draft-eckert-anima-acp-free-ani-00

ANIMA-WG, IETF123 Madrid

Toerless Eckert, Futurewei USA (tte@cs.fau.de)

Summary

This work is proposed as informational – in support of new planned ASA work!

ANIMA ANI = BRSKI + ACP + GRASP

Infrastructure to build network automation (and autonomy) on top of

We want to enable in-network automation/decentralised – well call it ASA

But ACP is challenging to implement (Routing, VRF, „Subinterfaces“, IPsec, ...)

~~Solution~~: Workaround „automation Network Infrastructure“ (aNI)

ANI without ACP = aNI

What can it do, what do we miss ?

aNI overview

Replace ACP simply with „Data Plane“

- Data Plane can still be (incrementally) auto-provisioned by controllers/orchestrators
- IPv4 and/or IPv6 – whatever the network needs/wants to use anyhow

GRASP used pretty much unchanged from ACP (RFC8994) GRASP

- „GRASP relay“ operating on every router. Hop-by-Hop connections via TLS
- But packets go via „Data Plane“ – need to decide IPv4 or IPv6
- GRASP relay provides network wide discovery of services / ASA

BRSKI pretty much unchanged

- Discovery of Join Proxy is link-local, Discovery of registrars uses GRASP relays.
- But for IPv4 only network, BRSKI needs to operate over IPv4.

Domain security concept unchanged

- All TLS communications uses aNI Domain Cert (from BRSKI)
- Includes the primary Data Plane address of router, otherwise like ACP certificate

aNI vs. ANI downsides vs. upsides

- Downsides:
  - Relies on some external entity (operators, controller, orchestrators)
    - ... to configure Data Plane
  - Including correct configuration of BRSKI/proxy/GRASP-relay
    - ... suggest simple „aNI“ config option
  - **When Data Plane has problems (misconfig) – aNI will also fail (mostly)**
    - Grasp relay will still work, but end-to-end connectivity will fail!

- Upside:
  - Easy to implement on every router OS:
    - BRSKI, GRASP relay are simple application level processes on every router.
    - Control-Plane only – no forwarding plane complexity (!hah!)
  - Easiest way to enable autoconfiguring distributed ASA
    - which would also be control-plane only

Complexities / „Extensions“

ACP also „poked“ through network segmentations

- Segments of networks with just IPv4 vs. Others with just IPv6
- Or across NAT in the data-plane
- Or between SP-Core and customer VRFs

This is replaced by aNI driven concept of GRASP relay++ driven connectivity

- Any router that separates Data-Plane connectivity...
- Can provide „proxied“ connectivity via combination of GRASP relay++ and (as needed) Data Plane functions
- Example NAT: If server on inside should be available outside, GRASP on the NAT node would need to allocate „proxy“ server socket and announce that as the service socket to the outside.
- Effectively the generalized concept of BRSKI proxy (and discovery proxying)

Draft describes various generic options for such a „segment edge router“

- Based on different type of forwarding plane segmentation

Questions ?

Please review / comment !

Thank you !