Bootstrapping Trust in a Homenet

draft-behringer-homenet-trust-bootstrap-00.txt

85th IETF, 7 Nov 2012

Michael Behringer

Max Pritikin

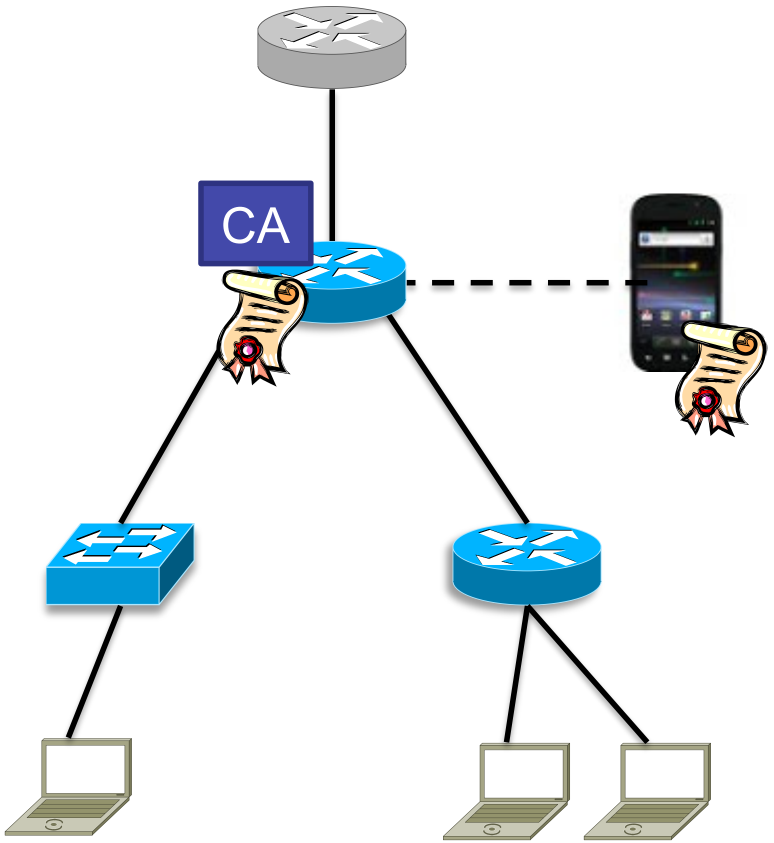
Steinthor Bjarnason

Problem Statement

- Find boundaries
- Establish trust to permit self-configuration
  - Devices need to know whether they are part of the homenet

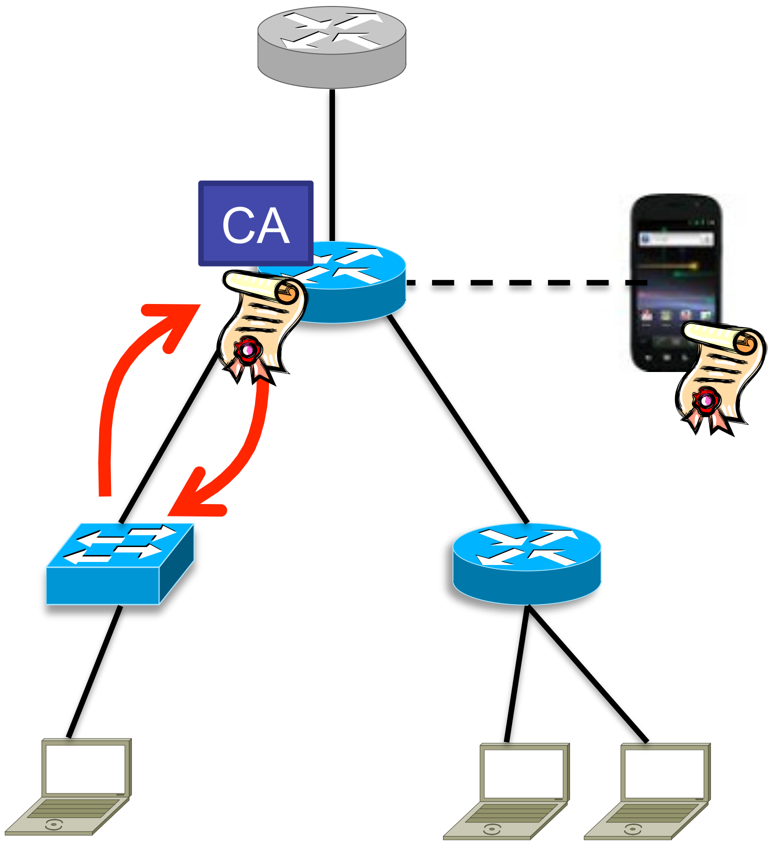
Approach:
1) Defining a Trust Anchor

- Pair smart phone with a homenet device
  - As today
- Tell homenet device: “You’re the trust anchor”
  - This enables a CA/RA function
  - Assign domain cert to smart phone
  - (Alternative: auto-select to be a trust anchor)



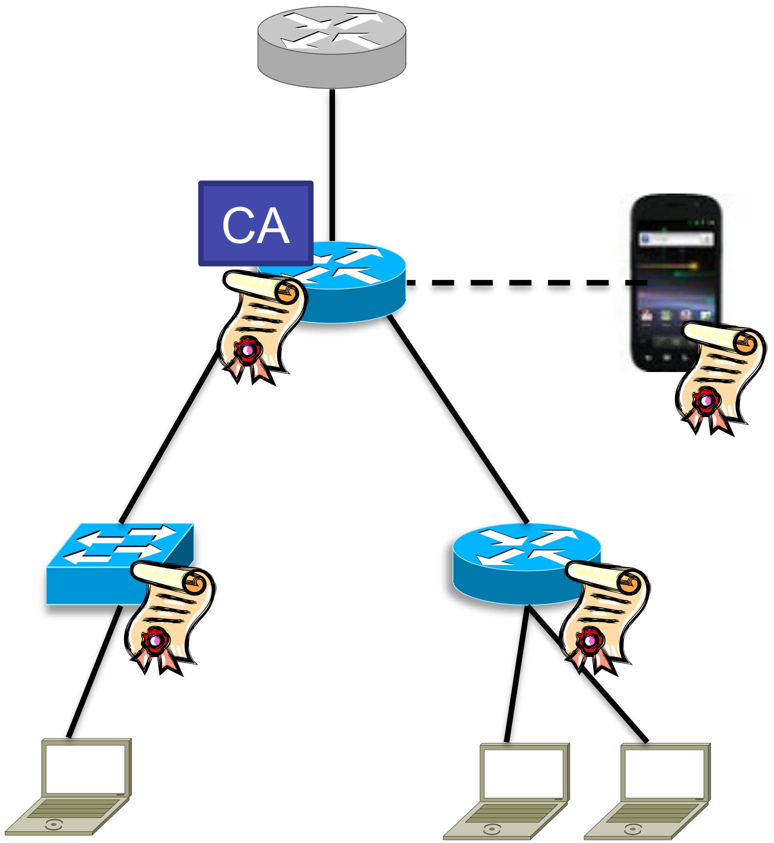
Approach:
2) Neighbor Discovery

- A homenet device sends discovery messages on all links
  - If it has a domain cert: Send this
  - If it doesn't, send a device ID



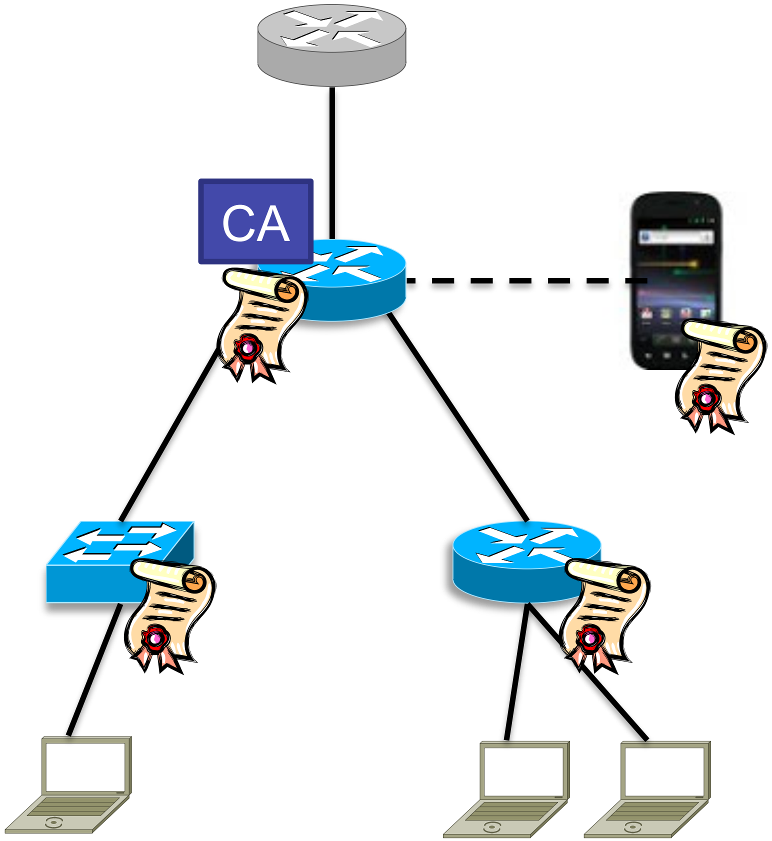
Approach:
3) Domain Join

- Device with domain cert invites device without domain cert
- Can validate on smart phone (optional)
- If new device accepted, it can enrol for a domain cert
- Result: All homenet devices have a domain cert



Result

- **Boundary detection:**
  - Peer doesn't respond to my messages, or
  - Peer is in a different domain
- **Trust for self-configuration:**
  - Routing
  - Addressing
  - …



More Thoughts…

- Default operation (without smart phone):
  - Homenet device (without domain cert) looks whether it can join an existing domain
  - If no response, auto-select to become trust anchor
  - Now, if new devices connect, they join that trust anchor
  - Allows only very simple policies
  - No security