



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

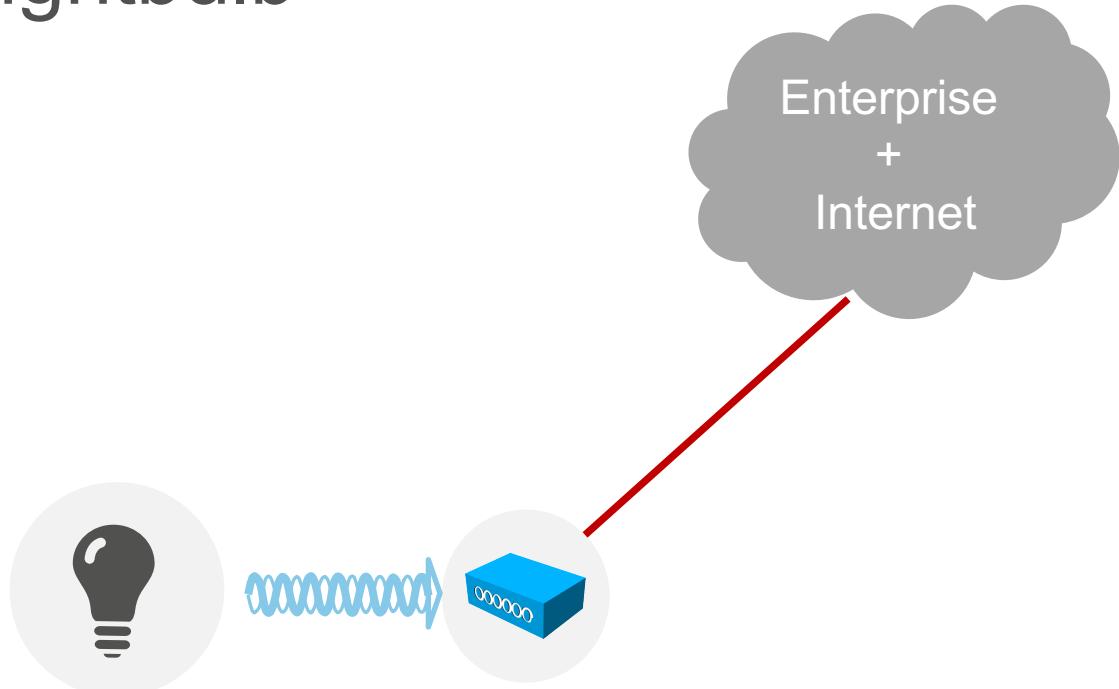


A non-networked light bulb



A networked lightbulb

On/Off
Dim (Power)
Color (R,G,B,W) %
Identity
Crypto
Data model
Discovery
S/W management
Network



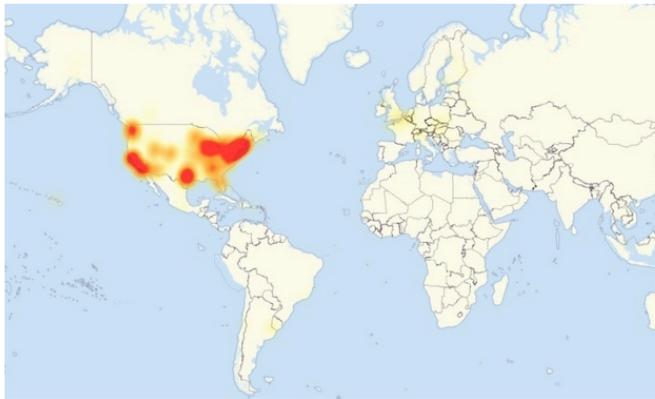
What do manufacturers wish to avoid

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

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?



By Michael Kan | Follow

IDG News Service | Oct 23, 2016 12:01 PM PT

≡ 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

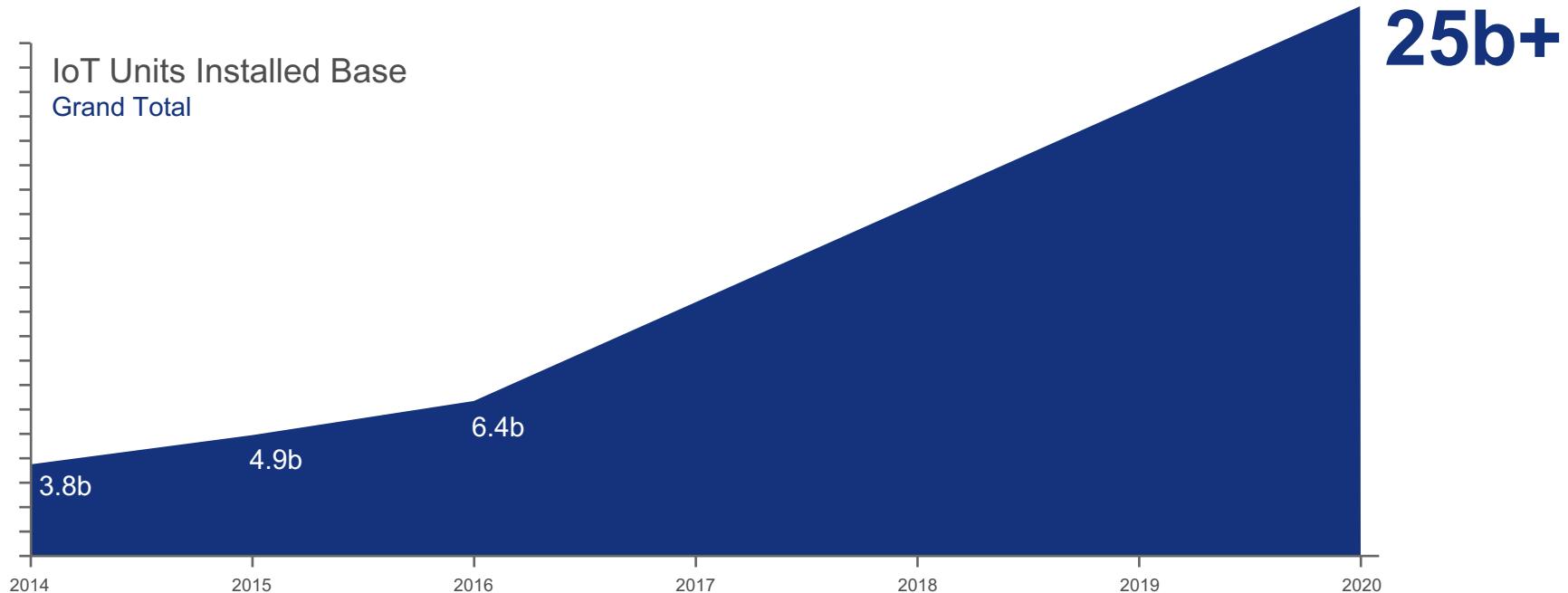
- Direct: Attacker causes device to not perform its function or to malfunction
- Indirect: Attacker uses device to attack other systems



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



The latest IoT Growth Chart



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

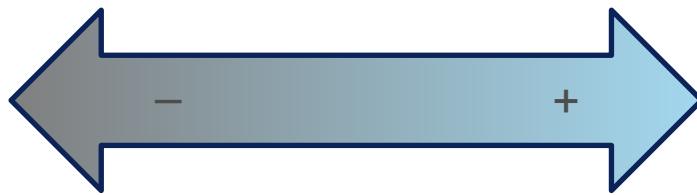
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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



Cost of configuration

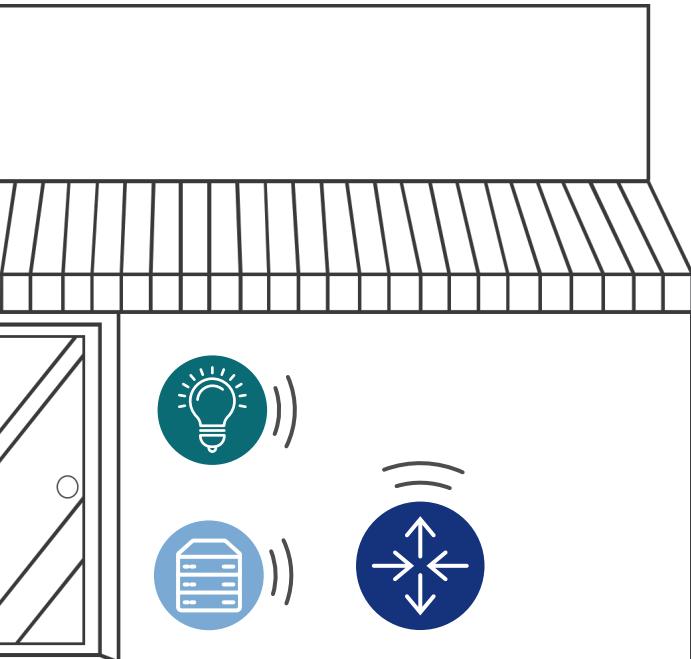
Static environments



Dynamic systems



How to secure manageability and security?



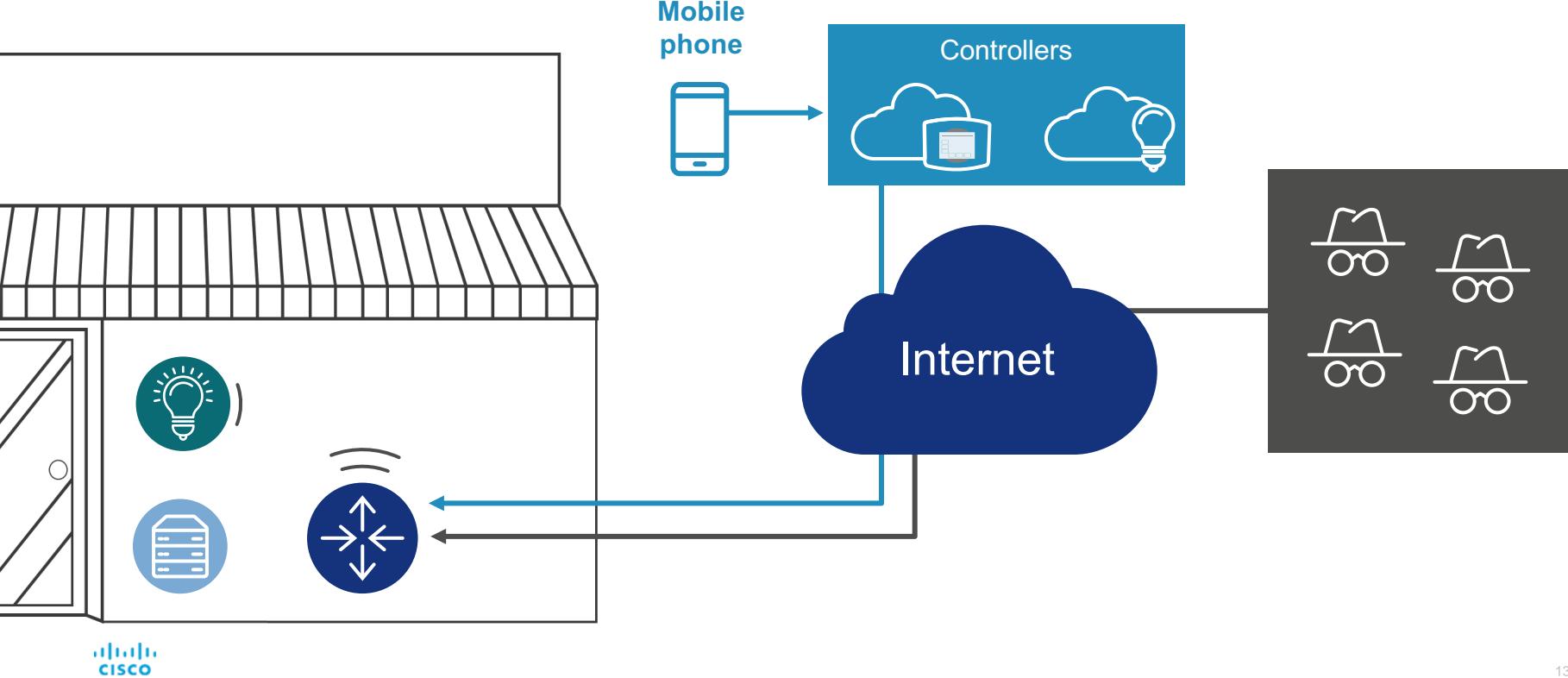
Device protects itself

- Secure development practices

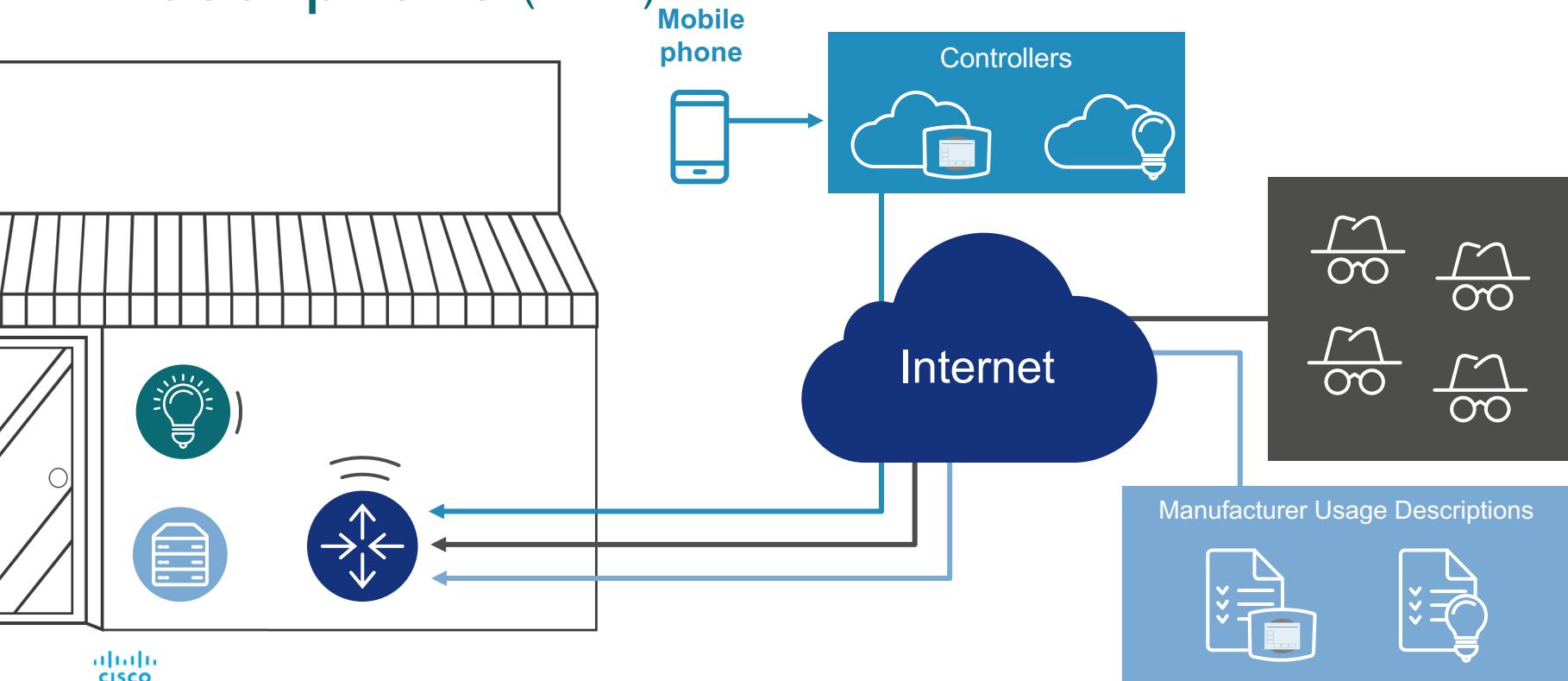
Network protects device

- Device identification
- Automated segmentation

Understanding the Attack Surface



Introducing the Manufacturer Usage Descriptions (MUD)



Assumptions and Assertions

Assumptions

A Thing has a single use or a small number of uses

Things are tightly constrained.
CPU and memory resource constraints are tight.

Even those Things that can protect themselves today may not be able to do so tomorrow

Network administrators are the ultimate arbiters of how their networks will be used

Assertions

Because a Thing has a single or a small number of intended uses, it all other uses must be unintended

Any intended use can be clearly identified

All other uses can be warned against in a statement

Manufacturers are in a generally good position to make the distinction

Drug Facts	
Active Ingredient (in each tablet)	Purpose Aspirin 325 mg Pain reliever
Uses To relieve the temporary relief of minor aches and pains or as recommended by your doctor. Because of its delayed release action, this product will not provide fast relief of headaches or other symptoms needing immediate relief.	
Do not use -if you have ever had an allergic reaction to any other pain relievers/ fever reducers.	
Warnings Reyes syndrome: Children and teenagers who have or are recovering from chicken pox or flu-like symptoms should not use this product. When using this product, if changes in behavior with nausea and vomiting occur, consult a doctor because these symptoms could be an early sign of Reyes's syndrome, a rare but serious illness. Ask a doctor before use if you have stomach problems (such as heartburn, acid stomach, or stomach pain) that last or come back bleeding problems -ulcers, asthma Ask a doctor or pharmacist before use if you are taking a prescription drug for -diabetes -gout -arthritis Allergy alert: Aspirin may cause a severe allergic reaction which may include -facial swelling -asthma (wheezing) -shock -hives Alcohol warning: If you consume 3 or more alcoholic drinks every day. Ask your doctor whether you should take aspirin or other pain relievers/fever reducers. Aspirin may cause stomach bleeding. Stop use and ask doctor if an allergic reaction occurs. Seek medical help right away... -Pain gets worse or lasts more than 10 days -redness or swelling is present -new symptoms occur -the ears or loss of hearing occur If pregnant or breast-feeding: ask a health professional It is especially important not to use aspirin during the first 3 months of pregnancy unless definitely directed to do so because it may cause problems in the unborn child and complications during delivery. Keep out of the reach of children. In case of an overdose, seek medical help or contact a Poison Control Center immediately.	
Directions Take one tablet with a glass of water with each dose. Adults and children 12 years of age and over: take 4 to 8 tablets a day as needed. Do not exceed 48 tablets in 24 hours unless directed. Children under 12 years: consult a doctor	
Other Information -store at room temperature Inactive Ingredients: colloidal silicon dioxide, sodium, FD&C Yellow #10 at lake, FD&C Yellow #6, methacrylic acid and copolymer, microcrystalline cellulose, talc, titanium dioxide, triethyl citrate	



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  
                                ]  
                            }  
                        }  
                    ]  
                }  
            }  
        ]  
    }  
}
```

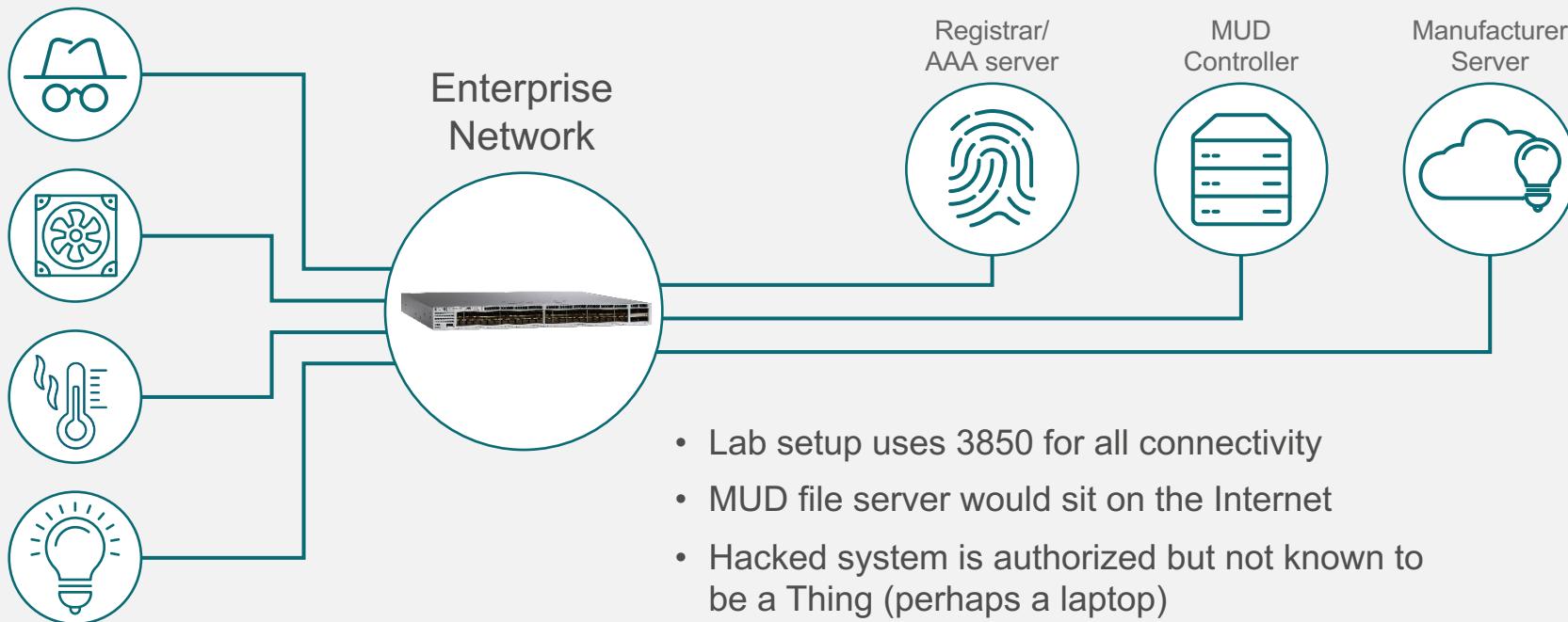
...

MUD File Abstractions in Practice

my-controller == permit to a DNS host

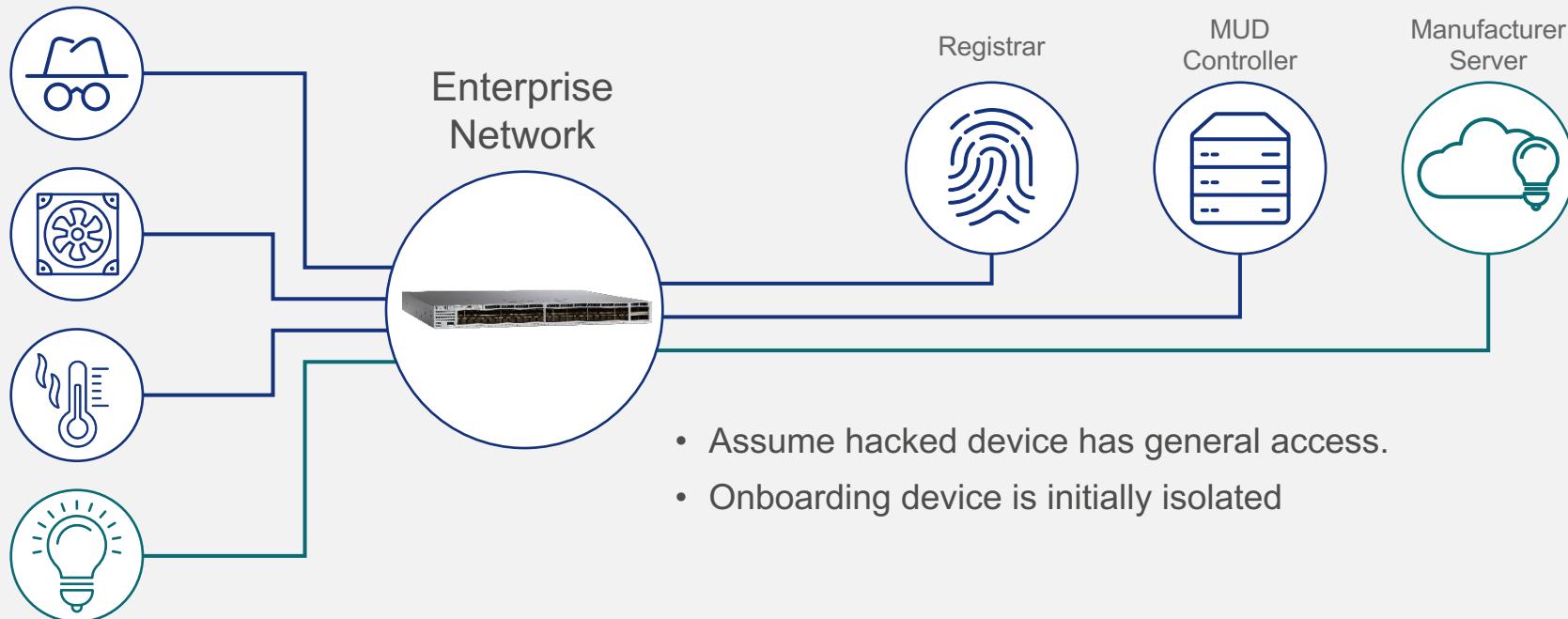
same-manufacturer = use VLAN or SGT segment

Initial Configuration



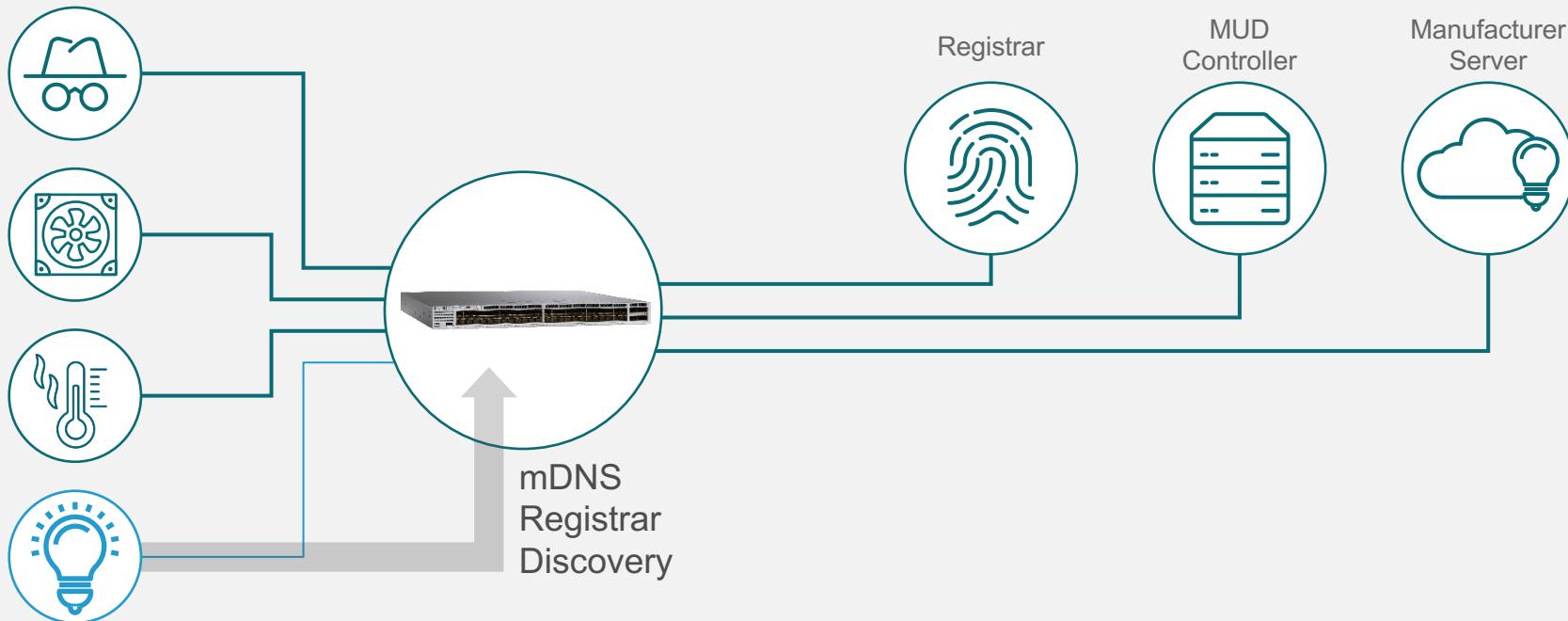
Onboarding Process

Device Connects



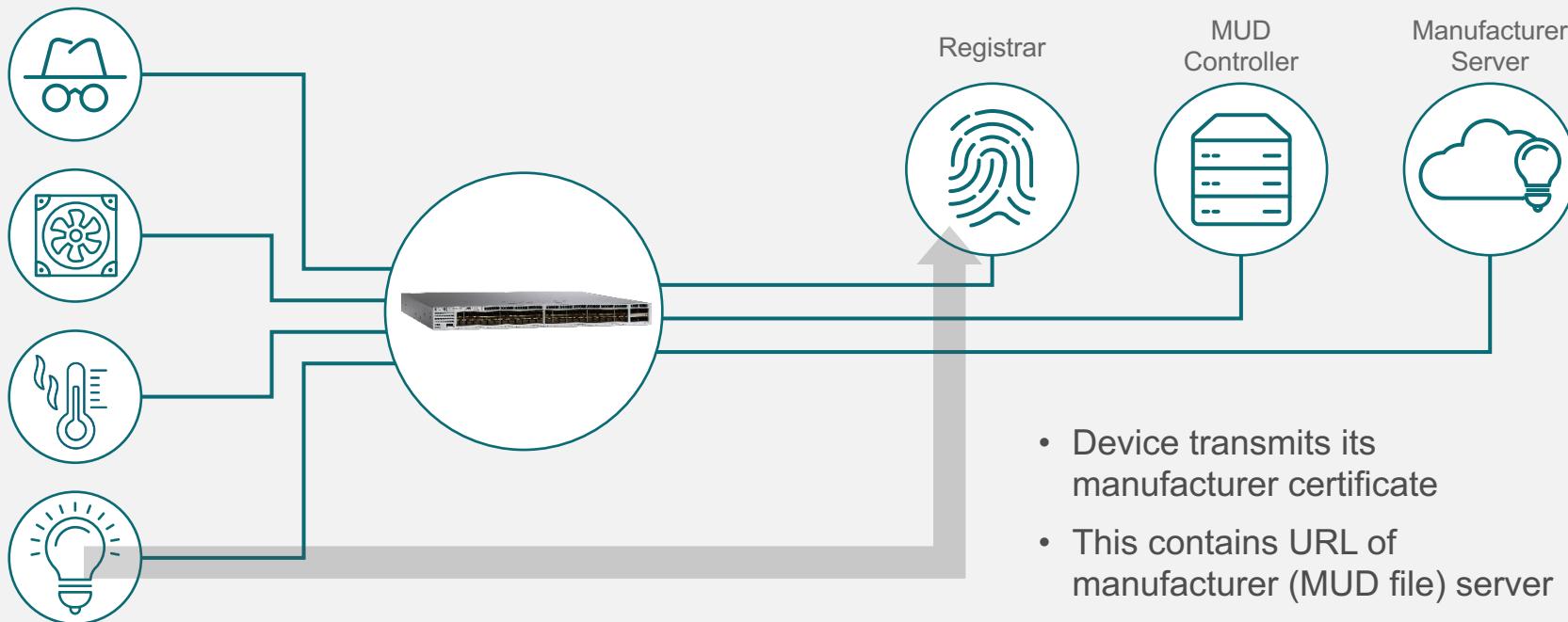
Bootstrap

Find Registrar



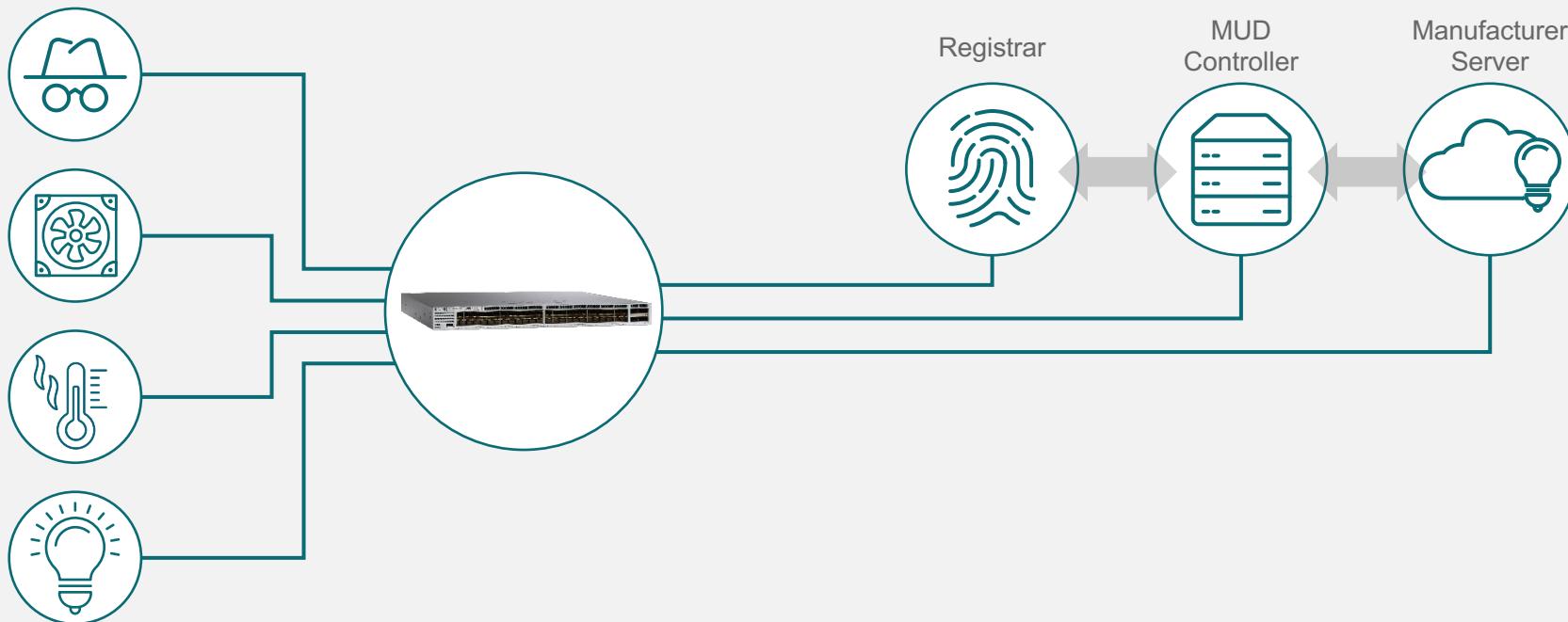
Bootstrap

Initiate Registration

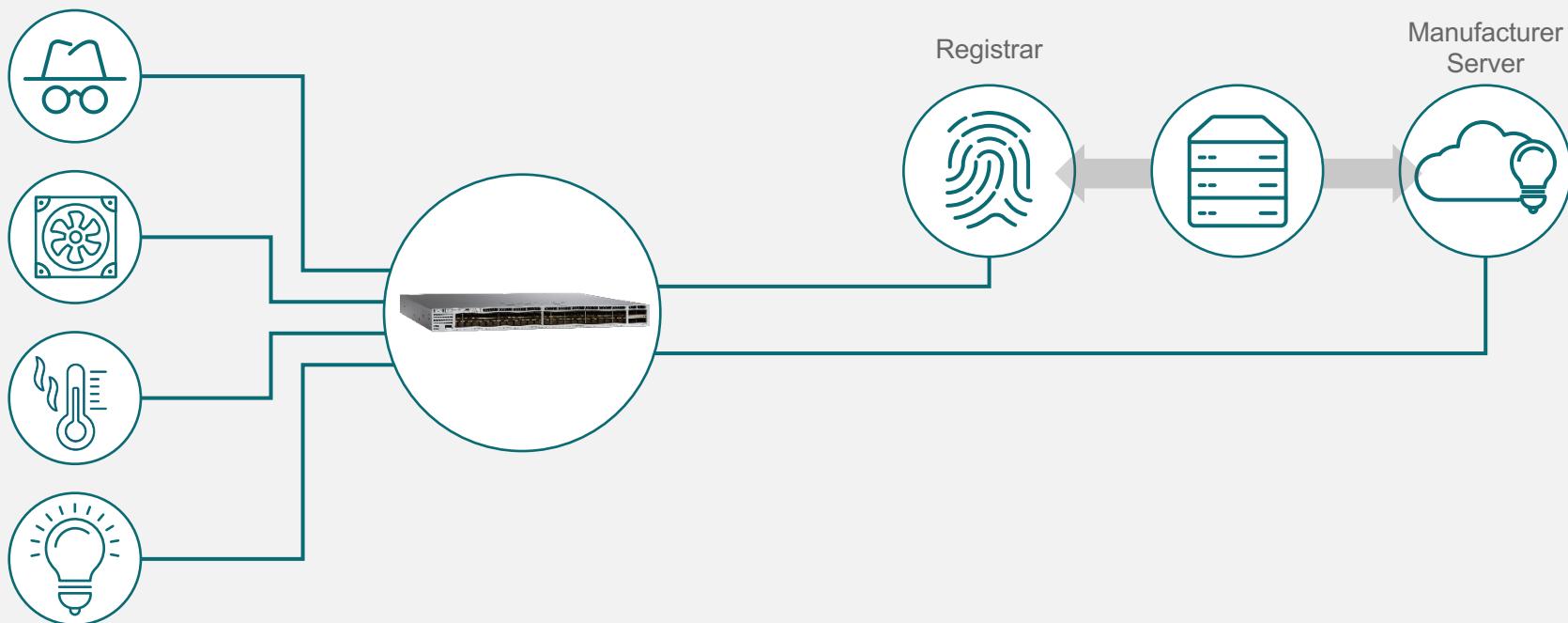


Bootstrap

Retrieve MUD File from Manufacturer, to Find MASA Server



Request A Voucher to Send to the Device

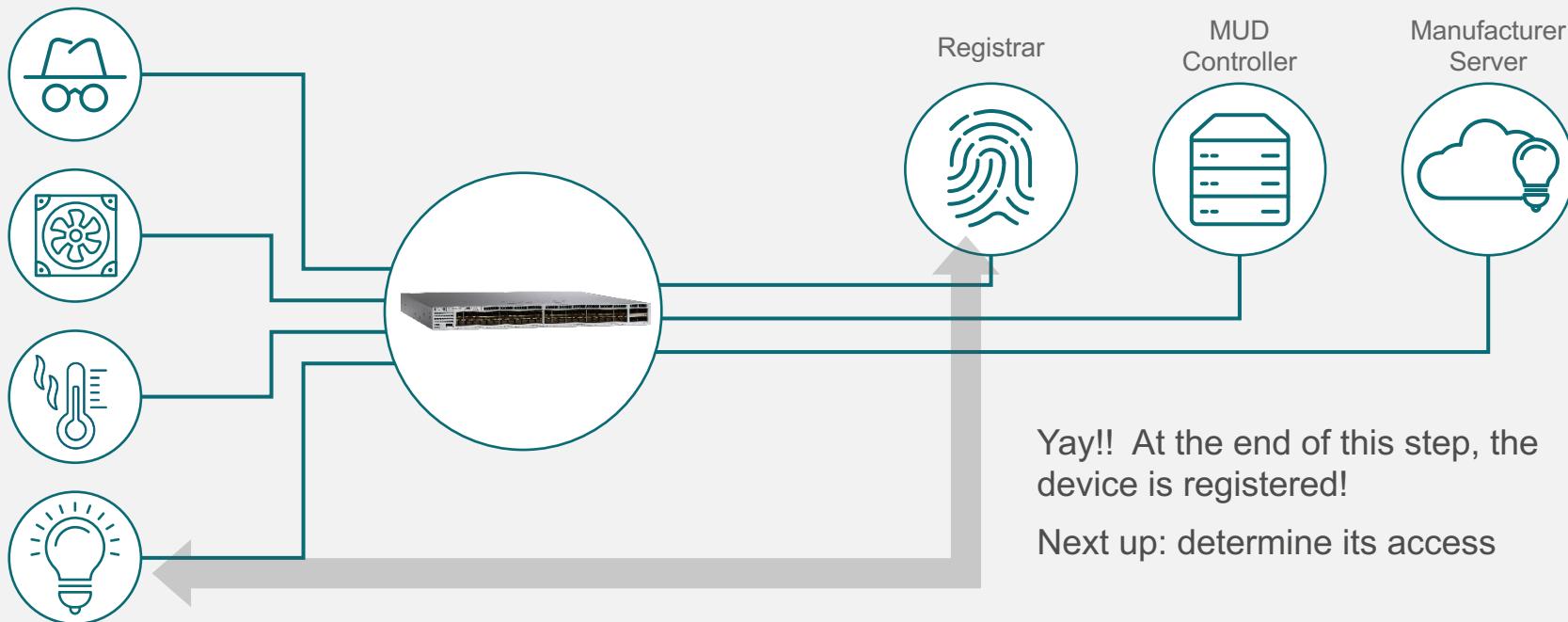


Administrative Approval, if Required

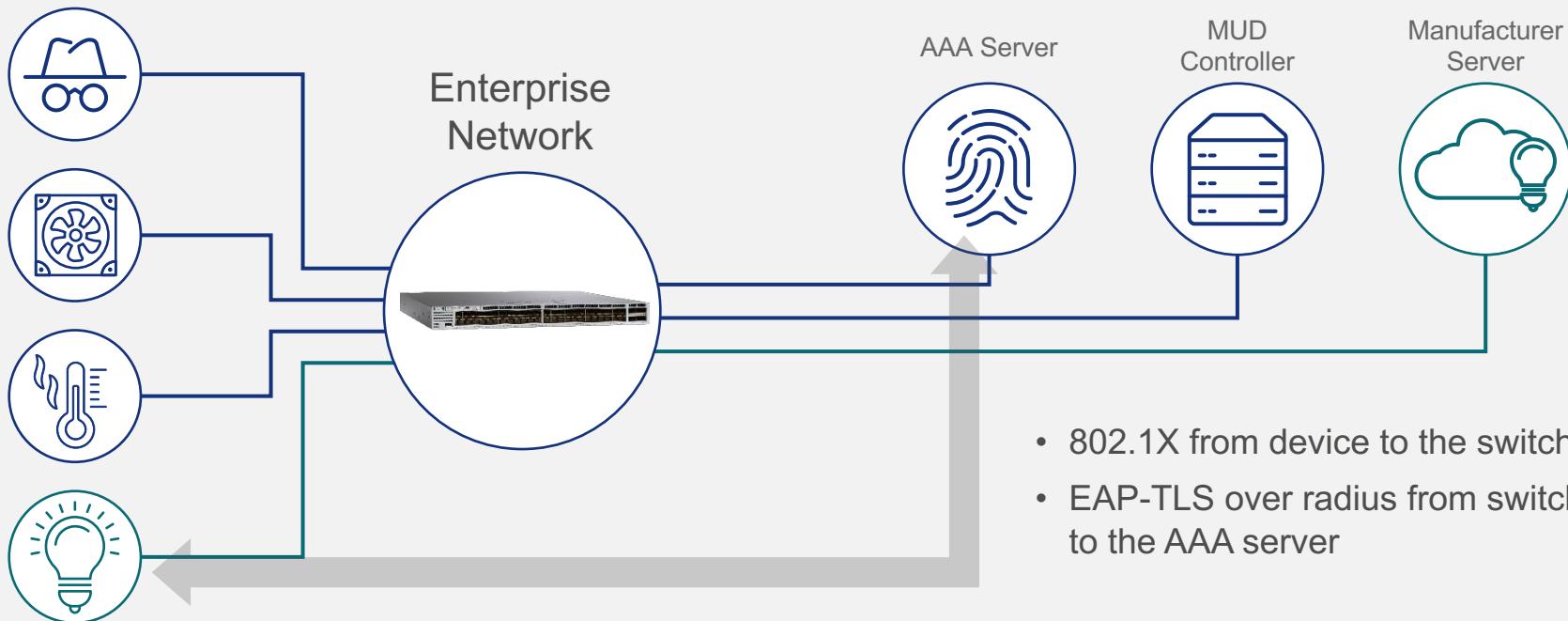
(Probably Only First of This Type of Device)



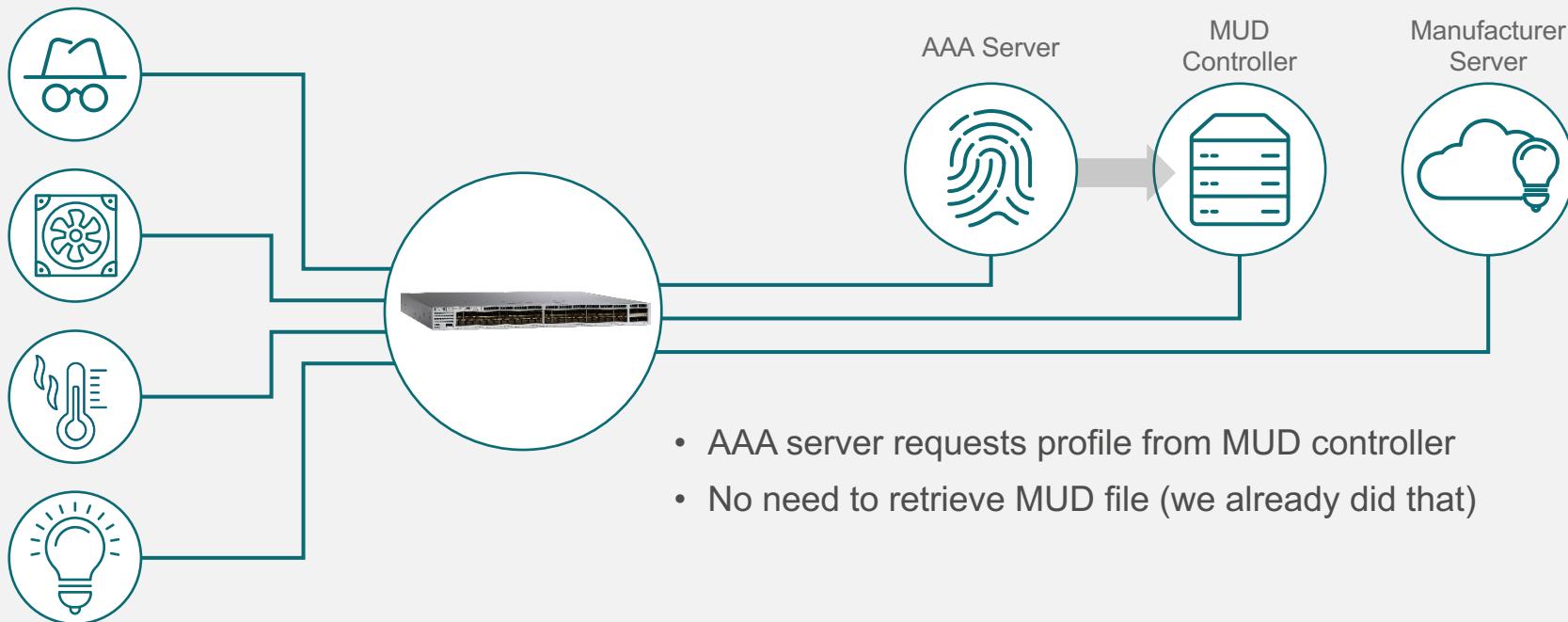
Install Trust Anchor and Perform EST Registration to Obtain A Local Certificate



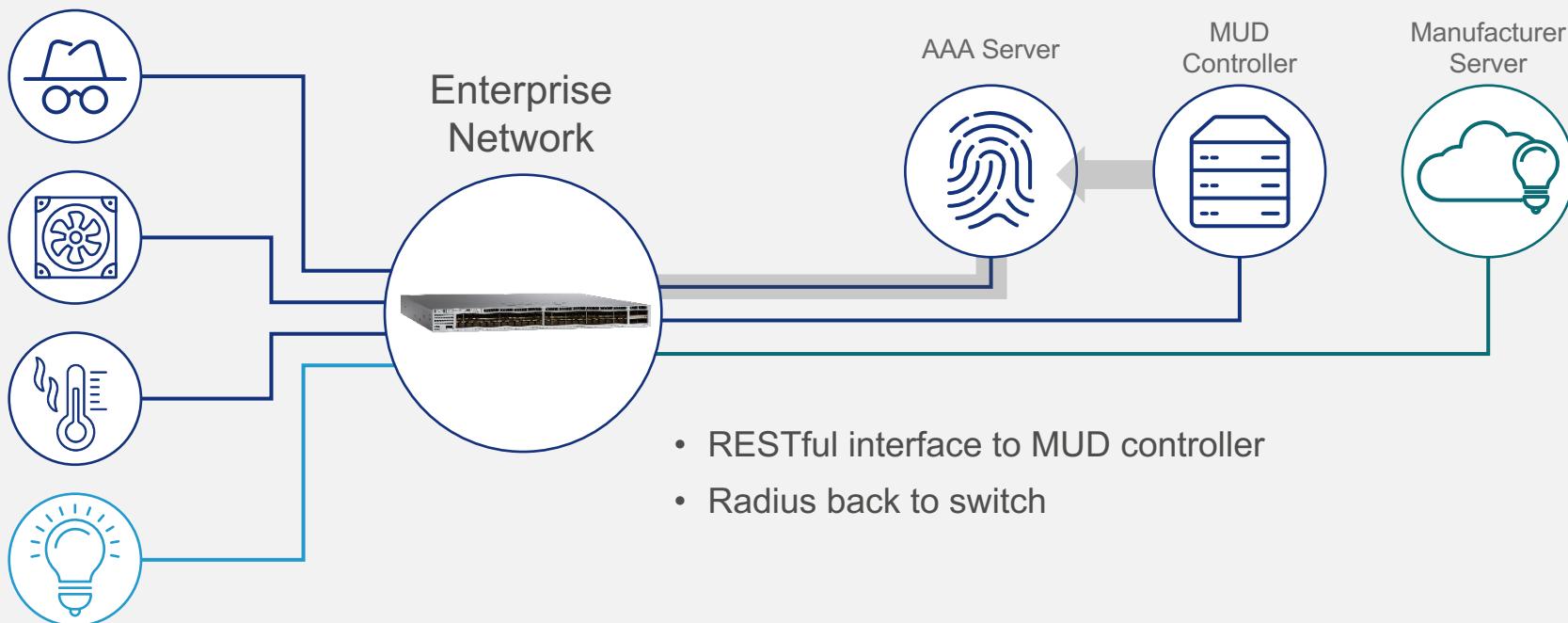
Now Device Authenticates Using 802.1X



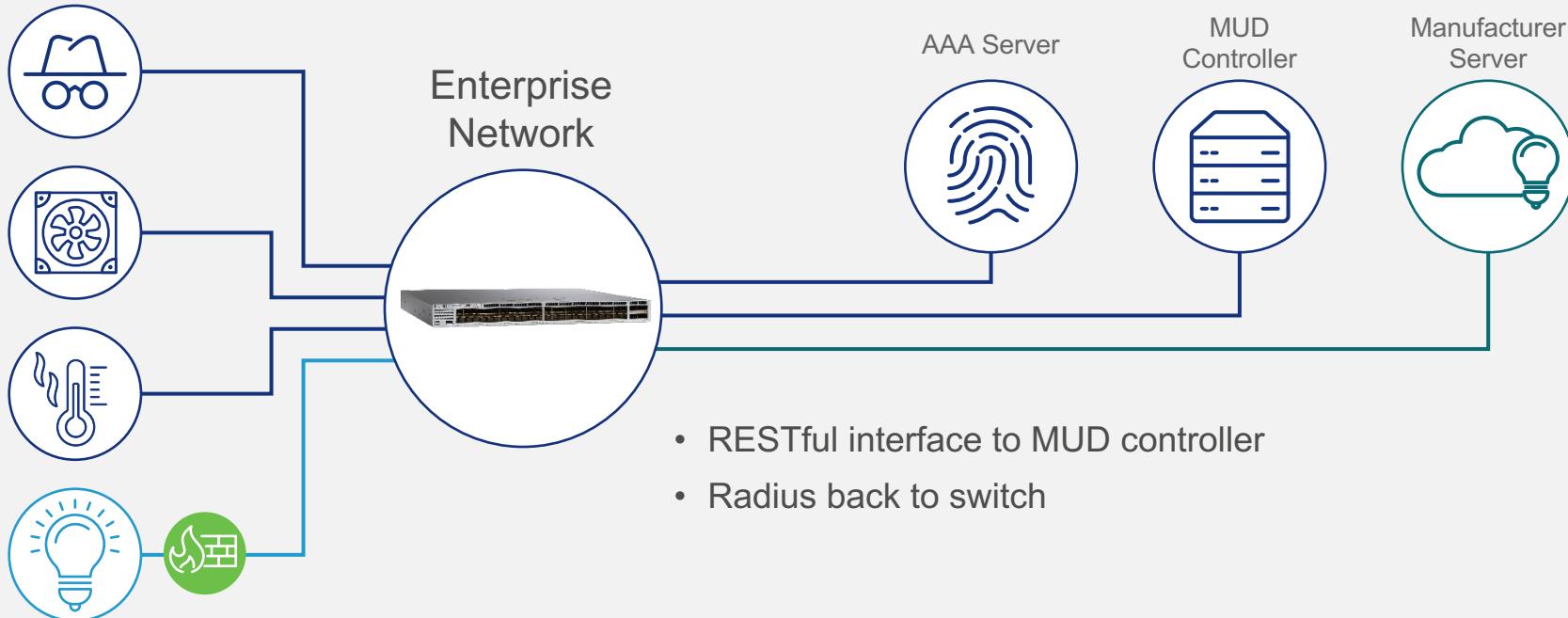
Determine Appropriate Authorization



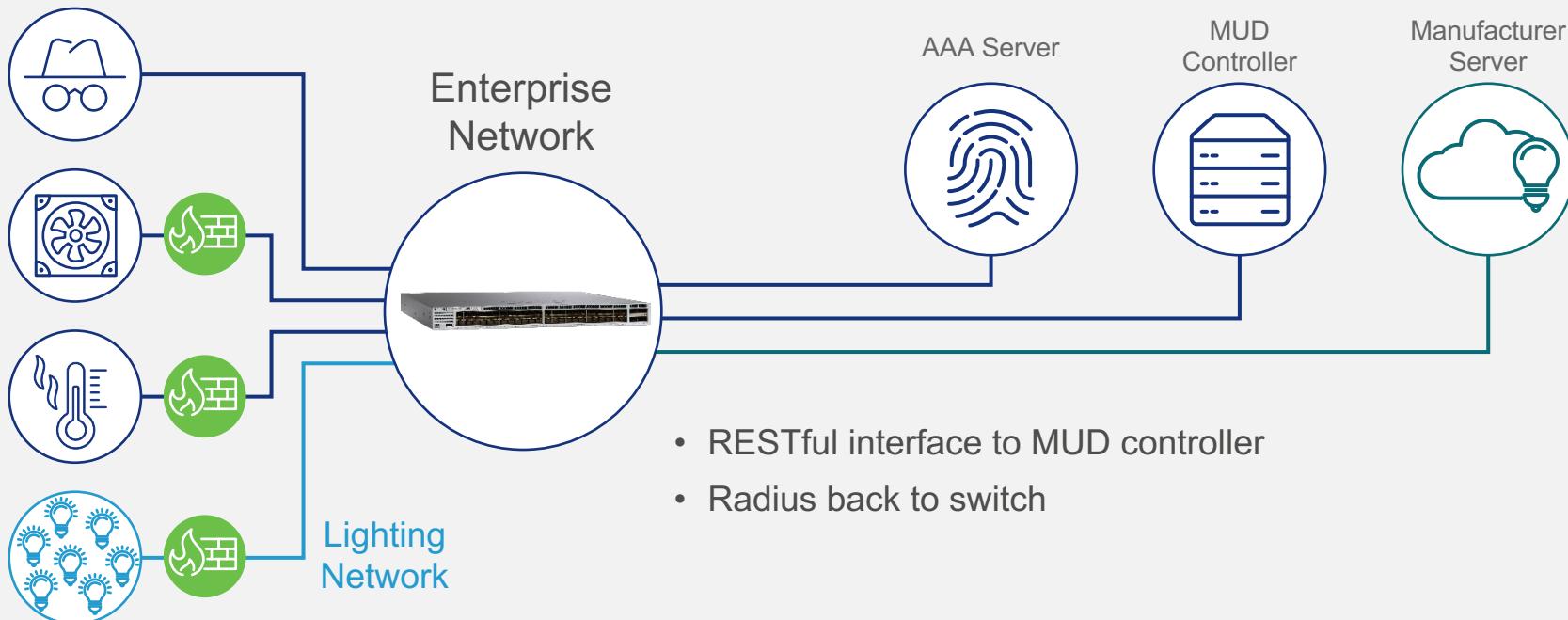
Effect Change of Authorization



Bad guy out of luck



Devices Get Appropriate Segmentation



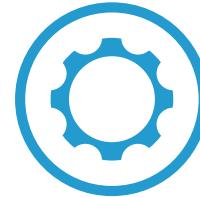
How to locate the policy? A URL

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 Own3ed	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](https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud-07)

