draft-ietf-anima-stable-connectivity-02.txt

IETF’99 Prague, July 2017

Toerless Eckert, Huawei (Futurewei Technologies USA)

tte@cs.fau.de

Status

- Shepherd review based update from ‘02 (Chicago) to ‘03 (now)
- Currently in WGLC until July 28

- Many small textual changes (based on thorough review)
- More detail into to what stable connectivity means
- Running on IPv6 but also meant to manage IPv4
- Refined challenges & limitations section to help with incremental adoption of ACP pending on how much ACP is supported.
  - Biggest challenge still missing IPv6 support in a lot of NMS application. Last IPv6 frontier.
  - 3 new paragraphs explaining this to justify the horrible workaround of IPv4/IPv6NAT
  - But that NAT works (tested myself), so why not document it. Its nasty enough no sane operator wold continue using it longer than necessary.
- Amended explanation of how to select whether to use dataplane and/or ACP to talk from NOC to devices
  - Concern of Sheng was to better understand what relevance DNS has:
  - DNS is just example of names used in NOC applications. These could be manually configured name to address tables as well. But in NOC apps, names are used.
- Completed references etc..

Stuff that didn’t make it

- Followup work I am interested in:
- Standards track work:
  - Explicit GRASP objective for large set of NOC services to be autoconfigured on every ACP node: Radius/Diameter server, TFTP-server, DNS server, DHCP server, NTP server, Netconf-Call-Home server, syslog server, …
  - Map GRASP<->DNS-SD for this
- Architecture / informational:
  - High performance / high resilience models for stable connectivity via ACP for even more evolved SDN solutions.
  - IGPs in DC have been built without inband signaling bit instead using out-of-band management network and centralized controller
    - What would we need to do to build designs like this with inband ACP (highest level of stable connectibity requirements)
  - Telemetry streaming

Drafts

Charter / WG items:

draft-ietf-anima-bootstrapping-keyinfra

draft-ietf-anima-voucher

draft-ietf-anima-autonomic-control-plane

draft-ietf-anima-grasp

draft-ietf-anima-reference-model

draft-ietf-anima-prefix-management

draft-ietf-anima-stable-connectivity

Associated:

draft-carpenter-anima-ani-objectives

Proposed GRASP text to be put into BRSKI/ACP drafts.
Draft meant to expire.

Maintained non-charter (yet) items

Authors would propose for them to be adopted after charter extension.

draft-liu-anima-grasp-api

draft-liu-anima-grasp-distribution

Candidate next work items

- Potentially within existing (ANI) charter (1)
  - *All the pieces that logically belong to the ANI*
  - *Need to validate with AD if these can be done without recharter*
  - Extending bootstrap beyond ANI:
    - For non ANI pledges connecting to ANI bootstrap proxy (was in main BRSKI draft but would be better explained / defined in more detail in separate document).
    - For pledges (ANI or non-ANI) with ”remote” bootstrap proxy.
  - Bootstrap signaling for IoT – TLS -> dTLS/CoAP
  - Bootstrap/ACP: Integrating ANI with network management backend
    - Yang data model to set up ANI (Registrar), troubleshoot, diagnose, control bootstrap/ANI enrollment.
  - ANI Topology service:
    - Discover topology of pledges and ANI devices by management backend and ASAs.
  - Dynamic GRASP based ACP channel negotiation
    - See details slide
  - GRASP
    - API for applications / ASA – (draft-liu-anima-grasp-api)
  - ANI Implementation/design options/considerations
    - Eg: userland vs. kernel options, GRASP daemon/ASA interactions,…

Candidate next work items

- Potentially within existing (ANI) charter (2) ??
  - *Somewhat "further" out ANI considerations*
  - Variations of "ACP" concept for controlled environments (informational)
    - Lightweight option without ability to carry IP (but only GRASP and other "application protocols"). For networks with autonomic data plane (IoT etc.). Should not be called ACP.
    - ACP variations with other encaps / routing protocols / (/IPv4). Eg: for use in Data Centers.
    - High resilience ACP (ACP with autonomic live-live routing)
      - When you outsource routing protocols onto ACP – like some Data Center routing designs relying today on a resilient out-of-band management network.
  - ANI in the presence of VMs, NFV
    - Unclear what it means.
  - ANI with slicing - draft-galis-anima-autonomic-slice-networking

Candidate next work items - after recharter

- Intent
- ASA
- Autonomic Functions

- APIs,
  - Refine / expand terminology ?!
    - IETF leadership (eg: Benoit) do not agree that network wide service or policy provisioning constitutes something that can be called “Intent”. Only “other” stuff would be intent.
    - ANIMA “intent” would/should be inclusive of service/autonomic-function provisioning and policy…
  - draft-du-anima-an-intent
    - Initial ANIMA intent definition
    - Covers distributed intent for autonomic-functions
  - Need framework to define how intent for autonomic functions (rendered distributed by ASA) relates to intent that is centrally rendered.
    - draft-li-intent-classification – can be a starting point ?!
  - draft-liu-anima-grasp-distribution
    - Use of GRASP for “information” distribution: Intent and potentially more.

Candidate next work items - after recharter

- ”Intent” (1)
  - Refine / expand terminology ?!
    - IETF leadership (eg: Benoit) do not agree that network wide service or policy provisioning constitutes something that can be called “Intent”. Only “other” stuff would be intent.
    - ANIMA “intent” would/should be inclusive of service/autonomic-function provisioning and policy…
  - draft-du-anima-an-intent
    - Initial ANIMA intent definition
    - Covers distributed intent for autonomic-functions
  - Need framework to define how intent for autonomic functions (rendered distributed by ASA) relates to intent that is centrally rendered.
    - draft-li-intent-classification – can be a starting point ?!
  - draft-liu-anima-grasp-distribution
    - Use of GRASP for “information” distribution: Intent and potentially more.

Candidate next work items - after recharter

- ASA
  - Interface / API between intent and ASA
  - Interface between ASA and (southbound) platform
  - Design models / options:
    - Short term: Build ASA as a “distributed intent rendering” on top of existing network device functions
      - Utilize scripting language to make ASA easily modified
      - Eg: automate/simplify operations of security for existing services (routing, multicast, 802.1ae,…)
    - “Native”: building autonomic functions with ASA
      - draft-carpenter-anima-asa-guidelines
        - Starting point
    - Platform for third party ASA
      - What is missing for this – ANI extensions etc.
      - Eg: Enable third parties to develop next-gen routing, telemetry,… as cross-vendor installable SW modules

Candidate next work items - after recharter

- Autonomic functions of interest
  - TBD: revisit past “thu/fri” drafts from ANIMA WG. Several autonomic functions mentioned
    - Eg: Comcast / Autonomic Diagnostics Functions
- Building / modelling autonomic functions
  - Beyond building ASA
  - Modelling relationships between autonomic functions
    - See drafts from Lauent
    - Eg: dependencies, conflicts
  - Modelling relationships between
    - intent (northbound of autonomic function)
    - southbound APIs / data-models
    - Aka: data-modelling behavior of autonomic function
      - Can start migrating autonomic functions from “software” to “data-modelled driven intent rendering engines”

Details: Dynamic ACP channel negotiation

- draft-ietf-anima-autonomic-control-plane-00 – 06 describe option to negotiate the hop-by-hop ACP ”security” protocol via GRASP
  - The description is more suggestive than descriptive: It is insufficient to build a working model out of it.
  - It was also met with concerns/opposition (Michael Richardson).
    - IKEv2 should be used for this.
    - IKEv2 has limited not very successful history of being adopted to protocols other than Ipsec – KARP, nonWG work on fiber channel.
  - Toerless Eckert: Designing a flexible negotiation protocol around reuseable components such as TLS/dTLS and GRASP may be more lightweight and easier extensible.
    - But would need to revisit functionality of IKEv2 and relate to it.
- Enough open question / open work to remove this part from ACP draft and put into new draft – to allow charter item draft to proceed to last call.
  - Quite important goal though: Negotiate eg: the best performing security/encryption option between diverse neighbors (Ipsec(/GRE), 802.1ae, dTLS, …)