Topics

• At IETF91 we discussed requirements
• This time:
  – Brief overview for people who didn’t read the draft
  – A quick protocol walkthrough
  – Open issues & discussion
GDNP Overview (1)

- Neutral platform for autonomic nodes to discover peers and synchronize or negotiate any type of configuration parameter with them.
- Specific parameters and methods are defined for individual use cases.
GDNP Overview (2)

• Discovery, Negotiation or Synchronization Objective: protocol element defining a specific network parameter.
• Initiator/Responder model: discovery, negotiation and synchronization proceed by simple message exchanges.
• Operates above Layer 3; IPv6 preferred.
• All messages must be authenticated, with replay protection.
GDNP Overview (3)

• Discovery starts on-link, but may be diverted off-link.
• Negotiation must converge (or fail) in a few steps (closed loop model).
• Synchronization does not require iteration (open loop model).
• Simple TLV (type-length-value) protocol model.
  – Value could be a complex data structure
  – Could run over UDP, TCP, DTLS or TLS.
Walkthrough (1)

CA

Registrar

Router 2

Registered & known to CA, have ULA prefix & addresses

Router 1

Factory condition, default configuration

Newbie
Walkthrough (2)

CA

Registrar

Router 2

Listening on GDNP port

Router 1

Newbie

Configures link-local address, waits for RA, configures ULA
Walkthrough (3)

- **CA**
- **Registrar**
- **Router 2**
- **Router 1**

- Discover “trust relay”
- Operating as relay for trust bootstrap

Newbie

- Enroll via relay, receives Domain ID and locator of CA*

* e.g. draft-pritikin-anima-bootstrapping-keyinfra
Walkthrough (4)

CA

Registrar

Router 2

Another box

Listening on GDNP port

Router 1

Discover “money”

Newbie

Is now known to CA so traffic can be authenticated
Walkthrough (6)

CA → Registrar → Router 2 → Autonomic agent for money → Response "money" → Router 1 → Waiting → Newbie
Walkthrough (7)

- CA
- Registrar
- Router 2
- Autonomic agent for money
- Router 1
- Locator for “money”
- Newbie

Receives locator and can connect with agent
Walkthrough (8)

CA

Registrar

Router 2

Autonomic agent for money

Router 1

Iterative negotiation with agent

Newbie
Walkthrough (9)

Newbie

- Negotiate("money", $100)
  - Negotiate("money", $50)
    - Negotiate("money", $75)
      - Negotiation-ending("accept")

New agent for money

Autonomic agent for money
Open issues (1)

- **1. UDP vs TCP.**
  - Complex objectives will exceed reasonable MTU size, but UDP multicast is necessary for discovery.

- **2. DTLS or TLS vs built-in security mechanism.**
  - Built-in mechanism requires costly (asymmetric) crypto. Maybe simpler to bite the bullet and just use TLS.
  - DTLS and IPsec not off the table yet.
  - Note that discovery will sometimes be insecure anyway, until trust has been established.

- **3. DoS Attack Protection TBD.**
Open issues (2)

• 4. DNS-like alternative approach to discovery?
  – Or DNS SD
  – Cannot use until initial discovery has succeeded, so built-in discovery remains necessary
  – Propose to defer this question for now

• 5. Expand description of requirements for the specification of an individual objective.

• 6. Document protocol walkthrough(s).

• 7. Cross-check against other ANIMA documents.

• 8. Write code...
Discussion

• Other open issues?
• General direction?