Aggregated reporting section changed.
Open Issues: Naming

4.1 Naming:

- "It is recommended that the names are generated by the autonomic nodes themselves." - how? Should names / addresses not come from the registrar? Suggestion: Name *and* ACP address should be assigned by the registrar at enrolment time. zone-id is dynamic, rest is fixed.

- "a specific naming convention is out of scope":
  Suggestion: We define a default naming and addressing scheme. 1st we settle on an addressing scheme from the ACP draft. That defines a "device-ID" (last n bits of ACP address). convert that to a string, and use it as a name. This would result in something like: 0123-4567-89ab-0001.example.com. The name would go into the domain certificate --> need to put this into the bootstrap draft as well.

- to write in the doc: "registrar picks a naming scheme; all registrars in a domain must use the same scheme. Example is: ...
Addressing – Base Scheme

• Base Scheme:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>40</td>
<td>3</td>
<td>77</td>
</tr>
</tbody>
</table>
+-----+-----+-----+-----+
| FD  | hash(domain) | Type | (sub-scheme) |
+-----+-----+-----+-----+

• Hash(domain) provides pseudo-random prefix, as required by RFC4193 (ULA)

• Operational view: Admin specifies domain name only, nothing else needed for addressing to work!

• Do we agree so far?
• Comments? Concerns?
## Addressing – Sub-Scheme 1

- **Sub-Scheme 1:**

```
  |          | Zone ID | Device ID |
  +----------+---------+-----------+
  | 51       |         |           |
  +----------+---------+-----------+
  | 13       |         |           |
  +----------+---------+-----------+
  | 64       |         |           |
  +----------+---------+-----------+
```

- Registrar assigns device ID
  - It is unique for a device in a domain
  - It does NOT specify a locator, but an identifier
  - Device ID does not change in the lifetime of a device

- **Zone-ID initially zero.**
  - When aggregation is required, use a zone-ID <> 0

---

*Probably not needed*

- Needs discussion
Addressing – Sub-Scheme 2

- Sub-Scheme 2:

<table>
<thead>
<tr>
<th>51</th>
<th>13</th>
<th>64-V</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>+-------------------------------+-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zone ID</td>
<td>Device ID</td>
<td>V</td>
</tr>
<tr>
<td>+-------------------------------+-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Add “Virtualisation” bits at the end
  - Allow addressing various virtual machines on a single node
- Keep routing simpler:
  - Node announces not a /128, but for example /127

• Needs discussion
Why the “V” bit(s)?

<table>
<thead>
<tr>
<th>(base scheme)</th>
<th>Zone ID</th>
<th>Device ID</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>+--------------------</td>
<td>---------</td>
<td>-----------</td>
<td>---</td>
</tr>
</tbody>
</table>

containers →

AN controller element

xxxx::2

AN controller element

xxxx::3

AN forwarding element

xxxx::1

physical node

containers →

xxxx::0/126

xxxx::0/126
Use Case for Aggregation / Zones: Connecting AN zones over MPLS VPN

IPv6 VPN “grey” or Internet

NOC
AAA, NTP, TFTP, ...

Non-AN PE

Only IP connectivity
• No ACP
• No intent

PE A
PE B

Zone A
Zone B

ACP

• No intent

Non-AN PE
Use Case for Aggregation / Zones: Connecting AN zones over MPLS VPN

IPv6 VPN “grey” or Internet

NOC
AAA, NTP, TFTP, ...

Non-AN PE

IPv6 VPN “grey” or Internet

PE A
AN node
AN node
AN node
AN node
Zone A

PE B
AN node
AN node
AN node
AN node
Zone B

PE
ACP

VPN “grey” or Internet

RT export: zoneprefix
RT import: other prefixes

AN VRF
- Router loopback, area 0
- Area <x> summary route
- Specifics (RPL) (not announced)
[This node is RPL grounded root]

Only IP connectivity
• No ACP
• No intent

Non-AN PE

RT export: zoneprefix
RT import: other prefixes

VPN “grey” or Internet
Open Issues: Intent Distribution

4.7 Intent Distribution
- This section should only explain the basics, real work is out of scope for this phase.
- should point to the intent distribution draft
- should explain that intent is flooded to all nodes in a domain (if we agree),
  or other methods (if not).
- should explain that we expect Intent to have a long life time (months), thus
  Intent distribution is expected to be very infrequent.
- should explain that the entire Intent file is flooded in one go (if we agree).
Open Issues: “Functional Overview”

5. Functional Overview
- title is not good. This section really describes how an autonomic node behaves. maybe call it "Behaviour of an autonomic node"?
- we need to describe the bring-up better, specifically insecure discovery,
  ACP negotiation, ACP bringup, and subsequent operations, and which protocols to use
  where. Or should this go into the ACP draft??
Adjacency Table

- Information about adjacent nodes
  - “Note down what you see” – no judgement yet!
- Used to control autonomic processes, such as constructing the ACP, bootstrapping, etc.

<table>
<thead>
<tr>
<th>Node-ID</th>
<th>i/f</th>
<th>Link address</th>
<th>ACP address</th>
<th>Domain</th>
<th>Certificate</th>
<th>Validity</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;UDI-1&gt;</td>
<td>Eth0</td>
<td>FE80:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>Full (In domain)</td>
</tr>
<tr>
<td>&lt;UDI-2&gt;</td>
<td>Eth1</td>
<td>FE80:...</td>
<td>-</td>
<td>Example1.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>No</td>
</tr>
<tr>
<td>&lt;UDI-3&gt;</td>
<td>-</td>
<td>2000:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>Valid</td>
<td>Full (In domain)</td>
</tr>
<tr>
<td>&lt;UDI-4&gt;</td>
<td>Eth2</td>
<td>FE80:...</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
# Feeding the Adjacency Table

<table>
<thead>
<tr>
<th>Node-ID</th>
<th>i/f</th>
<th>Link address</th>
<th>ACP address</th>
<th>Domain</th>
<th>Certificate</th>
<th>Validity</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;UDI-1&gt;</td>
<td>Eth0</td>
<td>FE80:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>Full (In domain)</td>
</tr>
<tr>
<td>&lt;UDI-2&gt;</td>
<td>Eth1</td>
<td>FE80:...</td>
<td>-</td>
<td>Example1.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>No</td>
</tr>
<tr>
<td>&lt;UDI-3&gt;</td>
<td>-</td>
<td>2000:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>Valid</td>
<td>Full (in domain)</td>
</tr>
<tr>
<td>&lt;UDI-4&gt;</td>
<td>Eth2</td>
<td>FE80:...</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Non-autonomic inputs:
- Configured adjacencies
- DHCP options for AN
- DNS based
- ...

- draft-ietf-anima-bootstrapping-keyinfra-00 section-5.3 or Reference model ??

AN discovery (local)

- draft-ietf-anima-grasp

AN discovery (cloud redirect)

AN discovery (local)

- draft-ietf-anima-grasp

Non-autonomic inputs:
- Configured adjacencies
- DHCP options for AN
- DNS based
- ...

- draft-ietf-anima-bootstrapping-keyinfra-00 section-5.3 or Reference model ??

AN discovery (local)

- draft-ietf-anima-grasp

AN discovery (cloud redirect)

AN discovery (local)

- draft-ietf-anima-grasp

Non-autonomic inputs:
- Configured adjacencies
- DHCP options for AN
- DNS based
- ...

- draft-ietf-anima-bootstrapping-keyinfra-00 section-5.3 or Reference model ??
## Using the Adjacency Table

<table>
<thead>
<tr>
<th>Node-ID</th>
<th>i/f</th>
<th>Link address</th>
<th>ACP address</th>
<th>Domain</th>
<th>Certificate</th>
<th>Validity</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;UDI-1&gt;</td>
<td>Eth0</td>
<td>FE80:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>Full (In domain)</td>
</tr>
<tr>
<td>&lt;UDI-2&gt;</td>
<td>Eth1</td>
<td>FE80:...</td>
<td>-</td>
<td>Example1.com</td>
<td>&lt;cert-info&gt;</td>
<td>valid</td>
<td>No</td>
</tr>
<tr>
<td>&lt;UDI-3&gt;</td>
<td>-</td>
<td>2000:...</td>
<td>FD...</td>
<td>Example.com</td>
<td>&lt;cert-info&gt;</td>
<td>Valid</td>
<td>Full (in domain)</td>
</tr>
<tr>
<td>&lt;UDI-4&gt;</td>
<td>Eth2</td>
<td>FE80:...</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Node has no domain
And I have domain
→ Be a proxy to bootstrap that node

Node has domain
And I don’t have domain
→ I bootstrap

Node has same domain
→ Build ACP
→ Add ACP parameters to table

If response = “redirect”
Enter the redirect target into adjacency table; use this node to bootstrap.

ACP based functions, e.g., Intent distribution, negotiation, Synchronisation, etc.

Intent driven behaviour (tbd)

Outside scope for now.

---

draft-ietf-anima-bootstrapping-keyinfra-00 section-3.2

draft-ietf-anima-bootstrapping-keyinfra-00 section-3.1

draft-ietf-anima-autonomic-control-plane Section 5.1
Open Issues: Security and Trust

6. Security and Trust Infrastructure
- needs a review from someone in the security space.
- we need to describe the certificate format; this should likely go into bootstrap draft. This draft should explain where the certificate format is described.
- the domain certificate should also contain the ACP IP address (where the zone bits are set to zero).
Open Issues

• I suggested a “Futures” section for all materials currently not in WG charter scope.
  – Then we can keep more content without “watering down” the main document.
  – only positive feedback → Will do this in next version.
  – not 100% black/white; some small bits should (IMO) remain in main text (ex: a short paragraph on Intent distribution)

• Certificate Format: Where should this go?
  – Current approach: bootstrap draft?
Summary

• Making good progress
• Open issues are being discussed, mostly
• Some questions need discussion:
  – Addressing!

Network with autonomic functions

Autonomic Networking Infrastructure:
GDNP, Bootstrap, ACP, Naming, addressing, Discovery

Node 1
Node 2
Node 3
Node 4
Node 5