CISCO

Possibilities

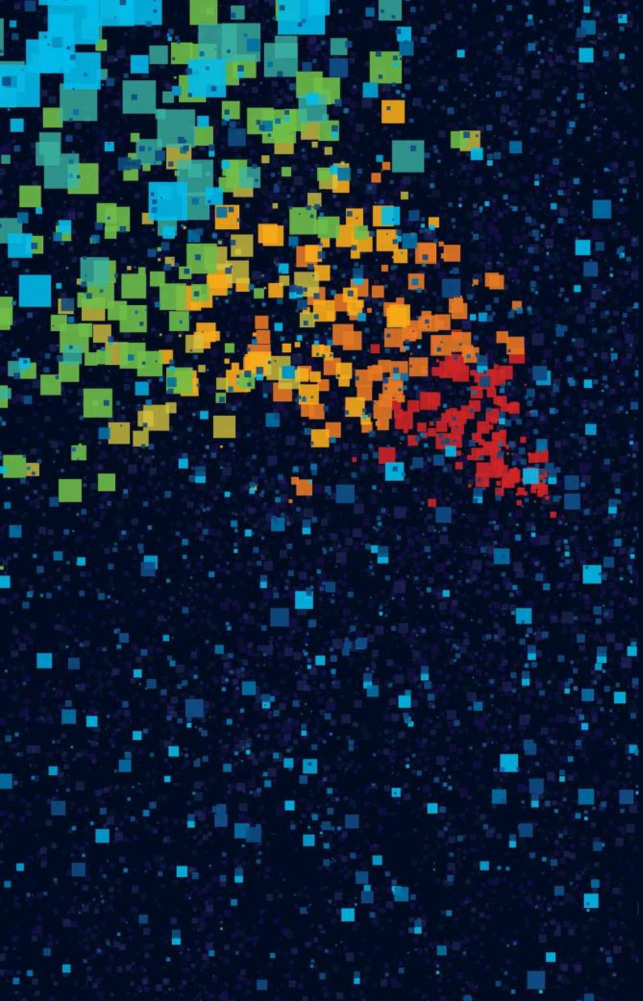
#CiscoLive

Best Practices to Onboard and Protect IoT Devices

A view toward the future

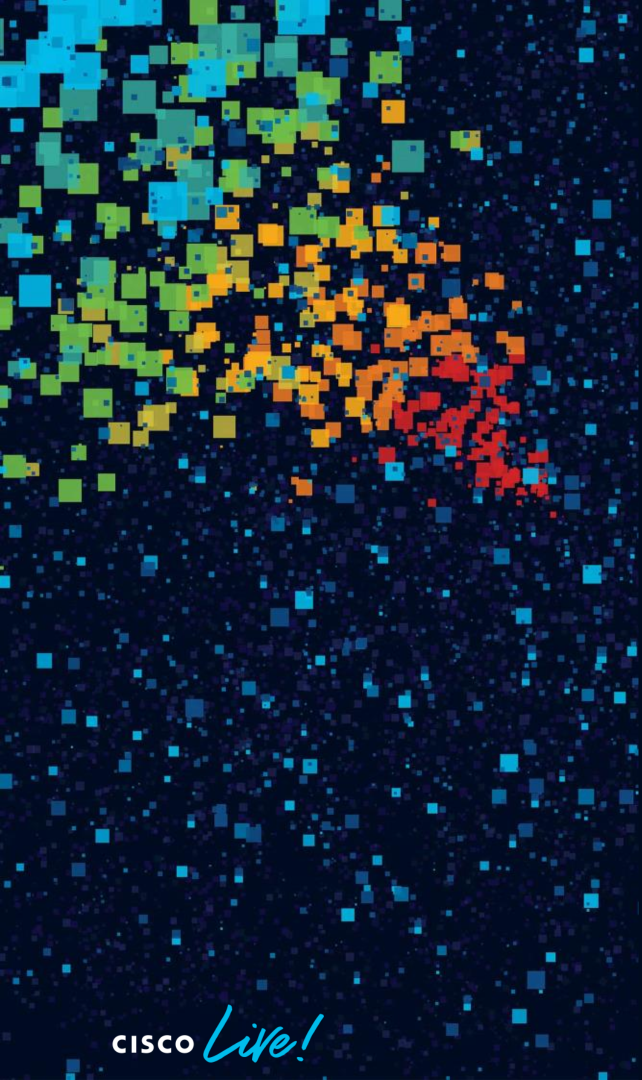
Eliot Lear, Principal Engineer

DGTL-BRKIOT-1553



Agenda

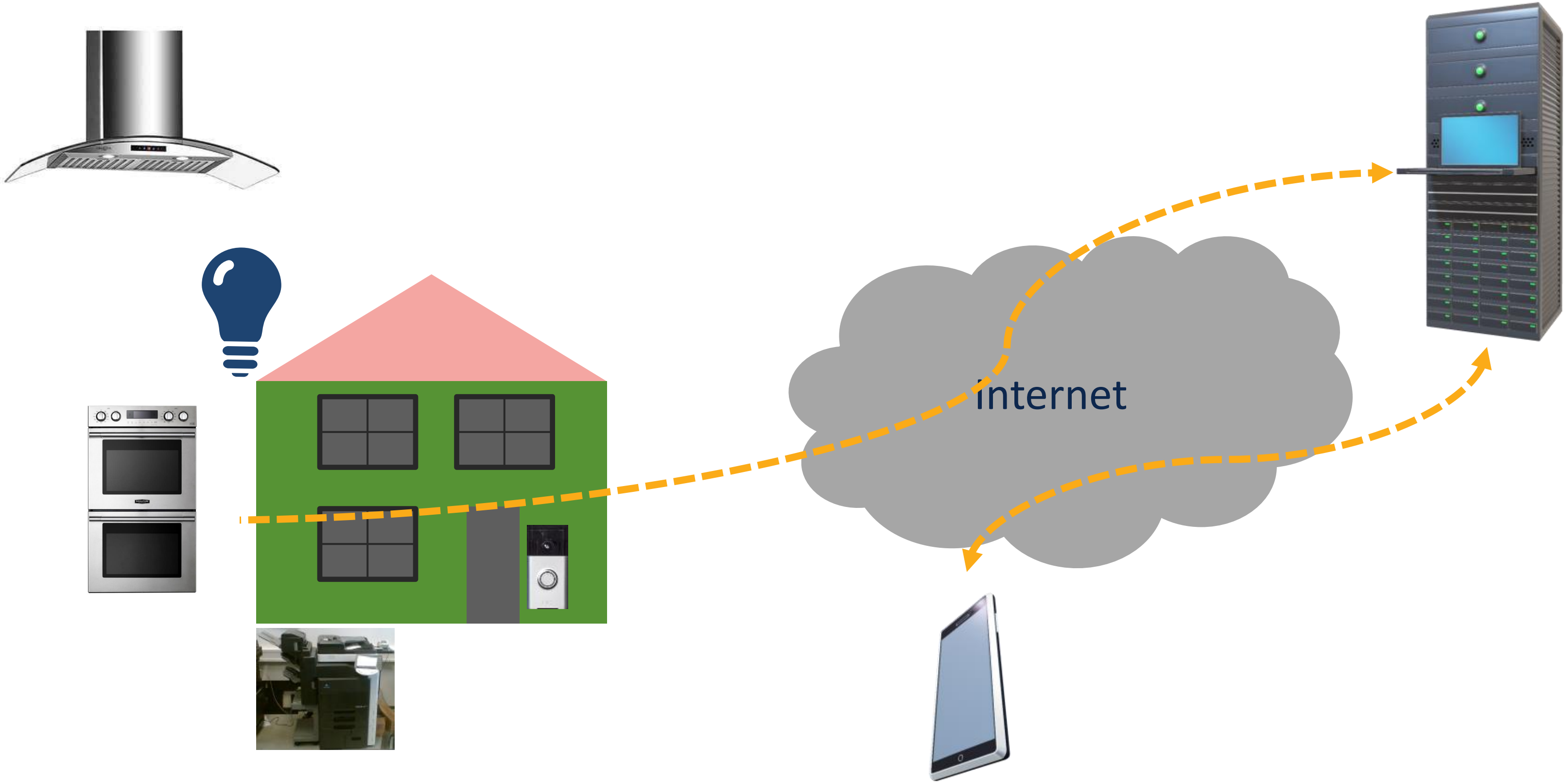
- Introduction: what’s so different about IoT?
- Protecting the device: learned and declared approaches
- Automated onboarding: what does it means and what is required?
- What’s there today, and where are we going?



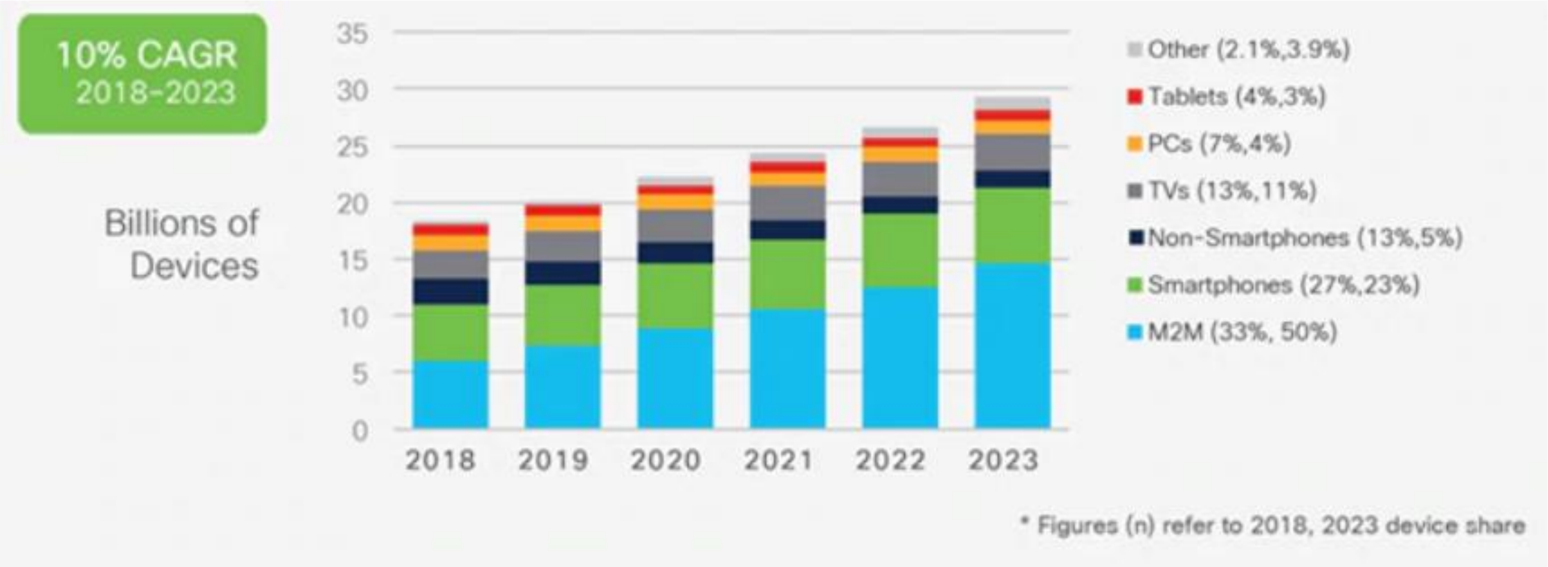
Agenda

- Introduction: What’s so different about IoT?
- Protecting the device: learned and declared approaches
- Automated onboarding: what does it means and what is required?
- What’s there today, and where are we going?

Let’s talk about an oven


internet

The Internet is already all about IoT



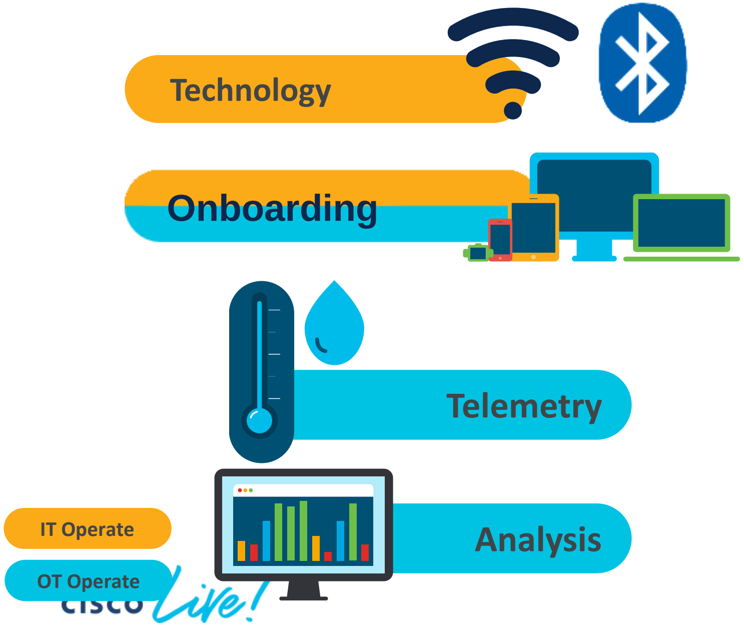
Source: Cisco 2020 Annual Internet Report

Endpoints in your business

Challenges of adding sensors, tags and endpoints:

IT: Deploying new sensors usually requires an overlay infrastructure that they need to manage.

Operations: Need to learn multiple systems that serve multiple purposes, consuming time and effort.



Cloud Applications

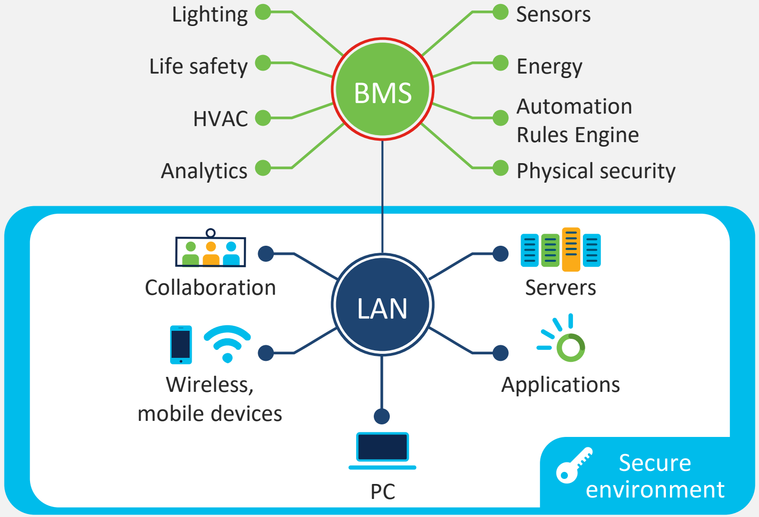
Wireless + BLE (1815, 4800)

Tags & Endpoints

IoT in the Enterprise -The Case for Convergence

Traditional approach

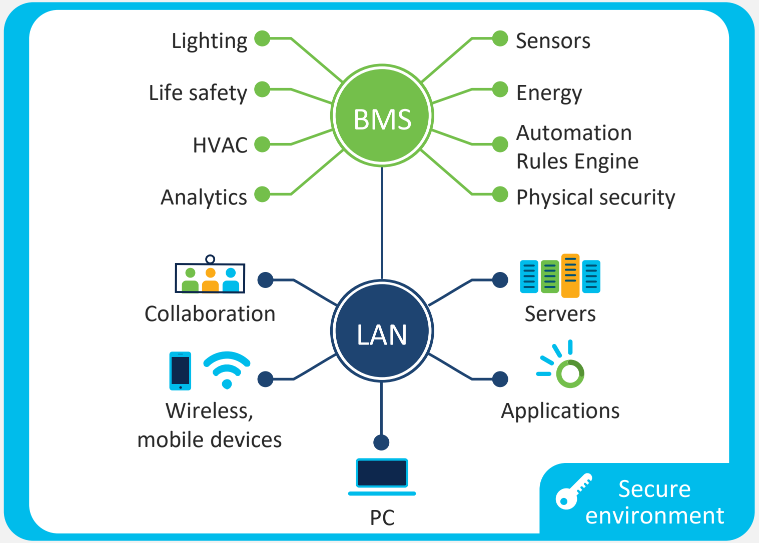
Although BMS is connected to the LAN, advanced security features are not used.



Cisco security applied to traditional networked devices

Converged approach

BMS and all smart building automation and control systems are connected by Cisco technology.



Cisco security applied to all networked devices including BMS

New Technologies Introduce New Threats

Today’s world of IoT and threats everywhere requires more advanced security and control measures to protect your integrated systems.

Who’s accessing the network?

What type of device is trying to connect?

Where is the device located?

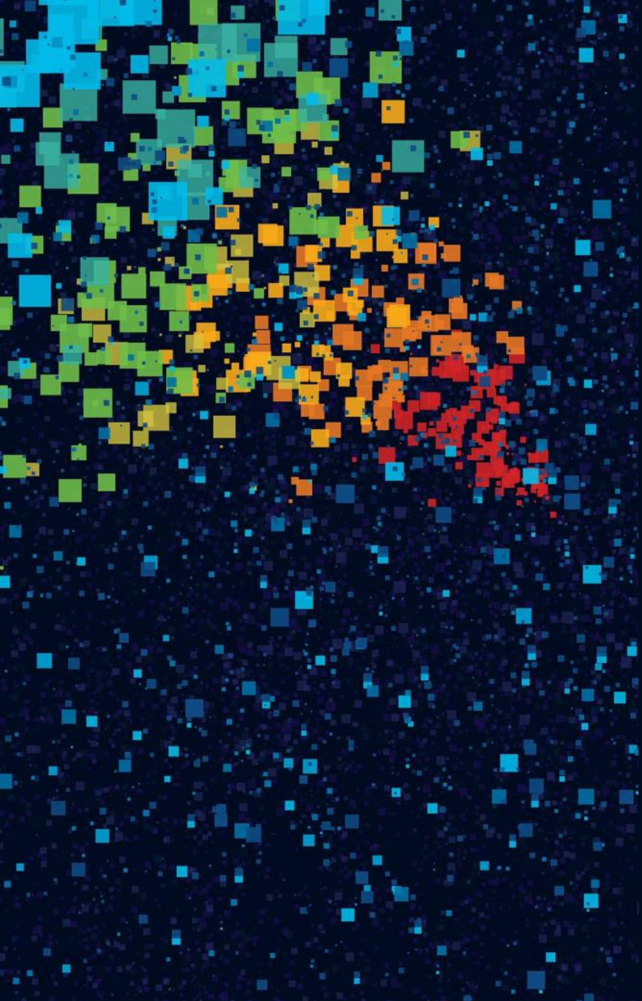
How is the device accessing the network?

What action is being attempted?

Is the device what it says it is? Is this a compliant device? Has it potentially been compromised?

Is the device trying to communicate with portions of the network it doesn’t need to?

Is the device behavior normal and expected?



Agenda

- Introduction: what’s so different about IoT?
- Protecting the device: learned and declared approaches
- Automated onboarding: what does it means and what is required?
- What’s there today, and where are we going?

A common threat: **printers**

Study cites multi-function printers as some of the most dangerous members of the IoT family

Bitdefender.com, 28 February 2019

What Sort of Access Do These Printers Require?

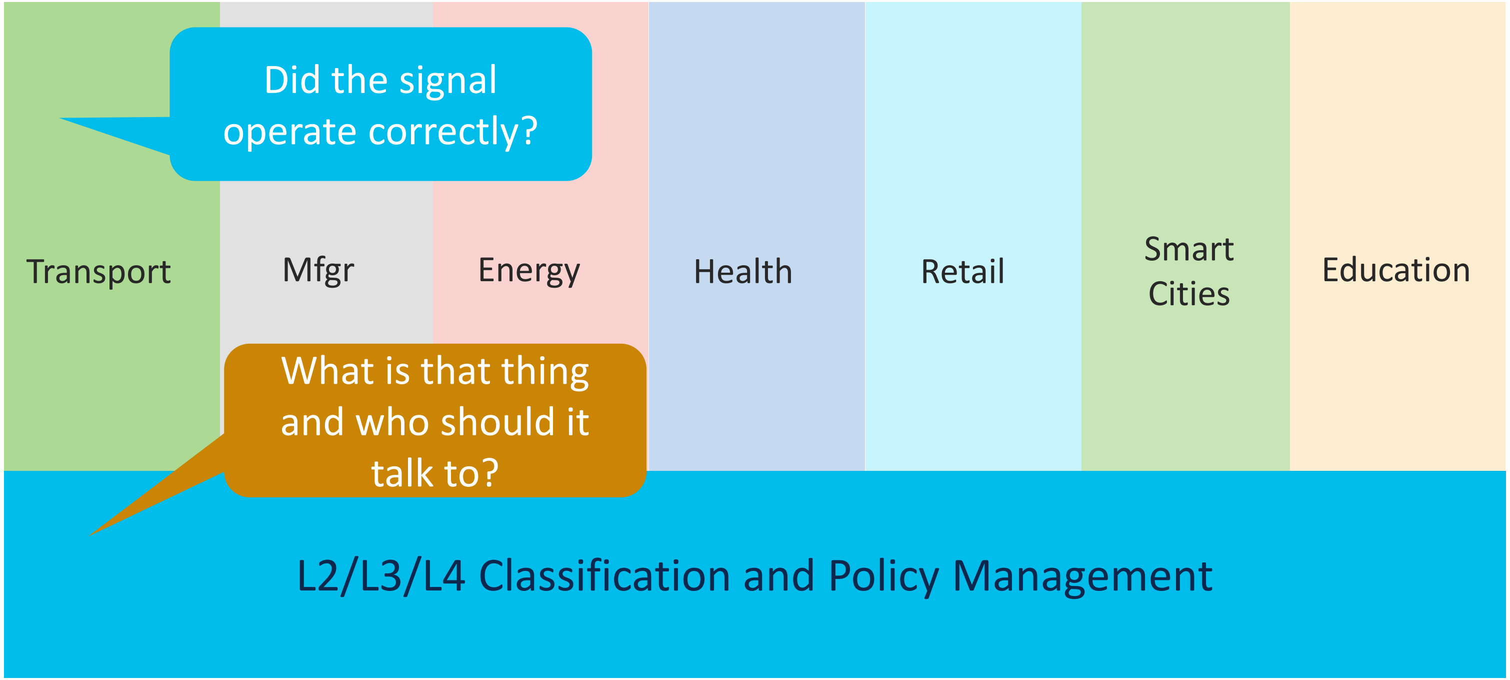
From	To	Protocol	Source Port	Destination Port(s)
Printer	xmpp009.hpeprint.com	TCP		80, 443, 5222,5223
Printer	DNS Server	UDP		53
Printer	chat.hpeprint.com	TCP		80,443
Printer	224.0.0.251/32	UDP		5353
Printer	220.0.0.252/32	UDP		5355
Printer	h10141.www1.hp.com	TCP		80
Printer	Local Networks	UDP	5353	
Printer	Local Networks	TCP	80	

Source: University of New South Wales, using mudgee

(not shown: L2 packets)

Scaling Problem: Number of **Types** of Things

Network Knowledge and Application Awareness



Did the signal operate correctly?

Transport

Mfgr

Energy

Health

Retail

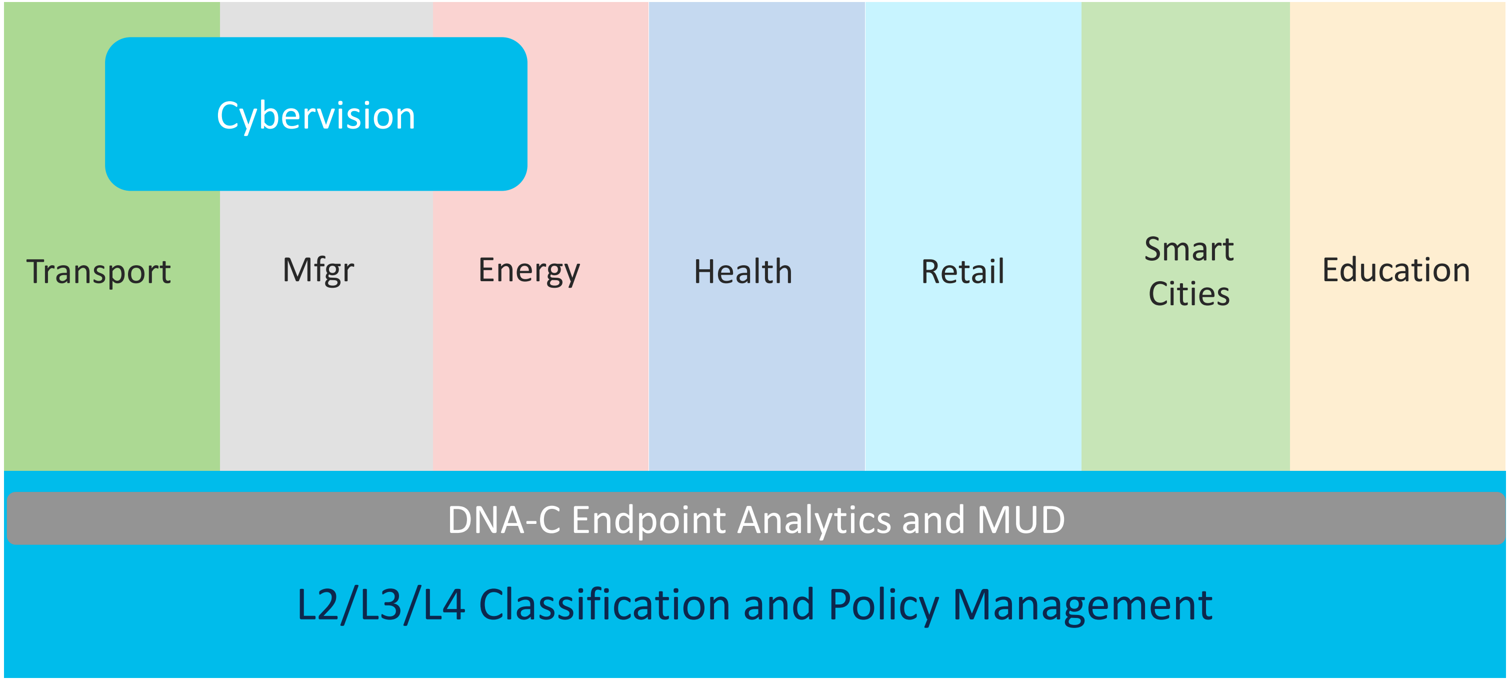
Smart Cities

Education

What is that thing and who should it talk to?

L2/L3/L4 Classification and Policy Management

Network Knowledge and Application Awareness



Cybervision

Transport

Mfgr

Energy

Health

Retail

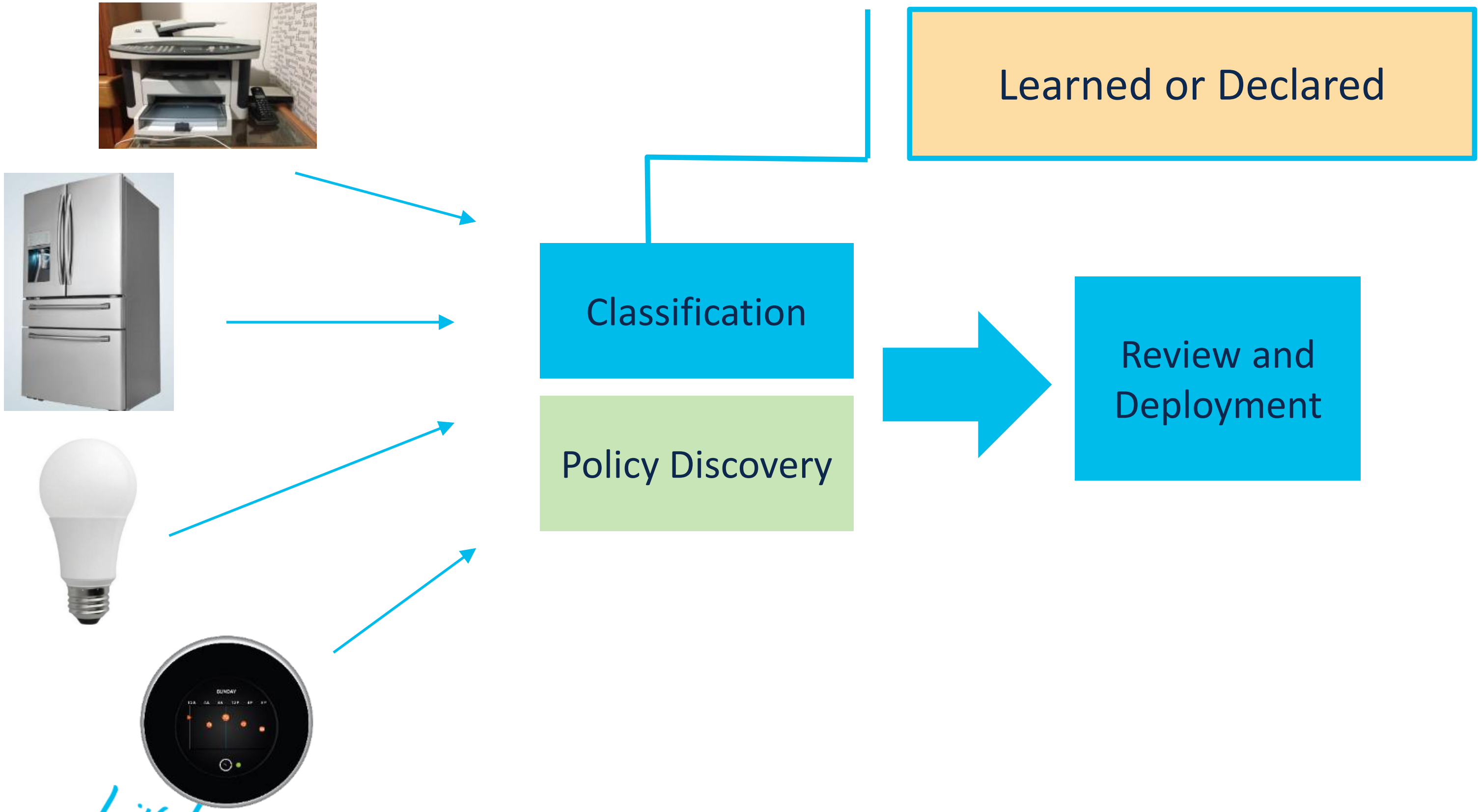
Smart Cities

Education

DNA-C Endpoint Analytics and MUD

L2/L3/L4 Classification and Policy Management

Figuring out what's what and what to do with it



Learned or Declared

Classification

Policy Discovery

Review and Deployment

Learned and Declared Models

	What is it?	Benefits	Drawbacks
Learned	Cisco-provided Expertise + your deployment knowledge	• Required for “brownfield” deployments for years to come • No ecosystem requirements	• Requires relearning from time to time • Can be compute intensive
Declared	Manufacturer-provided expertise plus your deployment knowledge	• Authoritative source of vendor information • Combines policy and classification	• Ecosystem must adopt these approaches

Good news! Use both!

Declared Approach: Assumptions and Assertions

Assumptions	Assertions
A Thing has a single use or a small number of uses.	Because a Thing has a single or a small number of intended uses, all other uses must be unintended.
Things are tightly constrained. Very little CPU, memory, and battery.	Any intended use can be clearly identified.
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to provide guidance to administrators.
Even those Things that can protect themselves today may not be able to do so tomorrow	A mechanism is needed to protect devices that may have vulnerabilities.

Translating intent into config

Any intended use can be clearly identified by the manufacturer

↓

```
access-list 10 permit host
controller.mfg.example.com
```

All other uses can be warned against in a statement by the manufacturer

↓

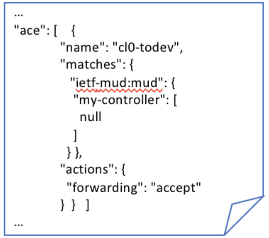
```
access-list 10 deny any any
```

Introducing Manufacturer Usage Descriptions (MUD)

A URL:

https://manufacturer.example.com/mydevice.json

A MUD File:

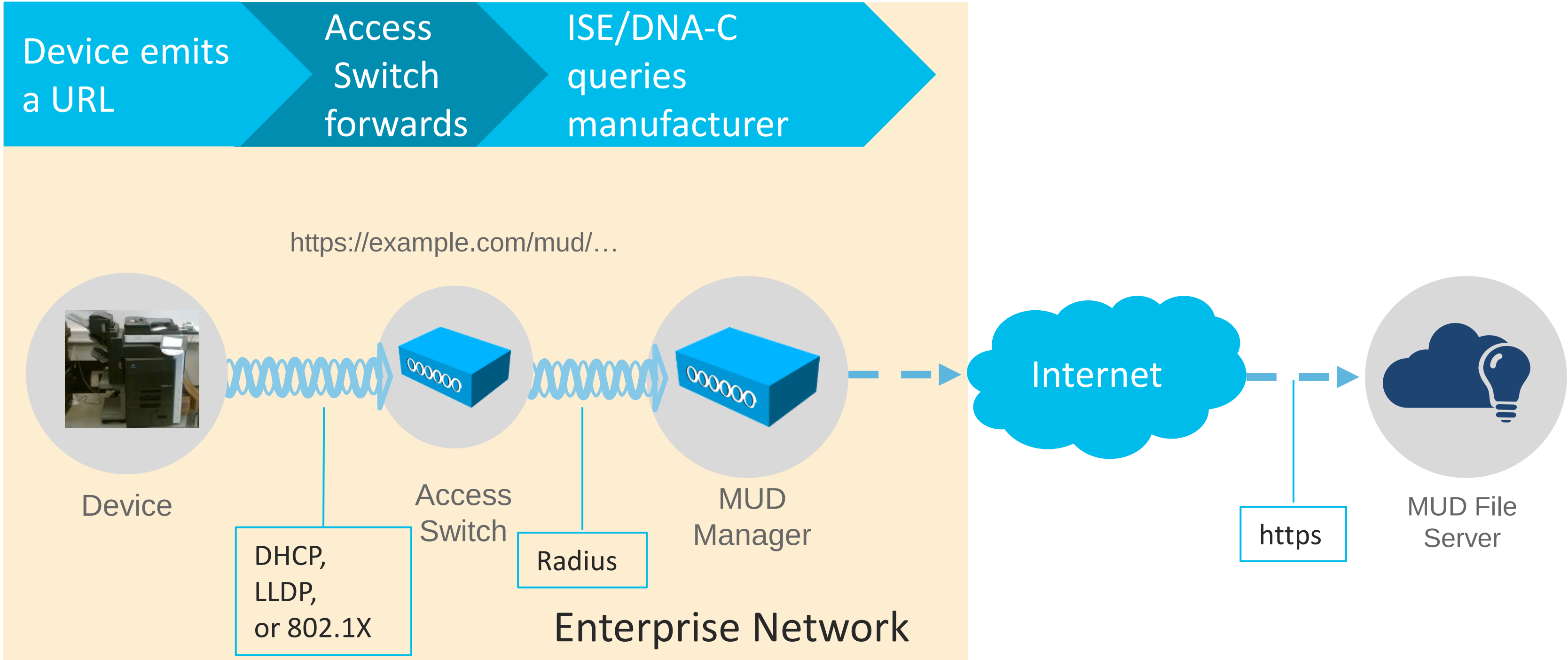


```
…
"ace": [    {
          "name": "cl0-todev",
          "matches": {
            "ietf-mud:mud": {
             "my-controller": [
              null
             ]
           } },
          "actions": {
           "forwarding": "accept"
          } }  ]
…
```

The MUD Manager:

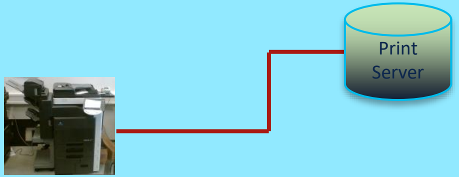
The MUD File Server:

Expressing Manufacturer Usage Descriptions

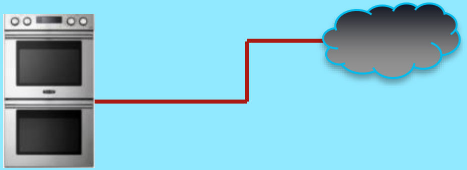


What Classes of Endpoints MUD provides access to

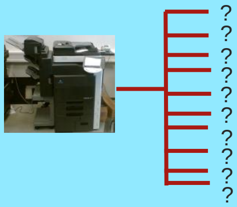
Controllers



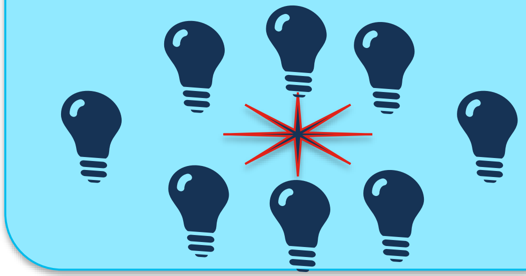
Domain-based Cloud Access



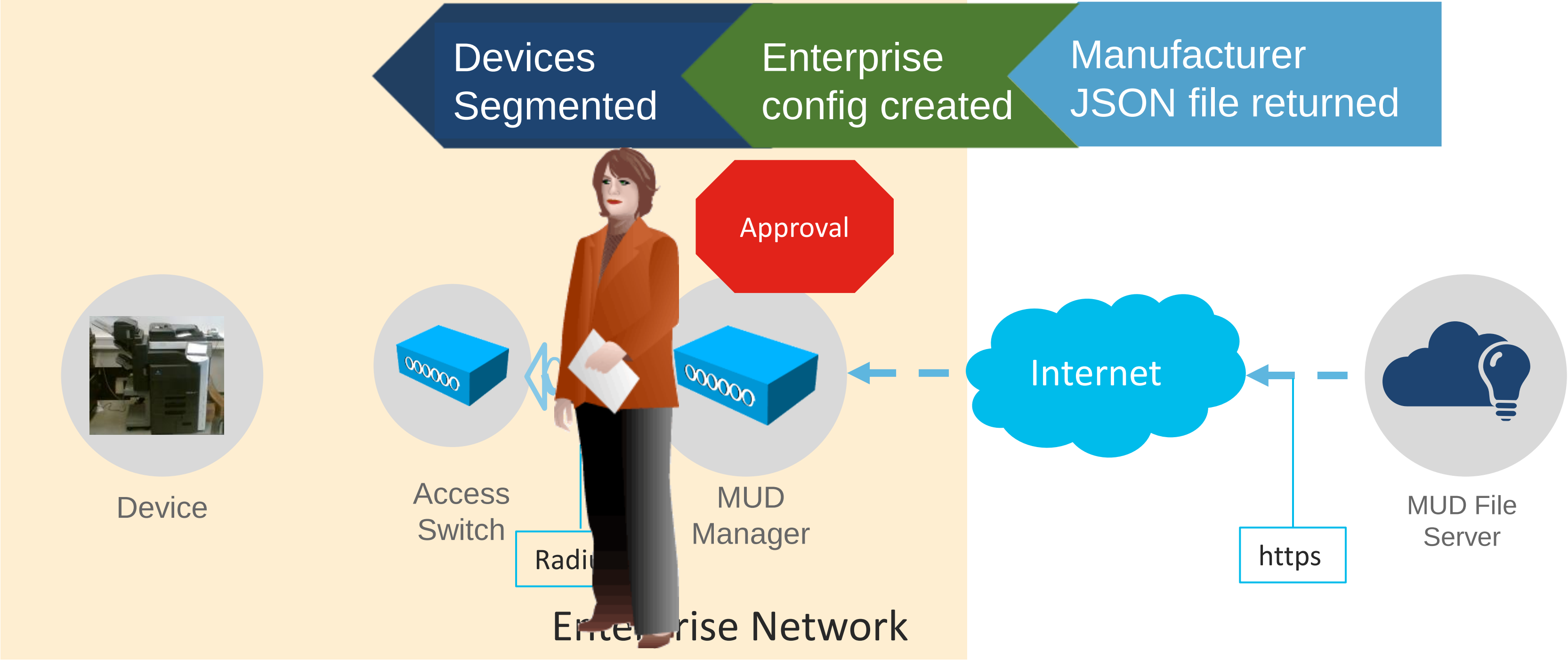
Local Access



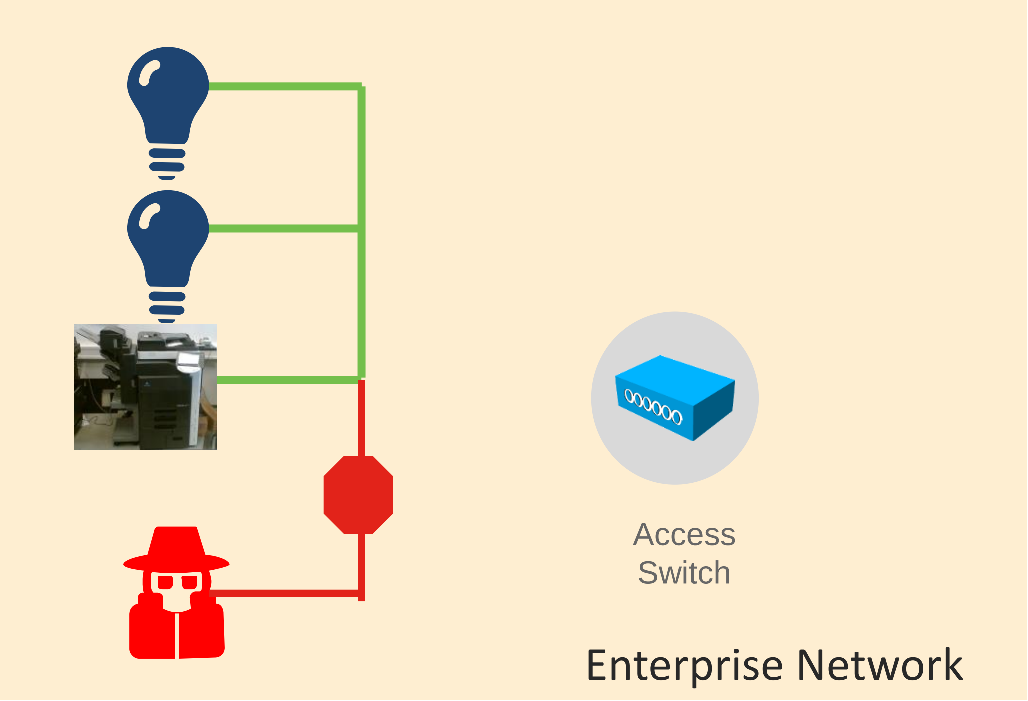
Same Manufacturer



Expressing Manufacturer Usage Descriptions

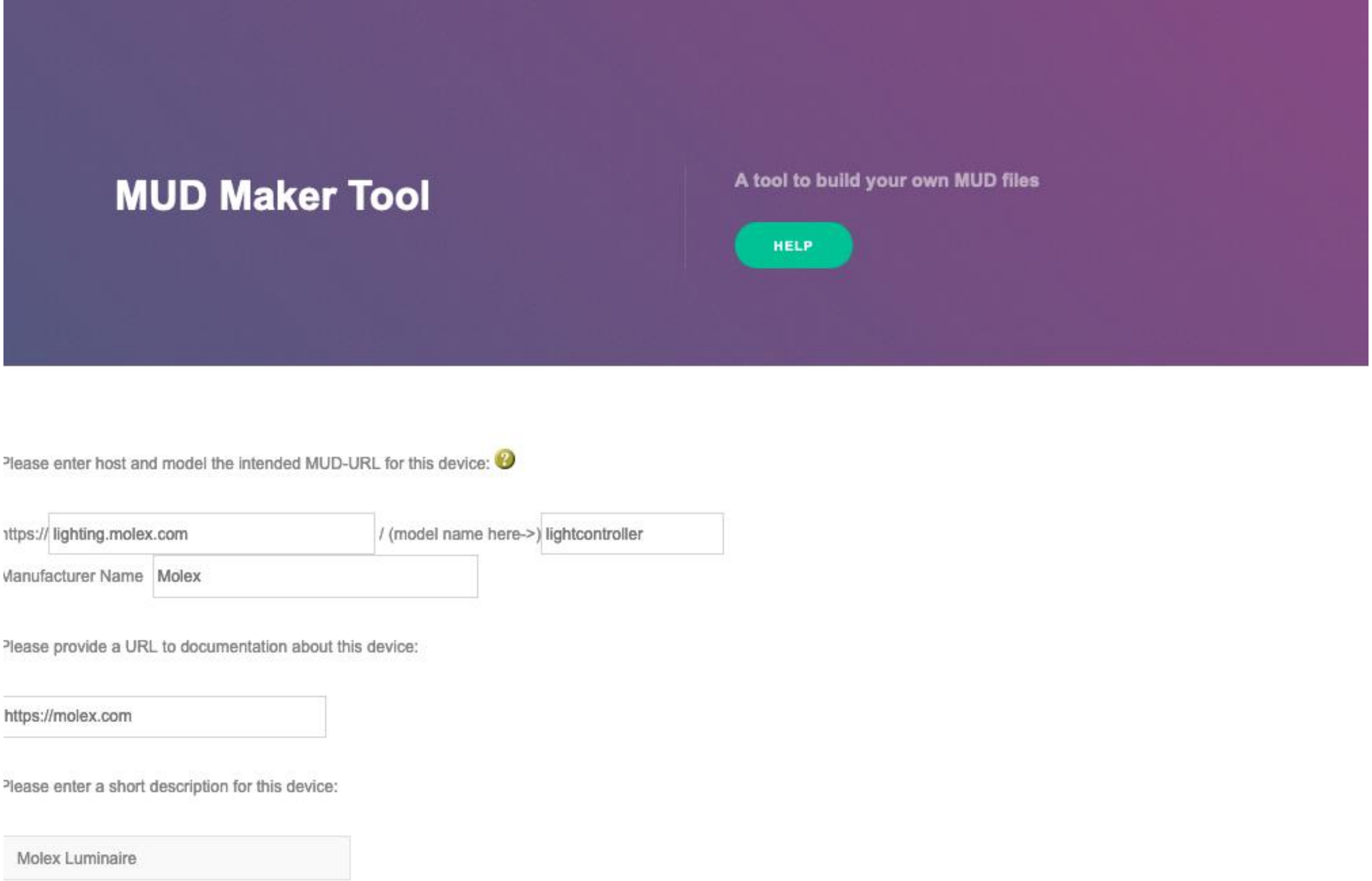


Results: Micro-segmentation of that printer



- Visibility of what’s on the network
- Access limited to devices based on manufacturer recommendations
- Policy choices easily identified by MUD file
- Hacked devices can’t probe for holes
- An additional layer of security
  - BUT- manufacturers should still **always** secure their devices

Let’s make a MUD file and see what that means



MUD Maker Tool

A tool to build your own MUD files

Please enter host and model the intended MUD-URL for this device:

https:// lighting.molex.com / (model name here->) lightcontroller

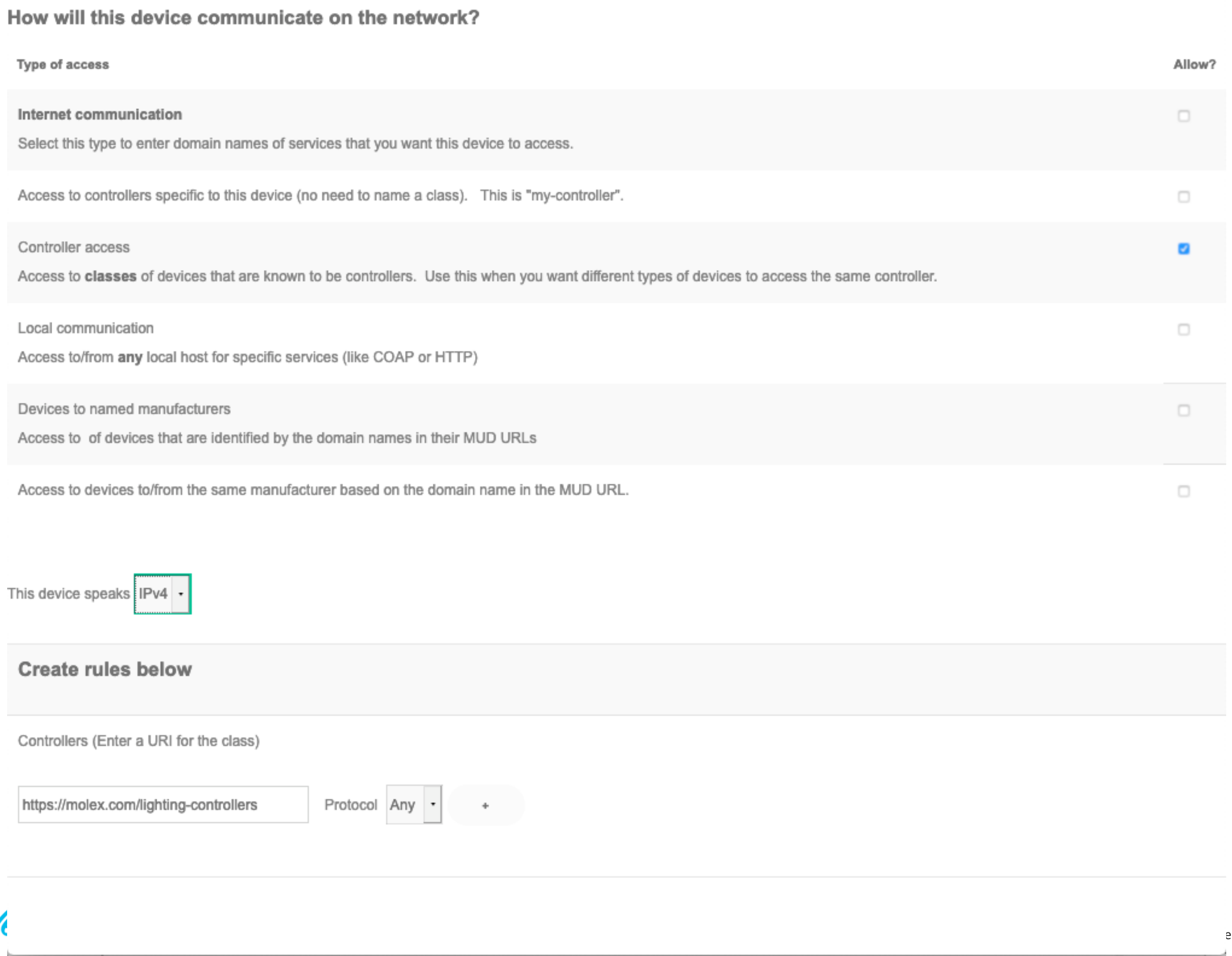
Manufacturer Name Molex

Please provide a URL to documentation about this device:

https://molex.com

Please enter a short description for this device:

Molex Luminaire



How will this device communicate on the network?

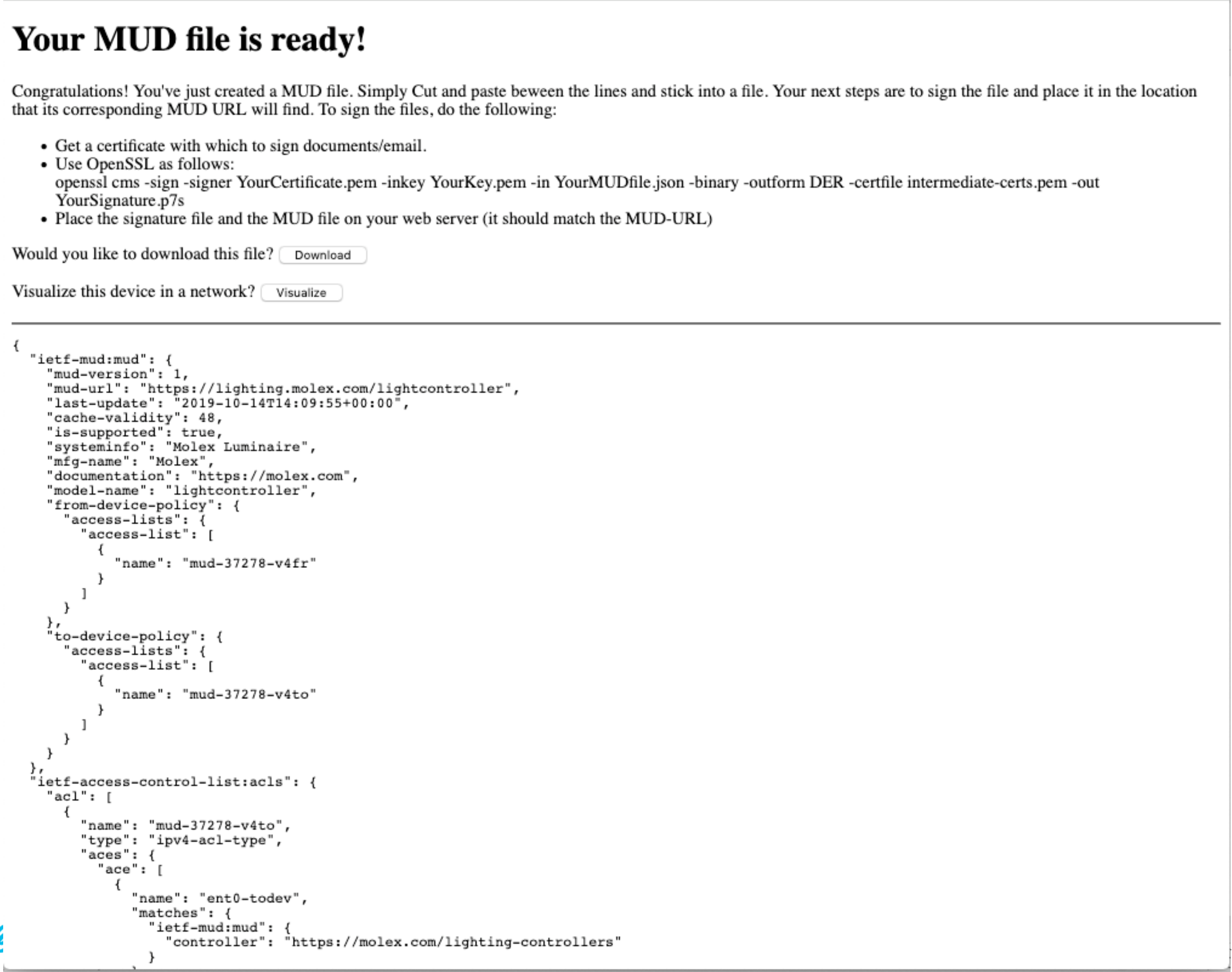
Type of access	Allow?
Internet communication Select this type to enter domain names of services that you want this device to access.	☐
Access to controllers specific to this device (no need to name a class). This is "my-controller".	☐
Controller access Access to **classes** of devices that are known to be controllers. Use this when you want different types of devices to access the same controller.	☑
Local communication Access to/from **any** local host for specific services (like COAP or HTTP)	☐
Devices to named manufacturers Access to of devices that are identified by the domain names in their MUD URLs	☐
Access to devices to/from the same manufacturer based on the domain name in the MUD URL.	☐

This device speaks IPv4

Create rules below

Controllers (Enter a URI for the class)

https://molex.com/lighting-controllers   Protocol Any



Your MUD file is ready!

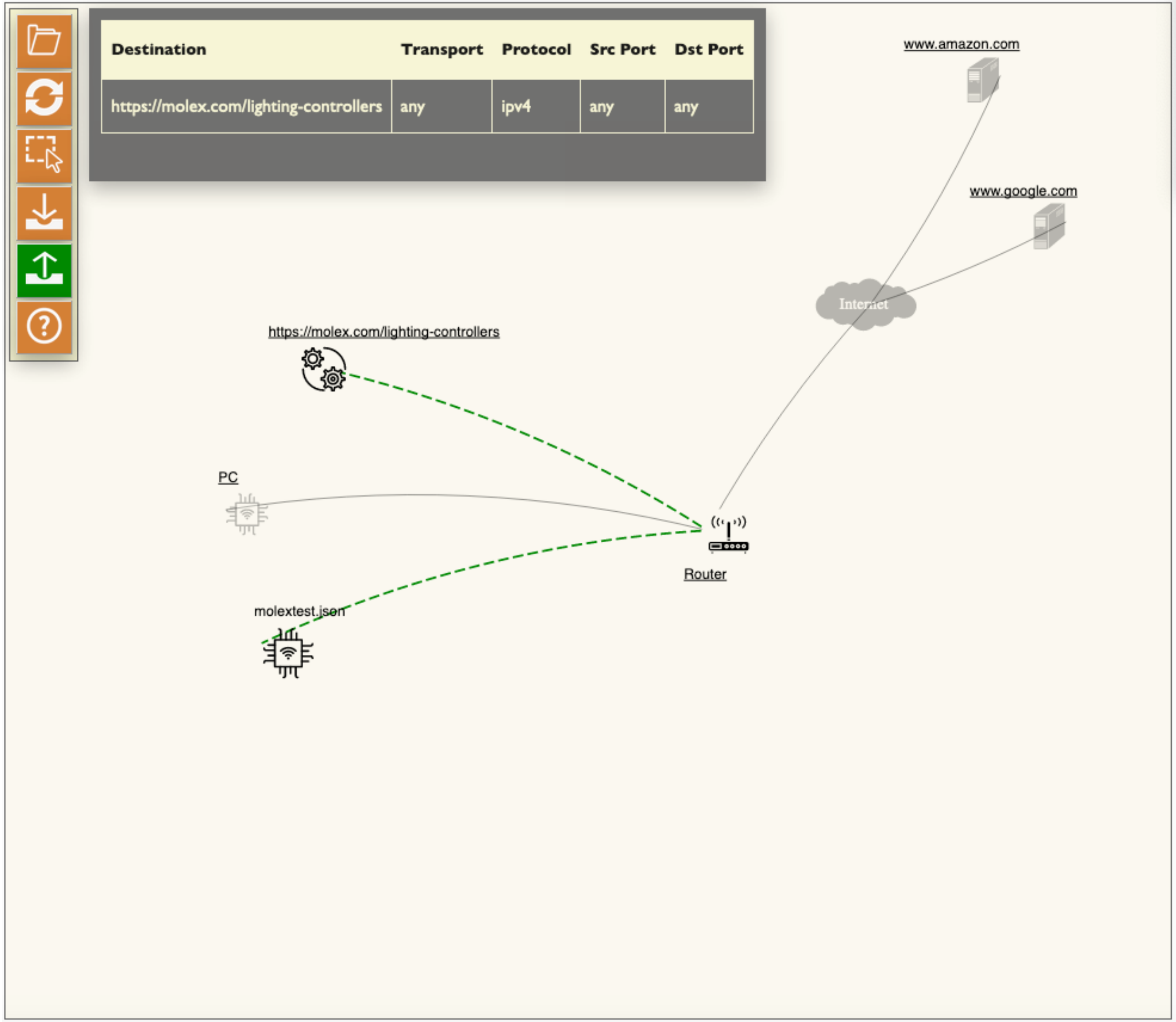
Congratulations! You've just created a MUD file. Simply Cut and paste beween the lines and stick into a file. Your next steps are to sign the file and place it in the location that its corresponding MUD URL will find. To sign the files, do the following:

- Get a certificate with which to sign documents/email.
- Use OpenSSL as follows:
  openssl cms -sign -signer YourCertificate.pem -inkey YourKey.pem -in YourMUDfile.json -binary -outform DER -certfile intermediate-certs.pem -out YourSignature.p7s
- Place the signature file and the MUD file on your web server (it should match the MUD-URL)

Would you like to download this file? Download

Visualize this device in a network? Visualize

```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://lighting.molex.com/lightcontroller",
    "last-update": "2019-10-14T14:09:55+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "Molex Luminaire",
    "mfg-name": "Molex",
    "documentation": "https://molex.com",
    "model-name": "lightcontroller",
    "from-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "name": "mud-37278-v4fr"
          }
        ]
      }
    },
    "to-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "name": "mud-37278-v4to"
          }
        ]
      }
    }
  },
  "ietf-access-control-list:acls": {
    "acl": [
      {
        "name": "mud-37278-v4to",
        "type": "ipv4-acl-type",
        "aces": {
          "ace": [
            {
              "name": "ent0-todev",
              "matches": {
                "ietf-mud:mud": {
                  "controller": "https://molex.com/lighting-controllers"
                }
```



Destination	Transport	Protocol	Src Port	Dst Port
https://molex.com/lighting-controllers	any	ipv4	any	any

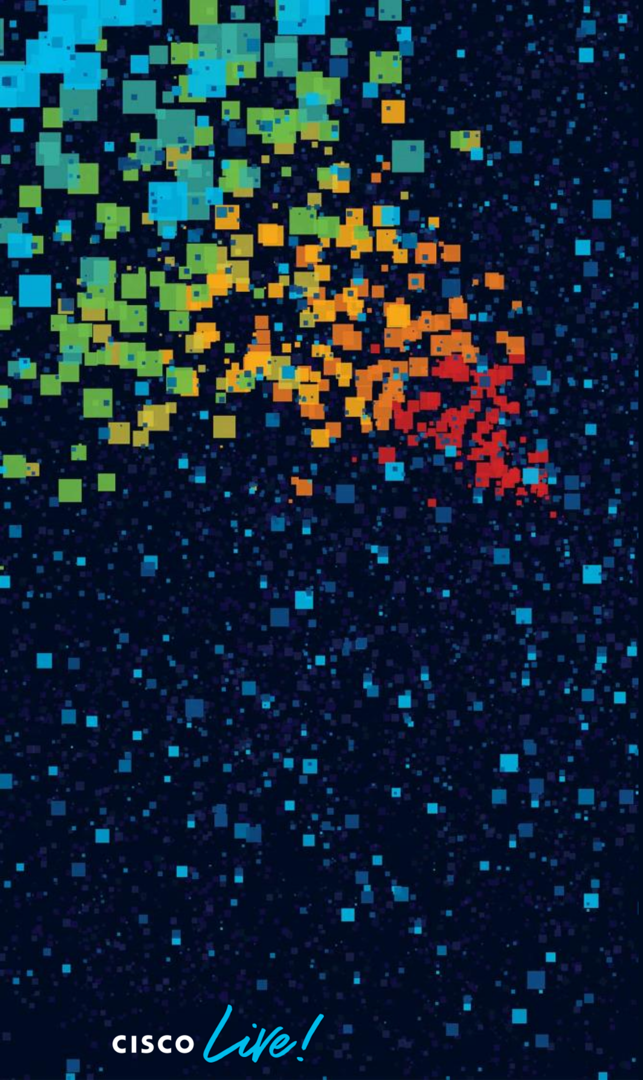
Benefits of MUD

Customer

- Reduces threat surface of exploding number of devices
- Almost no additional CAPEX
- Standard approach to determining manufacturer intent
- Eases and scales access management decisions

Manufacturer

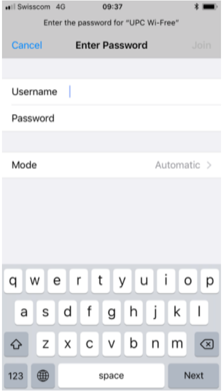
- Reduces manufacturer product risk at almost no cost
- Will increase customer satisfaction and reduce support costs
- Avoids the front page
- Standards-based approach



Agenda

- Introduction: What’s so different about IoT?
- Protecting the device: learned and declared approaches
- Automated onboarding: what does it means and what is required?
- What’s there today, and where are we going?

Why is IoT different?



Swisscom 4G 09:37

Enter the password for "UPC Wi-Free"

Username

Password

Mode Automatic

Screen to see which networks are available

Keyboard to type in credentials

Human being to select the network

No screen

No keyboard

Human has no way to apply his/her knowledge

Basic Requirement for Onboarding: Trust

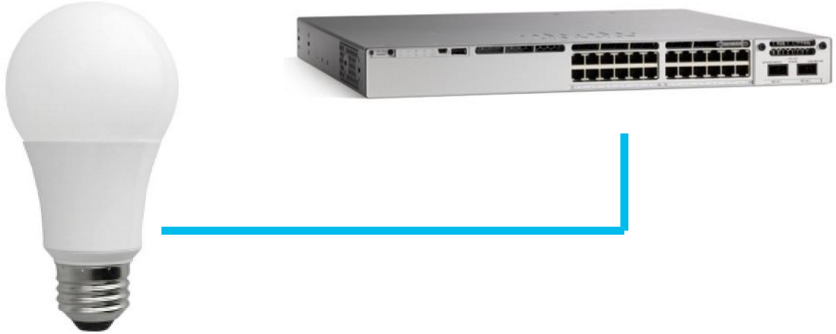
“Can that network prove to me that I should join it?”

“Is that thing supposed to join **my** network?”

The Easy Version of Trust: a wire!

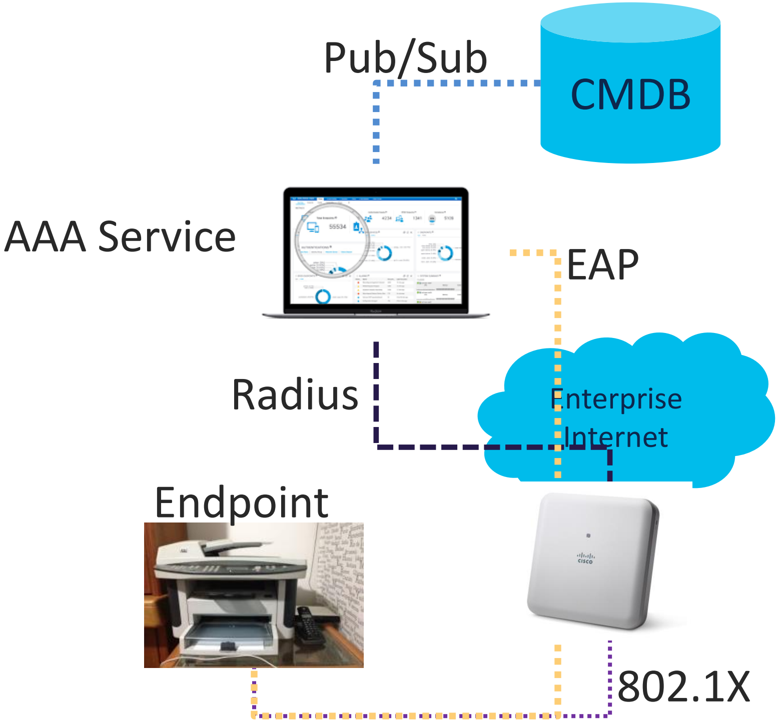
Threat model assumptions:

- Physical security
- Supply chain security



What’s there now?

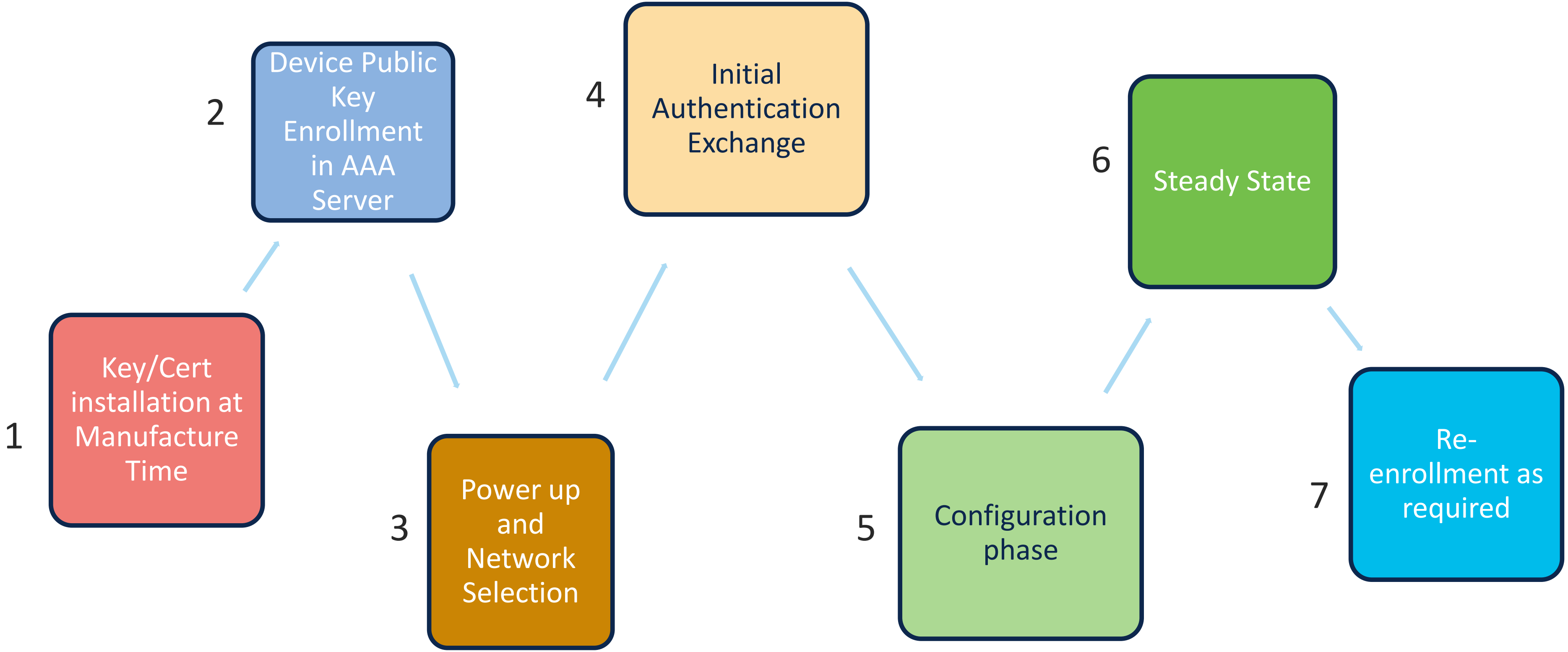
- The IoT Device
- AAA / policy server
- Radius and EAP control channels
- Wireless AP or switch
- An inventory control system
- End goal: **steady state with EAP**



How to Establish Trust?

Method	Benefits	Drawbacks
SIMs provisioned by manufacturer	• Standards mostly done • Plug and Play • Reset works fine • Handles supply chains	• Requires billing relationships be established for network usage • Offline limitations
Public key-based label/e-BOM mechanisms	• Scan once and import • Works great with no Internet • Reset only requires QR code • Can handle supply chains	• Not zero-touch (one touch) • Standards not complete
Online-based mechanisms	• Zero touch per-device • Works across any telco (or none at all)	• Requires Internet • Requires very simple supply chains

Generic Onboarding Flow



1 Key/Cert installation at Manufacture Time

2 Device Public Key Enrollment in AAA Server

3 Power up and Network Selection

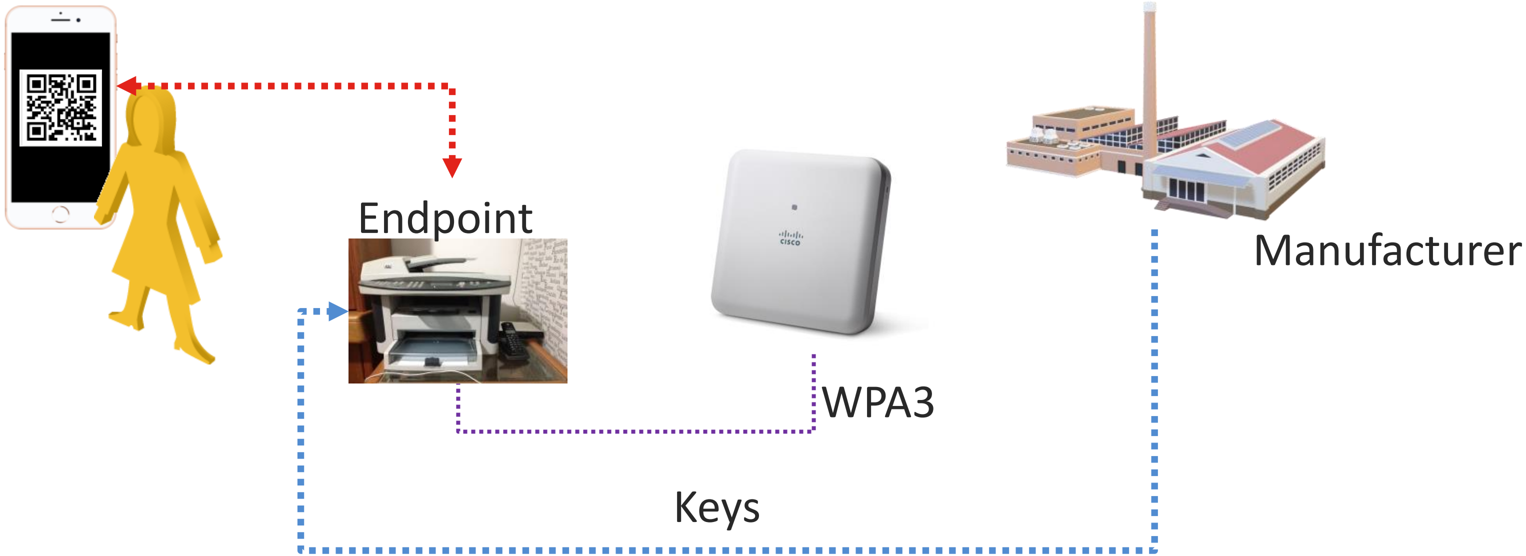
4 Initial Authentication Exchange

5 Configuration phase

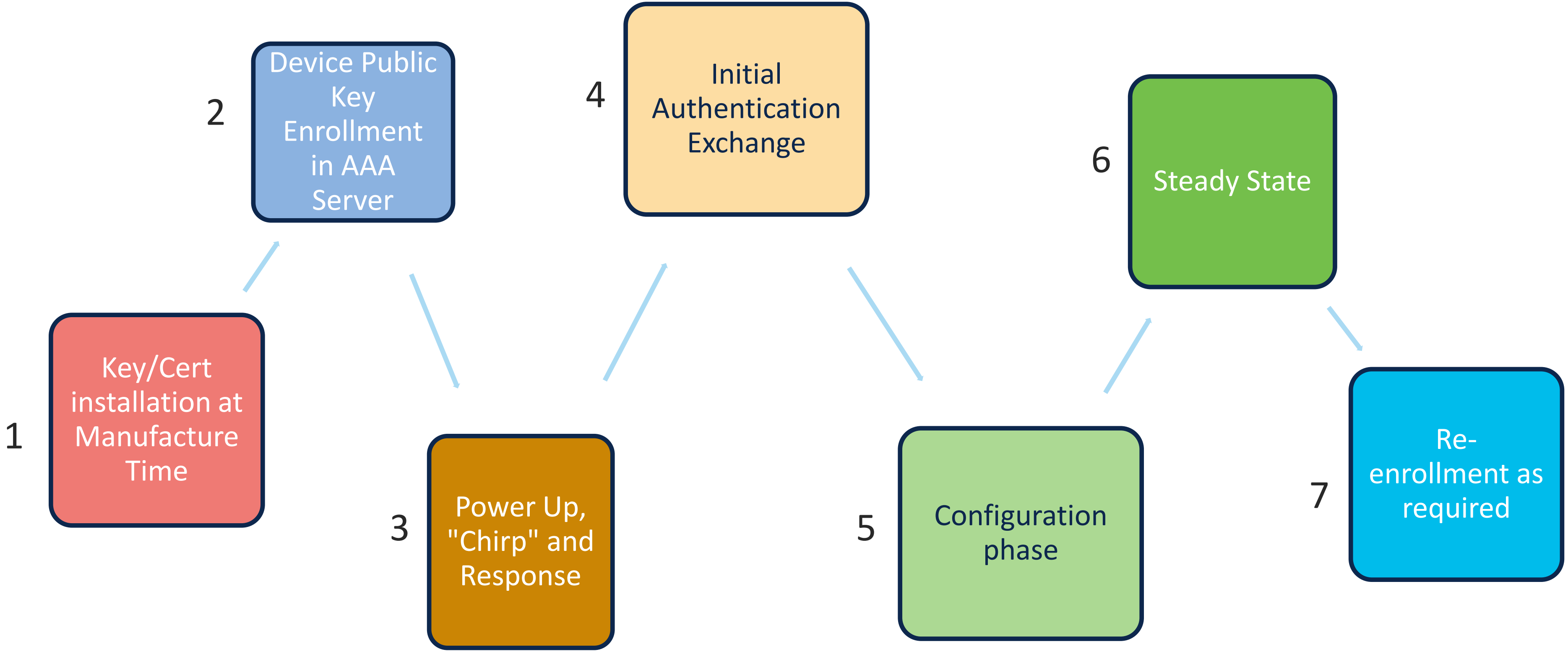
6 Steady State

7 Re-enrollment as required

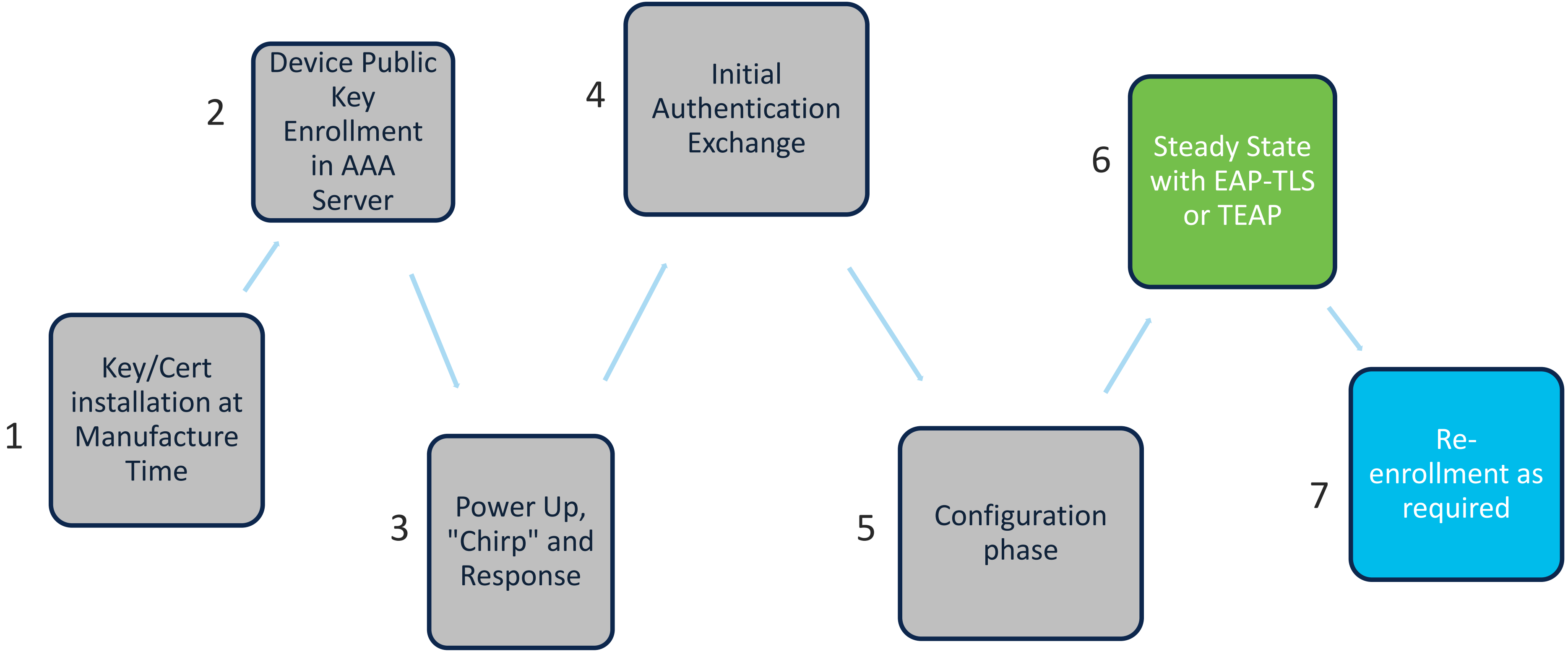
Wifi Alliance DPP Architecture



Device Provisioning Protocol


1
Key/Cert installation at Manufacture Time
2
Device Public Key Enrollment in AAA Server
3
Power Up, "Chirp" and Response
4
Initial Authentication Exchange
5
Configuration phase
6
Steady State
7
Re-enrollment as required

Device Provisioning Protocol (DPP) + TEAP/EAP



1 Key/Cert installation at Manufacture Time

2 Device Public Key Enrollment in AAA Server

3 Power Up, "Chirp" and Response

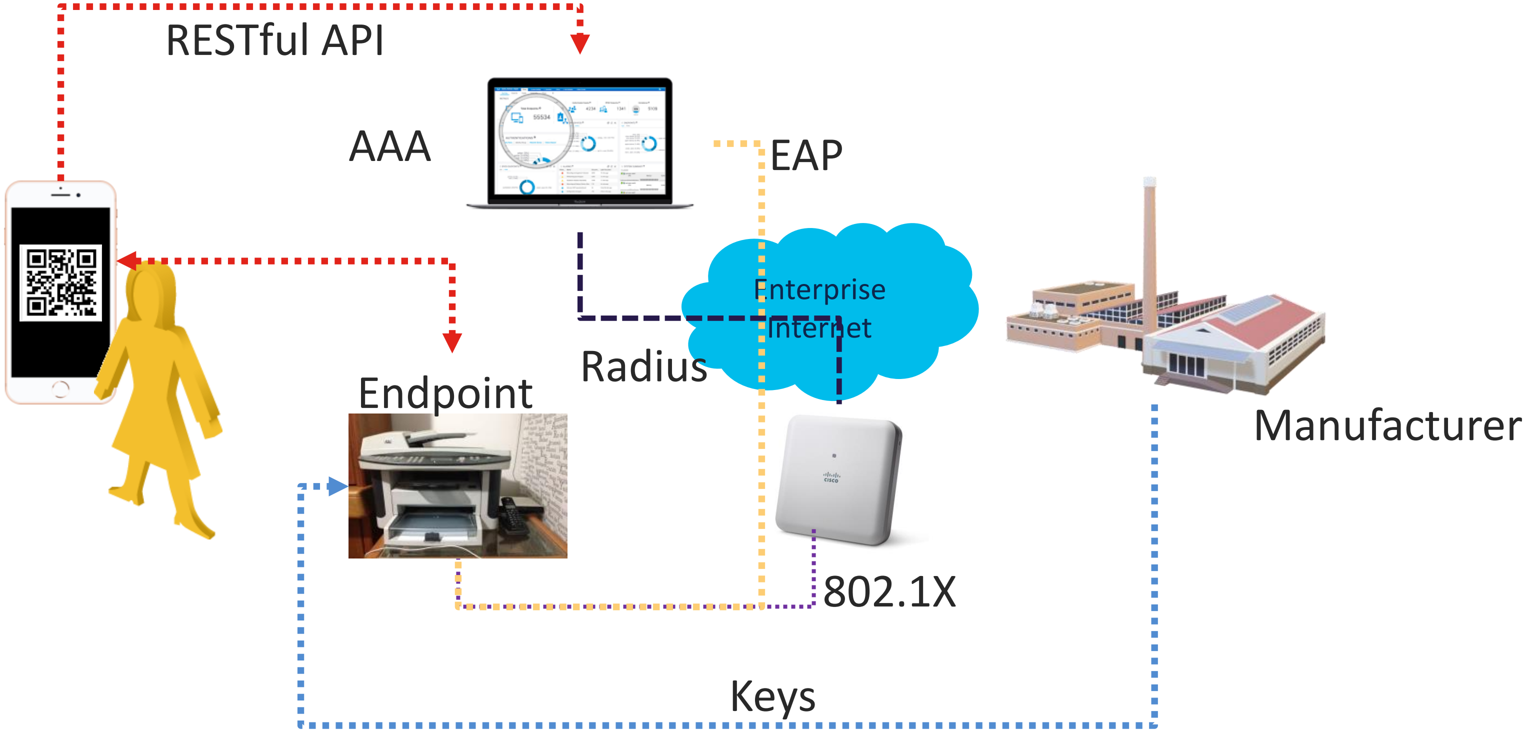
4 Initial Authentication Exchange

5 Configuration phase

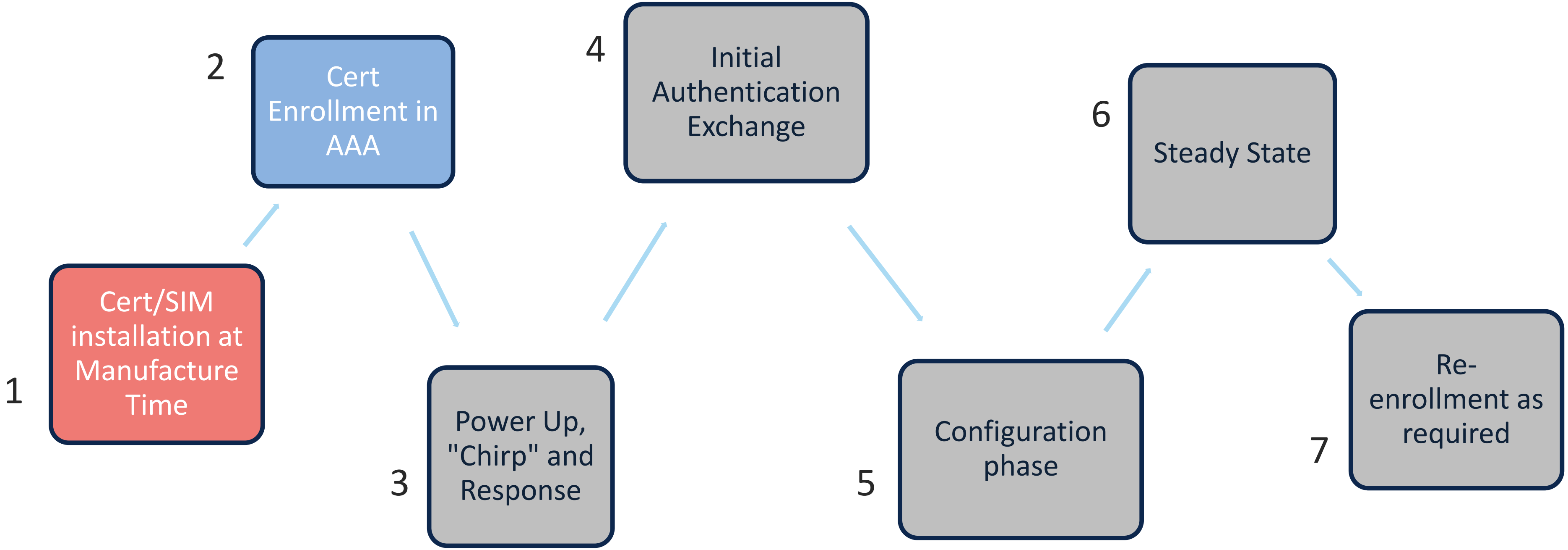
6 Steady State with EAP-TLS or TEAP

7 Re-enrollment as required

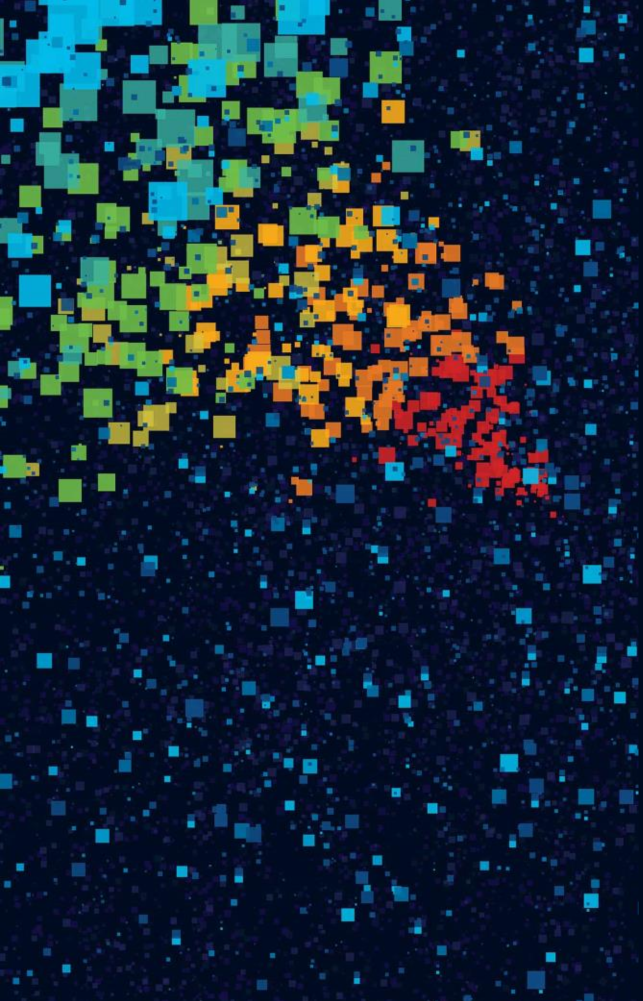
DPP/TEAP architecture (for the future)



Pre-Provisioned/SIM/e-SIM Onboarding Flow



1
Cert/SIM installation at Manufacture Time
2
Cert Enrollment in AAA
3
Power Up, "Chirp" and Response
4
Initial Authentication Exchange
5
Configuration phase
6
Steady State
7
Re-enrollment as required

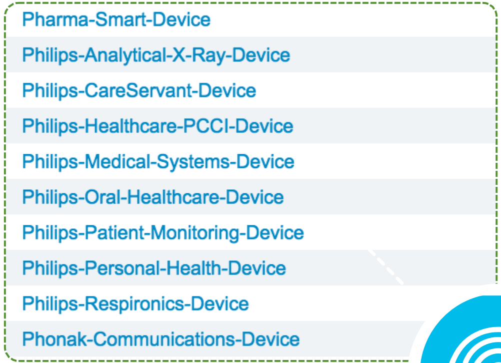


Agenda

- Introduction: what’s so different about IoT?
- Protecting the device: learned and declared approaches
- Automated onboarding: what does it means and what is required?
- What’s there today, and where are we going?

ISE device profiles

Medical profiles XML upload. Profiling data collection via usual means



- Pharma-Smart-Device
- Philips-Analytical-X-Ray-Device
- Philips-CareServant-Device
- Philips-Healthcare-PCCI-Device
- Philips-Medical-Systems-Device
- Philips-Oral-Healthcare-Device
- Philips-Patient-Monitoring-Device
- Philips-Personal-Health-Device
- Philips-Respironics-Device
- Phonak-Communications-Device

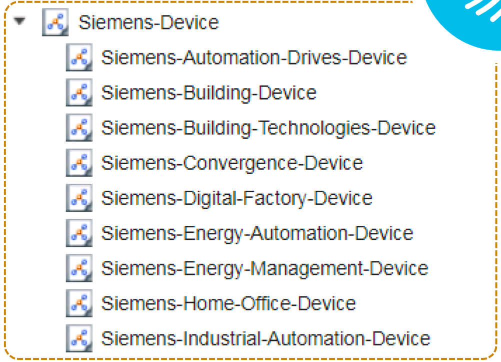
Printers
Scanners
Cameras
CCTV
Game Consoles
Access Points
Workstations
Laptops
Mobile devices

Amazon Echo
Raspberry Pi
UPS
Cable modem
Windows
Embedded
Misc. enterprise devices.

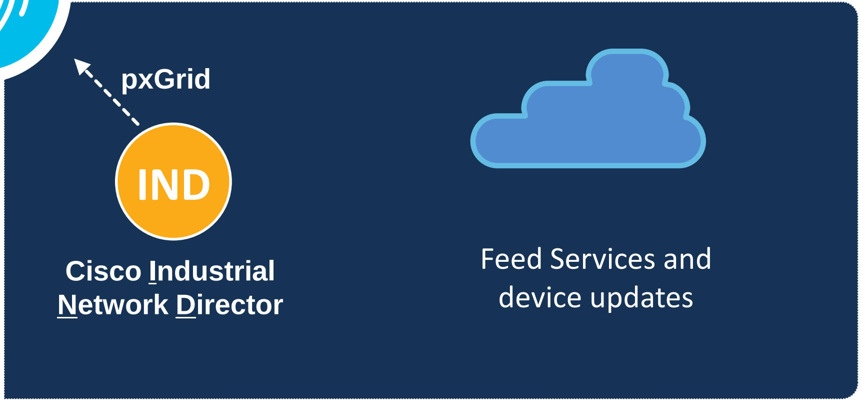
700+ Enterprise device profiles

300+ Medical device profiles

700+ Automation and Control profiles



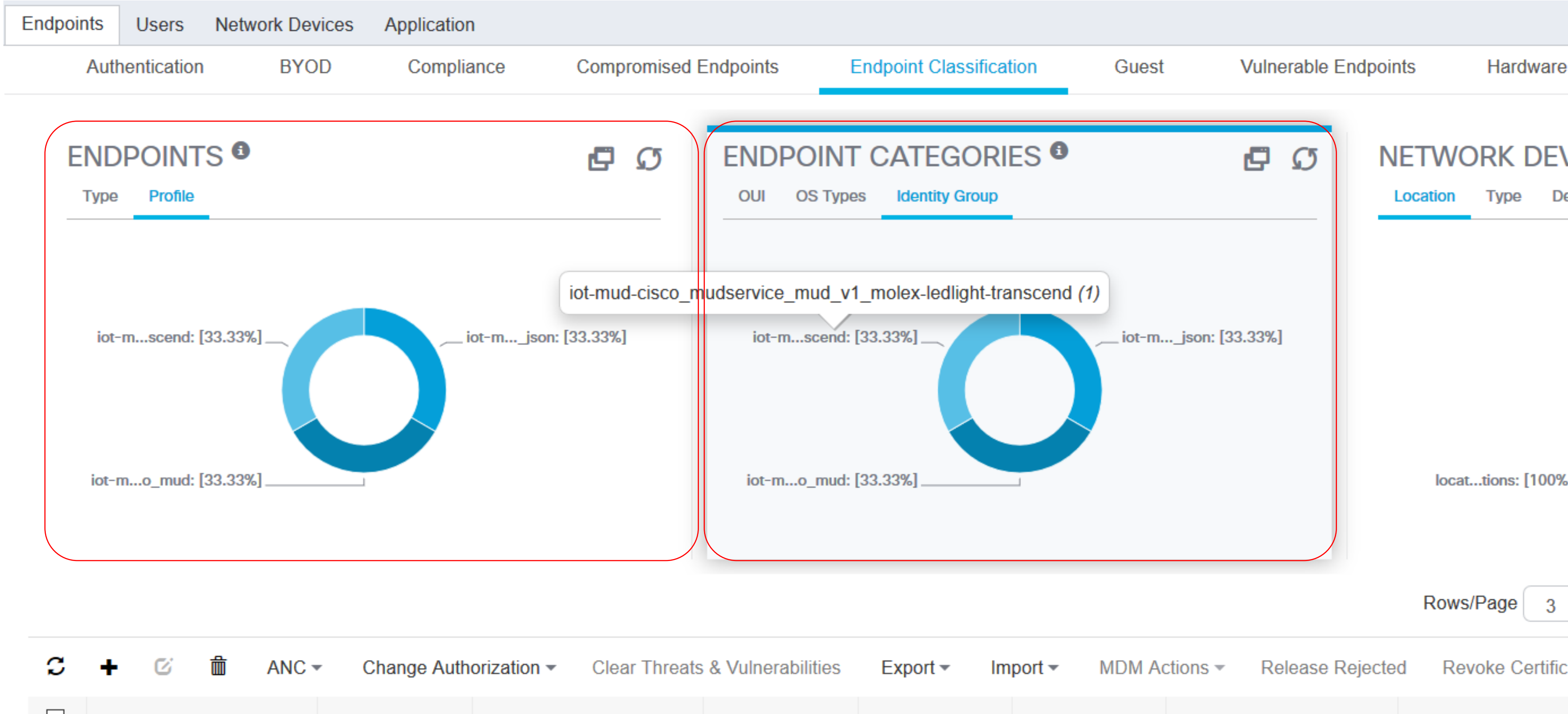
- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device



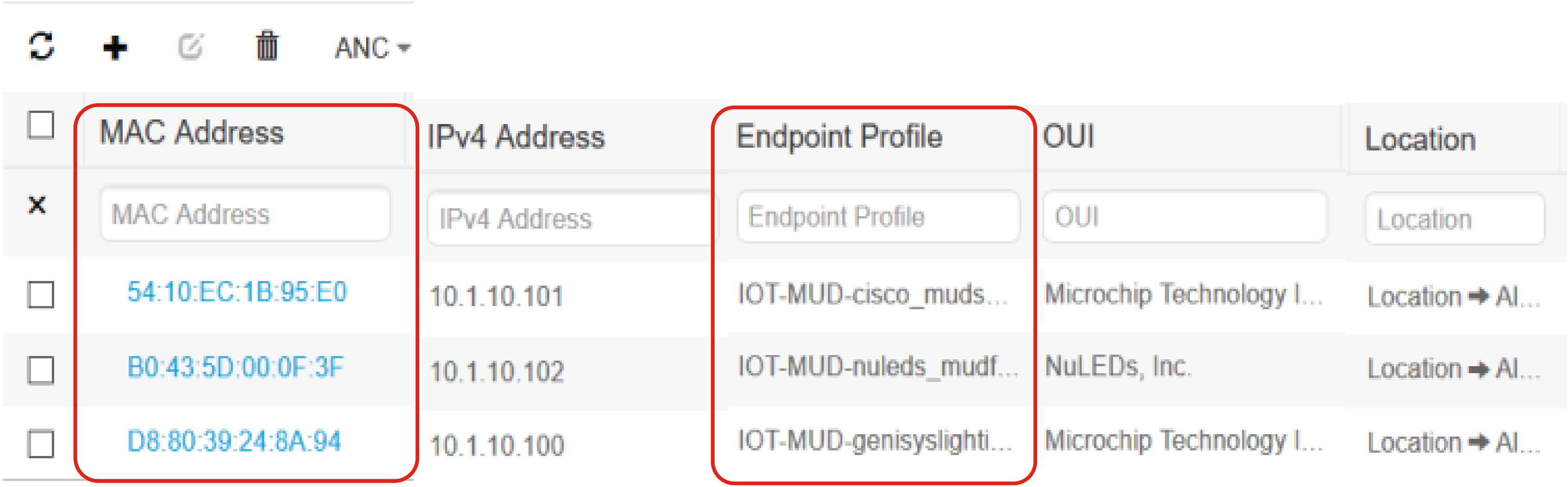
Cisco Industrial Network Director

Feed Services and device updates

Endpoint Classification - Dashboard

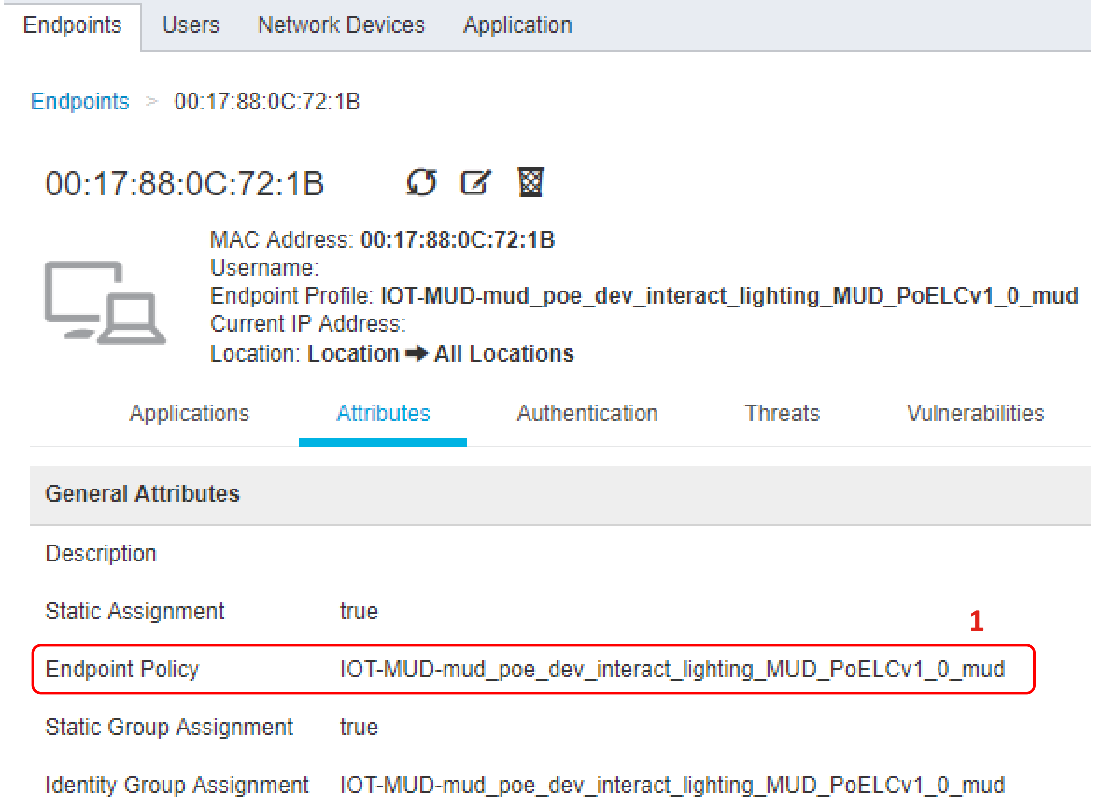


Endpoint classification – list view



□	MAC Address	IPv4 Address	Endpoint Profile	OUI	Location
×	MAC Address	IPv4 Address	Endpoint Profile	OUI	Location
□	54:10:EC:1B:95:E0	10.1.10.101	IOT-MUD-cisco_muds...	Microchip Technology I...	Location ➡ Al...
□	B0:43:5D:00:0F:3F	10.1.10.102	IOT-MUD-nuleds_mudf...	NuLEDs, Inc.	Location ➡ Al...
□	D8:80:39:24:8A:94	10.1.10.100	IOT-MUD-genisyslighti...	Microchip Technology I...	Location ➡ Al...

Endpoint identification and details



Endpoints | Users | Network Devices | Application

Endpoints > 00:17:88:0C:72:1B

00:17:88:0C:72:1B

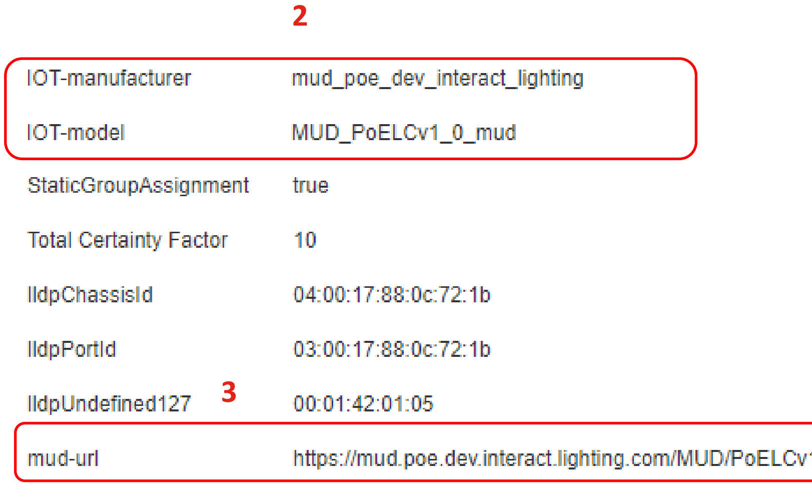
MAC Address: **00:17:88:0C:72:1B**
Username:
Endpoint Profile: **IOT-MUD-mud_poe_dev_interact_lighting_MUD_PoELCv1_0_mud**
Current IP Address:
Location: **Location ➜ All Locations**

Applications | Attributes | Authentication | Threats | Vulnerabilities

General Attributes

Description	
Static Assignment	true
Endpoint Policy	IOT-MUD-mud_poe_dev_interact_lighting_MUD_PoELCv1_0_mud
Static Group Assignment	true
Identity Group Assignment	IOT-MUD-mud_poe_dev_interact_lighting_MUD_PoELCv1_0_mud

1



2

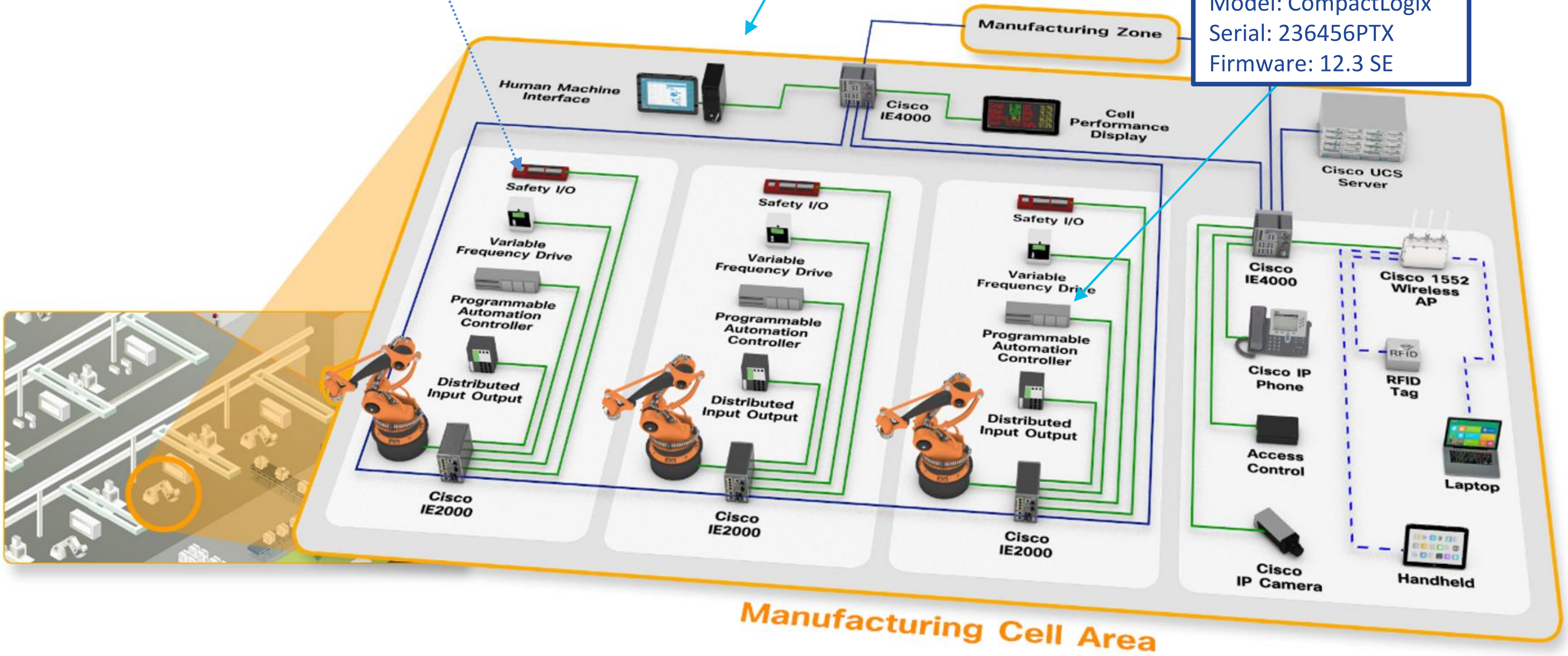
IOT-manufacturer	mud_poe_dev_interact_lighting
IOT-model	MUD_PoELCv1_0_mud
StaticGroupAssignment	true
Total Certainty Factor	10
lldpChassisId	04:00:17:88:0c:72:1b
lldpPortId	03:00:17:88:0c:72:1b
lldpUndefined127	00:01:42:01:05
mud-url	https://mud.poe.dev.interact.lighting.com/MUD/PoELCv

3

Manufacturing floor – Cell Area Zones

Human machine interface

Devices(process focused)



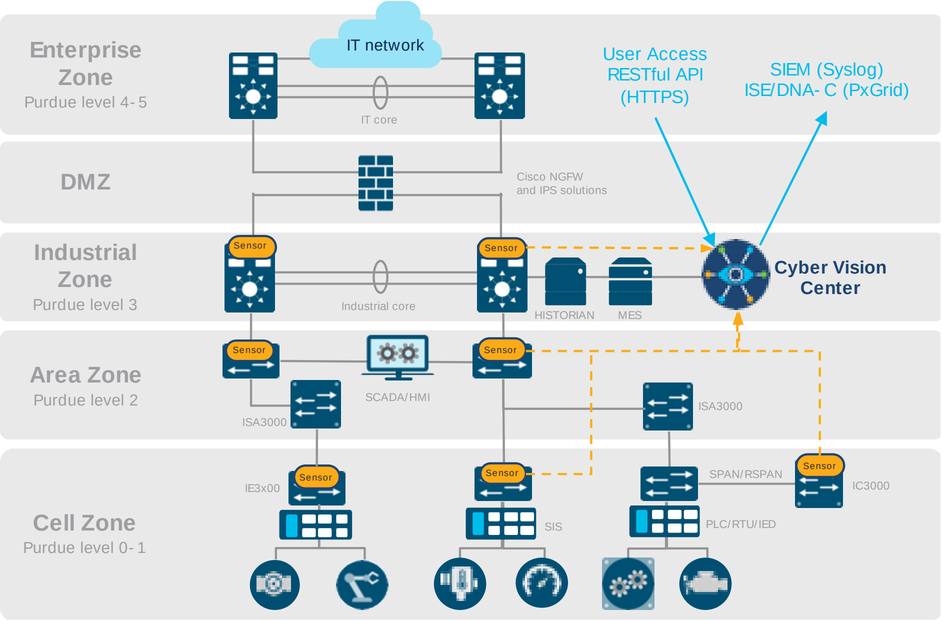
IND

Asset Identity

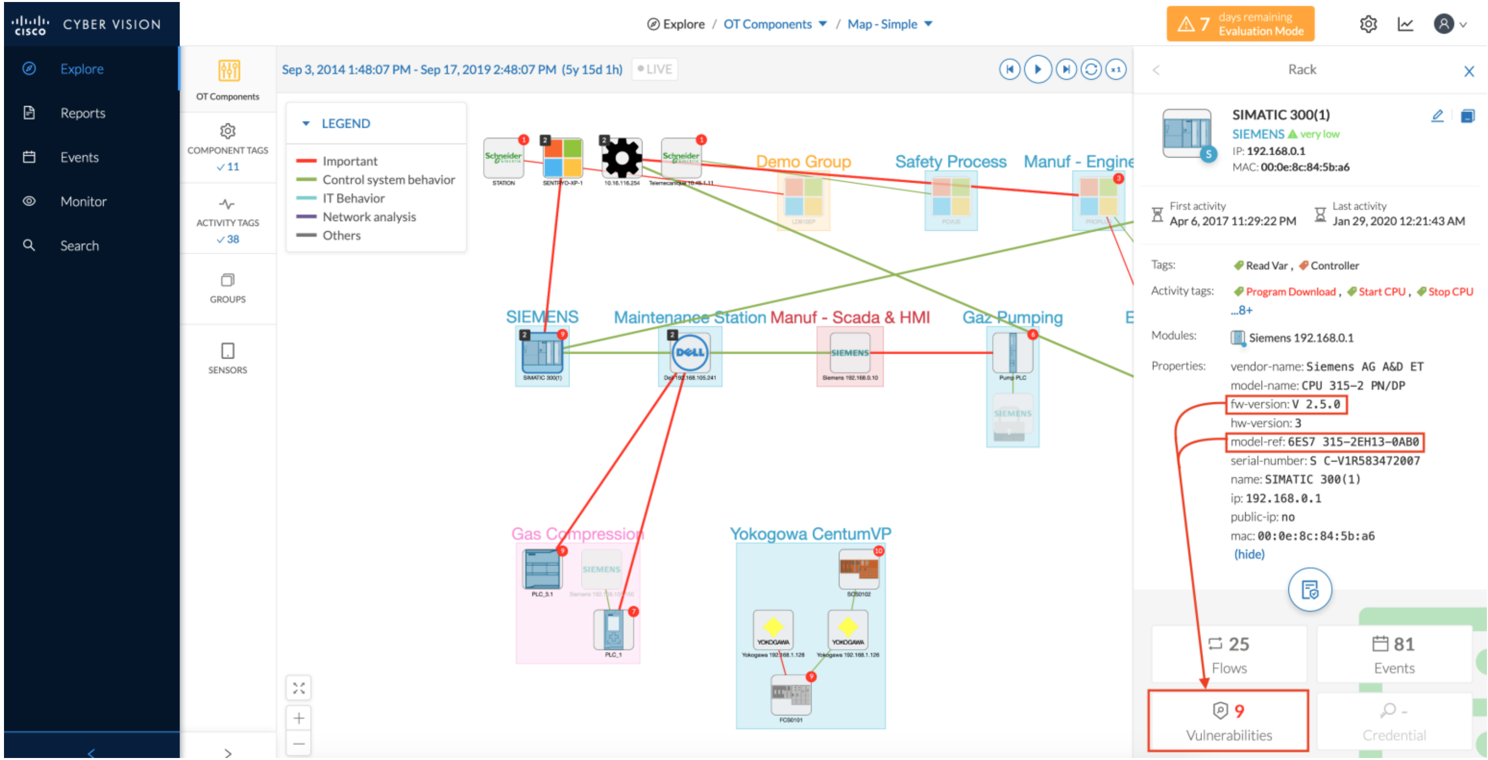
Device: PLC
Vendor: Rockwell
Model: CompactLogix
Serial: 236456PTX
Firmware: 12.3 SE

Context – Cyber Vision

- Cyber Vision use Deep Packet Inspection on Industrial Protocols to **observe** :
  - *Asset Properties* (ex: Firmware version, Model Ref)
  - *Asset Behavior* (ex: Read/Write Variable, Start/Stop CPU, Download Program)
  - *Asset Variables* (ex: MW 300.1 or TEMPVALVE1)
  - Network Statistics (ex: number of packets)



Example



Sep 3, 2014 1:48:07 PM - Sep 17, 2019 2:48:07 PM (5y 15d 1h)

LEGEND

- Important
- Control system behavior
- IT Behavior
- Network analysis
- Others

Rack

SIMATIC 300(1)
SIEMENS very low
IP: 192.168.0.1
MAC: 00:0e:8c:84:5b:a6

First activity Apr 6, 2017 11:29:22 PM
Last activity Jan 29, 2020 12:21:43 AM

Tags: Read Var, Controller

Activity tags: Program Download, Start CPU, Stop CPU ...8+

Modules: Siemens 192.168.0.1

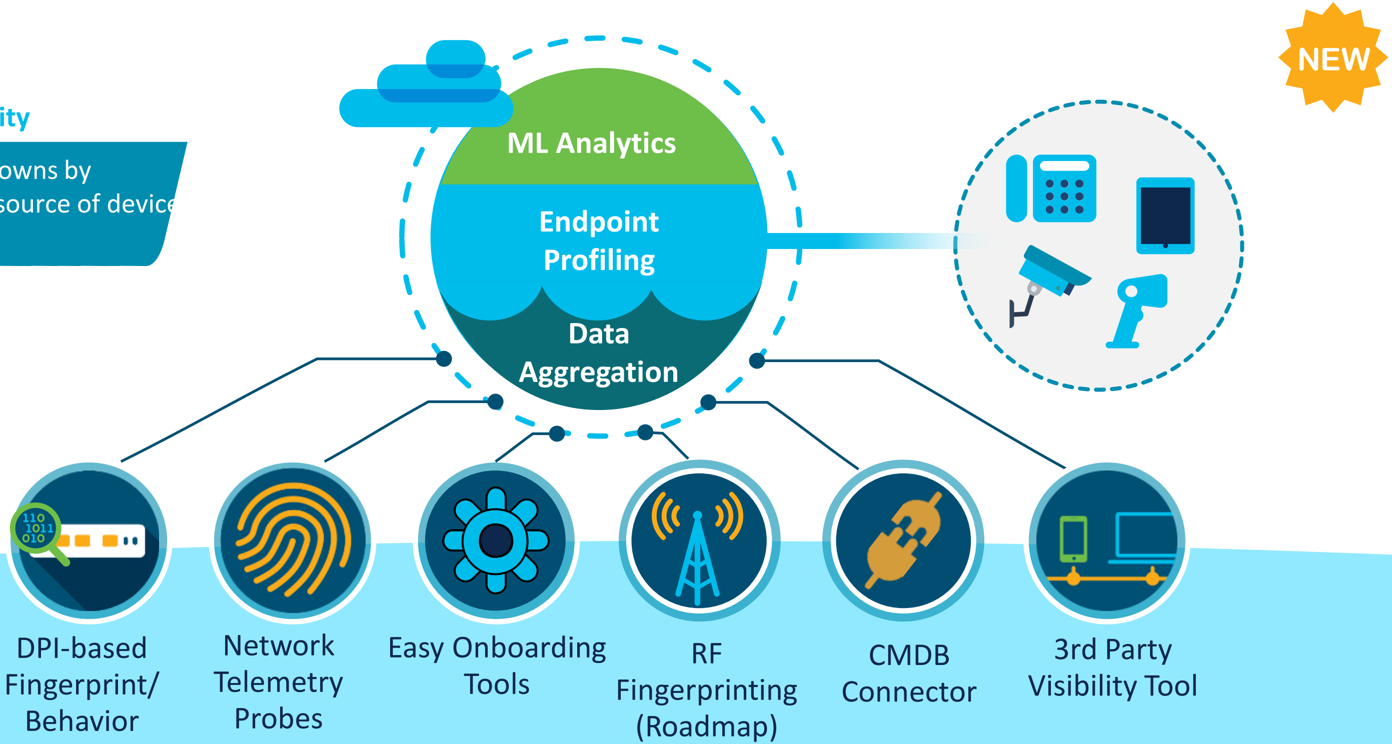
Properties:
vendor-name: Siemens AG A&D ET
model-name: CPU 315-2 PN/DP
fw-version: V 2.5.0
hw-version: 3
model-ref: 6ES7 315-2EH13-0AB0
serial-number: S C-V1R583472007
name: SIMATIC 300(1)
ip: 192.168.0.1
public-ip: no
mac: 00:0e:8c:84:5b:a6
(hide)

25 Flows
81 Events
9 Vulnerabilities
- Credential

Learned: Endpoint Analytics on Cisco DNA Center

High Fidelity Visibility

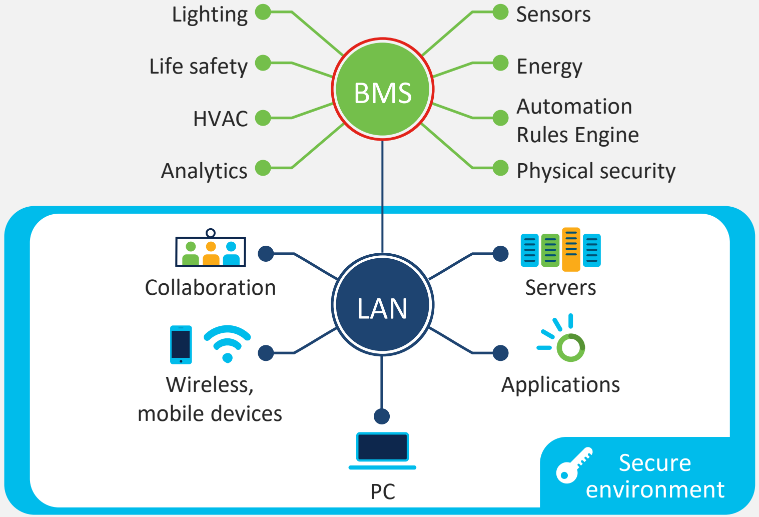
Rapidly reduce unknowns by aggregating various source of device fingerprints



Benefits - Convergence

Traditional approach

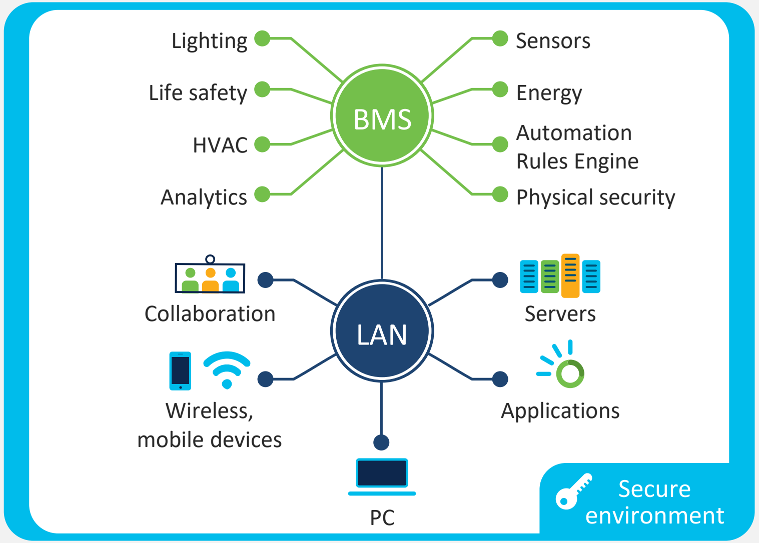
Although BMS is connected to the LAN, advanced security features are not used.



Cisco security applied to traditional networked devices

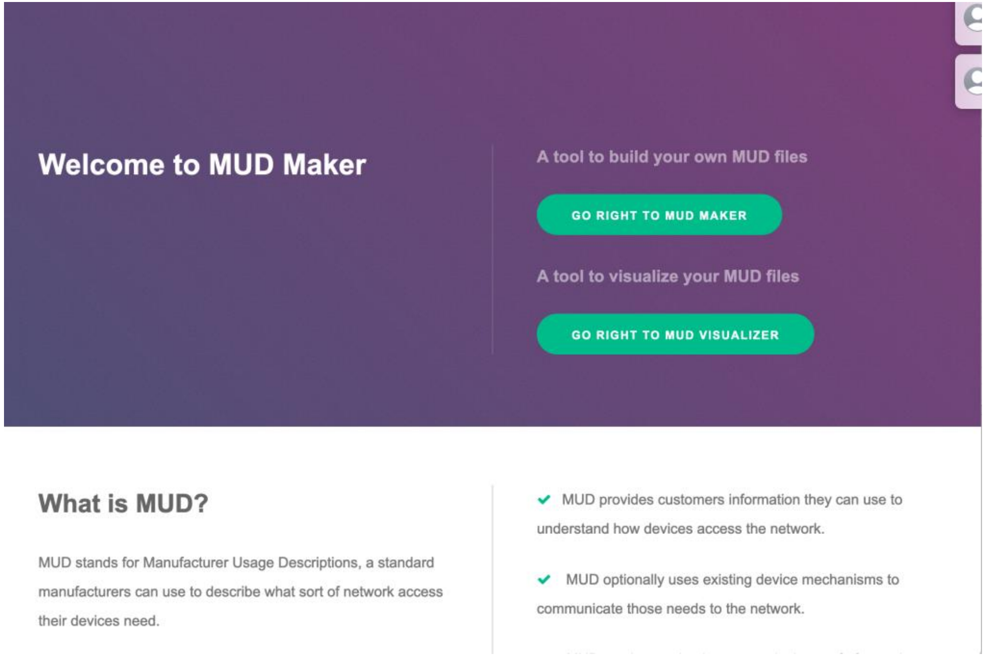
Converged approach

BMS and all smart building automation and control systems are connected by Cisco technology.



Cisco security applied to all networked devices including BMS

Mud Maker



Welcome to MUD Maker

A tool to build your own MUD files

A tool to visualize your MUD files

What is MUD?

MUD stands for Manufacturer Usage Descriptions, a standard manufacturers can use to describe what sort of network access their devices need.

- ✓ MUD provides customers information they can use to understand how devices access the network.
- ✓ MUD optionally uses existing device mechanisms to communicate those needs to the network.

How easy is it to implement Manufacturer Usage Descriptions?

LLDP	DHCP	Device Certificates

# sh lldpmud https://example.com/mudfiles/device	In dhclient.conf: 	
	
	option mudurl code 161 = text;
	send mudurl "https://example.com/mudfiles/device";
		(Modified X.509 config)

In systemd: [LLDP] MUDURL=”https://example.com/…”	In systemd: [DHCPv4] MUDURL=“https://example.com/...” [DHCPv6] MUDURL=“https://example.com/...”	
NetworkManager set connection.mud-url “https://example.com/...”		

Something the industry is thinking about…

- Spotting problems on devices early
  - Software Bills of Materials (SBOMs)
- If hackers already know your vulnerabilities, shouldn’t you?
- If you know, what can you do?
- MUD is being extended to find SBOMs

Next Steps

- Try out some of the tools
  - www.mudmaker.org
- Read the standard: RFC 8520
- Read the NIST NIST work of DDOS Protection with MUD
  - https://csrc.nist.gov/publications/detail/sp/1800-15/draft
- Read Cisco IoT Onboarding Paper
  - https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/white-paper-c11-743623.html
- Work with one of your vendors to implement it
- Get visibility

Protecting the device

- RFC 8519 – the ACL Model
- IEEE 802.1X and 802.1AR – identifying the device
- RFC 8520 – Manufacturer Usage Descriptions
- NIST-1800-5 NIST recommendations on using MUD
- RFC 2131 DHCP
- IEEE 802.1AB – LLDP to announce MUD file

Thank you

Possibilities

#CiscoLive