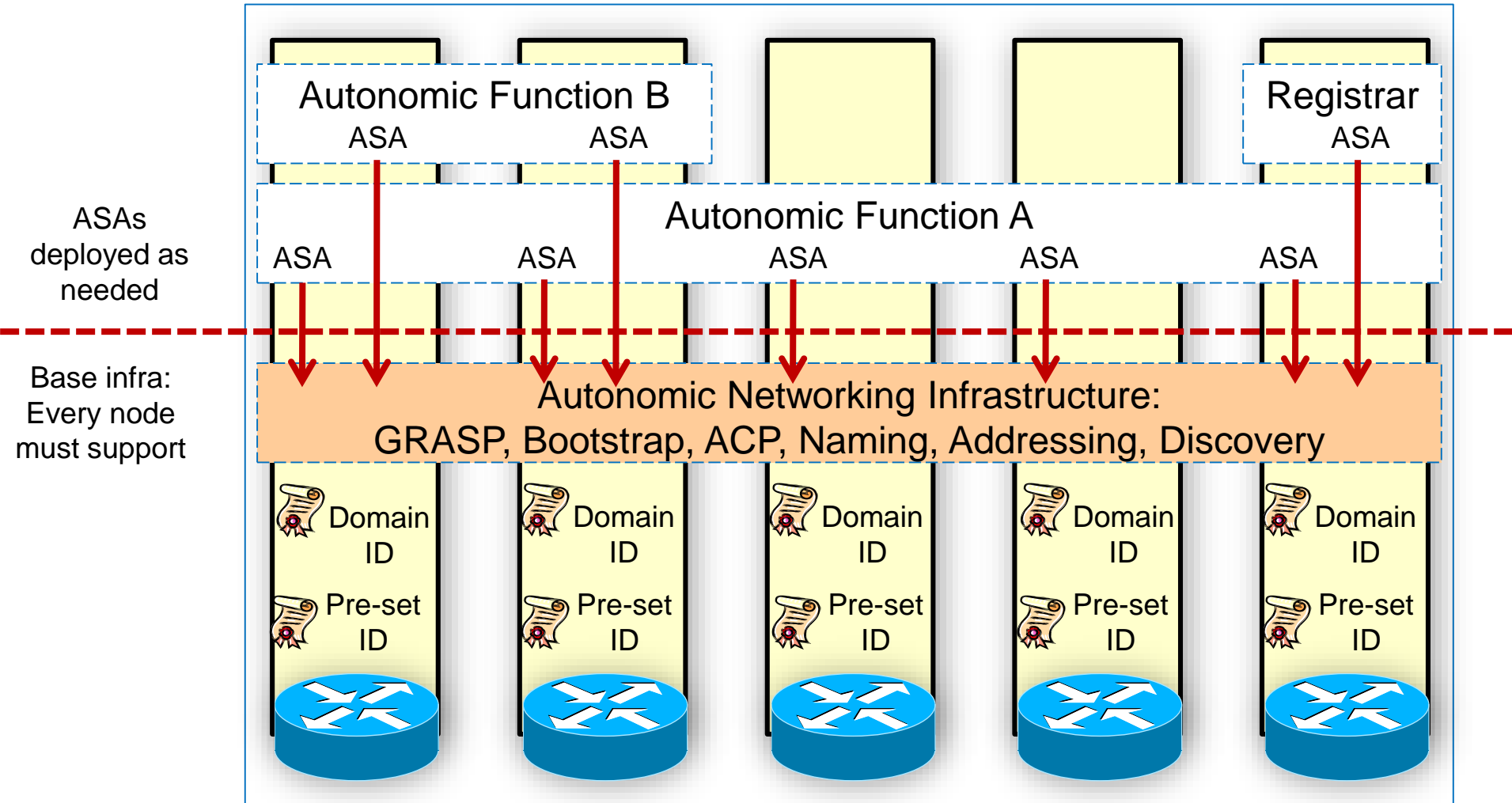# A Reference Model for Autonomic Networking

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 Function B

ASA   ASA

Registrar

ASA

Autonomic Function A

ASA   ASA   ASA   ASA   ASA

ASAs deployed as needed

Base infra: Every node must support

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

Domain ID   Domain ID   Domain ID   Domain ID   Domain ID

Pre-set ID   Pre-set ID   Pre-set ID   Pre-set ID   Pre-set ID

Network with autonomic functions

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."** → **Needs more thinking**

Addressing Section

- **The proposed addressing schemes are now in ACP draft (as per chair's request)**
- **→ Pointing to ACP draft**

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.
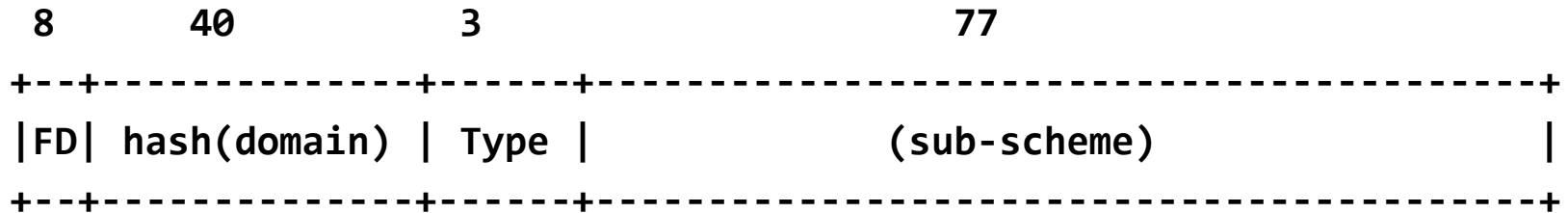**That defines a "device-ID" (last n bits of ACP address).**
convert that to a string, and use it as a name. This would result in something like: 0123-4567-89ab-0001.example.com.
The name would go into the domain certificate --> need to put this into the bootstrap draft as well.

- 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:

```
 8      40               3                           77
+--+---------------+-----+---------------------------------------+
|FD| hash(domain) | Type |              (sub-scheme)             |
+--+---------------+-----+---------------------------------------+
```
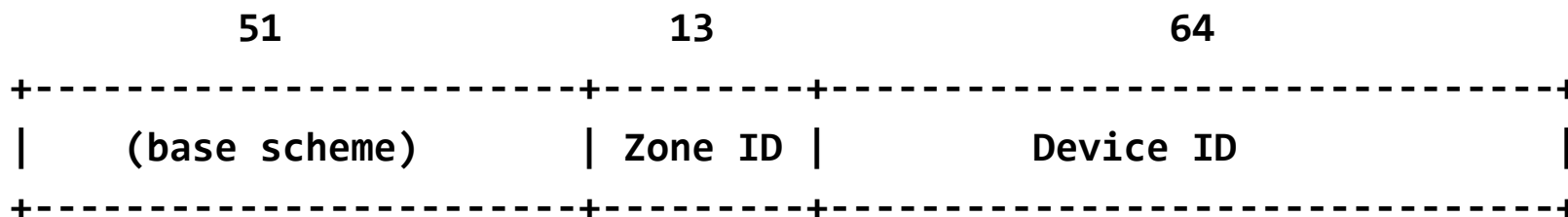
- ## Hash(domain) provides pseudo-random prefix, as required by RFC4193 (ULA)

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

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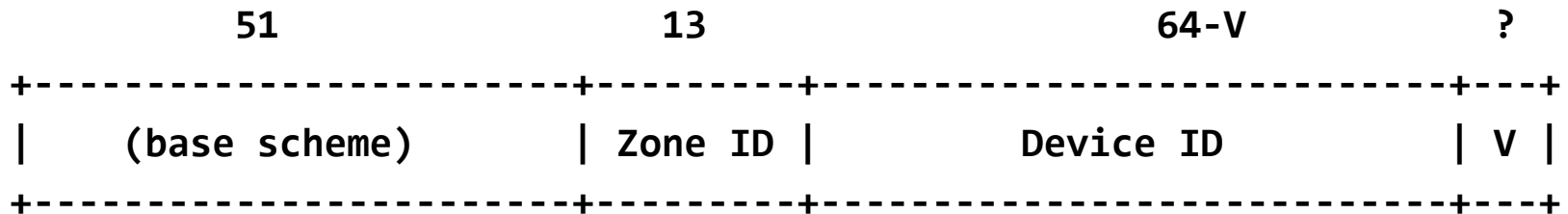
Addressing – Sub-Scheme 1

• **Needs discussion**

• **Sub-Scheme 1:**

```
        51                     13                      64
+------------------------+---------+-----------------------------+
|     (base scheme)      | Zone ID |         Device ID           |
+------------------------+---------+-----------------------------+
```

• **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**

Addressing – Sub-Scheme 2

- **Sub-Scheme 2:**

```
       51                      13                    64-V          ?
+-----------------------+---------+---------------------------+---+
|     (base scheme)     | Zone ID |         Device ID         | V |
+-----------------------+---------+---------------------------+---+
```
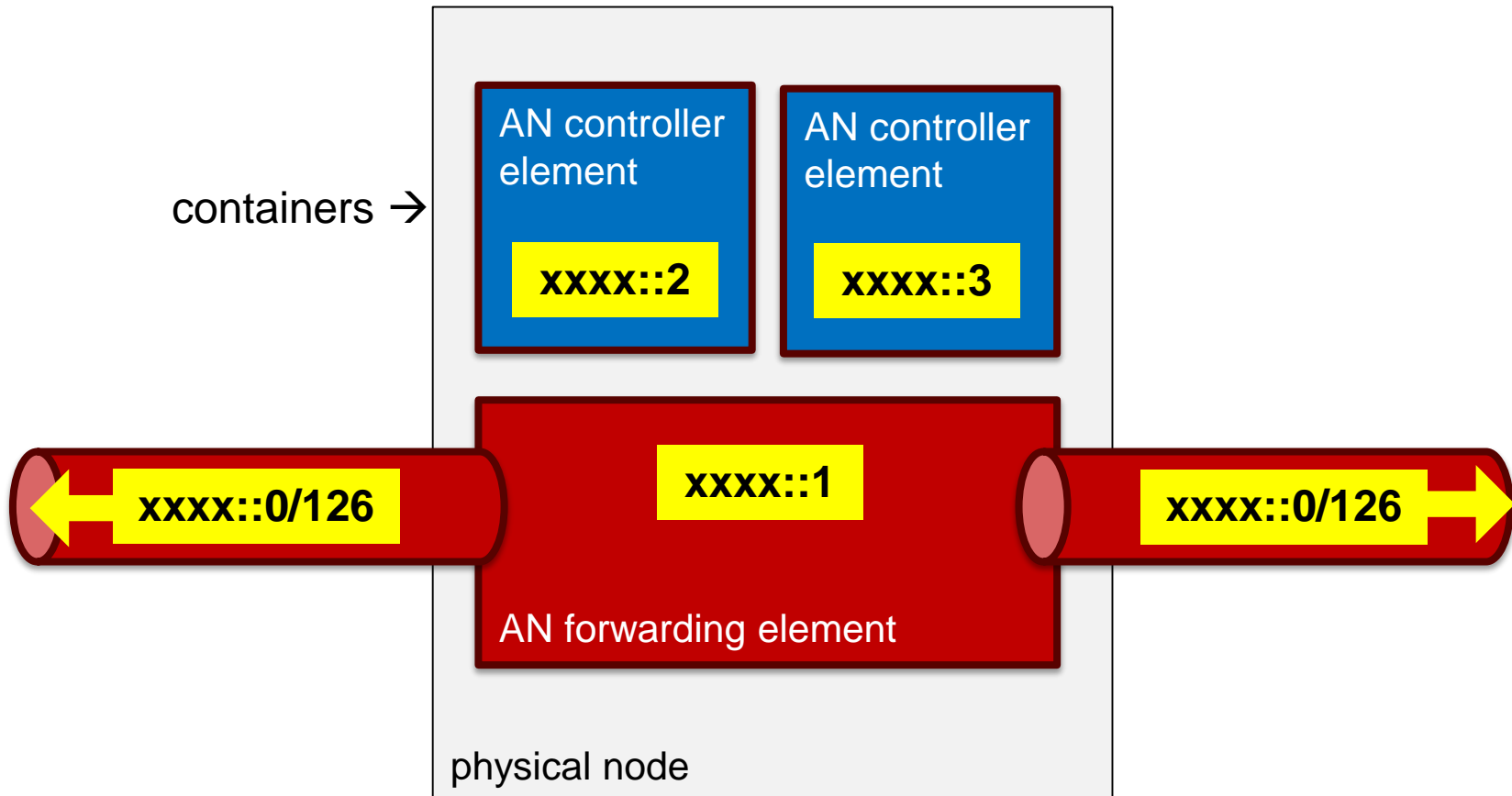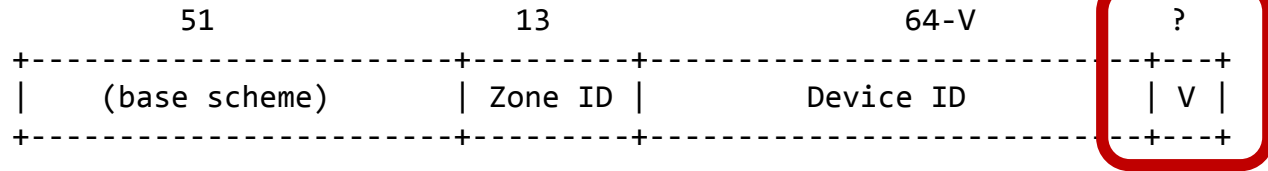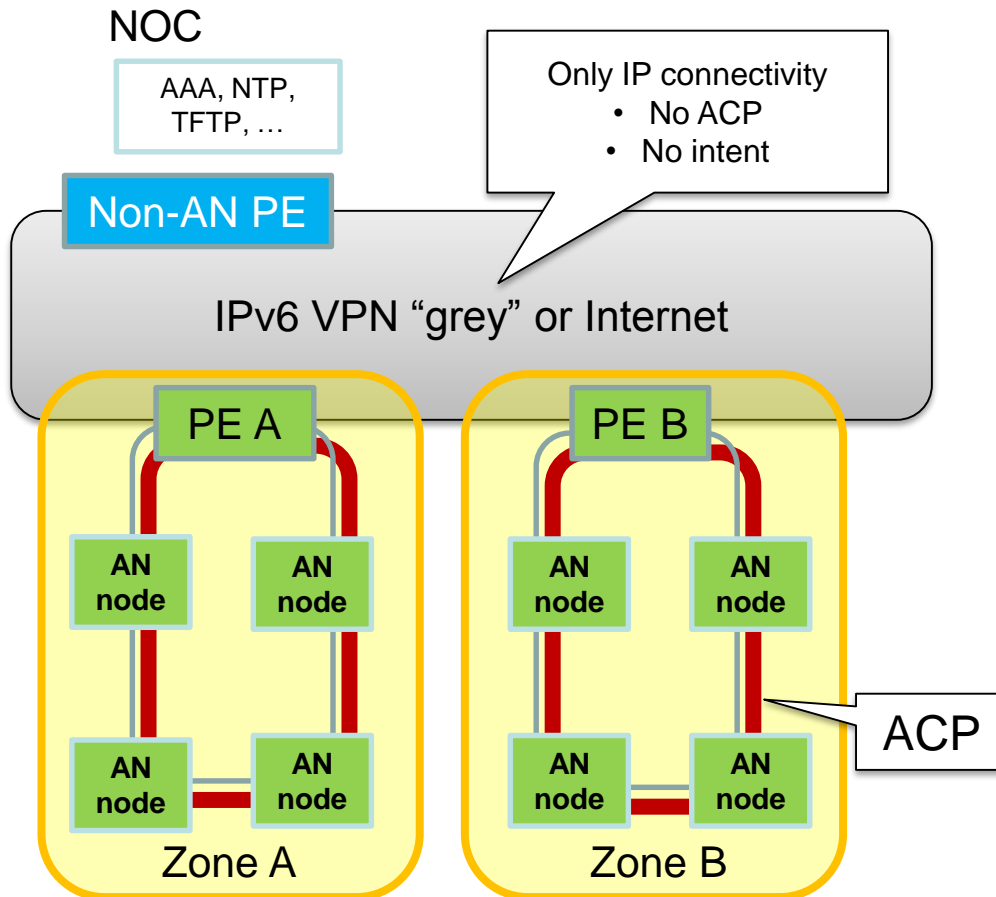
- **Add "Virtualisation" bits at the end**
  - **Allow addressing various virtual machines on a single node**
- **Keep routing simpler:**
  - **Node announces not a /128, but for example /127**

- Needs discussion

Why the "V" bit(s)?

```
         51                    13              64-V          ?
+-----------------------+---------+---------------------------+---+
|     (base scheme)     | Zone ID |         Device ID         | V |
+-----------------------+---------+---------------------------+---+
```


containers →

AN controller element
xxxx::2

AN controller element
xxxx::3

xxxx::1

xxxx::0/126

xxxx::0/126

AN forwarding element

physical node

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

NOC

AAA, NTP, TFTP, …

Only IP connectivity
- No ACP
- No intent

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

ACP

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

NOC

AAA, NTP, TFTP, …

Only IP connectivity
- No ACP
- No intent

Non-AN PE

IPv6 VPN "grey" or Internet

PE A

PE B

AN node

AN node

AN node

AN node

AN node

AN node

AN node

AN node

ACP

Zone A

Zone B

VPN "grey" or Internet

PE

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]

ACP

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.**

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:..	-	-	-	-	-

Feeding the Adjacency Table

AN discovery
(local)

draft-ietf-anima-grasp

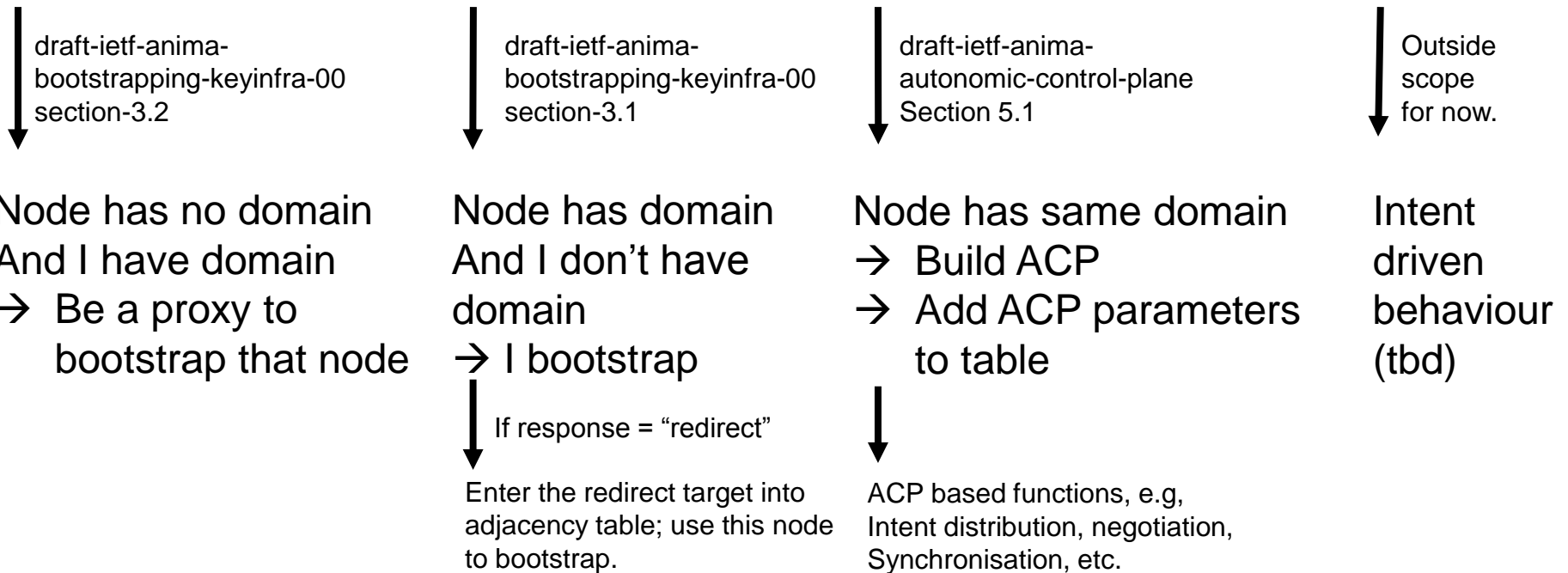AN discovery
(cloud redirect)

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

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

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:..	-	-	-	-	-

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

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

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

Outside scope for now.

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

If response = "redirect"

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

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

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

Intent driven behaviour (tbd)

Open Issues: Security and Trust

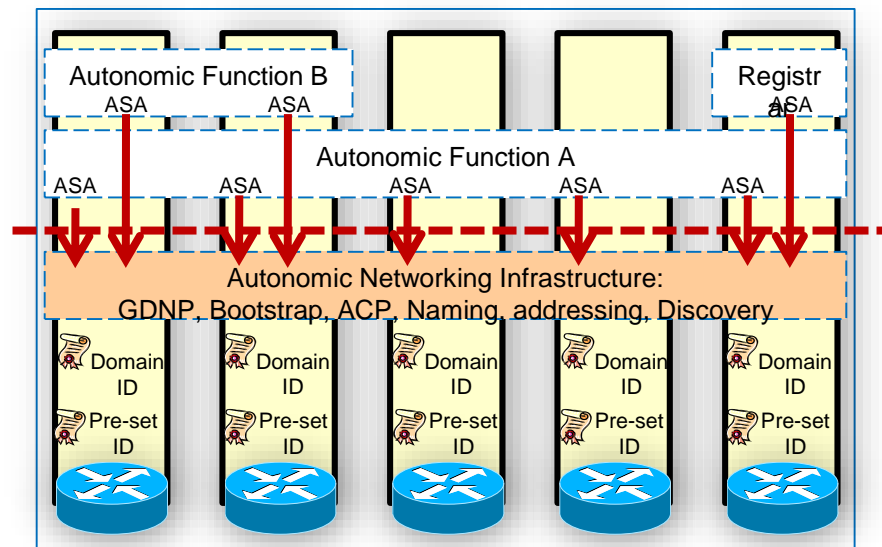**6. Security and Trust Infrastructure**

- 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