Auto-Onboarding a Network Device in NMS

Manufacturer Playing an Active Role in Zero Touch Deployment

Table of Contents

List of Figures

References

Zero Touch IETF Draft

Executive Summary

A typical telecom customer procures network devices from manufacturers and then has the network management system (NMS) manage them. A customer would like to have the devices onboarded to NMS seamlessly when they are powered on. This white paper provides a proposal where one or more devices can be onboarded to the NMS without any intervention from the customer.

Introduction

The solution presented in this document is an extension to the solution presented in the *Zero Touch IETF Draft*. This solution covers the scenario where a device connects to a manufacturer-hosted bootstrap server returning "redirect information," and the manufacturer-hosted redirect server securely connects to the deployment-specific NMS to provide just-in-time device registration. In comparison, the *Zero Touch IETF Draft* leaves open how the NMS is configured, assuming that the customer might do it after having received device shipping information from the manufacturer.

This solution automates the registration of a device to an NMS, so the NMS knows that it should expect the device and can establish a secure connection to the device. This solution automates the device registration into NMS without any involvement from the customer. The customer is notified by NMS at completion of device registration. However, this solution does not cover NMS. Once the connection is established, NMS can complete the operational configuration of the device—part of the bootstrapping process.

The entities that participate in this solution are described in the following table:

Entity	Description
Customer/device owner	Procures telecom equipment and uses NMS to manage them.
Manufacturer	A manufacturing telecom equipment reseller or partner.
NMS	A management system that manages the telecom equipment. This can be an NMS hosted by an owner/manufacturer/third-party.

Use Cases

A customer/device owner procures a network device from a manufacturer. (This can apply to one or more devices from one or more manufacturers.) The customer identifies the NMS that will be used to manage the device. The customer then registers the manufacturer with the NMS. The NMS provides handshaking details to the customer for the manufacturer. The customer shares this information with the corresponding manufacturer. Once the customer installs the device and powers it on, the device connects to the manufacturer. The manufacturer then validates the device, informs NMS that a new device is going to connect to it, and informs the device how to connect to NMS. The device then connects to NMS, which onboards the device.

The following sections provide the workflow for this use case. The workflow covers the following basic steps (interactions):

1. Customer/device owner signs up.
2. Handshaking occurs between the manufacturer and NMS.
3. Device powers up.
4. Device onboarding occurs.
5. Customer/device owner notification occurs.

Solution Overview

Figure 1 gives an overall workflow of interactions between various entities involved in onboarding a device. The workflow is divided into logical steps, with each interaction or step explained in the subsequent sections.

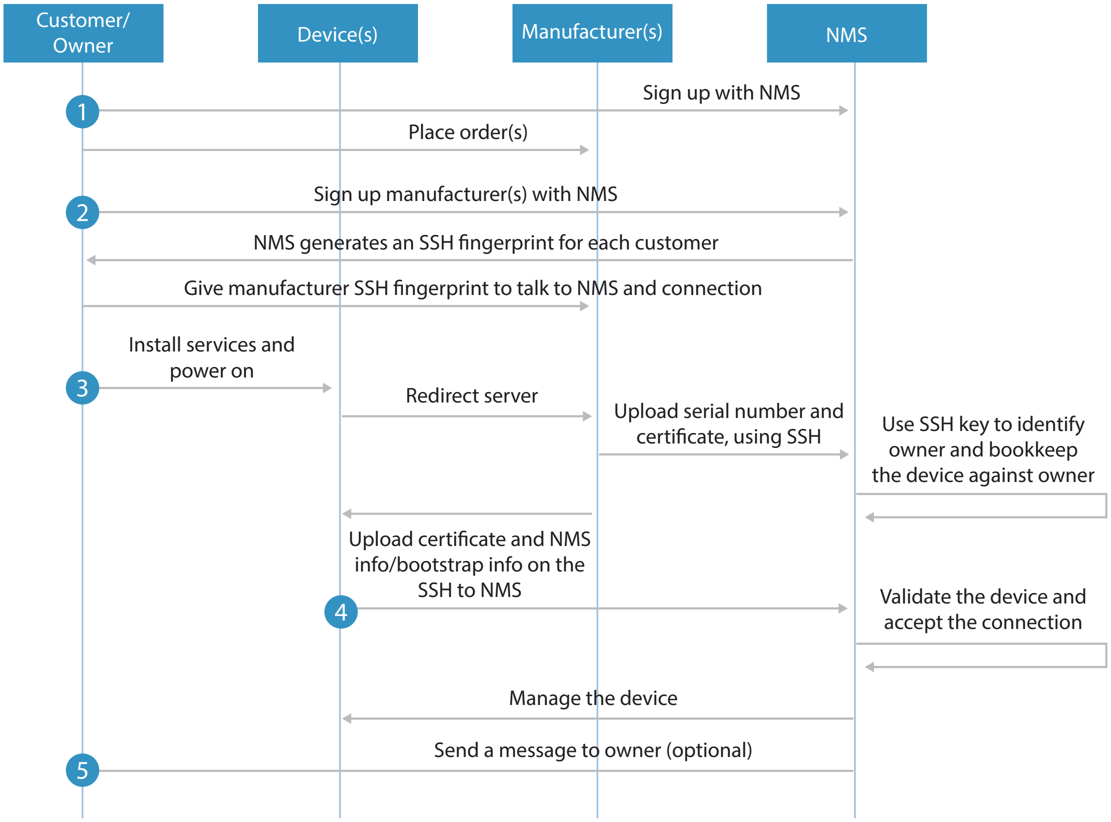
Customer/ Owner
Device(s)
Manufacturer(s)
NMS
1
Sign up with NMS
Place order(s)
2
Sign up manufacturer(s) with NMS
NMS generates an SSH fingerprint for each customer
Give manufacturer SSH fingerprint to talk to NMS and connection
3
Install services and power on
Redirect server
Upload serial number and certificate, using SSH
Use SSH key to identify owner and bookkeep the device against owner
Upload certificate and NMS info/bootstrap info on the SSH to NMS
4
Validate the device and accept the connection
Manage the device
Send a message to owner (optional)
5

Figure 1: Solution Overview

Step One – Signing Up

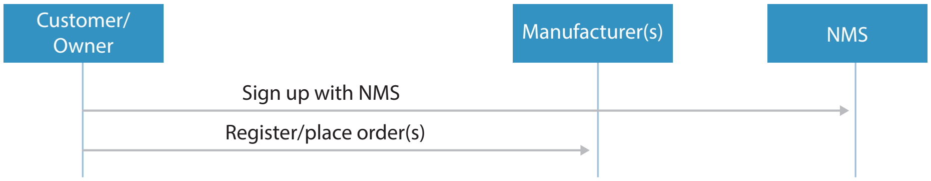

Figure 2: Step One - Signing Up

The first step is the customer/device owner registering with NMS and the manufacturer.

The order should not matter. However, here we have kept the manufacturer later as it is possible that a customer might work with multiple manufacturers and expect a single NMS to manage multivendor devices.

Step Two - Handshake Between Manufacturer and NMS

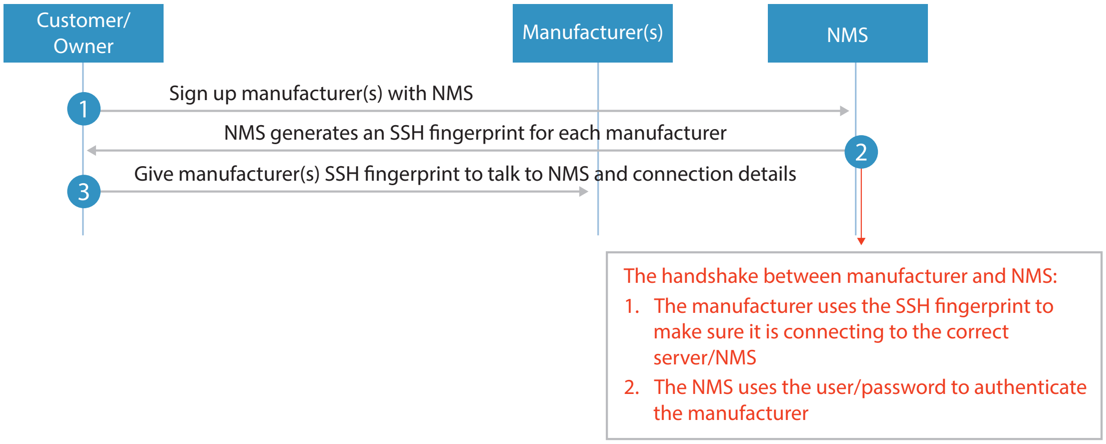
Customer/ Owner
Manufacturer(s)
NMS
1
Sign up manufacturer(s) with NMS
NMS generates an SSH fingerprint for each manufacturer
2
3
Give manufacturer(s) SSH fingerprint to talk to NMS and connection details
The handshake between manufacturer and NMS:
1. The manufacturer uses the SSH fingerprint to make sure it is connecting to the correct server/NMS
2. The NMS uses the user/password to authenticate the manufacturer

Figure 3: Step Two - Handshake Between Manufacturer and NMS

This interaction looks into the mechanism for a secure handshake between the manufacturer and NMS. Following are the details:

1. The customer/device owner registers the manufacturer. The NMS collects the following information:
   - Manufacturer name
   - Manufacturer server/DNS name
2. NMS creates a user account, generates a passphrase for the manufacturer, and provides the following information:
   - Generates an SSH key for the user.
   - Shares the SSH fingerprint for the user.
   - Shares the username and password.
   - Provides activation server details/deployment-specific bootstrap server. Both of these entities can be the NMS itself.
   - Provides outbound SSH connection details.

     This can also be done during manufacturer and NMS handshake at device power-on.
3. The customer/device owner shares this information with the manufacturer.

Step Three - On Device Power-Up

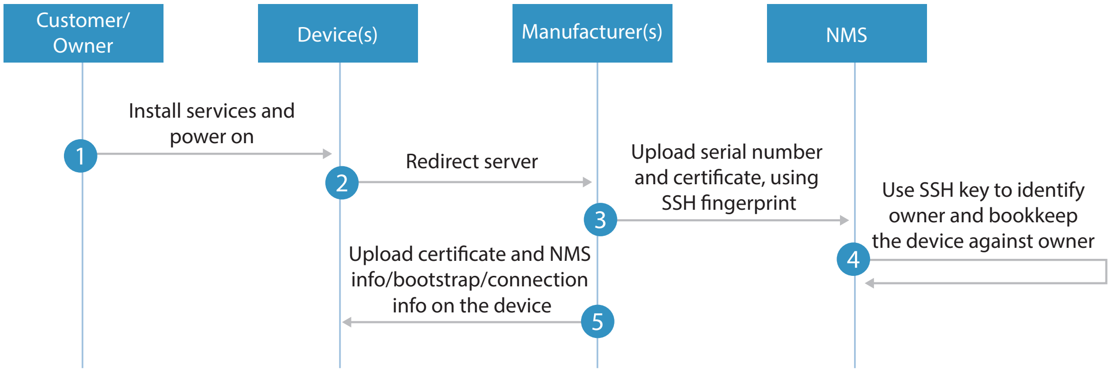
Customer/ Owner
Device(s)
Manufacturer(s)
NMS
Install services and power on
1
Redirect server
2
Upload serial number and certificate, using SSH fingerprint
3
Use SSH key to identify owner and bookkeep the device against owner
4
Upload certificate and NMS info/bootstrap/connection info on the device
5

Figure 4: Step Three - On Device Power-Up

This interaction handles handshaking between the manufacturer and NMS:

1. Customer/device owner installs the device and powers it on.
2. Device connects to the redirect server. The redirect server uses the serial number of the device and determines what has to be done.

a. On device power-up, it looks for redirect information. This can be available from:

- Default factory settings
- Using a USB flash drive connected to it.
- Connecting to a DHCP server, which provides redirect information.

b. A redirect server can/will behave as a redirect or bootstrap server.

c. The redirect server will first authenticate the device to make sure it is genuine; this can be done by:

- Validating a preinstalled/factory default certificate
- Using a secure key

d. The server will also do the job of handshaking with the NMS (activation server/deployment specific bootstrap/ NMS itself) and the device.

3. Manufacturer connects (via SFTP) to NMS:

a. Uses the NMS information associated with the customer/device owner.

b. Connects to the NMS using SSH username/passphrase. Only SFTP needs to be allowed, as the primary purpose of this handshake is bookkeeping for NMS.

c. Uses SSH fingerprint to authenticate the server (NMS).

d. Shares device information as an XML file (Yang-based):

- Serial number, customer/device owner name
- Uploads the certificate

4. This step can happen parallel with step 5. If this needs to be done in steps, NMS should happen first, followed by the device.
The NMS takes the following action when the manufacturer connects to it:

a. Authenticate the user/manufacturer.

Uses the customer information to determine if the manufacturer is authorized by the customer.

b. Bookkeep the device serial number and certificate.

5. The manufacturer pushes the bootstrap server details/activation server details/connection details on to the device.

Step Four - Device Onboarding

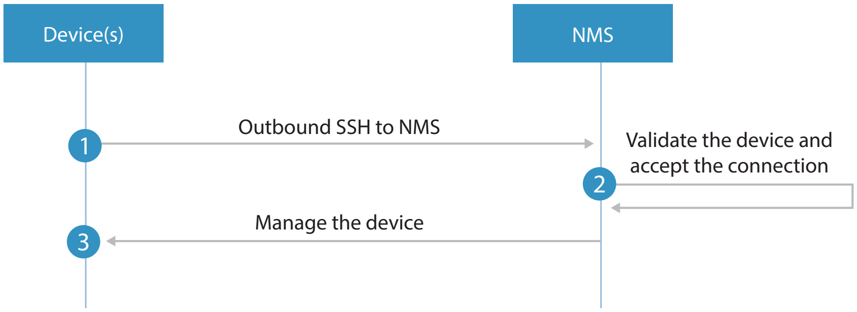

Figure 5: Step Four - Device Onboarding

This step handles the handshake/connection between the device and the NMS:

1. The device uses outbound SSH to connect to NMS.
2. NMS authenticates the device and accepts the connection.

   The certificate and serial number are used to authenticate the device.

3. NMS is now ready to manage the device, and can also perform any preconfiguration on the device.

Step Five - Owner Notification

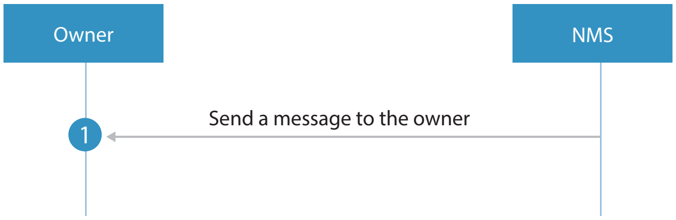

Figure 6: Step Five - Customer/Device Owner Notification

This interaction handles the notification of device onboarding to the customer/device owner:

1. NMS sends a notification to the customer/device owner about the device being onboarded.
2. The customer can now use the device for operations.

Once all the devices from a manufacturer are onboarded, the customer can disable manufacturer access to the NMS.

Conclusion

Any network device owner expects that as soon as a device is installed, it should be onboarded as soon as possible and start performing its intended function. However, in reality there are a lot of thresholds and bottlenecks. Any steps to reduce these bottlenecks will be highly commended by the customer/device owner. By making the manufacturer an integral part of the device onboarding process, we can automate many of the steps that the customer otherwise has to do manually.

In addition, involving the manufacturer as an integral part of the solution has advantages for both the manufacturer and customer:

- Reduces the customer involvement in onboarding.
- Reduces customer worry about the authenticity of the device.
- Helps the manufacturer tab spoofed devices.
- Helps the manufacturer know how the inventory is being used by the customer.

In turn, NMS gives flexibility to the customer on how devices can be onboarded.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701