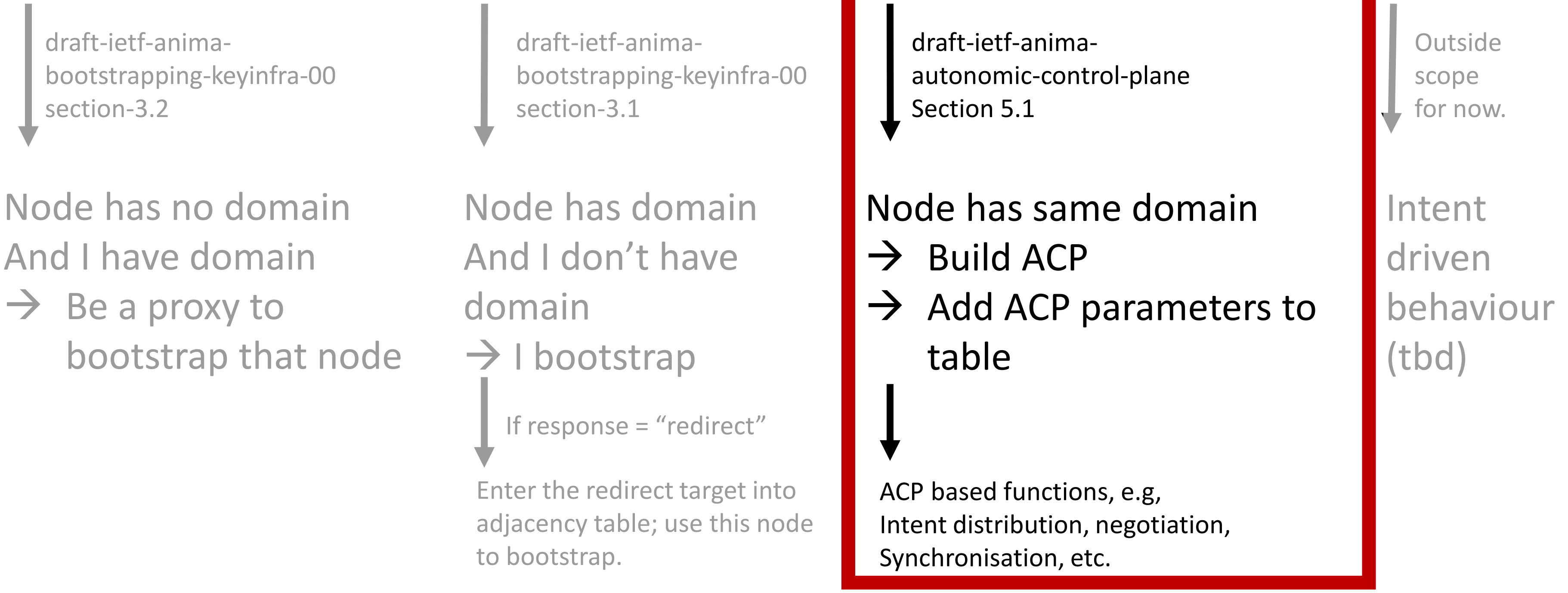
An Autonomic Control Plane
draft-ietf-anima-autonomic-control-plane-03.txt

96th IETF, 18 July 2016

Michael Behringer (editor), Toerless Eckert, Steinthor Bjarnason

Using the Adjacency Table

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



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

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

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

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

If response = "redirect"

Enter the redirect target into adjacency table; use this node to bootstrap.

draft-ietf-anima-autonomic-control-plane Section 5.1

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

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

Outside scope for now.

Intent driven behaviour (tbd)

Changes from -02: Insecure Adjacency Discovery: mDNS

Needs Discussion

- Text in ACP draft
  - Normative, cannot be in reference model
- Reasons for mDNS:
  - Bootstrap should also work outside ANIMA
  - Should introduce few new elements
  - mDNS assumed well known and likely pre-existing, even in IoT devices
  - Using GRASP insecure and secure seen as a security risk
- in GRASP section, removed “insecure GRASP”

Changes from -02: Certificate Requirements (5.1.1)

- Goal: As simple as possible
- Do not use the common fields (ou, etc)
  - They may be used by the operator
  - Avoid potential conflicts; allow for maximum parallelism
- But: Use a standard field (!)
  - Otherwise, in practice integration problems on CA / RA side.
- Should include ACP address (in zone 0)
- Suggestion: subjectAltName / rfc822Name
  - anima.acp+<ACP address>@<domain>
  - An example: anima.acp+FD99:B02D:8EC3:0:200:0:6400:1@example.com

Changes from -02:
Focus on a single addressing scheme

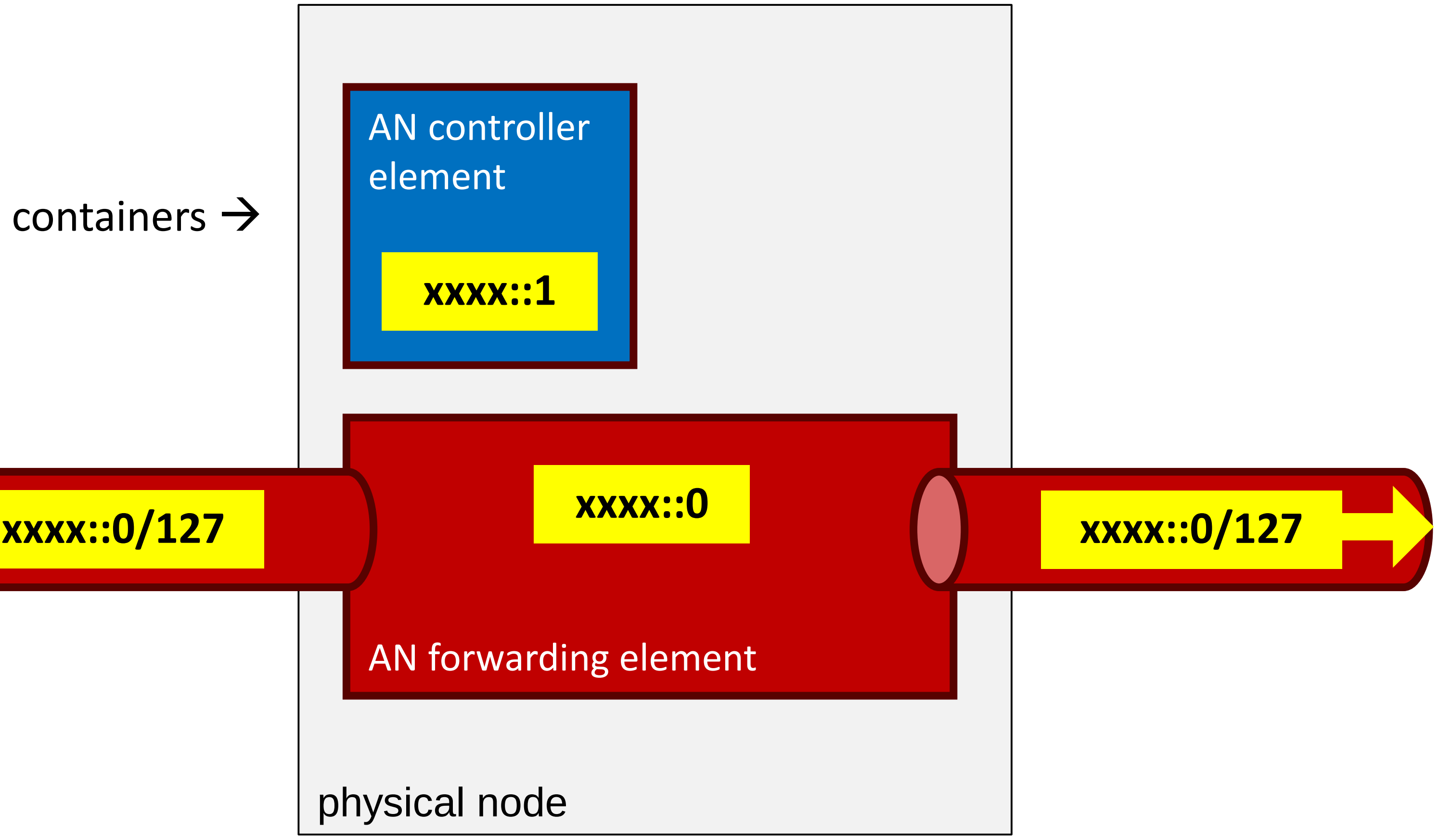
- Proposed addressing scheme:

```
  8      40           3       13                     63             1
+--+--------------+------+---------+----------------------------+---+
|FD| hash(domain) | Type | Zone ID |         Device ID          | V |
+--+--------------+------+---------+----------------------------+---+
```

- Add “Virtualisation” bit at the end
  - Allow addressing a virtual machine on a single node
- Keep routing simpler:
  - Node announces not a /128, but /127

Why the “V” bit?

```
       51                 13                     63               1
+------------------------+---------+----------------------------+---+
|    (base scheme)       | Zone ID |         Device ID          | V |
+------------------------+---------+----------------------------+---+
```



Changes from -02

- Deleted appendix on “ACP without separation”
  - As previously decided
- Editorial changes, references, etc.