#### draft-ietf-netconf-zerotouch-00

Zero Touch Provisioning for NETCONF Call Home

## Introduction

Zero Touch is a technique for establishing a secure NETCONF connection between a newly deployed IP-based device, configured with just its factory default settings, and the new owner's Network Management System (NMS).

# **Updates since IETF 89**

#### From I-D to -00

- Major structural update; the essence is the same, but most every section was rewritten to some degree.
- Added a Use Cases section clearly articulating the local vs 3rd-party network cases
- Added diagrams for "Actors and Roles" and "NMS Precondition" sections, and greatly improved the "Device Boot Sequence" diagram
- Removed support for physical presence or any ability for Configlets to not be signed.
- Now Configlet is a header (target-requirements) + body (anyxml)
- Defined the ZeroTouch Information DHCP option
- Added an ability for devices to also download images from Configuration Servers
- Added an ability for Configlets to be encrypted
- Now Configuration Servers can only support HTTP/S no other schemes possible
- Device now MUST access URL via UID, before trying raw URL
- Now uses IEEE 802.1AR-2009 IDevID (Initial Device Identifier)

### **Use Cases**

- Connecting to a remotely administered network
  - DHCP server administered by 3<sup>rd</sup>-party
  - Device may not be able to receive site-specific information
  - Device must reach out to network for initial configuration

- Connecting to a locally administered network
  - DHCP server can be customized
  - Device may receive some site-specific information
  - Device falls back to network if no local information received

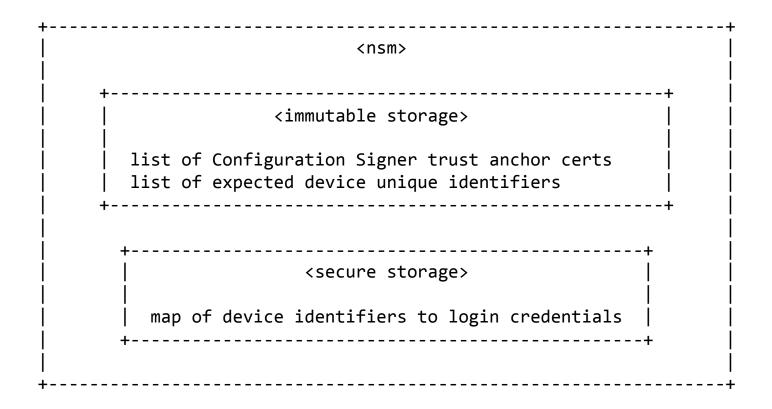
## **Actors and Roles**

```
+----+ fetches Configlet
-----| Device |-----+
call home
                          Config
                           Server | <---+
         produces
    +----- delegates trust
      Vendor |----+
                         | Config |
          imports
                          Signer
         trust
          anchor
    +----+ requests signing |
               places signed Configlet onto
```

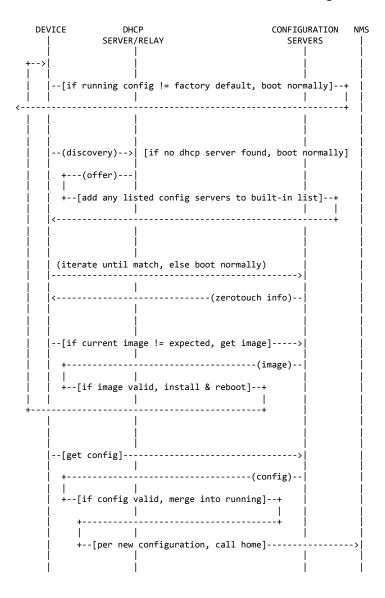
# Device's Factory Default State

```
<device>
                <immutable storage>
 list of Configlet Signer trust anchor certificates
 list of Configuration Server trust anchor certs
                  <other storage>
two sets of Configuration Server URIs
IDevID entity & associated intermediate certificate(s)
                  <secure storage>
                 IDevID private key
```

## NMS's Precondition



## **Device Boot Sequence**



# Device Boot Sequence (1/2)

```
DEVICE
                DHCP
                                            CONFIGURATION
                                                           NMS
            SERVER/RELAY
                                              SERVERS
  |--[if running config != factory default, boot normally]--+
  |--(discovery)-->| [if no dhcp server found, boot normally]
    +--[add any listed config servers to built-in list]--+
    (iterate until match, else boot normally)
         -----(zerotouch info)--
```

# Device Boot Sequence (2/2)

#### [Continuation from previous slide]

```
|--[if current image != expected, get image]---->
 +--[if image valid, install & reboot]--+
--[get config]----->
             -----(config)--
 +--[if config valid, merge into running]--+
    +--[per new configuration, call home]----->
```

## Configlet Data Model

### **IANA** Considerations

- "ZeroTouch Information" DHCP Option
  - Returns a list of Configuration Server URIs

- Media Types for Images and Configurations
  - application/zerotouch-configlet
  - application/zerotouch-bootimage

[This is why only HTTP/S is supported now]

# Open Issues

No known issues at this time

Questions / Concerns ?