Zero Touch Provisioning for NETCONF/RESTCONF Call Home

draft-ietf-netconf-zerotouch-04

NETCONF WG
IETF 94 Yokohama
Updates Since IETF 93

- Major update to draft
- Addresses privacy issue discussed at IETF 93
- Now compatible with ANIMA draft

Very positive responses so far!
Guiding Principles

• Trust anchors

• Conveying trust
  – Ownership voucher
  – Transport-level security
  New!

• Ownership
  – Signed data (insecure transport okay)
  – API contract (secure transport required)
  New!
Information Types

• Bootstrap-information
  – Same as before
    • Boot image
    • Initial configuration

• Redirect-information
  – List of 2-tuples:
    • The target bootstrap server’s address
    • The target bootstrap server’s trust anchor certificate

Either type may be provided via API or signed data.
Sources for Bootstrapping Data

• Removable storage
  – Data MUST be signed!

• DHCP server
  – Data MUST be signed!

• Internet service
  – Data MAY be unsigned
    • assuming secure connection to trusted server

• Etc.
Owner Stages the Network for Bootstrap

1. Device modeled

2. Stage bootstrap information

3. (Optional) Configure redirect server

4. (Optional) Configure DHCP server

5. (Optional) Store bootstrapping artifacts on media
Device Powers On

1. if not factory default, then exit.

2. check
   # if signed redirect information found
   # either NMS-initiated connection
   # or device-initiated connection
   # else if signed bootstrap information found (call home)

3. check
   # (do something similar to above)

4. check
   # (do something similar to above)

5. loop or wait for manual provisioning.
Loose Ends

• Signature algorithm needs to be defined

• Signed data format needs to be confirmed

• Redirect-information should be a list of tuples
Final Stretch

• Update draft to address loose ends

• Request Last Call (~ IETF 95)

Comments / Questions?