# ACP status

*draft-ietf-anima-autonomic-control-plane-18*

Toerless Eckert tte+ietf@cs.fau.de (Huawei USA)
Michael Behringer michael.h.behringer@gmail.com
Steinthor Bjarnason sbjarnason@arbor.net

v1.0

# Status

- IETF 102:
  - draft-ietf-anima-autonomic-control-plane-16
  - On IESG Telechat beginning of August
- draft-ietf-anima-autonomic-control-plane-17/18
  - Alissa Cooper review
  - Elwyn Davies review (GEN-ART)
  - Frank Xialiang (early SECDIR)
  - Missing fix from Pascal Thuberts review
- Staging -19. security review

# Main changes -16 -> -18 (1)

- Introduced option “0” for ACP address in certificate
  - Required for NOC nodes that assign local address differently
    - Especially connected via ACP connect, normal IPv6 subnet procedures
  - Certificate now indicates that the address is not assigned via Cert
  - Currently no ANI mechanism relies on verifying ACP address, only node itself uses it to as sign its ACP address
- Marked all sections normative/informative
  - Requirements section is INFORMATIVE
  - Use _MUST_, _SHOULD_ to indicate these are solutoin requirements, not RFC2119 style r equirements
- Removed almost all “futures” considerations from normative text
  - Created appendix A.10 for the ones we want to document
- Clarified “rsub” is important NOW, not only future
  - E.g.: also helps to avoid any ULA hashes in interconncted ACPs.

# Main changes -16 -> -18 (2)

- A.8 Intent
  - Elaborated more extensively here about the key issue of designing any Intent solution (or information distribution) carrying ACP Intent/Information:
  - Circular dependencies:
  - Intent/Information says something about ACP that the ACP would need to know before ACP can be correctly built
  - This must be understood and avoided for future work on information distirbution / Intent.
  - Section gives some ideas:
  - Example: Connecting multicast ACP domains. Allow ONLY “intent” information to be passed between them, then that inten determines how ACP continues to autoconfigure itself.
  - Mostly a problem statement, not a proposed solution.
  - Important to keep in ACP doc as appendix because we do want to work on information distribution.

# Main changes -16 -> -18 (3)

- A.10.2 Dependency against IPv6 data plane (from Alissa’s review)
  - Misconfiguring IPv6 data plane so that there is not even link-local IPv6 connectivity will break this specifications ACP connectivity.
  - Relying on Data-Plane IPv6 link-local for encapsulation was conscious choice of ACP authors to keep complexity limited
  - All better solutions are maybe not difficult, but might not work across all possible media for all possible platforms
  - Aka: better link-encap than data-plane link-local is best done as simple add-on documents
  - A.10.2 outlines some options
  - Not all options require actual spec/interop extensions, just impleemntation local
  - Example: SR-IOV: second MAC on NIC
    - Use one MAC for ACP, another for data-plane
    - Different virtual interfaces, data-plane does not see ACP virtual-NIC

# Main changes -16 -> -18 (4)

- A 10.5 Role assignments
  - One of the main security issues with the “simple” ACP group security model is that it can not distinguish which node/ACP-certificate can do what.
  - Aka: If we use ACP domain certificate to allow NetConf/SSH/CLI configuration of devices, then this could be triggered from any device
    - Some router in ACP is hacked into, now worst case you could configure from this router a ny other router.
    - Ongoing work towards -19 also documents this better (security issue)
  - Suggested future work option/solution:
    - Put simple role flags into certificte
    - “normal ACP node” vs. “privileged NOC node”
  - Will see if/how this will be refined through security review

# Main changes -16 -> -18 (5)

## A.10.4. RPL enhancements

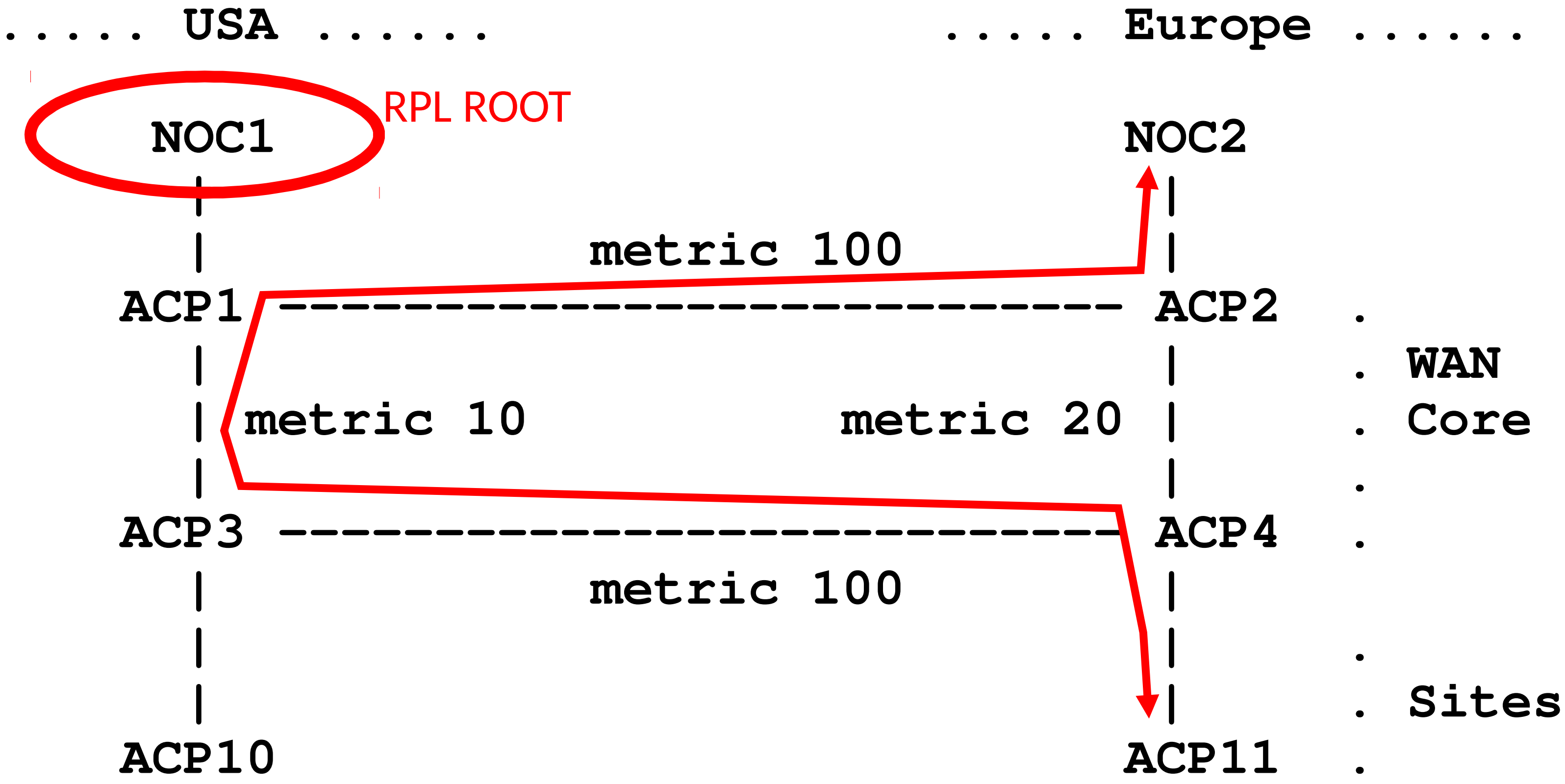

Figure 16: Dual NOC

# Next up

- SecDir / SEC AD review -> version -19
  - Benjamin Kaduk / Eric Rescorla
  - 70% through (first round reply).
- Unfortunately delayed (time alloc issue last two months)
- Some important issues:
  - Lowest common denominator security profile that can be support in commonly expect ed router accelerated crypto HW:
    - AES256 bits ok ?! GTM mode ok ?
    - Elliptic Curve vs. RSA should be fine, no HW impact I am aware of ?
  - Constrained device support in ACP “opportunistic”
    - We do want Ipsec/DTLS to be specified for secure channels
      - To ensure we get practical support for extensible autoconfig choice of security protocol
    - BUT: Tha is NOT complete support for constrained devices
      - TCP use by ACP-GRASP likely not sufficient for constrained devices
      - Have/improved text how this can be added later on (DTLS)
      - Do not feel confident about standardizing this part now in ACP though.

# Thank You!