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) New!
  - API contract (secure transport required)

Information Types

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

- Redirect-information   New!
    - 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 <u>secure</u> connection to <u>trusted</u> server

- ## Etc.

Owner Stages the Network for Bootstrap

```
                             +----------+   +------------+
                             |Deployment|   |Manufacturer|
                             | Specific |   |   Hosted   |    +------+
                 +---+       |Bootstrap |   |  Redirect  |    | Local|    +---------+
                 |NMS|       | Server   |   |   Server   |    | DHCP |    |Removable|
                 +---+       +----------+   +------------+    |Server|    | Storage |
                   |              |               |           +------+    +---------+
                   |              |               |              |            |
        activate   |              |               |              |            |
        modeled    |              |               |              |            |
    1.  device     |              |               |              |            |
    ---------->|              |               |              |            |
                   |              |               |              |            |
                   | 2. stage bootstrap           |              |            |
                   |    information               |              |            |
                   |---------->|               |              |            |
                   |              |               |              |            |
                   | 3. (optional) configure      |              |            |
                   |    redirect server           |              |            |
                   |------------------------->|              |            |
                   |              |               |              |            |
                   |              |               |              |            |
                   | 4. (optional) configure DHCP server         |            |
                   |------------------------------------------>|            |
                   |              |               |              |            |
                   |              |               |              |            |
                   | 5. (optional) store bootstrapping artifacts on media |
                   |-------------------------------------------------------->|
                   |              |               |              |            |
                   |              |               |              |            |
```
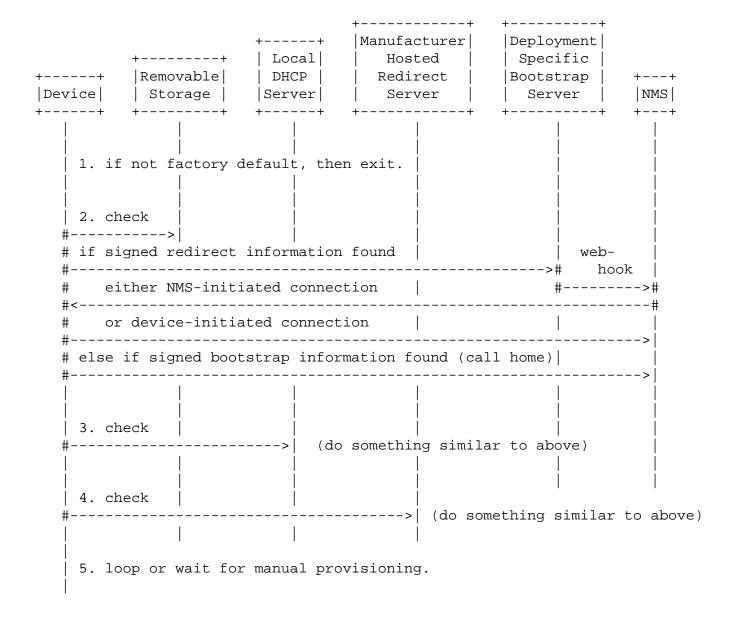
Device Powers On

```
                                    +------------+  +----------+
                          +------+   |Manufacturer|  |Deployment|
               +---------+| Local|   |  Hosted    |  | Specific |
   +------+    |Removable|| DHCP |   |  Redirect  |  |Bootstrap |   +---+
   |Device|    | Storage || Server|  |   Server   |  |  Server  |   |NMS|
   +------+    +---------++------+   +------------+  +----------+   +---+
      |             |          |           |              |          |
      |             |          |           |              |          |
      | 1. if not factory default, then exit.|            |          |
      |             |          |           |              |          |
      |             |          |           |              |          |
      | 2. check    |          |           |              |          |
      #------------>|          |           |              |          |
      # if signed redirect information found |         web- |          |
      #----------------------------------------------------->#   hook |
      #    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 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?