Generic Discovery and Negotiation Protocol for Autonomic Networking

draft-carpenter-anima-gdn-protocol-02

Brian Carpenter
Bing Liu

IETF 92
March 2015

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.

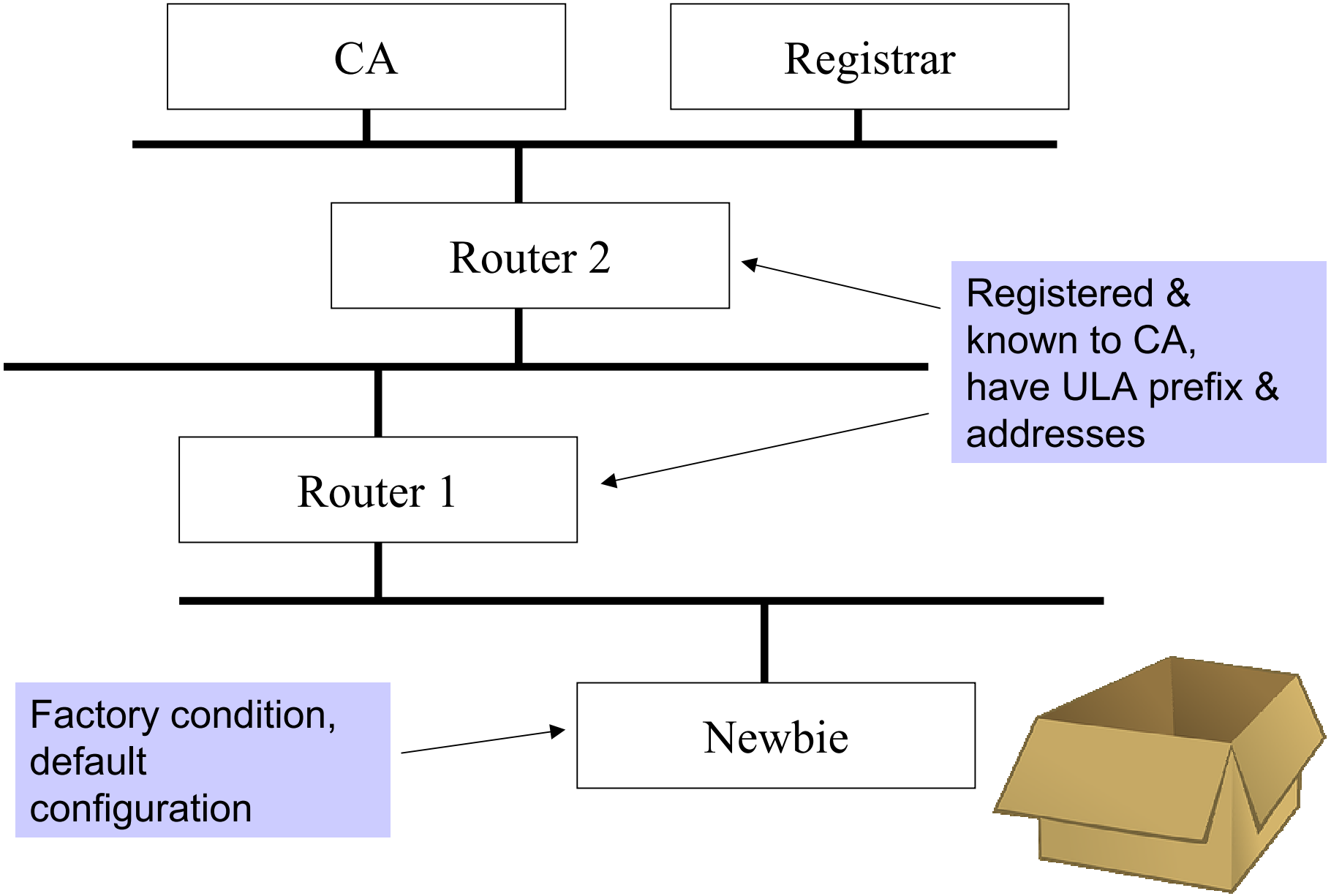
GDNP Overview (2)

- 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.

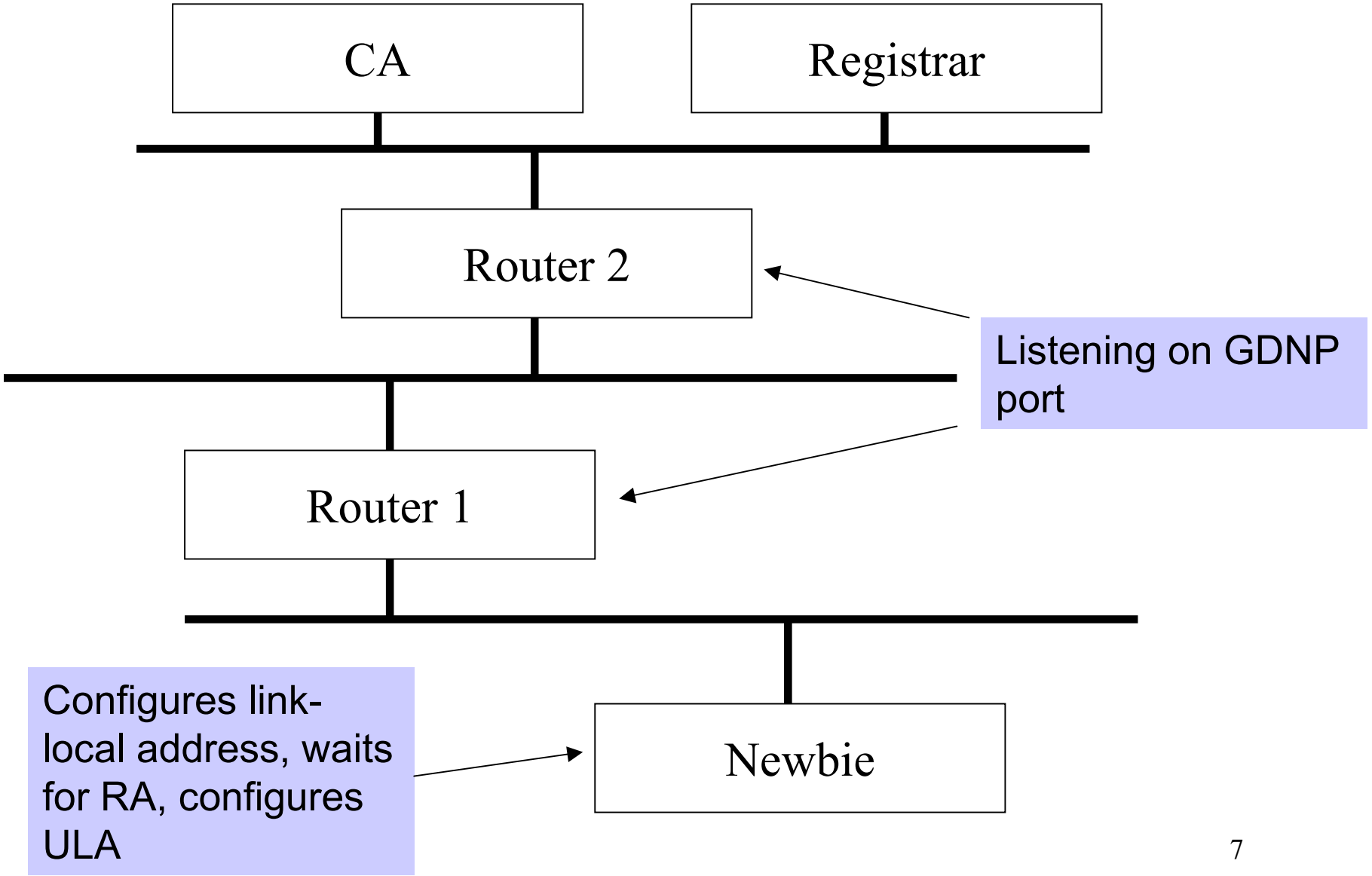
GDNP Overview (3)

- 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.

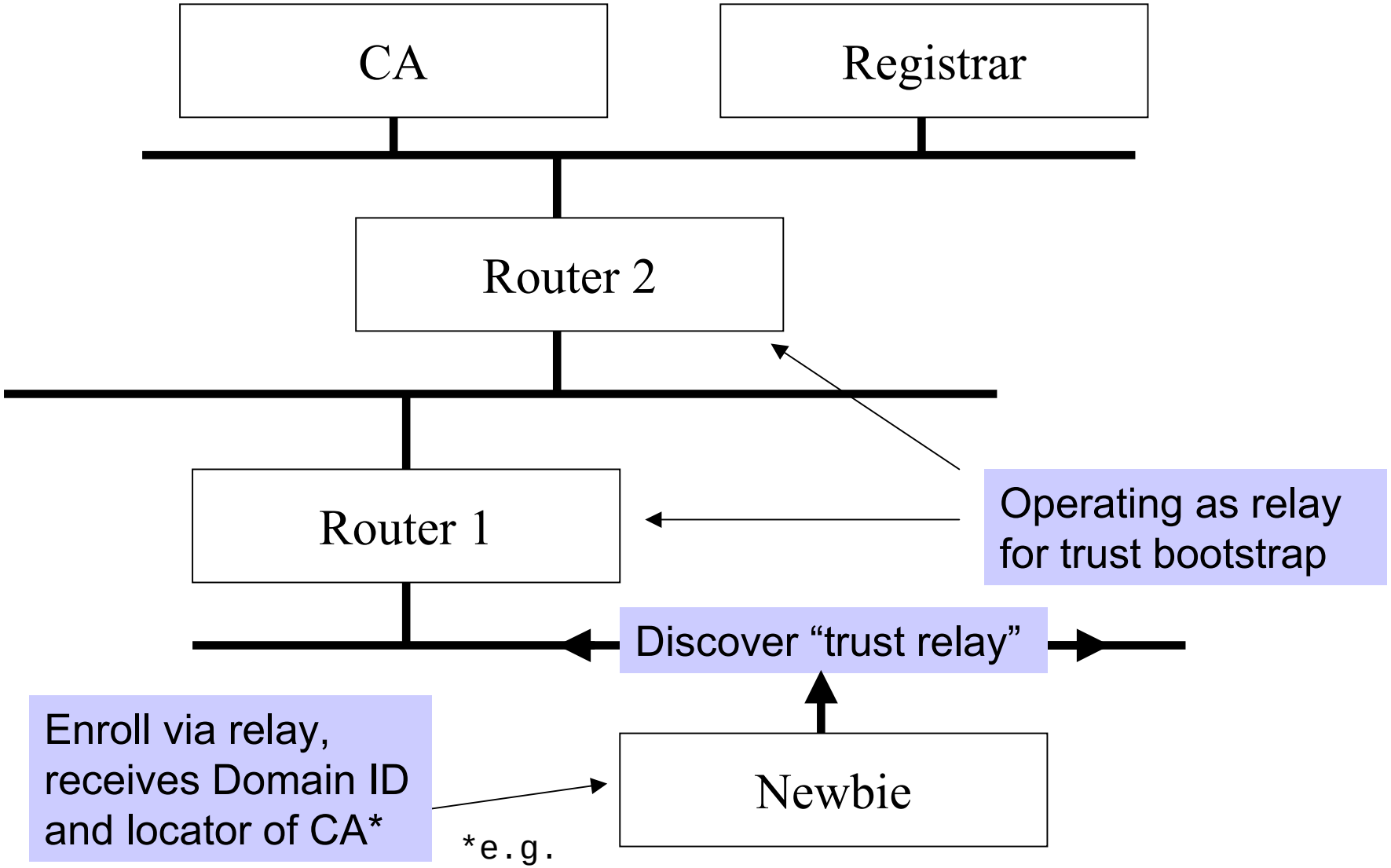
Walkthrough (1)



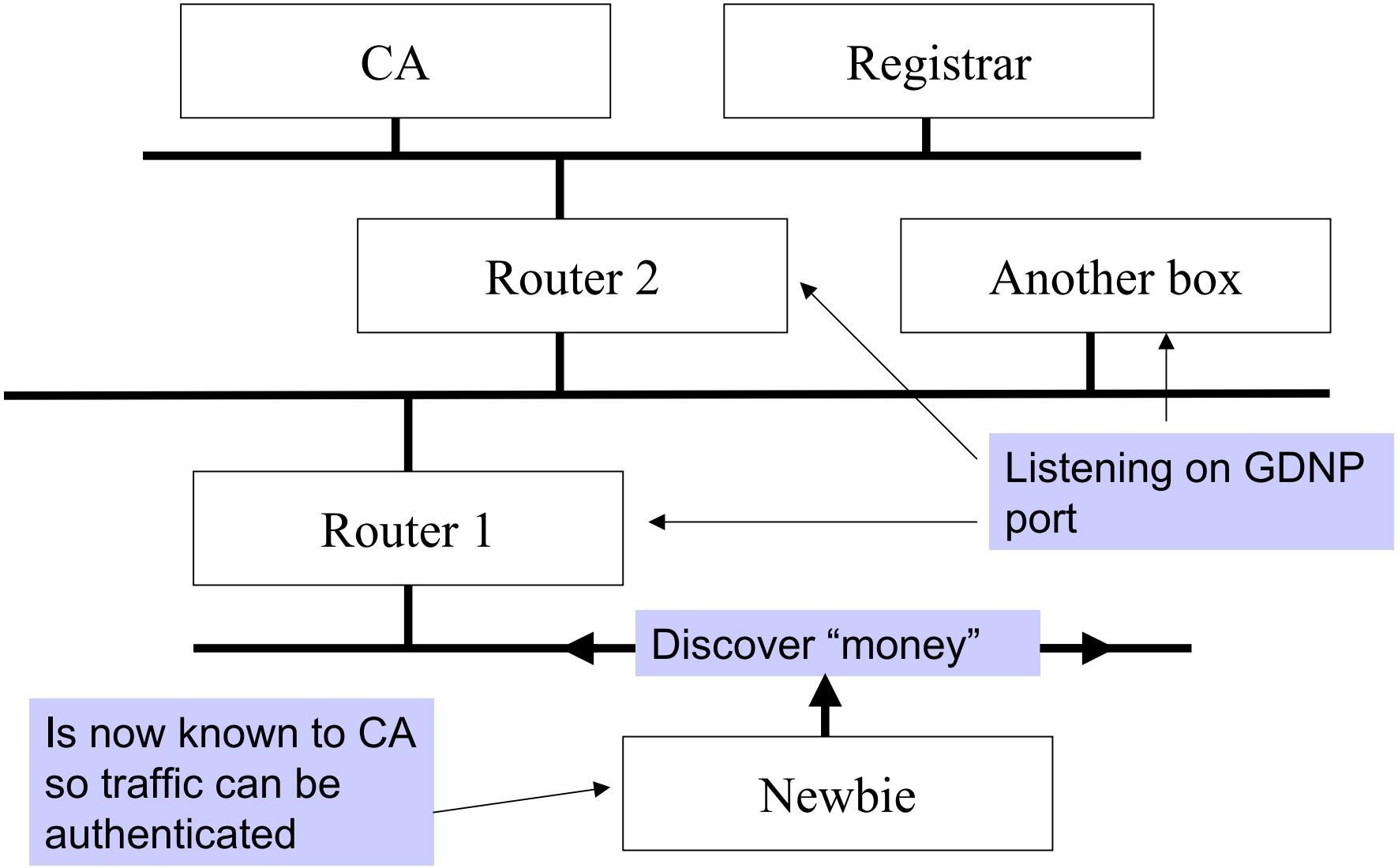
Walkthrough (2)



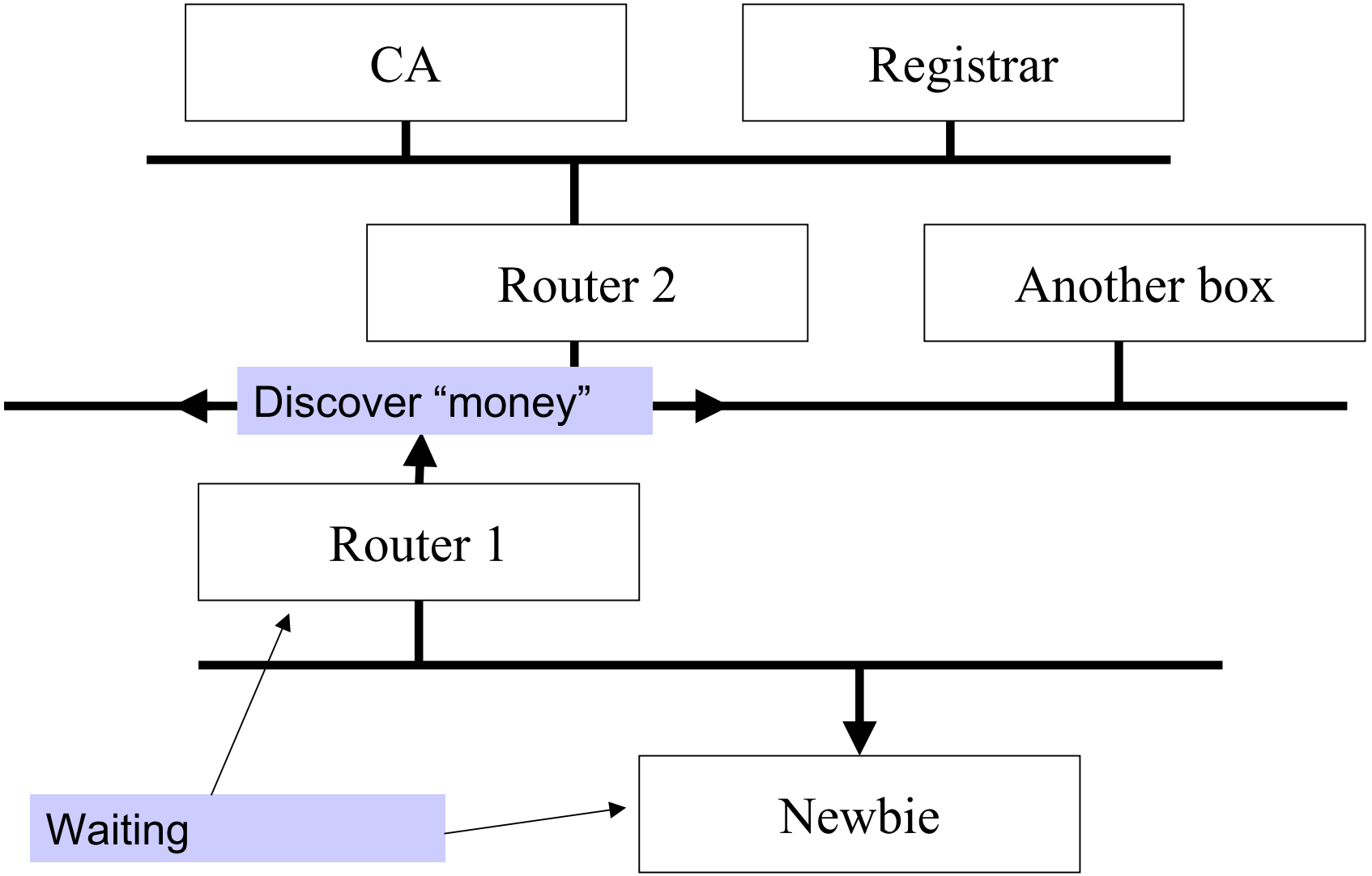
Walkthrough (3)



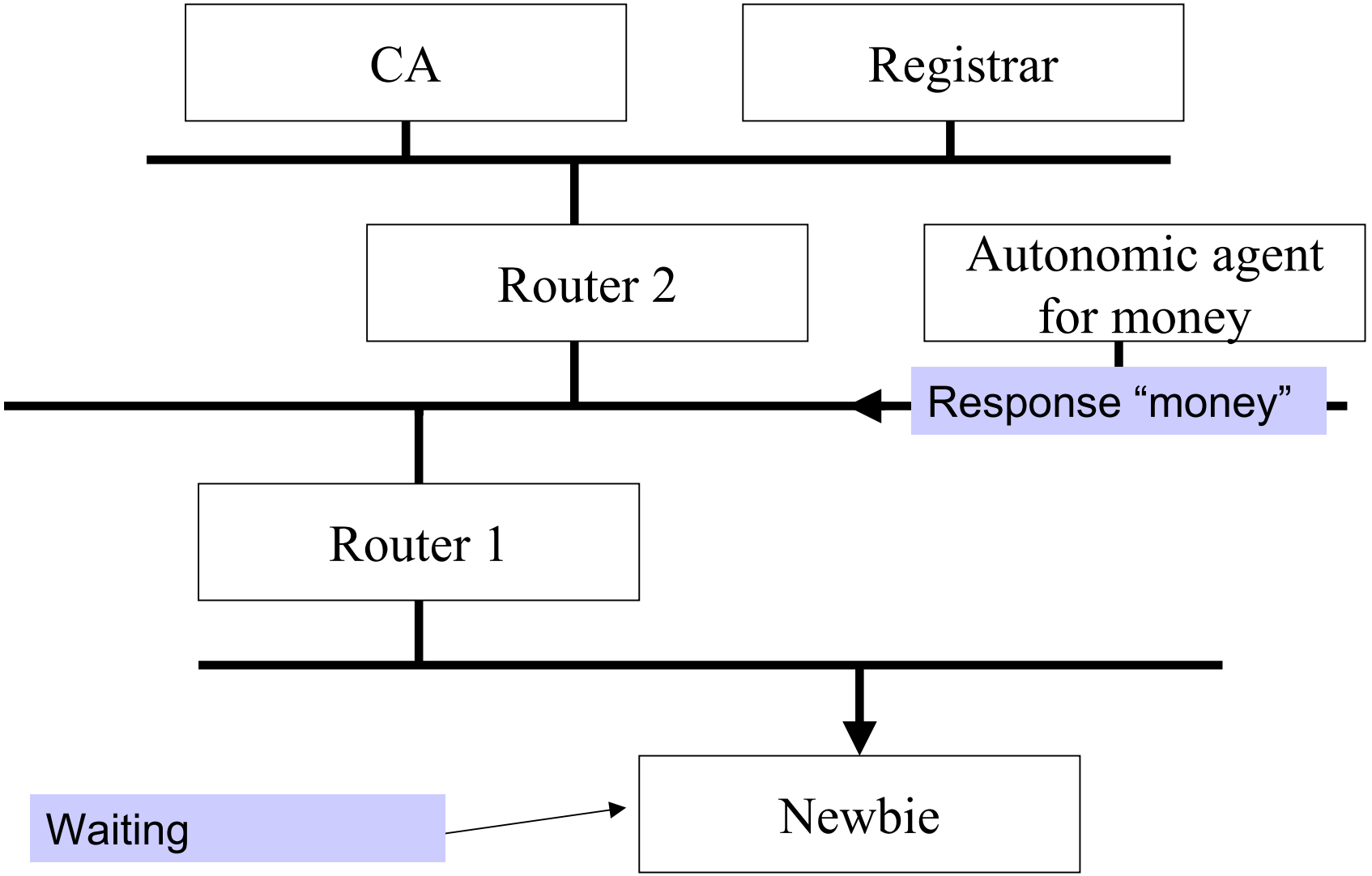
Walkthrough (4)



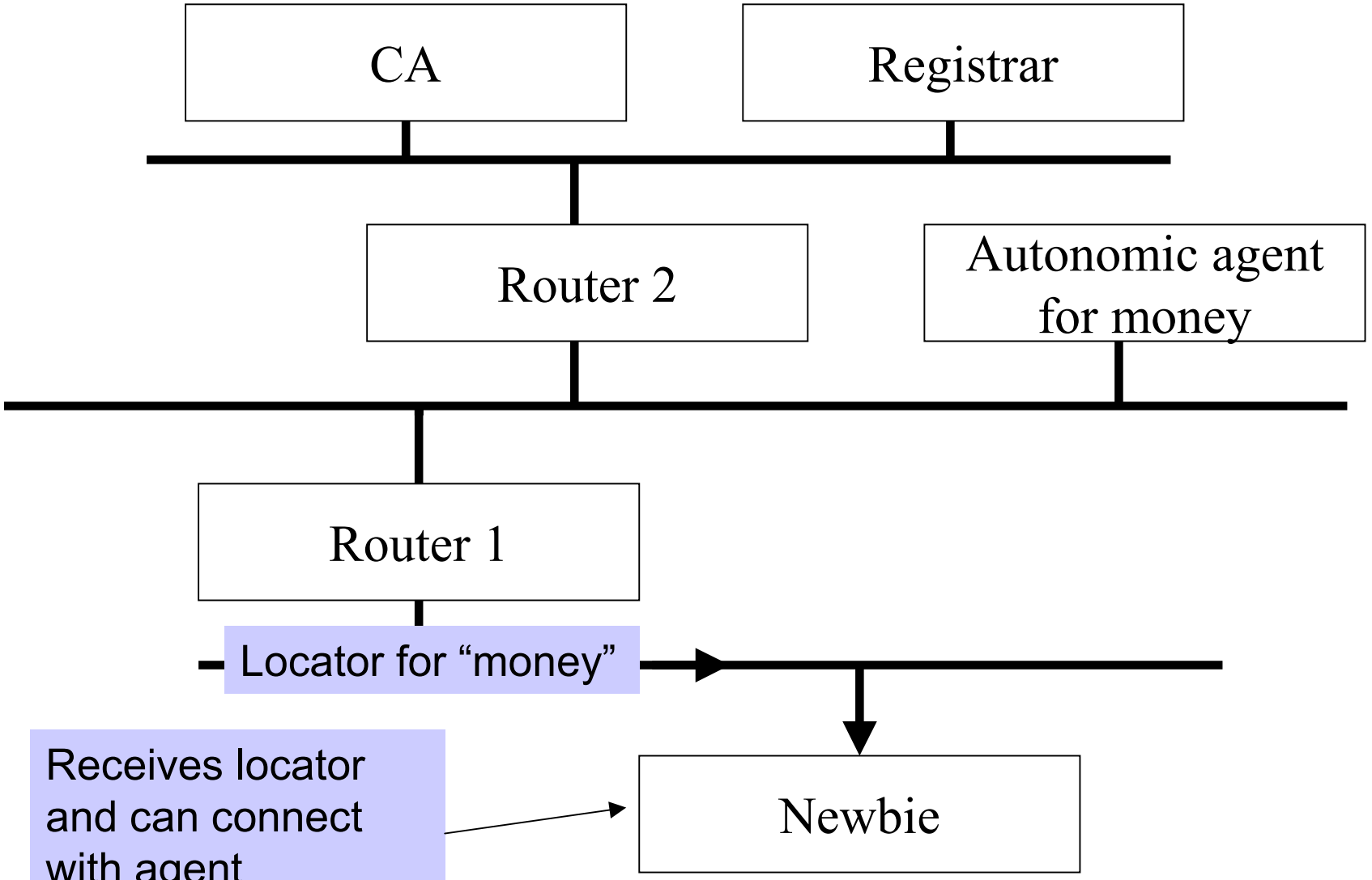
Walkthrough (5)



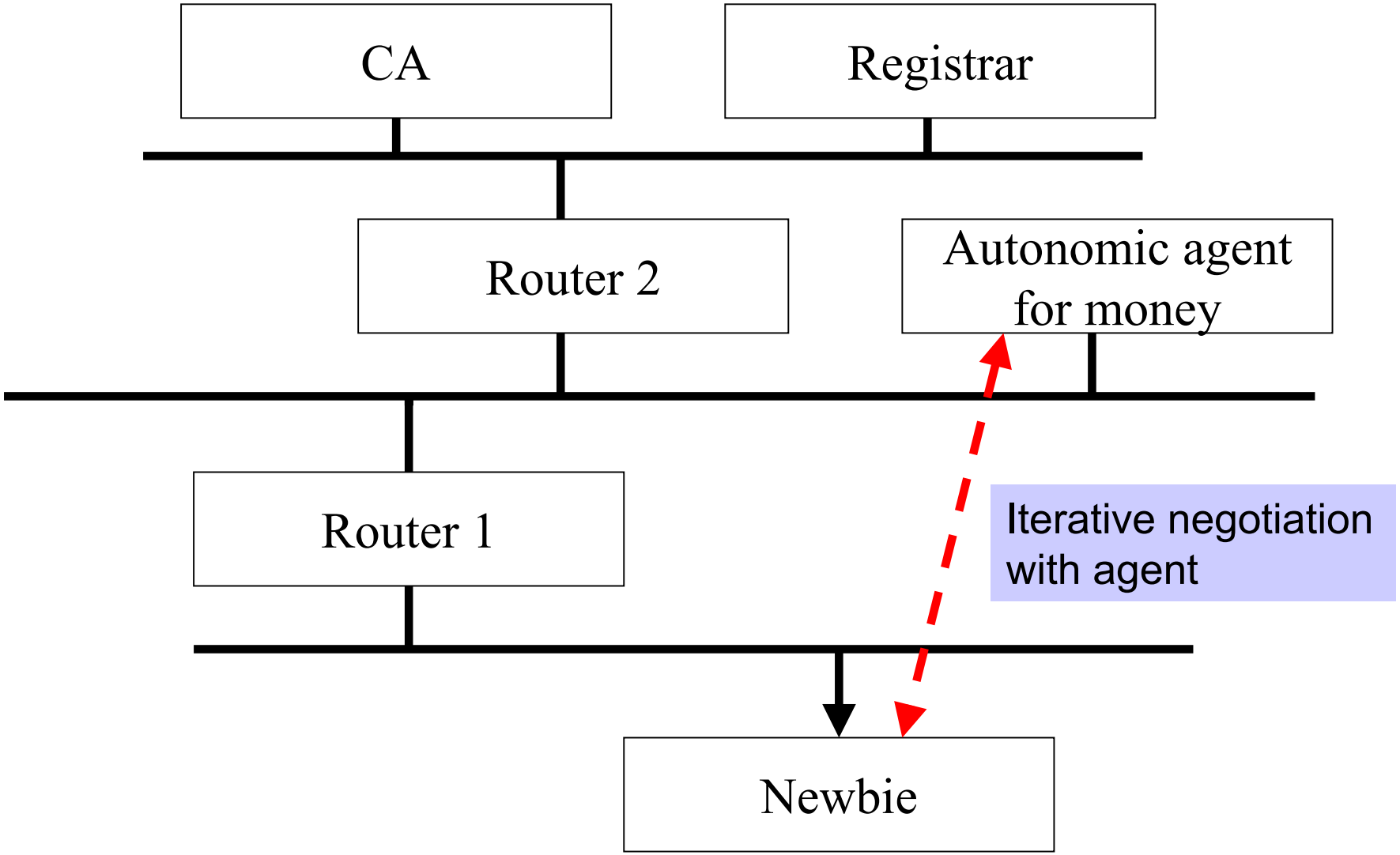
Walkthrough (6)



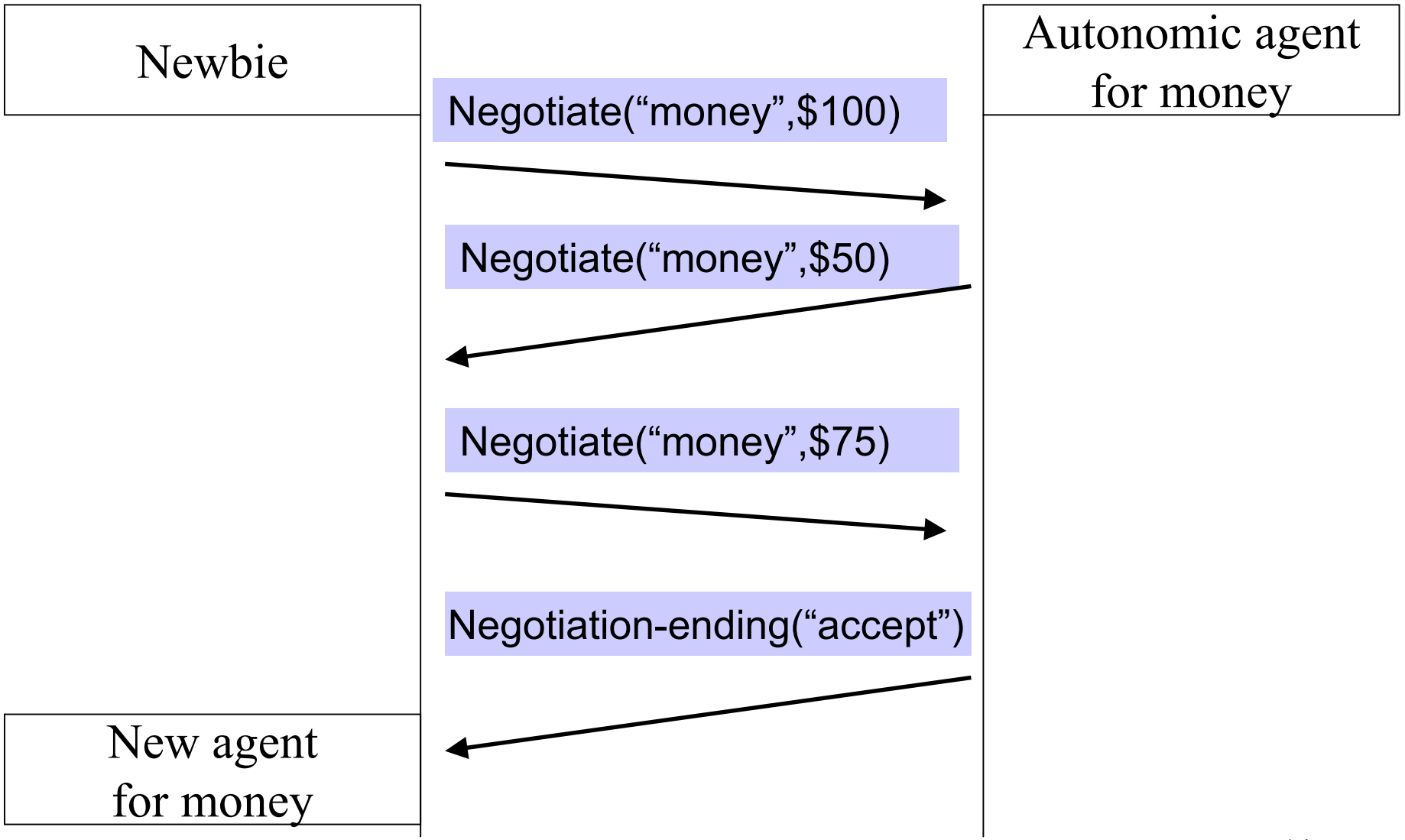
Walkthrough (7)



Walkthrough (8)



Walkthrough (9)



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?