Cyber Security - IT Security Meets OT Security

Paul Didier
Manufacturing Solution Architect
Cisco Systems

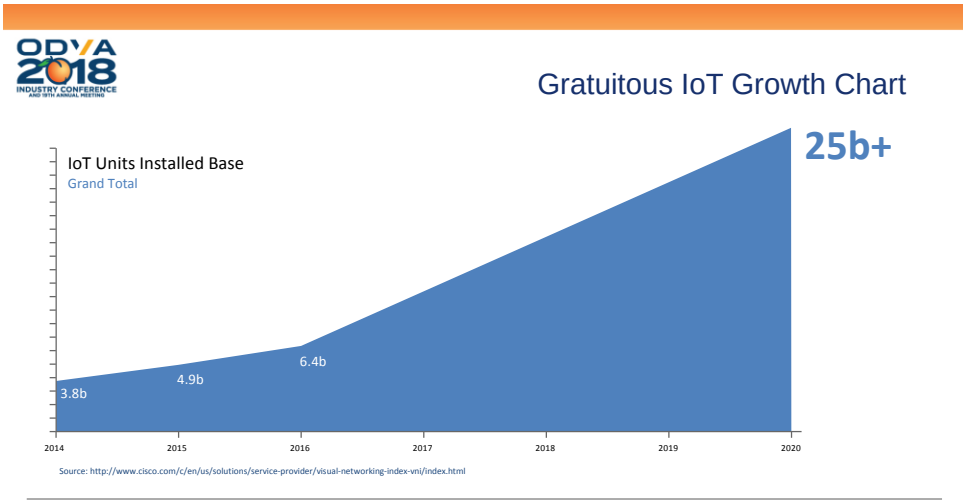
Presented at the ODVA
2018 Industry Conference & 18th Annual Meeting
October 10, 2018
Stone Mountain, Georgia, USA

Abstract

This paper will look at how CIP Security can be used in-conjunction with current and in-development IT Security tools and technologies to significantly improve plant floor security and protection. We will discuss how to apply network access control and Plant and Cell-Area zone segmentation policies in a structured, scaleable manner. As well, we will review the value of monitoring network and security health through the use of traffic flow monitoring (NetFlow/IPFIX, IETF RFC 7011-7015) features and security monitoring applications. Lastly, we will look at some advanced, under-development standards to automatically apply trust and policy based on IETF standards such as Bootstrapping Remote Secure Key Infrastructure (BRSKI) and Manufacturer Usage Description (MUD) specifications

Introduction: Why are we talking about this

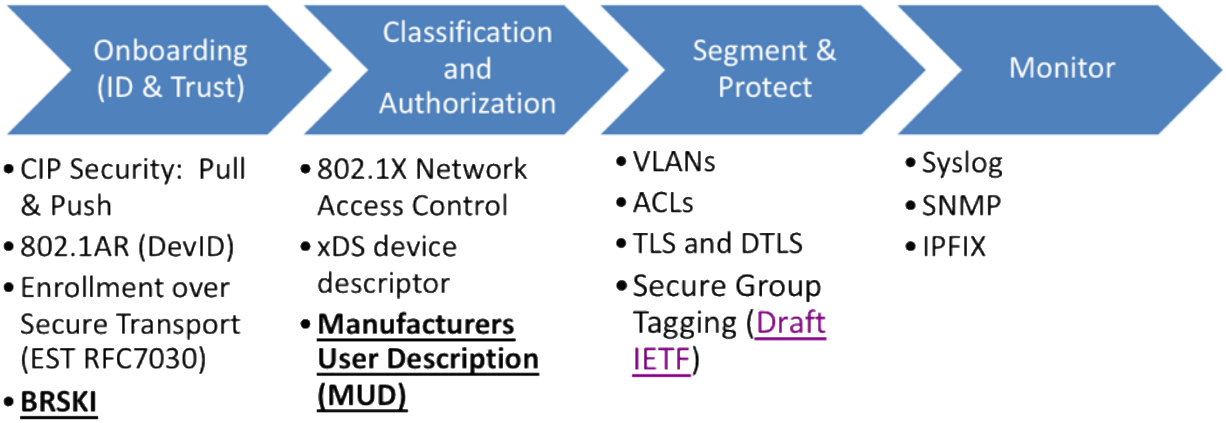
The IoT is expected to grow rapidly over the upcoming years. Below is a chart of estimated IoT units/things that are expected to be connected. That large growth of things poses challenges in ecosystems that are expected to manage closely the devices that are connected, such as Manufacturing.



This rapid growth will be a significant problem for administrators of the networks that are the focus of this growth, such as production facilities, factories and plants found in Manufacturing. A key consideration will be how to automate the on-boarding and policy deployment for new things on the network. To that point, some "IT" new standards are being developed to help solve those challenges. But those can only be effectively deployed with the cooperation of the thing makers – of which the ODVA is a good ecosystem of device vendors.

Security Standards – A thing's view

This paper will introduce 2 developing IT-based, IETF standards that should help automate the security processes for Industrial Automation and Control devices as they become operational in machine builder, customer or system integrator's processes. They help automation the onboarding by automatically deploying secure credential to devices (BRSKI) and help Manufacturers express key characteristics about how the device should be classified and authorized – key steps to eventually segment and protect the devices and the Industrial Automation and Control System where they operate. The table below depicts some of the key standards in that process of securing devices.



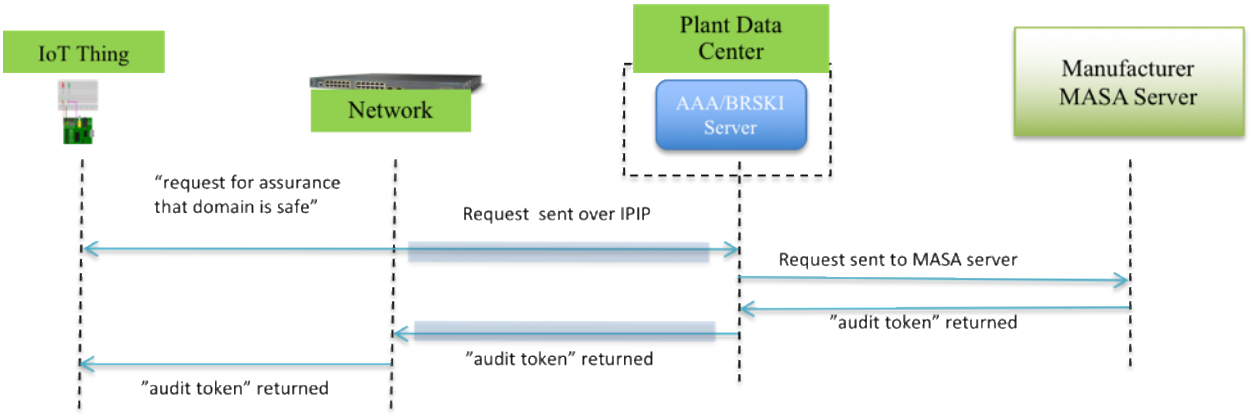
BRSKI – An overview of Bootstrapping Remote Secure Key Infrastructure

The ODVA has established standards for devices around Identification and Authorization in the CIP Security standards. Recently, a "pull-model" has been adopted as a mechanism to automate the delivery of secure credentials to a CIP device. In the IETF, the Autonomic Networking Integrated Model and Approach (ANIMA) Working Group is developing a standard (RFC) around Bootstrapping Remote Secure Key Infrastructure (BRSKI). The BRSKI standard outlines means to automatically deploy identity to devices so that they can be authorized on the network and establish secure communications. This enables Zero-touch provisioning of IACS devices that meets both the needs of OT for known devices to be on the network and IT to do that in automatic and secure mechanisms.

The necessary components for this process to occur include:

- The device is manufactured with an X.509 certificate and private key that conform to IEEE 802.1AR.
    - This is a standard definition of a “manufacturing certificate”
- The device & production network support a multi-vendor bootstrapping protocol (BRSKI)
    - draft-ietf-anima-bootstrapping-keyinfra-04
- The IoT device manufacturer supports a Manufacturer Authorized Signing Authority (MASA), which keeps a log of which devices have been installed in which IT or OT domains
- At the end of the BRSKI protocol, the device and production network have a mutual trust, and the IoT device can be admitted to the network.

Below is a depiction of the key components and the process outlined in BRSKI:

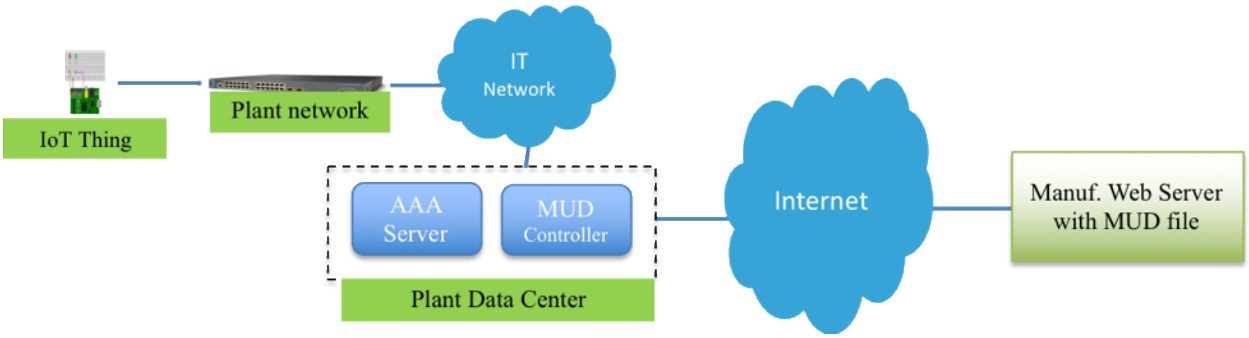


This model should be relevant for device vendors, machine builders, system integrators and customers as a key part of securing the chain of suppliers needed to build production systems.

MUD – An overview of Manufacturer’s User Descriptions

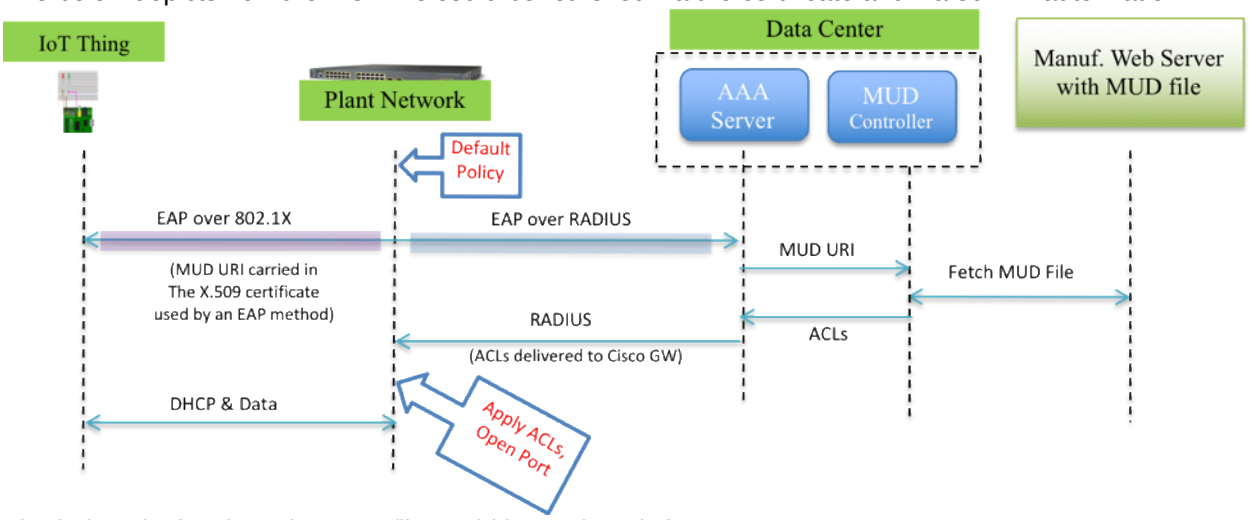
In the IETF’s Operations and Management Area Working Group (opsawg), they are working on the Manufacturer Usage Descriptor (MUD) specification. The MUD “file” would be a means for manufacturer’s to describe policy about devices that can help classify and authorize devices as they join production networks. This information can be used to help establish network policies around segmentation to protect IAC devices and systems. The same working group also established IP Flow Information and Export protocol (IPFIX) used to monitor communications in IP networks, such as a CIP EtherNet/IP network.

The depiction below describes how a device can express where to find the relevant MUD file and how IACS production network can retrieve, store and maintain those files. The device expresses this via a Universal Resource Locator (URL).

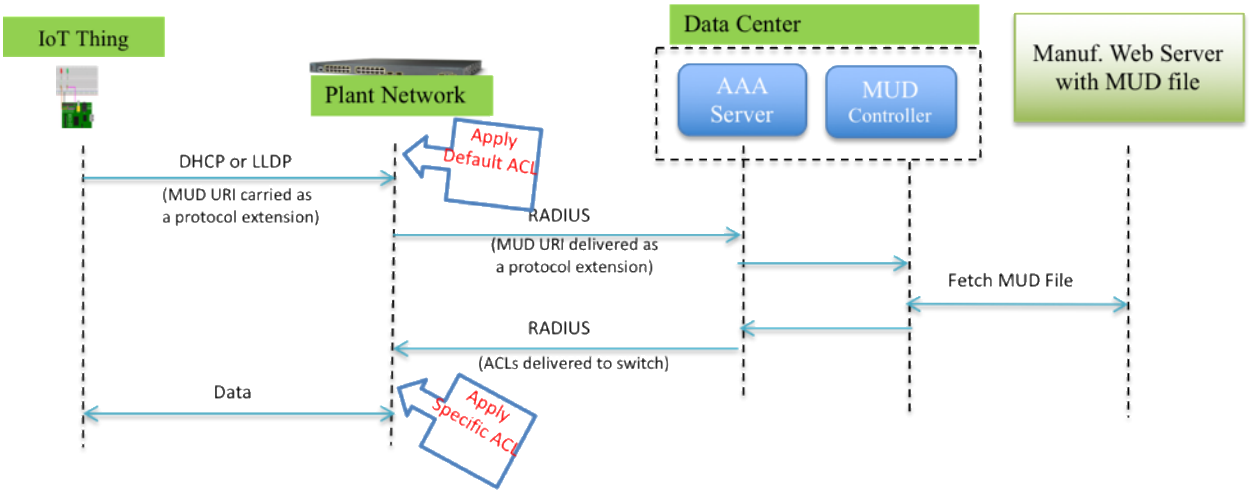


There are two basic means envisioned to support how a device can express where to find it's MUD URL. First the URL could be contained within a devices certificate, for example its CIP-Security certificate. Or it can be programmed to express the URL via common network discovery or addressing functions, such as LLDP or DHCP.

The below depicts how the MUD file could be retrieved via the certificate and via 802.1x autorization:



The below depicts how the MUF file could be retrieved via LLDP or DHCP



The end results of deploying MUD information is that the production system and network can establish segmentation. This still requires more input and process from both the IT and OT communities, but it's a key step in the process of automating these security procedures.

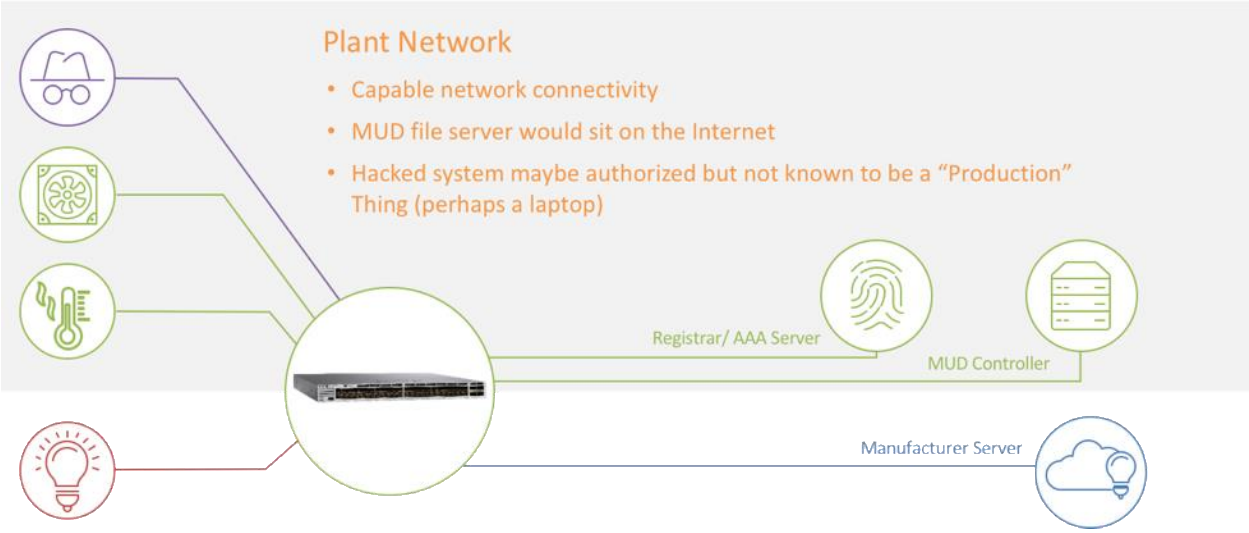
How it could Work – Simple

Together, BRSKI and MUD can be combined to automate much of the security deployment and implementation for IACS devices, such as CIP, in production networks.

In a simple example envisioned for brownfield deployments with largely SW-based enhancements to devices. Below is a depiction of the process:

1. Initial Configuration

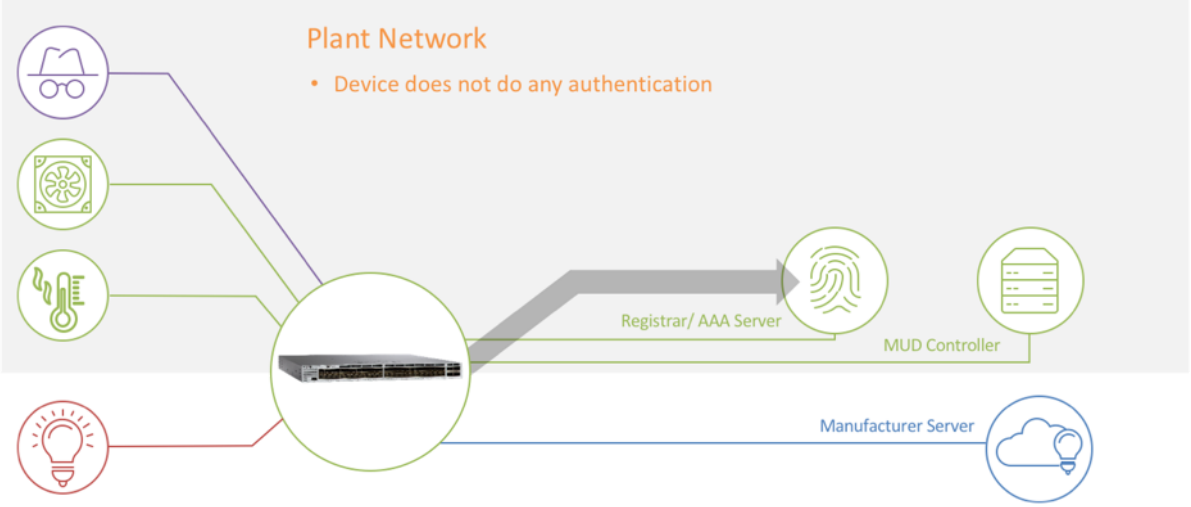
Initial Configuration (the same as before)



2. Onboarding process

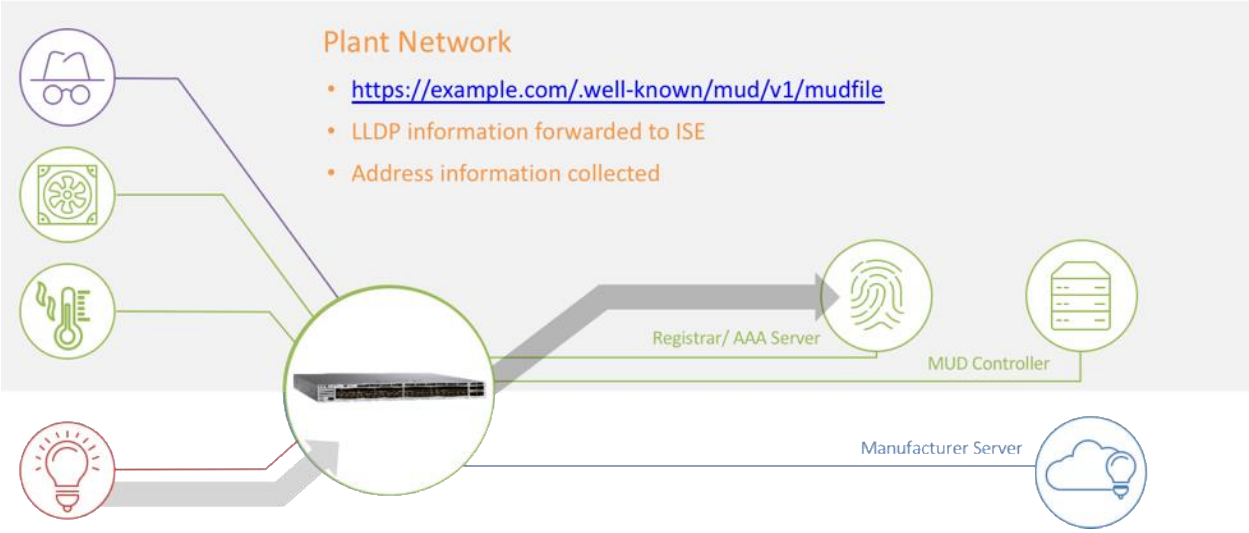
Onboarding Process

MAC authenticated Bypass (MAB)



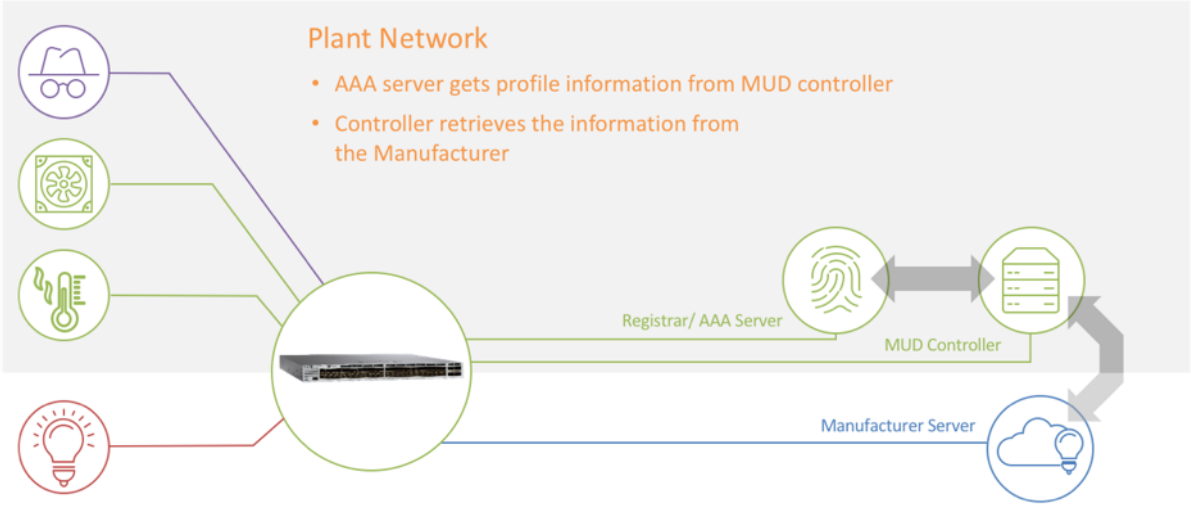
3. Device announces itself via LLDP or DHCP

Device States What It Is via LLDP MUD-URL



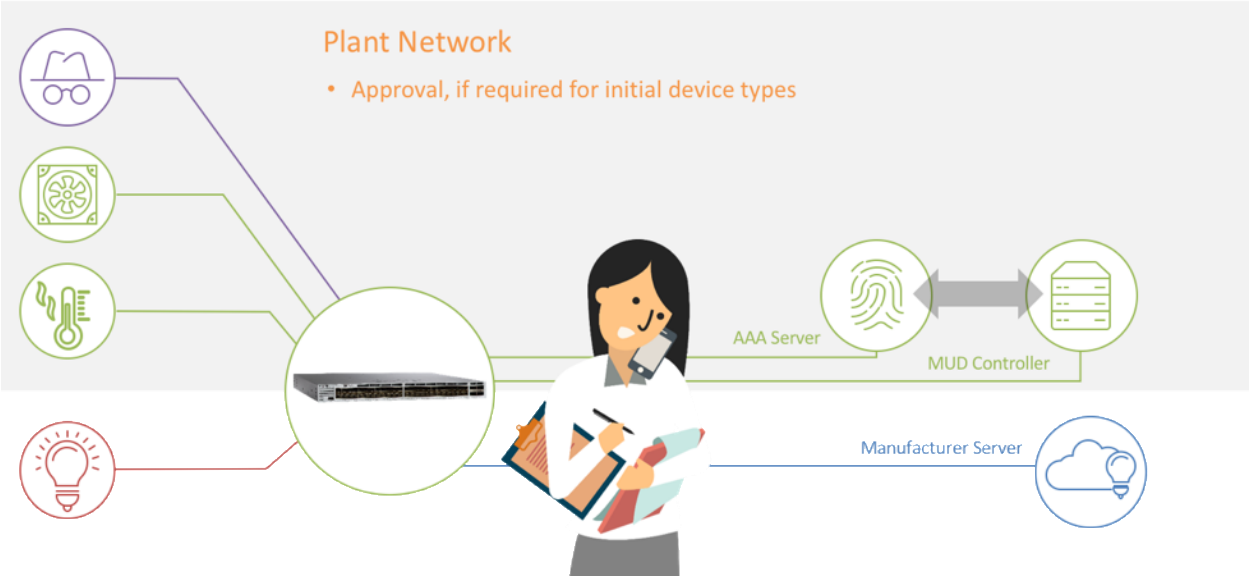
4. MUD File is retrieved

Retrieve Manufacturer Information



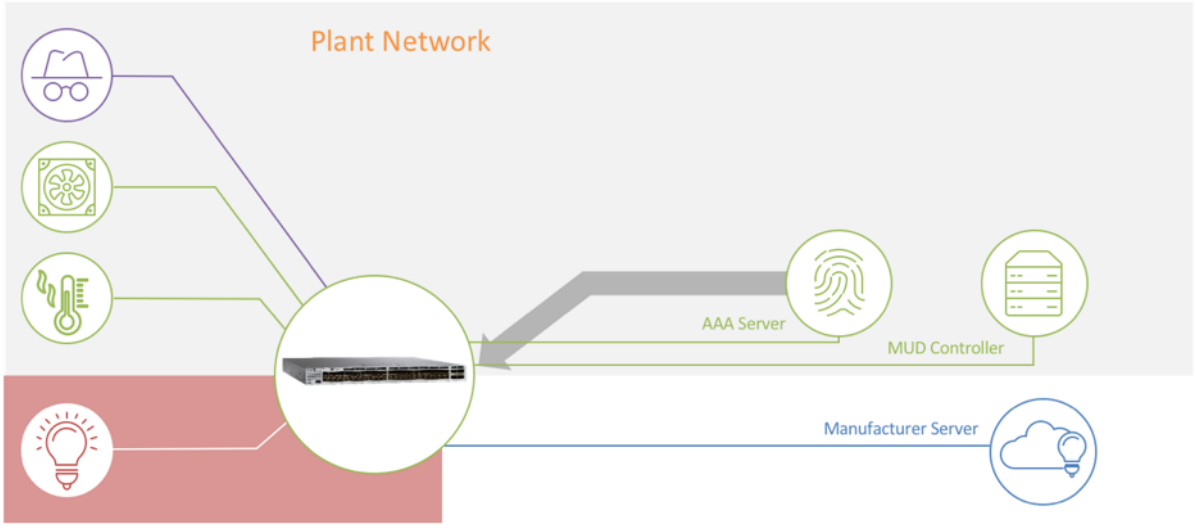
5. Approval given and Policy Assigned

Approval and Access List Generation



6. Network Access Control granted based on Policy

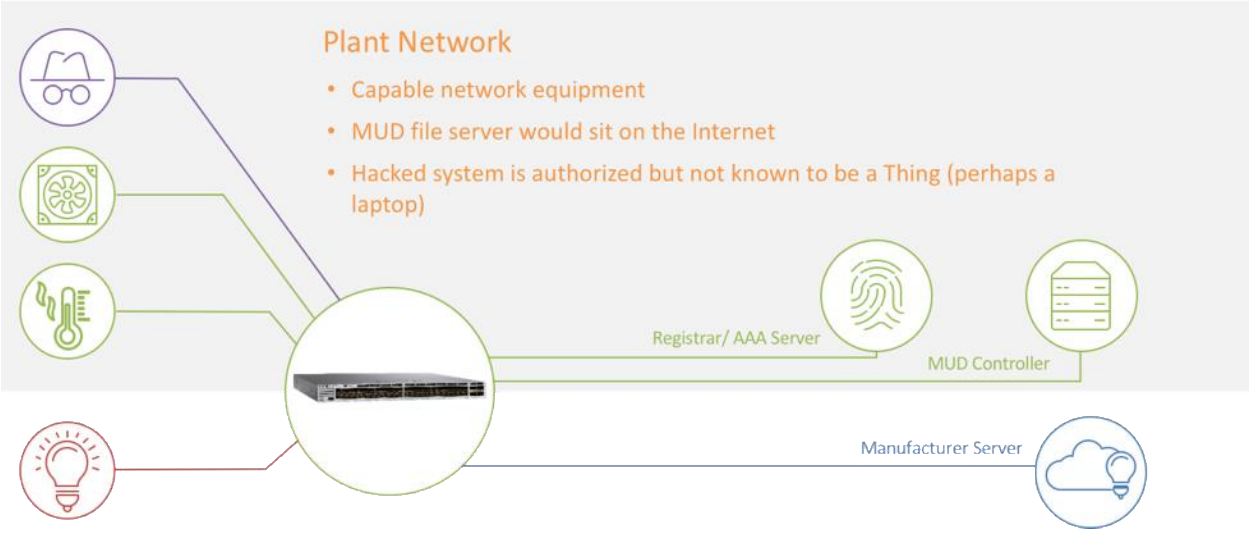
Issue Change of Authorization



How it could Work – Complex

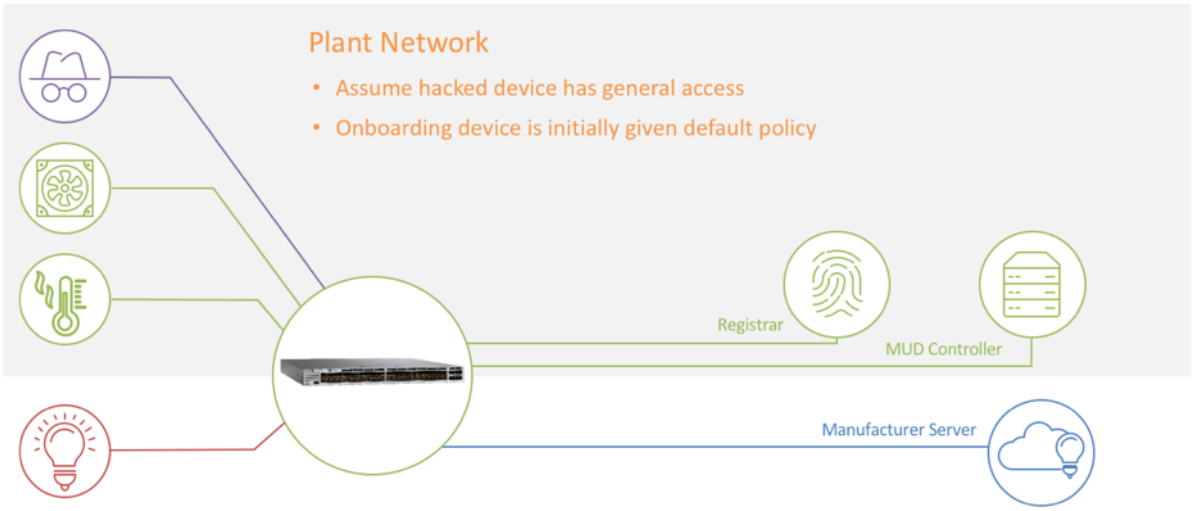
1. Initial Configuration

Initial Configuration

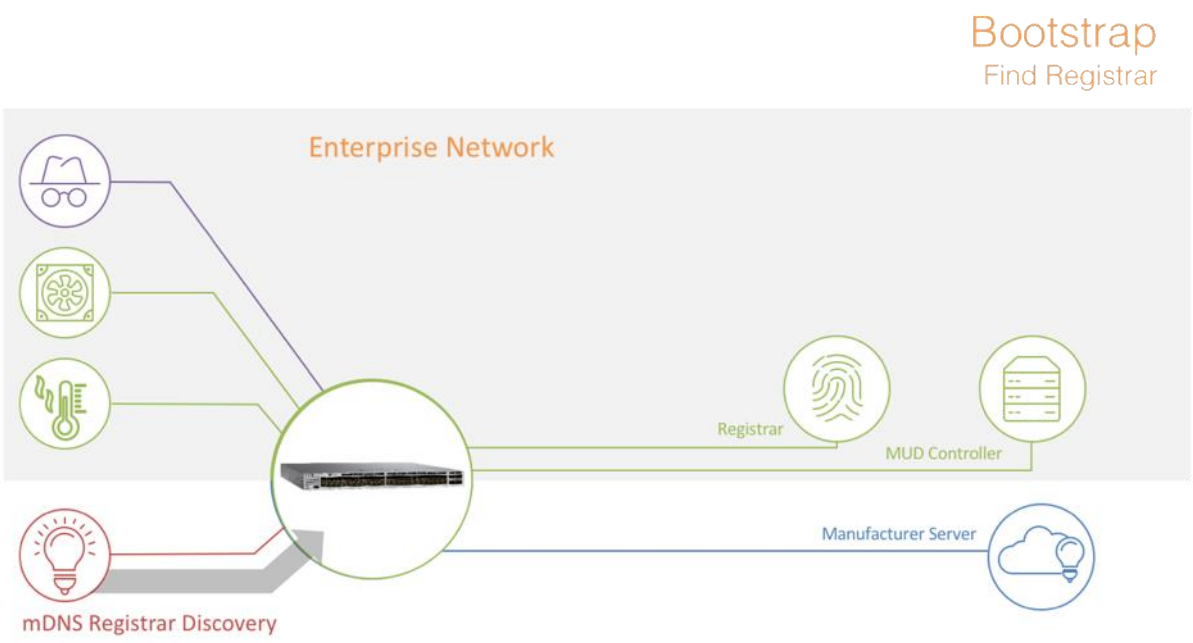


2. Onboarding Process
    a. Device Connects

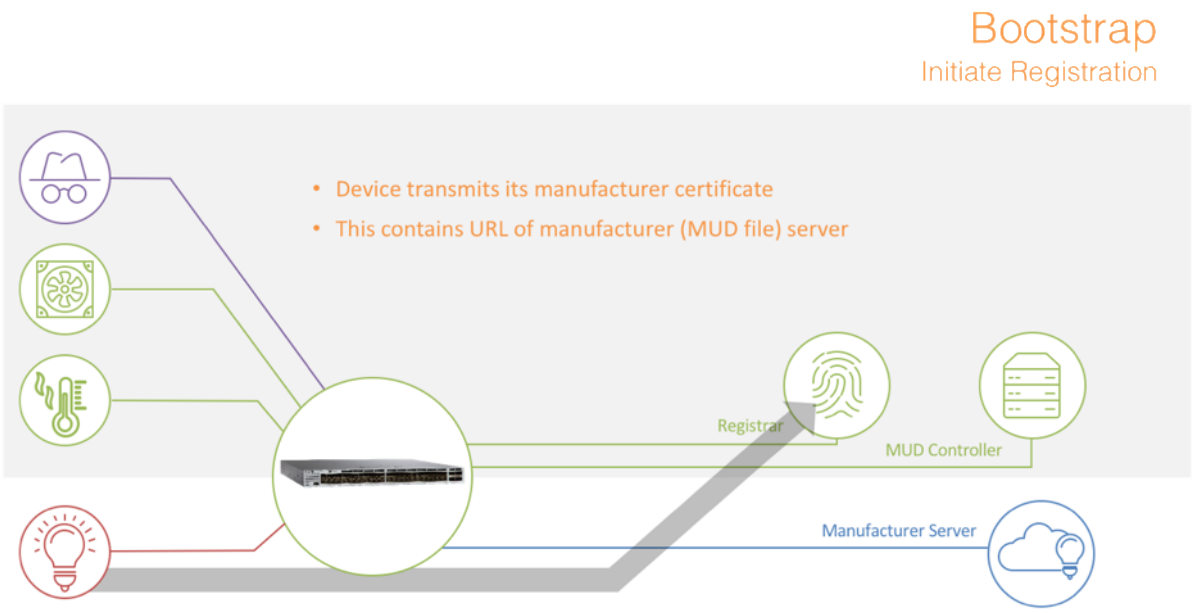
Onboarding Process
Device Connects



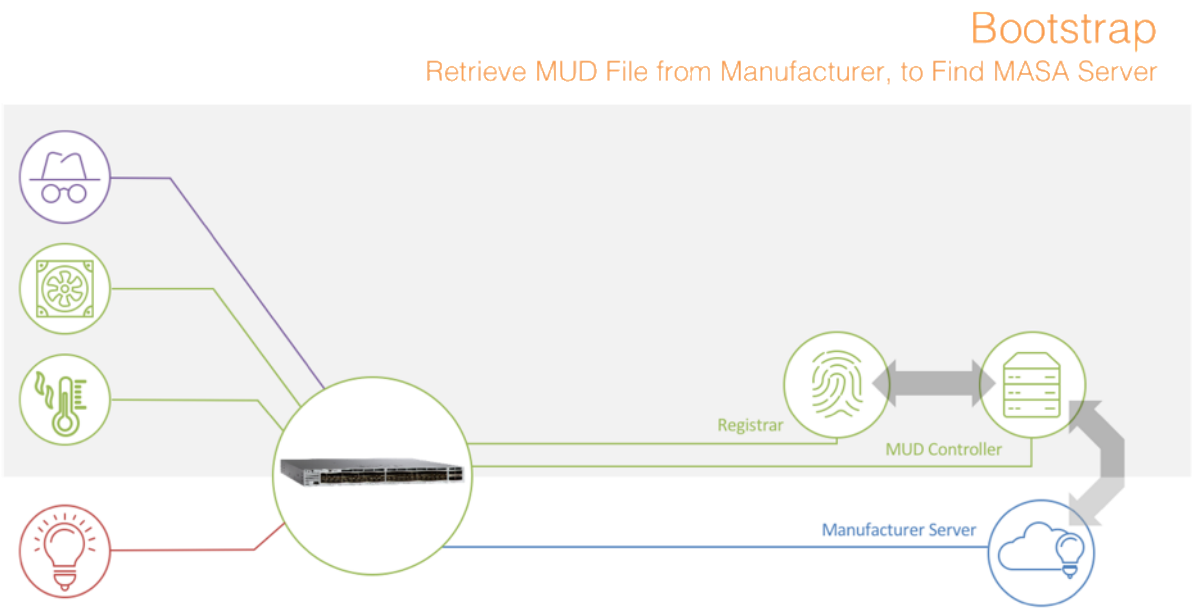
    b. Bootsrapping starts – find registrar



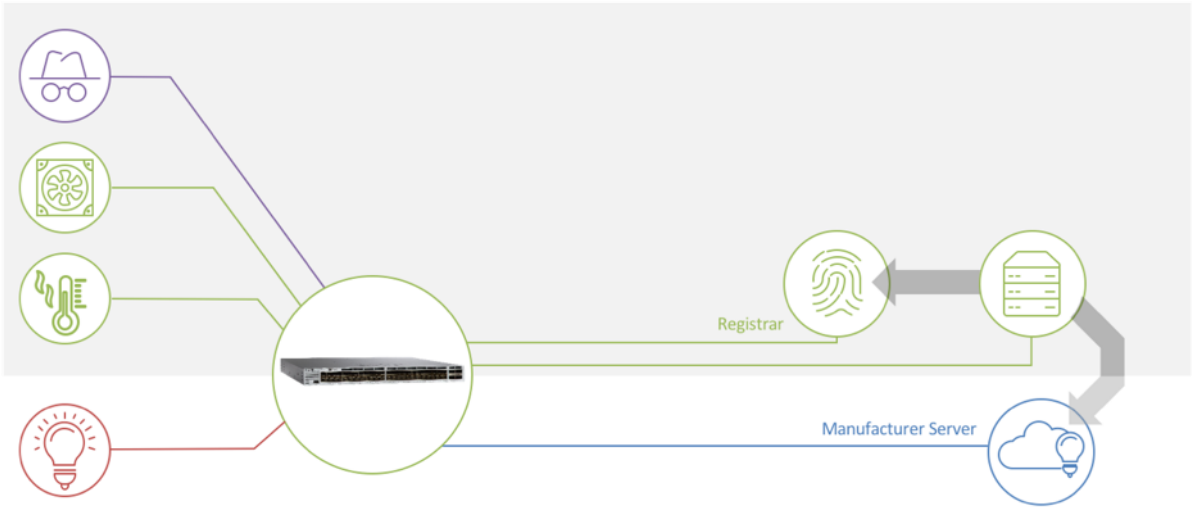
c. Initiate Registration – express MUD URL



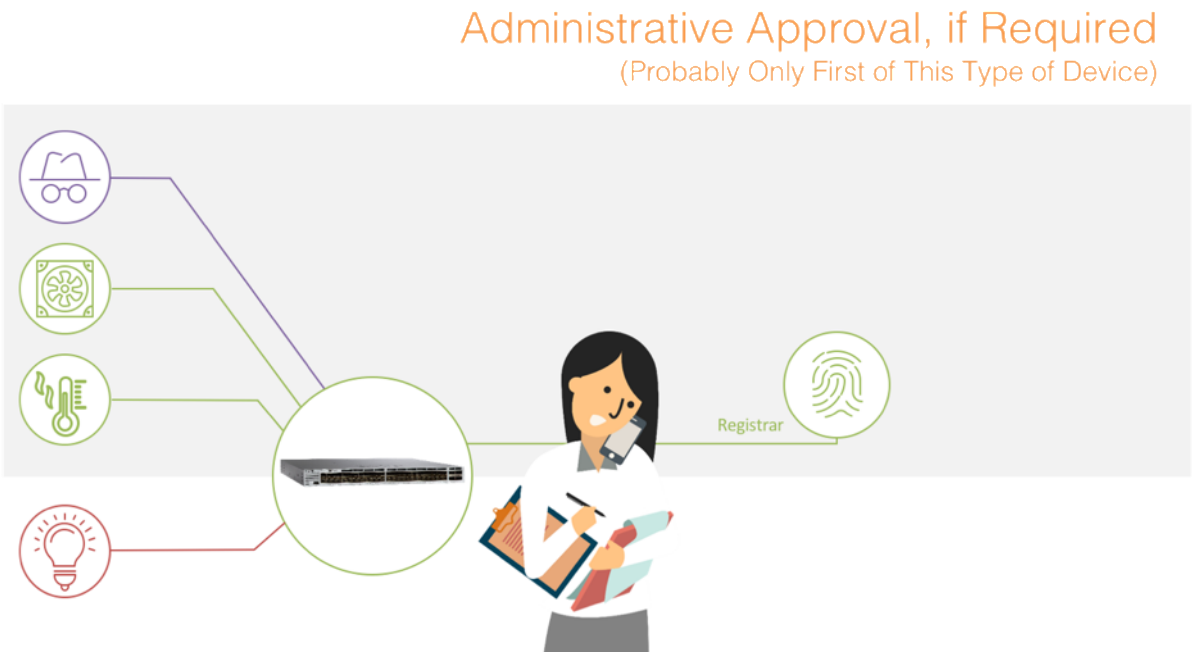
d. Retrieve MUD file



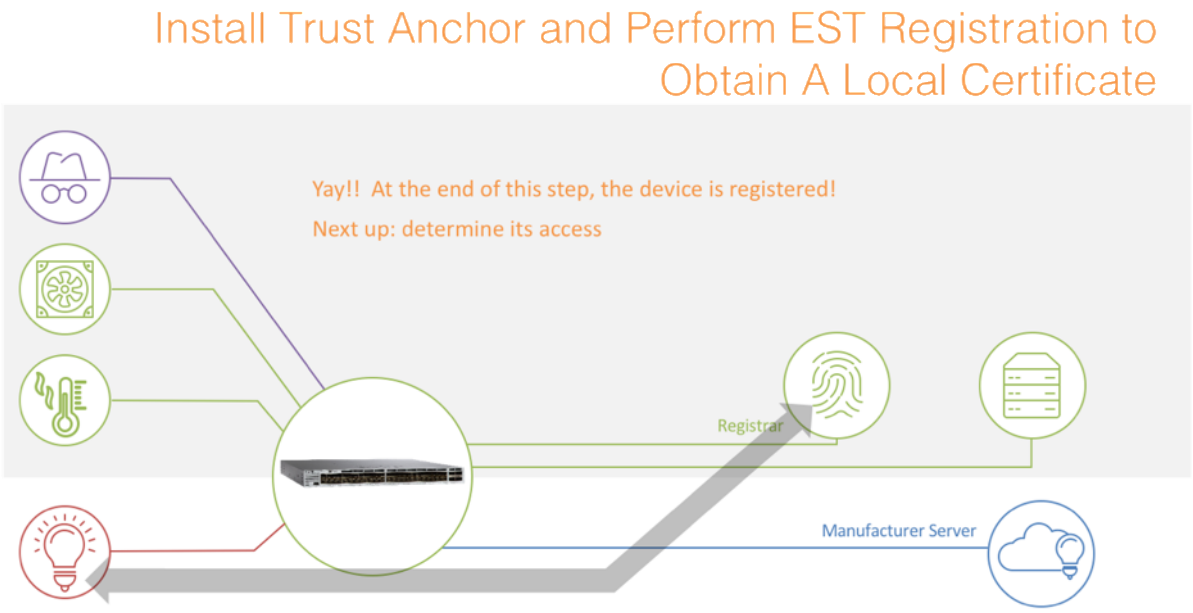
e. Request Voucher



f. Approval (for first time device types)

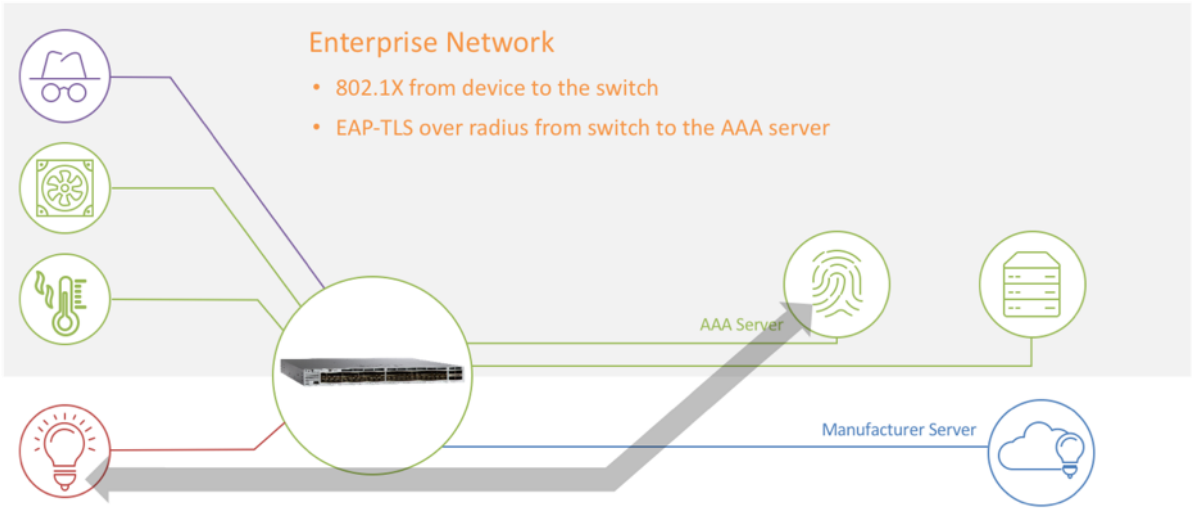


3. Install Trust Anchor



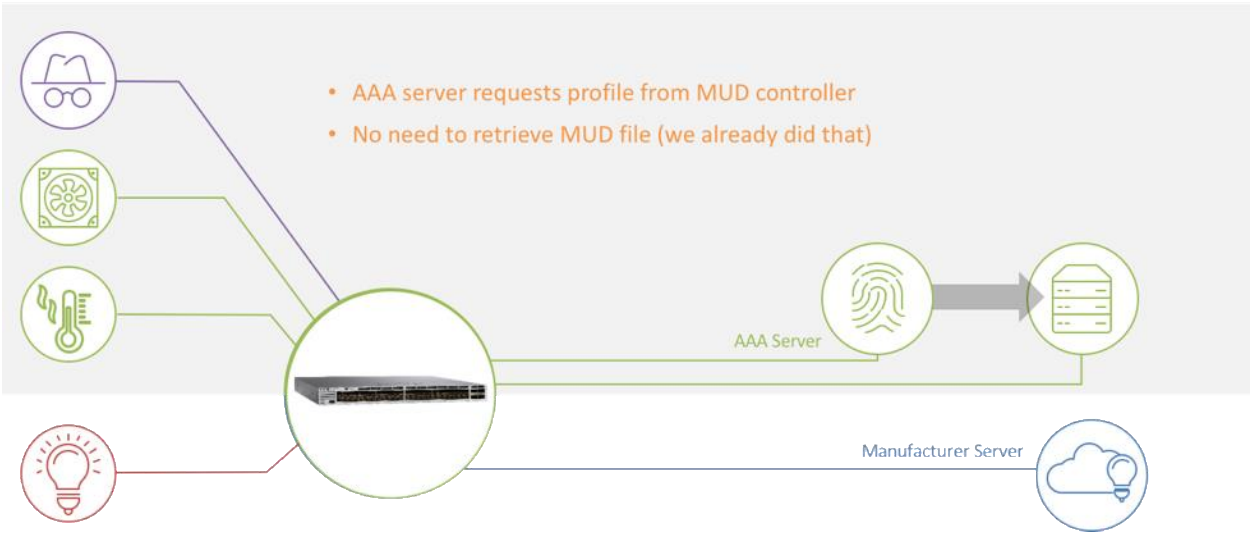
4. Authenticate via 802.1x

Now Device Authenticates Using 802.1X



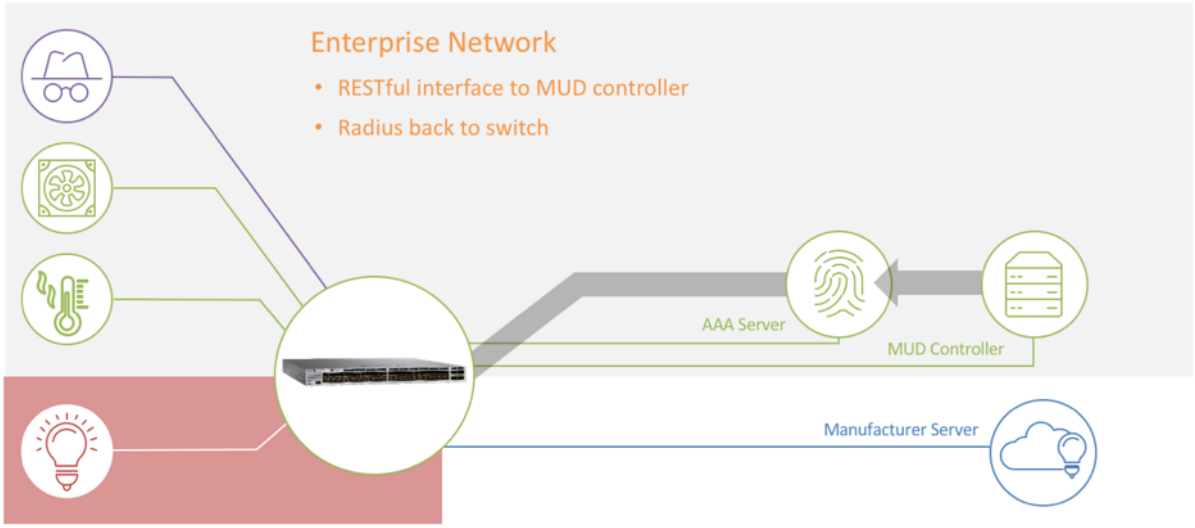
5. Determine Authorization

Determine Appropriate Authorization



6. Network Access Control granted based on Policy

Effect Change of Authorization



References (optional)

IETF's Anima Working group
Website: https://datatracker.ietf.org/wg/anima/about/
Email: anima@ietf.org
IETF's BRSKI specification: https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/

IETF's Operations and Management Area Working Group
Website: https://datatracker.ietf.org/wg/opsawg/documents/
Email: opsawg@ietf.org
IETF's MUD specification: https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
IETF's IPFIX specification: https://datatracker.ietf.org/doc/draft-ietf-opsawg-ipfix-bgp-community/

****