Improving IoT Security: the role of the manufacturer

Eliot Lear

Introduction

A View Through a Light Bulb

- Connected Spaces is a big deal
- Automated and efficient lighting
- Room assignment and scheduling
- Changing of conditions for different customer profiles

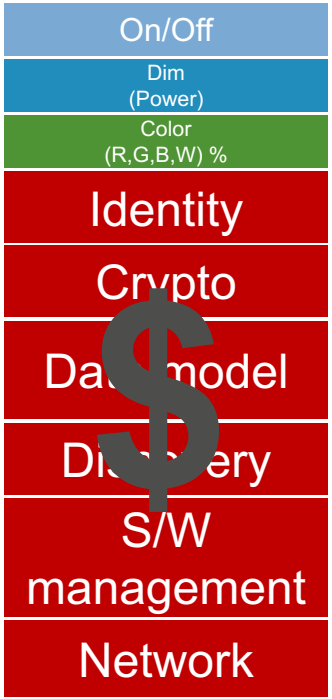
A non-networked light bulb

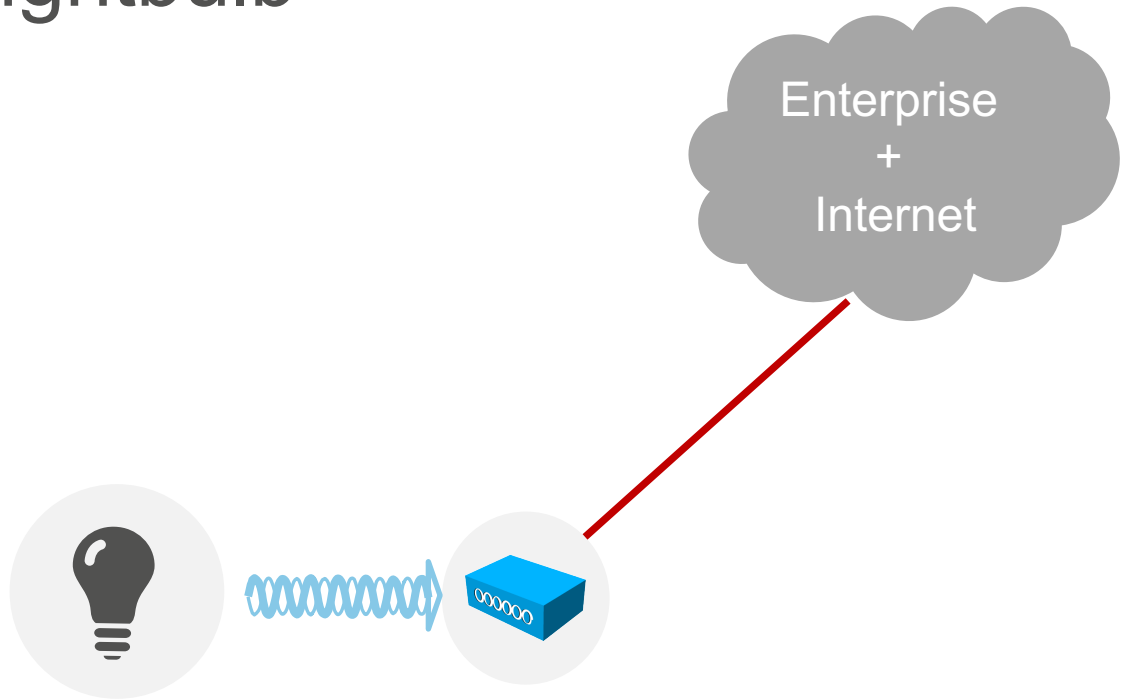
On/Off

Dim
(Power)

Color
(R,G,B,W) %

A networked lightbulb





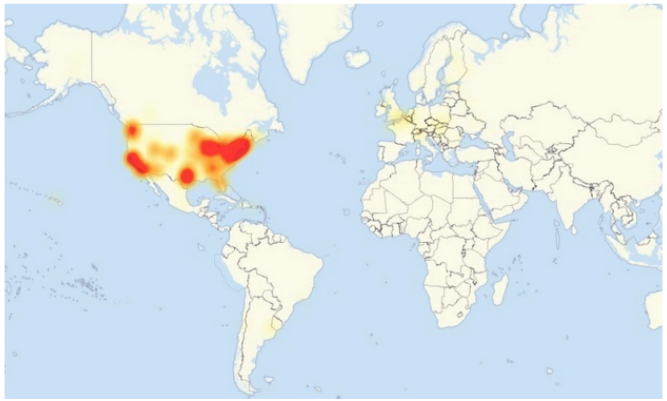
What do manufacturers wish to avoid

NETWORKWORLD FROM IDG

INSIDER Sign In | Register

Home > Security

Chinese firm admits its hacked products were behind Friday's massive DDOS attack



A map of Friday's massive DDOS attack and the internet outages involved. *Credit: Downdetector*

Botnets created from the Mirai malware were involved in Friday's cyber attack

By Michael Kan | Follow
IDG News Service | Oct 23, 2016 12:01 PM PT

RELATED

IoT botnets used in unprecedented DDoS against Dyn DNS; FBI, DHS investigating

IoT botnets powered by Mirai continue to grow

Record IoT DDoS attacks raise bar for defenders

on IDG Answers
Can company see that I'm using their internet?


SECTIONS

The New York Times

TECHNOLOGY

Why Light Bulbs May Be the Next Hacker Target

By JOHN MARKOFF NOV. 3, 2016

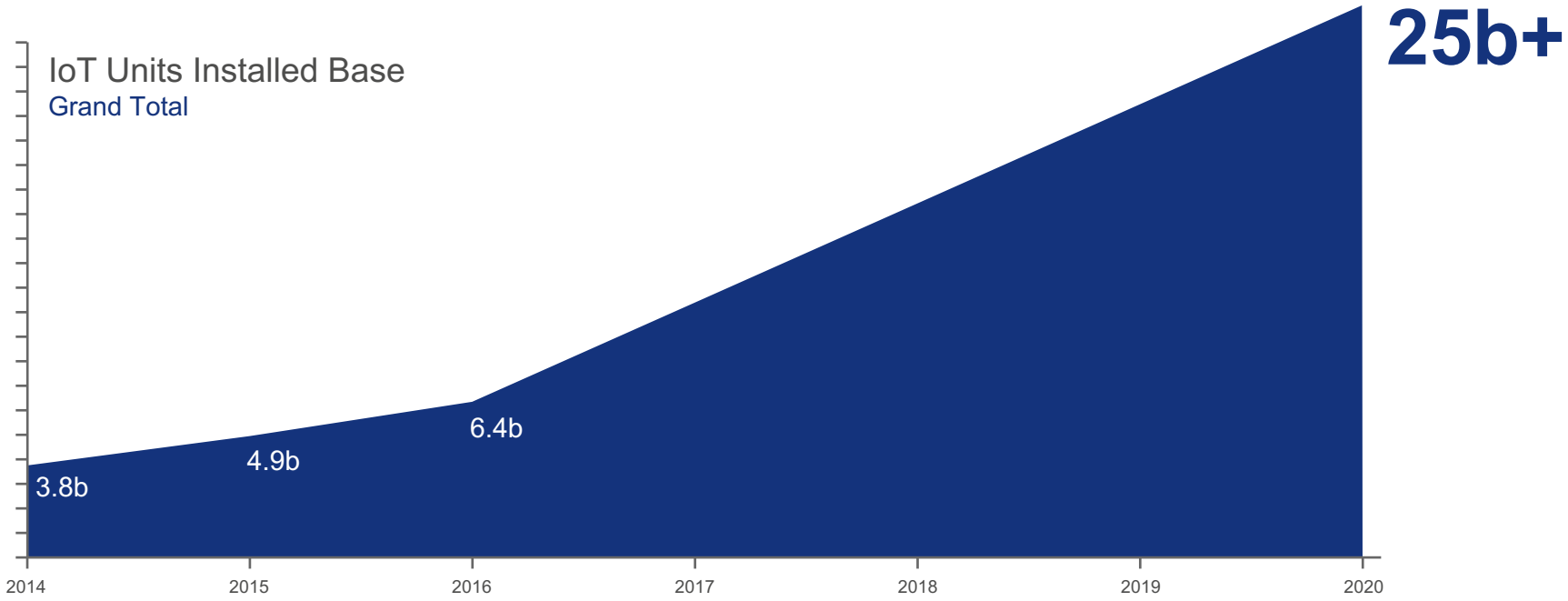
General Threats To Defend Against

- Direct: Attacker causes device to not perform its function or to malfunction

By AMIR MARINE (Wikimedia) - Own work, CC BY-SA 3.0,

- Indirect: Attacker uses device to attack other systems

The latest IoT Growth Chart



Source: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

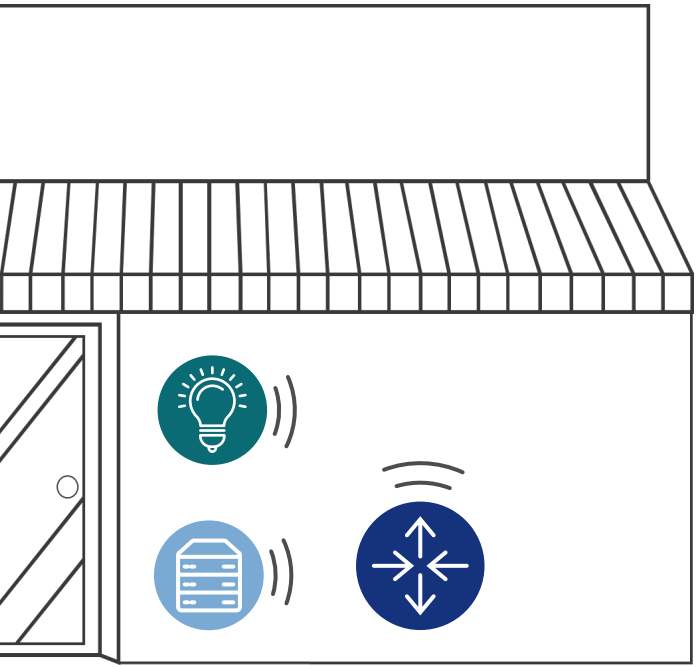
The Network Administrator's Problem: Number of **Types** of Things

Cost of configuration

Static environments

Dynamic systems

How to secure manageability and security?



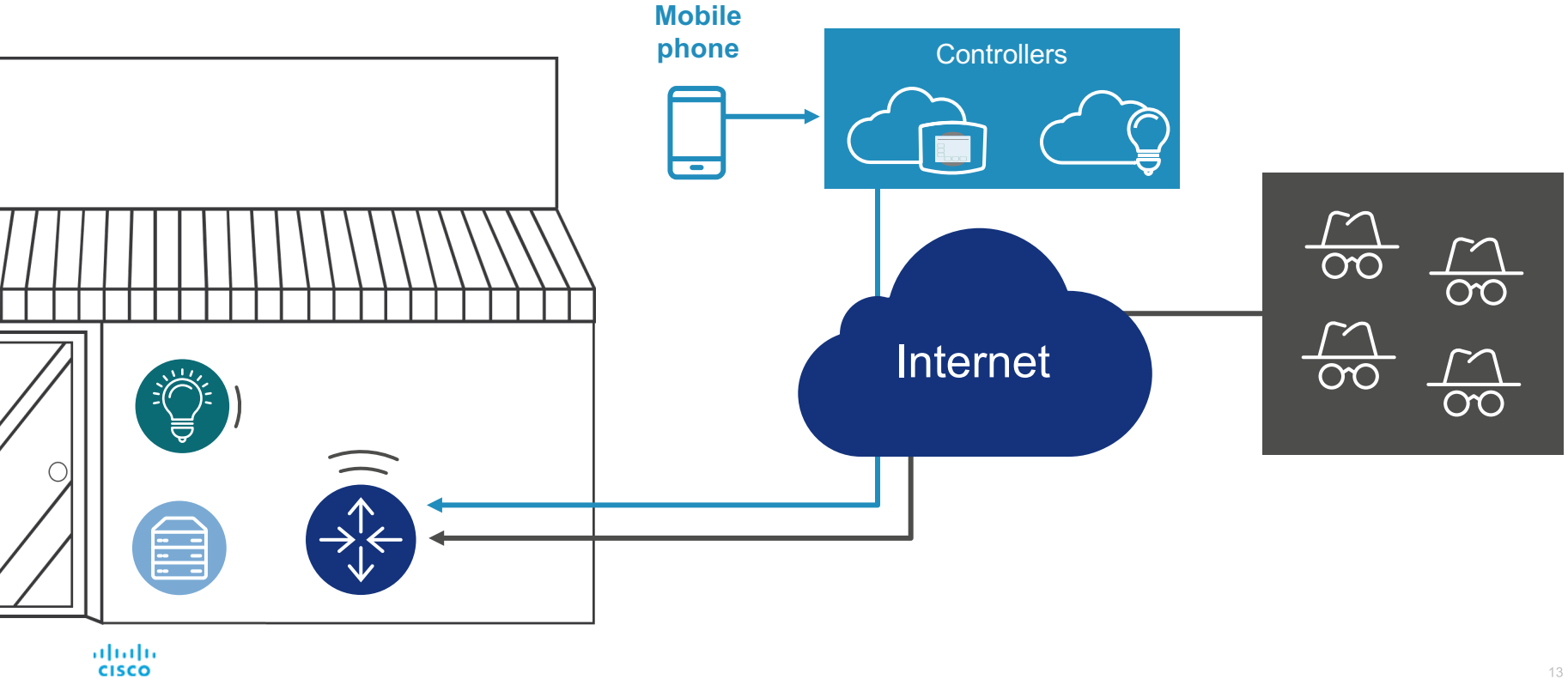
Device protects itself

- Secure development practices

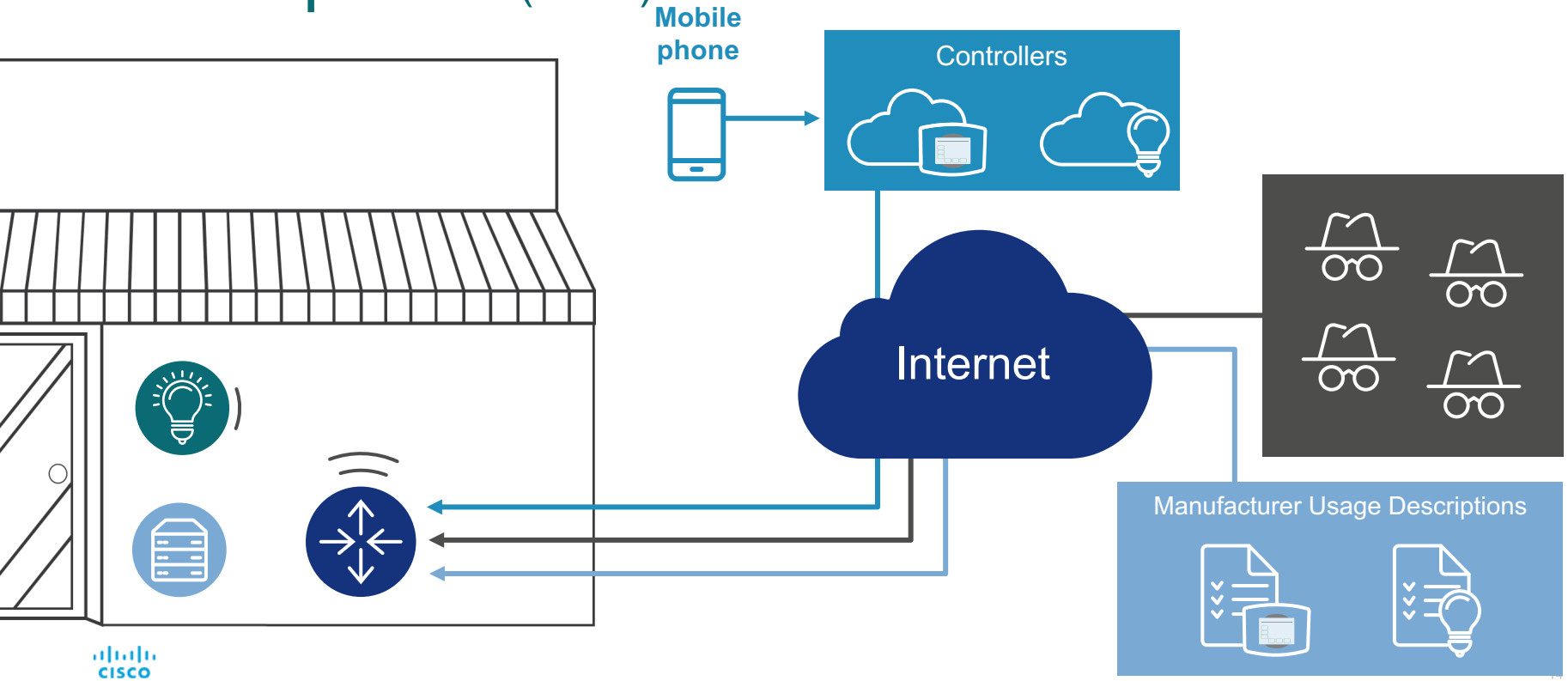
Network protects device

- Device identification
- Automated segmentation

Understanding the Attack Surface



Introducing the Manufacturer Usage Descriptions (MUD)



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, it all other uses must be unintended
Things are tightly constrained. CPU and memory resource constraints are tight.	Any intended use can be clearly identified
Even those Things that can protect themselves today may not be able to do so tomorrow	All other uses can be warned against in a statement
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to make the distinction

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

The MUD File

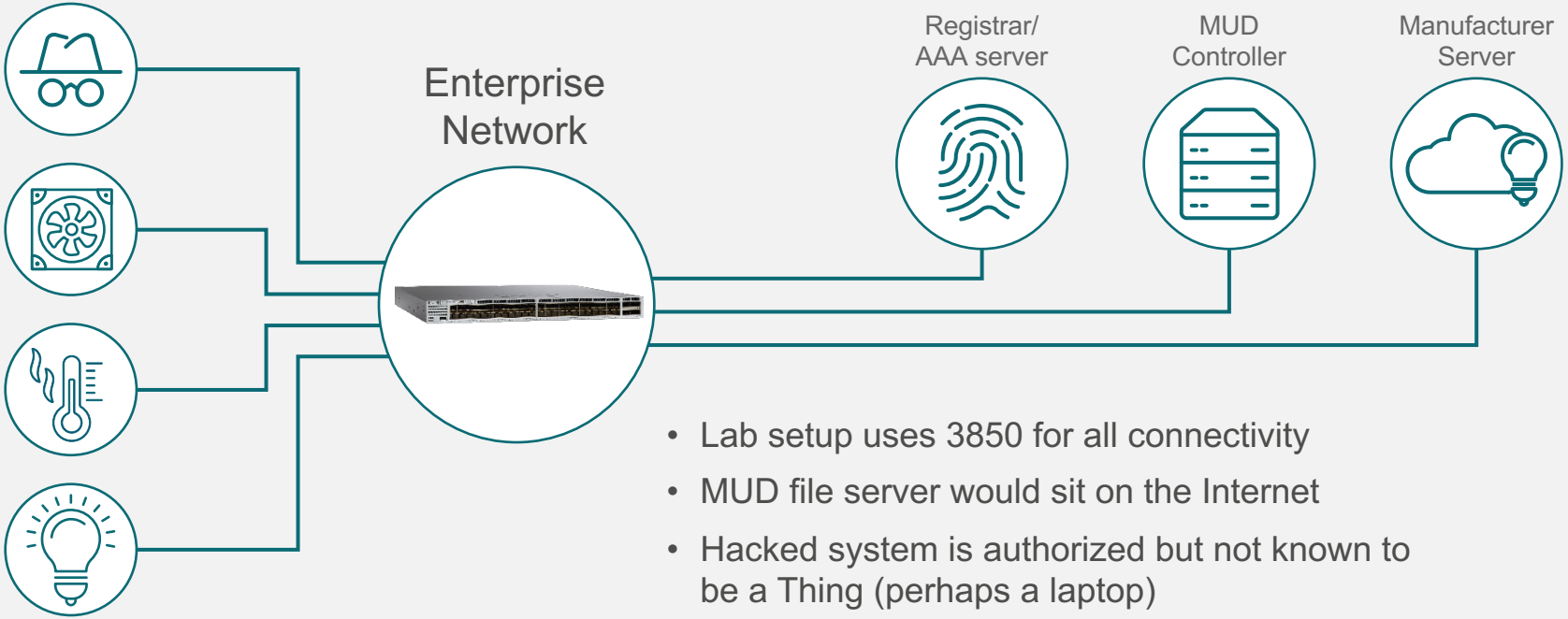
```
{
 "ietf-mud:meta-info": {
  "lastUpdate": "2017-06-06T01:19:25+02:00",
  "masa-server": "http://masa.lightingmfg.com",
  "systeminfo": "luminaire",
  "cacheValidity": 1440
 },
 "ietf-acl:access-lists": {
  "acl": [
   {
    "acl-name": "mud-37632-v4in",
    "acl-type": "ipv4-acl",
    "ietf-mud:packet-direction": "to-device",
    "access-list-entries": {
     "ace": [
      {
       "rule-name": "myctlout0-in",
       "matches": {
        "ietf-mud:direction-initiated": "from-device",
        "ietf-mud:my-controller": [
         null
        ],
         "protocol": 6,
        "source-port-range": {
         "lower-port": 1883,
         "upper-port": 1883
        }
       },
      },
       "actions": {
        "permit": [
         null
        ]
       }
      }
     ]
    }
   },
 ...
```

MUD File Abstractions in Practice

my-controller == permit to a DNS host

same-manufacturer = use VLAN or SGT segment

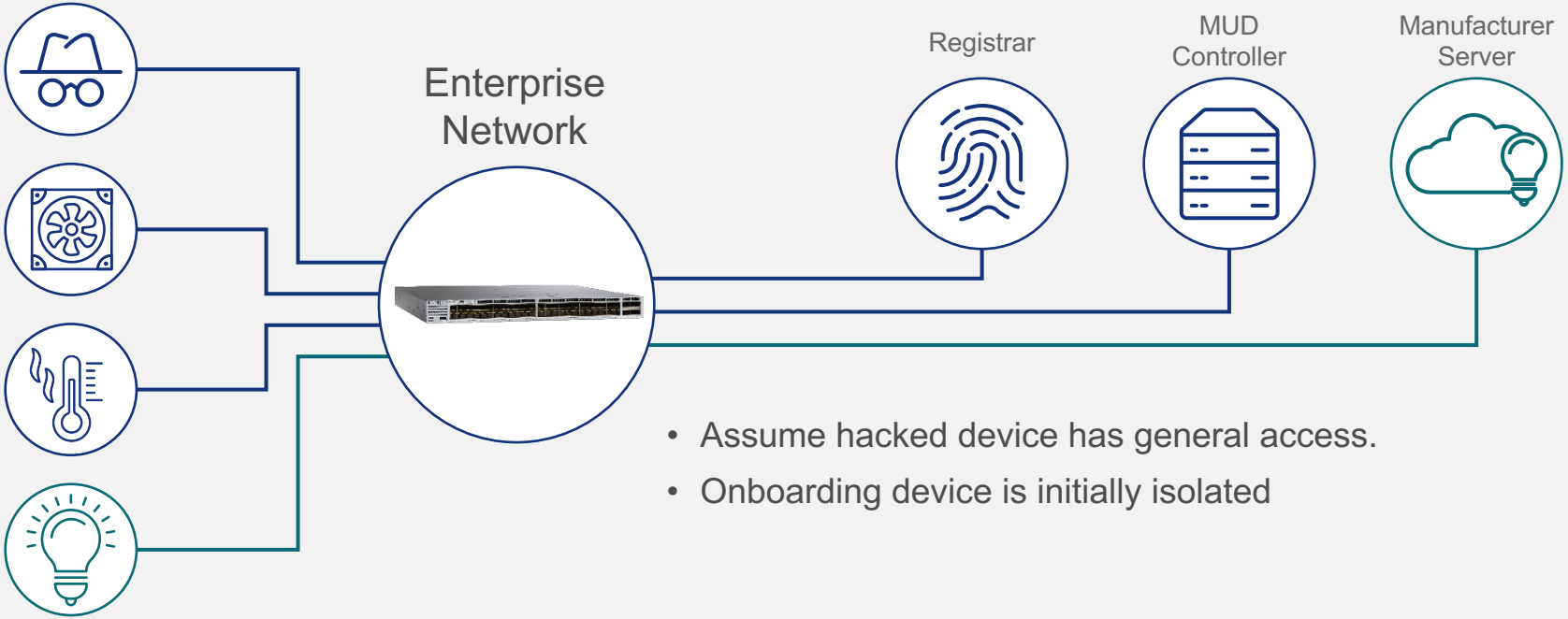
Initial Configuration



- Lab setup uses 3850 for all connectivity
- MUD file server would sit on the Internet
- Hacked system is authorized but not known to be a Thing (perhaps a laptop)

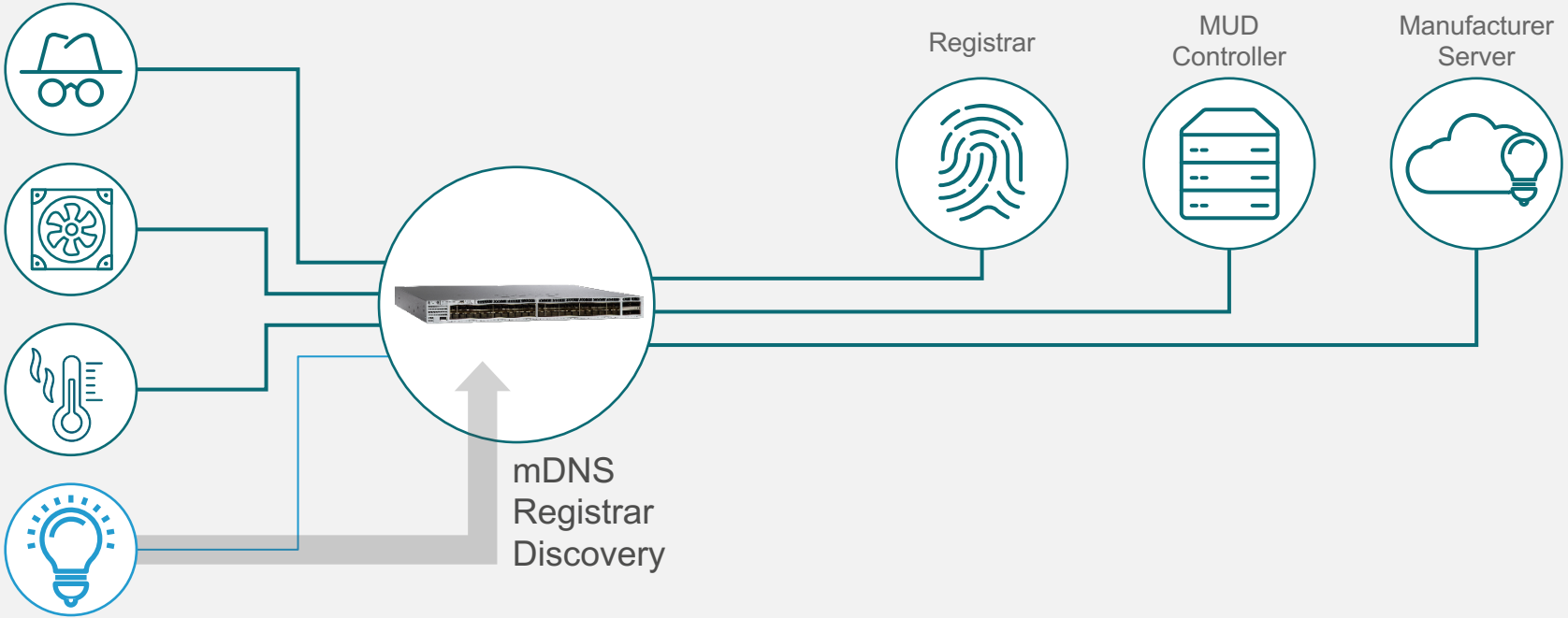
Onboarding Process

Device Connects

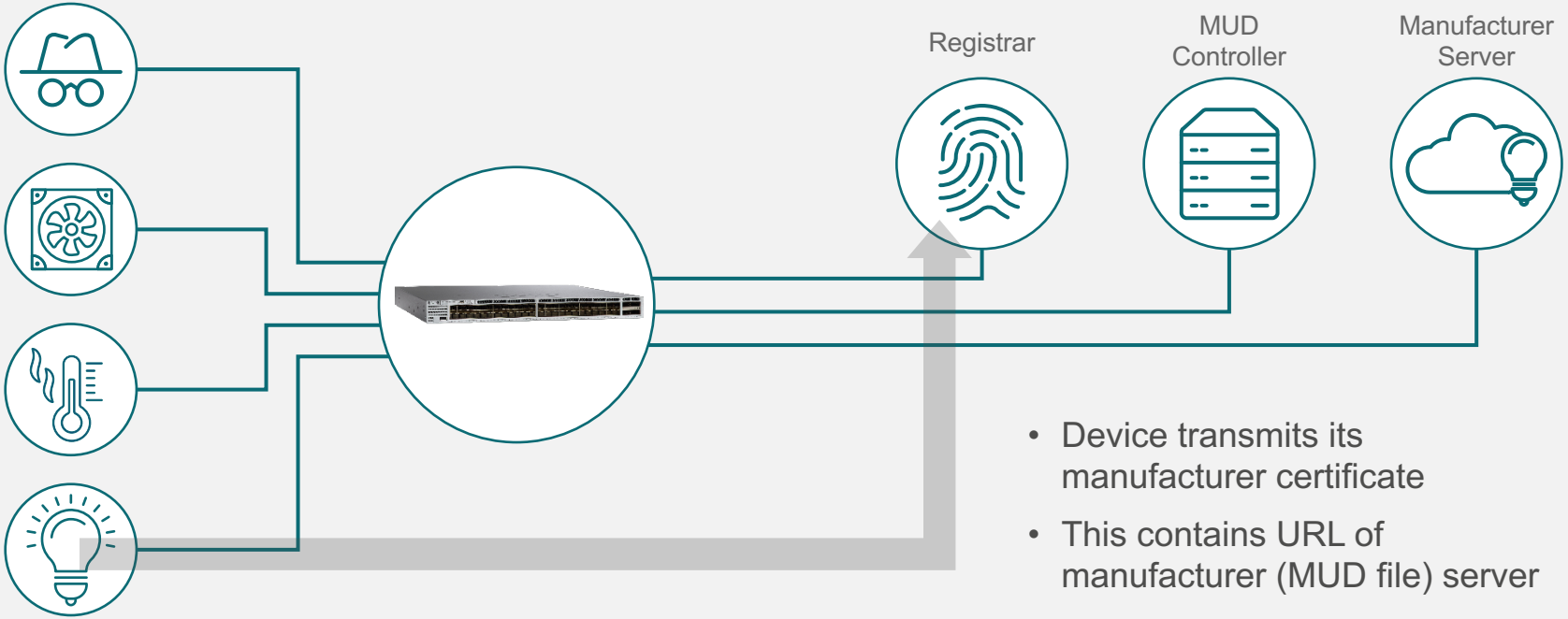


- Assume hacked device has general access.
- Onboarding device is initially isolated

Bootstrap
Find Registrar



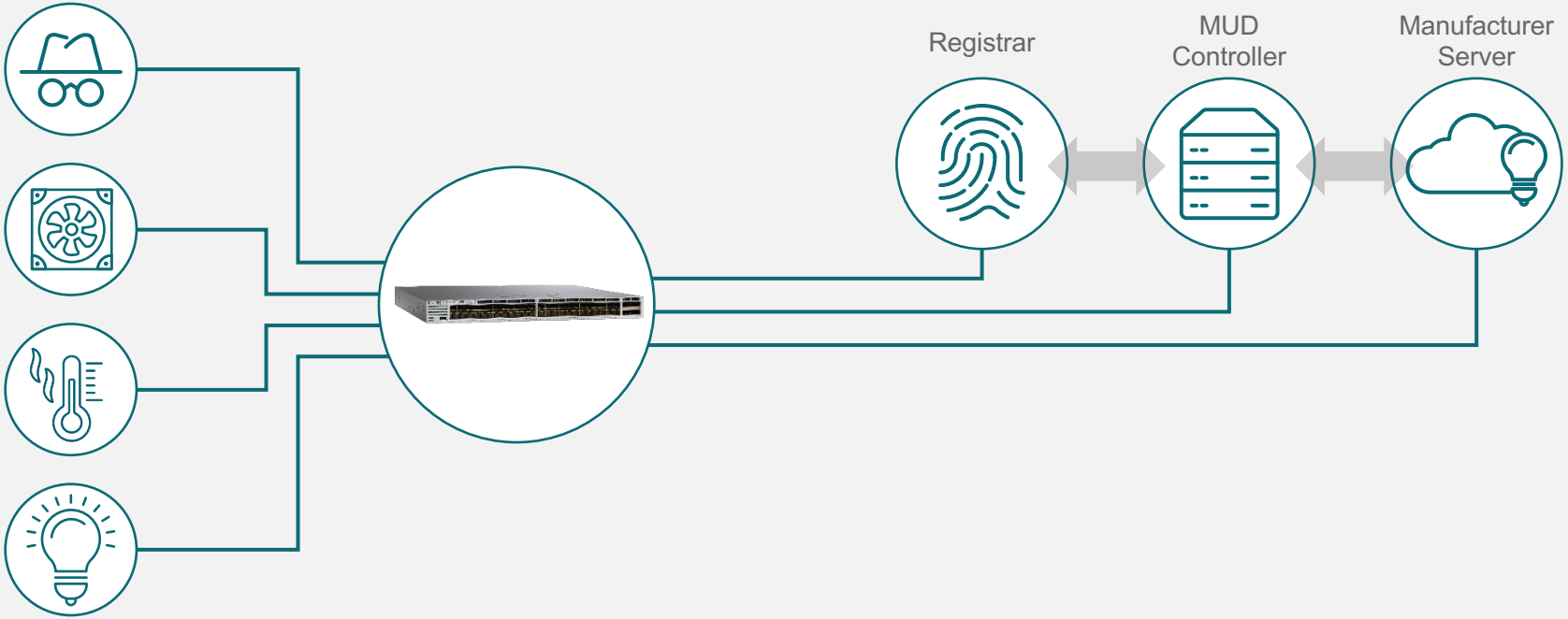
Bootstrap
Initiate Registration



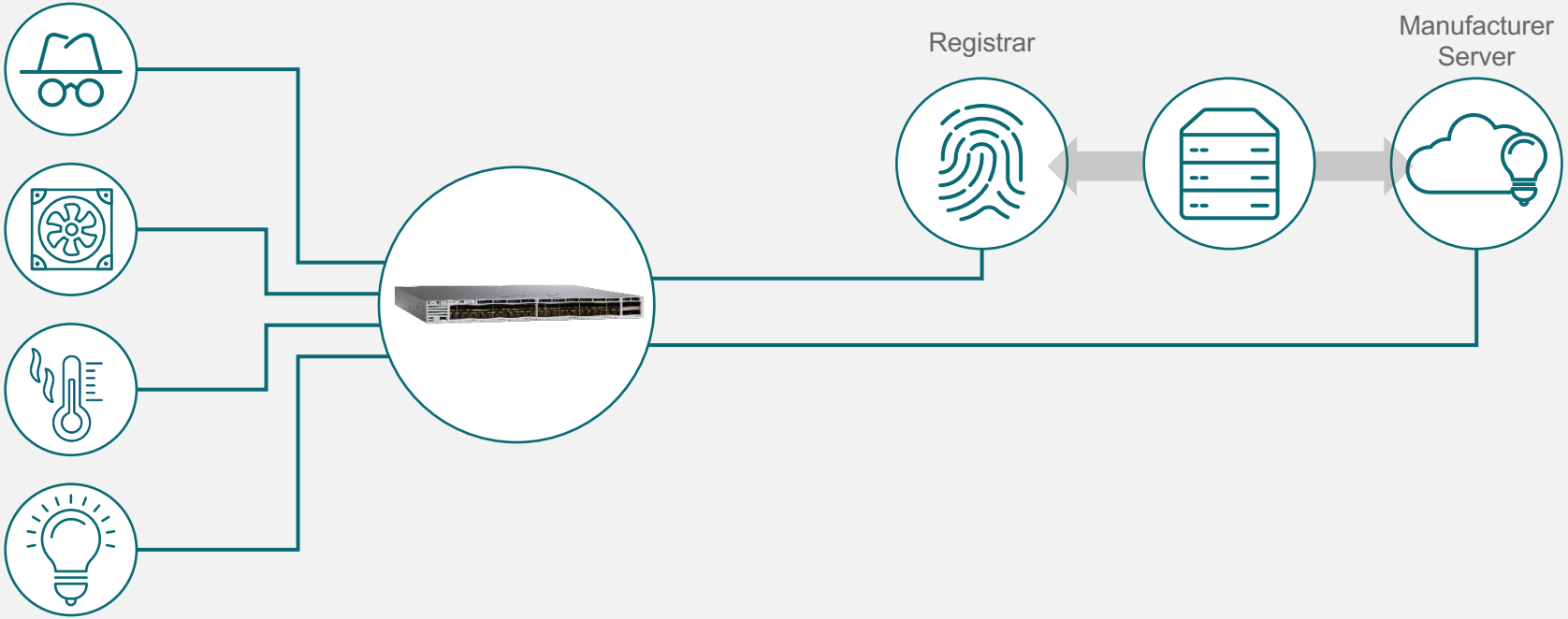
- Device transmits its manufacturer certificate
- This contains URL of manufacturer (MUD file) server

Bootstrap

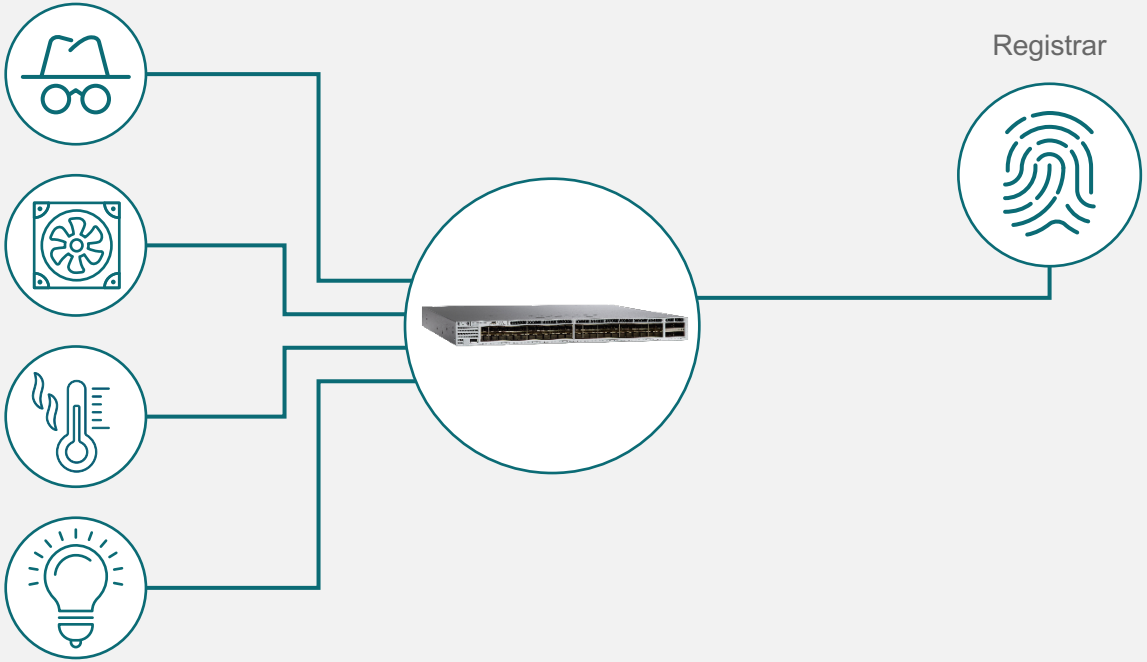
Retrieve MUD File from Manufacturer, to Find MASA Server



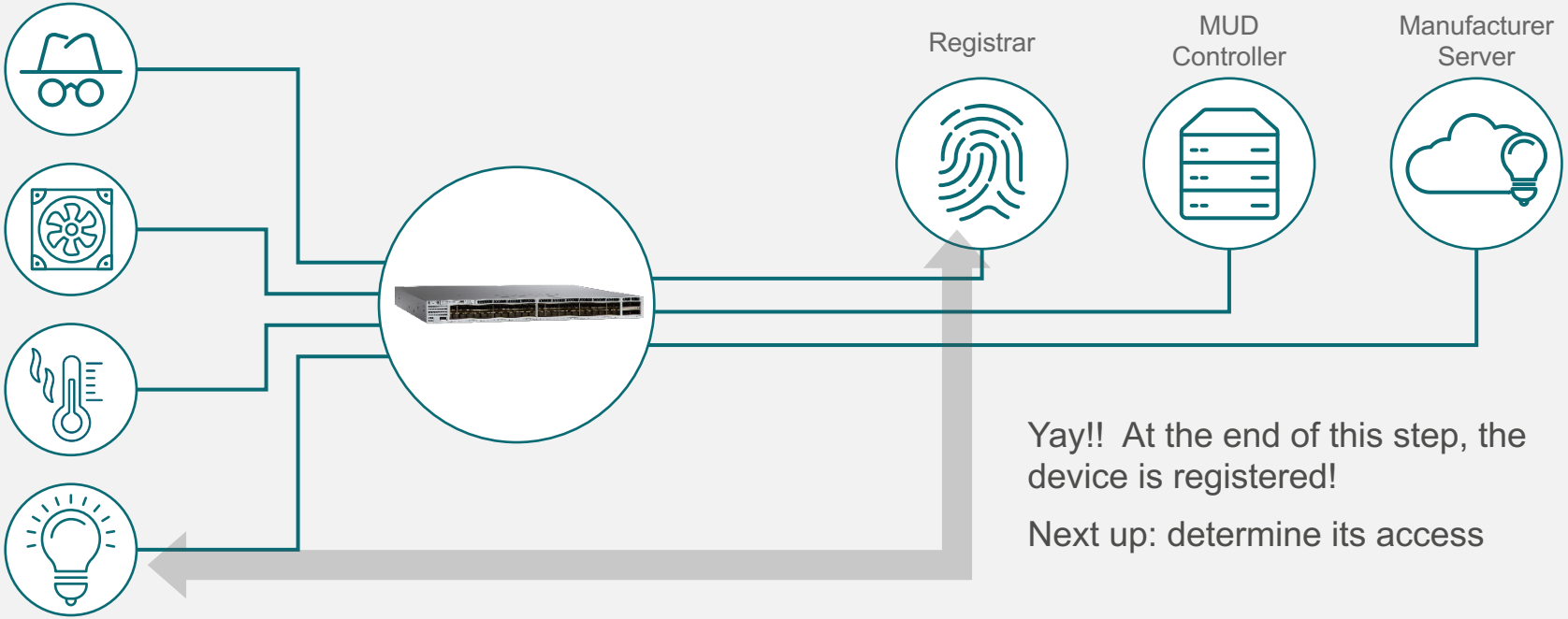
Request A Voucher to Send to the Device



Administrative Approval, if Required
(Probably Only First of This Type of Device)



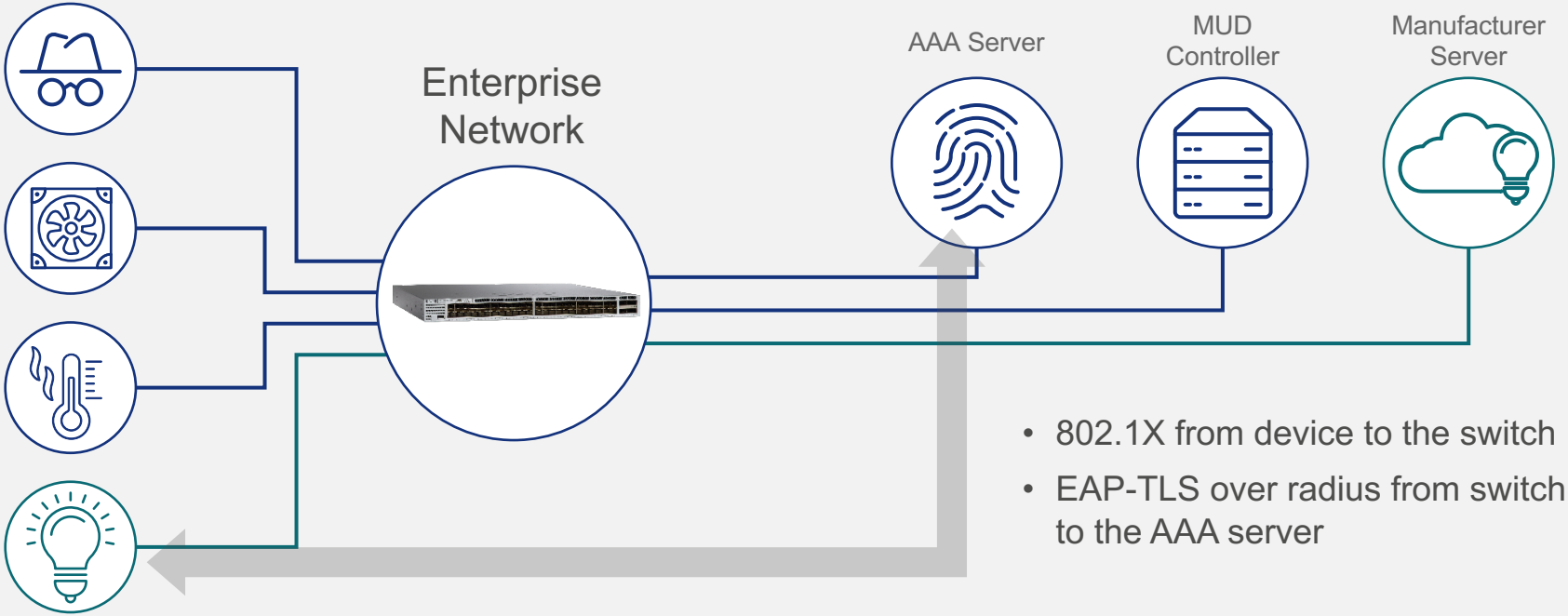
Install Trust Anchor and Perform EST Registration to Obtain A Local Certificate



Yay!! At the end of this step, the device is registered!

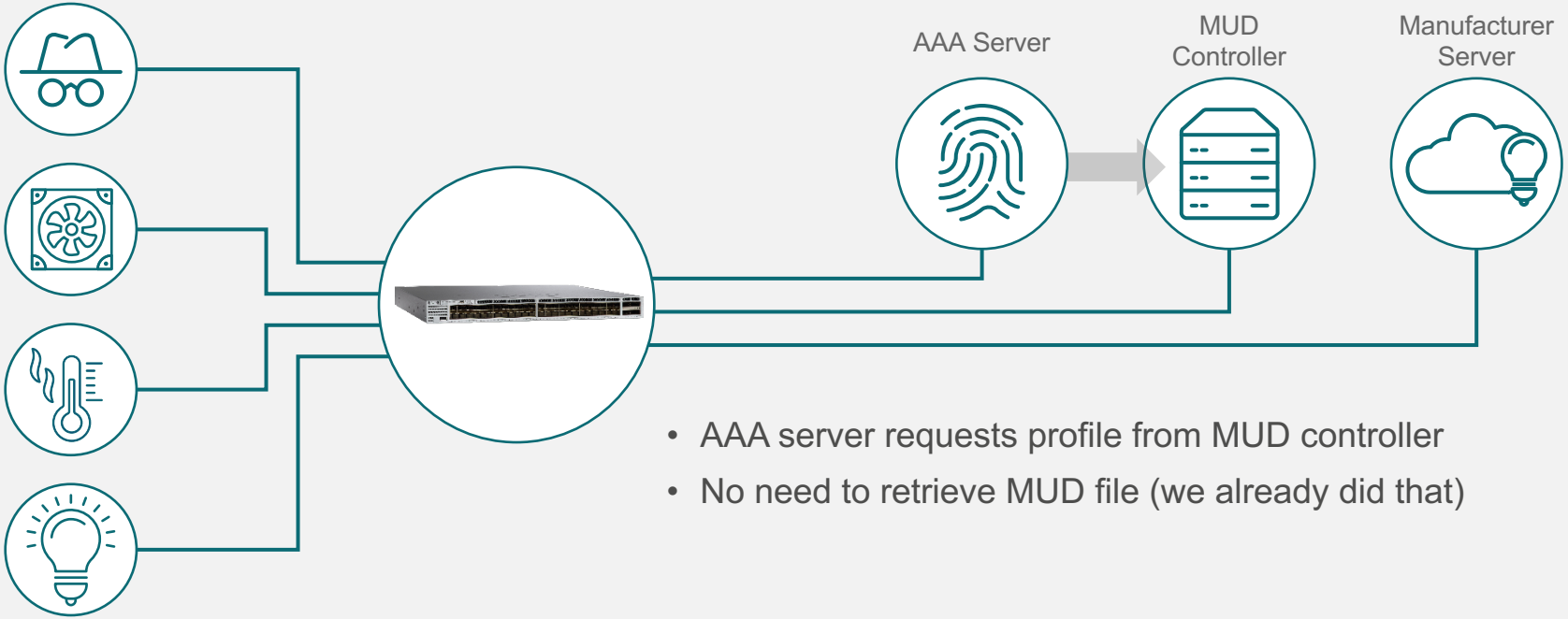
Next up: determine its access

Now Device Authenticates Using 802.1X



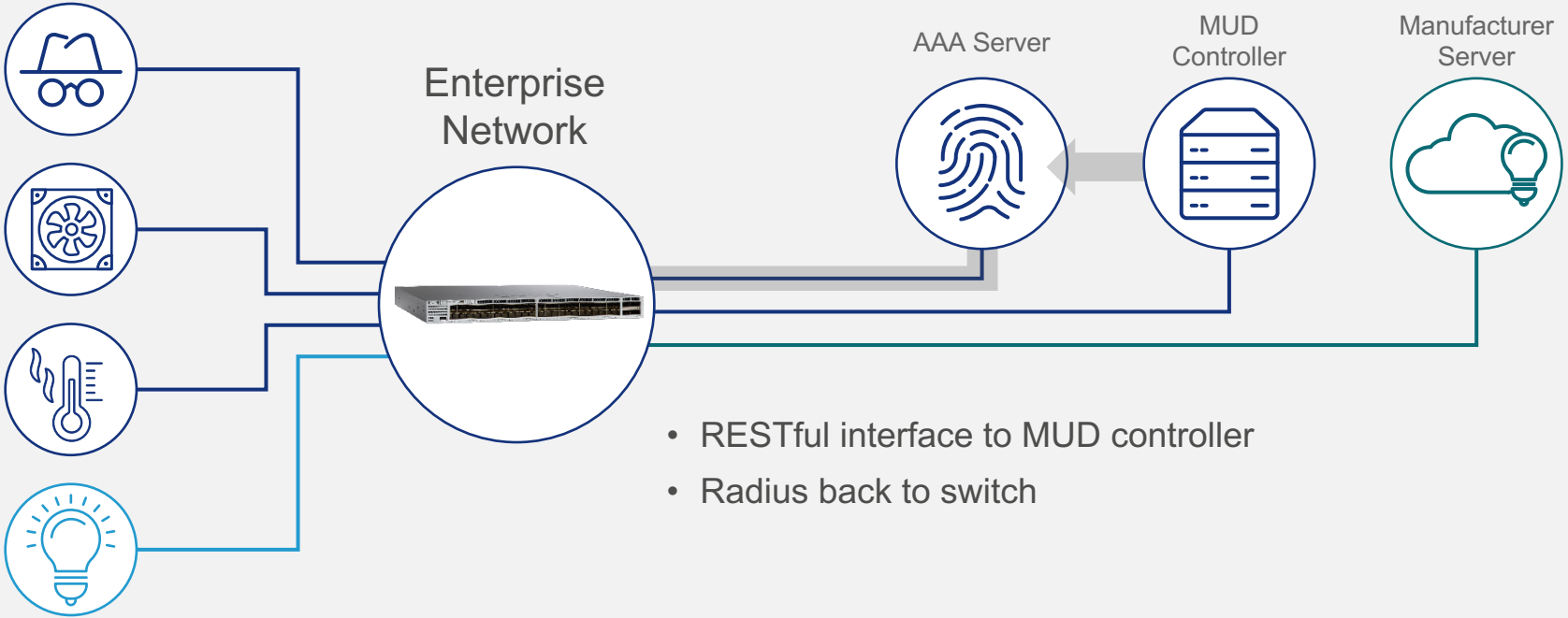
- 802.1X from device to the switch
- EAP-TLS over radius from switch to the AAA server

Determine Appropriate Authorization



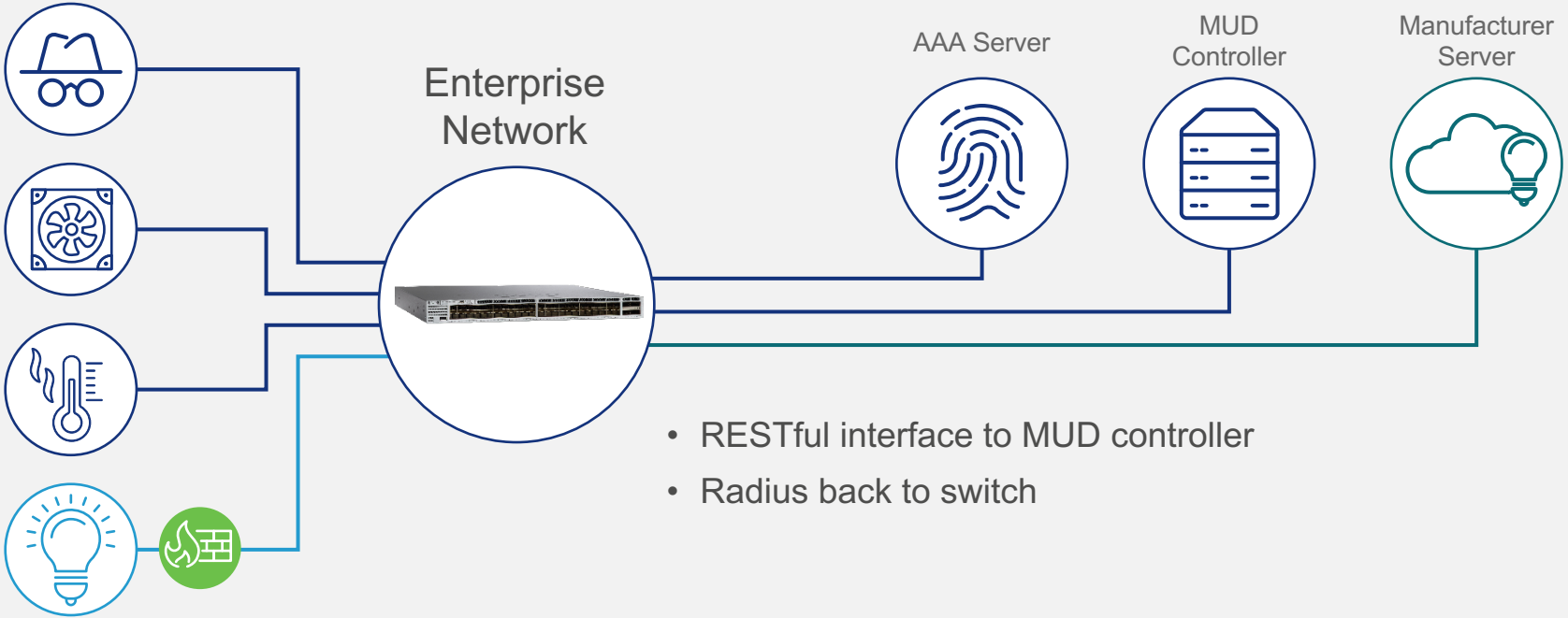
- AAA server requests profile from MUD controller
- No need to retrieve MUD file (we already did that)

Effect Change of Authorization



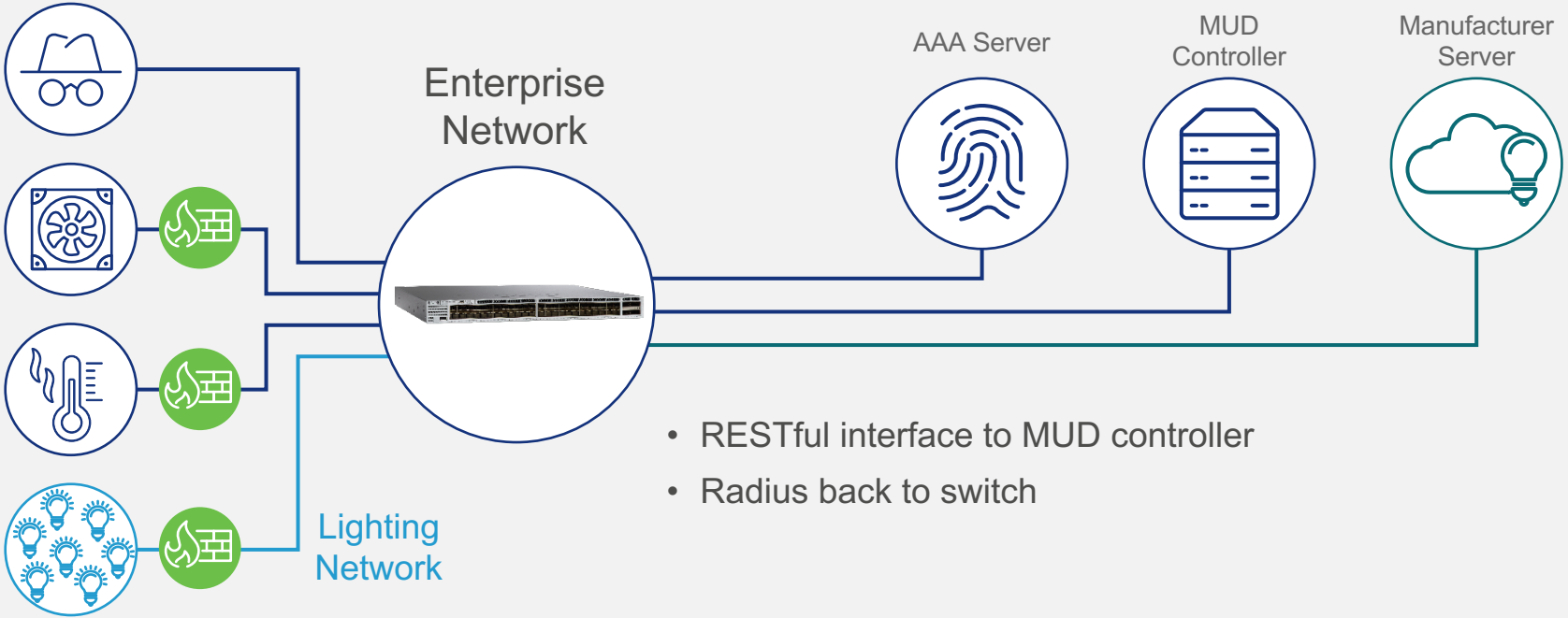
- RESTful interface to MUD controller
- Radius back to switch

Bad guy out of luck



- RESTful interface to MUD controller
- Radius back to switch

Devices Get Appropriate Segmentation



- RESTful interface to MUD controller
- Radius back to switch

How to locate the policy? A URL

https://mud.mfg.example.com/.well-known/mud/v1/CAS11LCDLversion2.12

"Manufacturer"

Model

Benefits

Customer

- Reduces threat surface of exploding number of devices
- Almost no additional CAPEX
- Avoids lateral infections in the network
- 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

What does it mean to be connected?

?

Open Access	Limited Access
Open Innovation, devices get 0wn3ed	Permission required to innovate, but safer applications.

Summary: Manufacturer Usage Descriptions

- A URI
- Use of {dhcp, EAP-TLS, lldp} to get it out
- Retrieval of a MUD file from a server
- Instantiation of class information onto the router

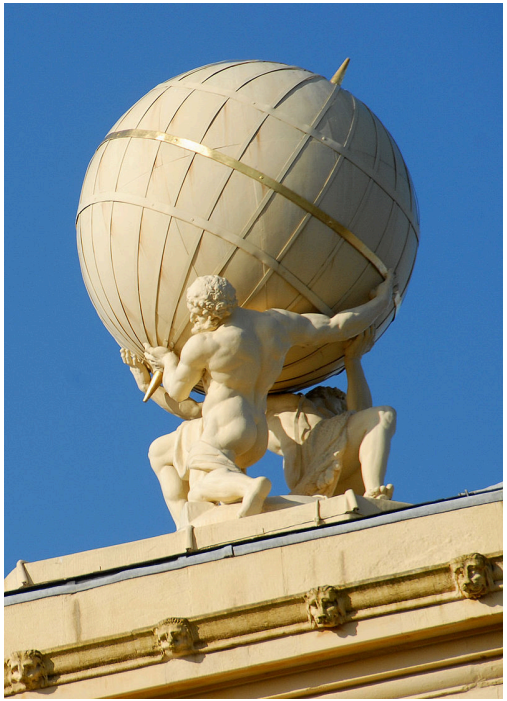
So… what should manufacturers do?

1. Recognize that they have to do some stuff
2. Make use of good coding practices (like turning off unused services)
3. Establish an incident response capability
4. Establish appropriate software management processes
5. **Identify device and its profile to the network**

(Nearly) all of this has been done by others!

Future work: the heavy lifting

- WPA Personal in is **suboptimal**



By Cwawebber - Own work, CC BY 3.0

More information

- mud-interest@cisco.com
- lear@cisco.com
- draft-ietf-opsawg-mud-07


CISCO