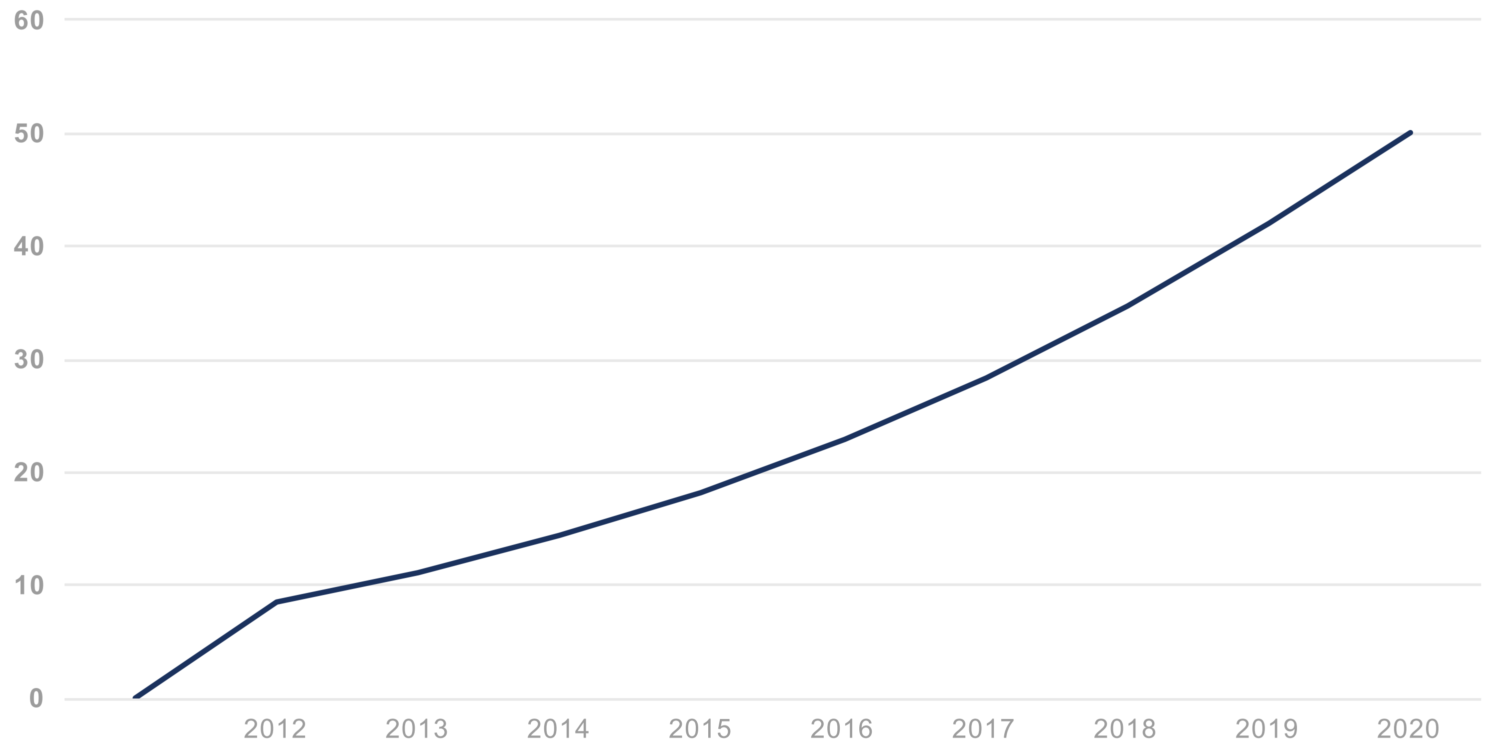
Challenges and Possibilities with IoT Security

Eliot Lear, Michael Behringer, Hannes Tschofenig

Number of connected devices (Billions)



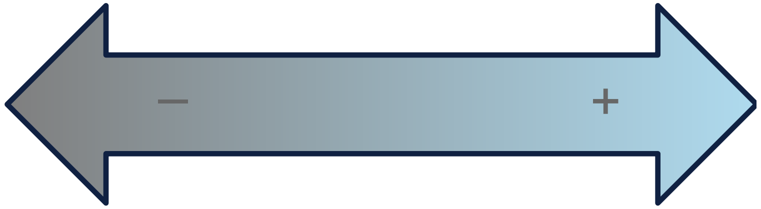
Big Problem

- We know how to manage large numbers of the same device (e.g., ca. 120 – 300 million iPhones)

- We don’t know how to manage larger numbers of **types** of devices

Many different dimensions to consider

Static environments



Dynamic systems

The Network Needs Two Pieces of Information

- What the device is
  - Trusted introduction between the network and the device so that each trusts the other
- How the network should protect it
  - Who/what is the device intended to communicate with, and how?

At the IETF

- What the device is
  - Trusted introduction between the network and the device so that each trusts the other
- How the network should protect it
  - Who/what is the device intended to communicate with, and how?

- ANIMA bootstrapping
- ACE
- Zerotouch deployment

- MUD (in various groups)
- Autoattach (opsawg/IEEE)

What the device is: trusted introduction

Bootstrapping Key Infrastructures

draft-ietf-anima-bootstrapping-keyinfra-02

Max Pritikin, Michael Richardson, Michael Behringer, Steinthor Bjarnason

Objective

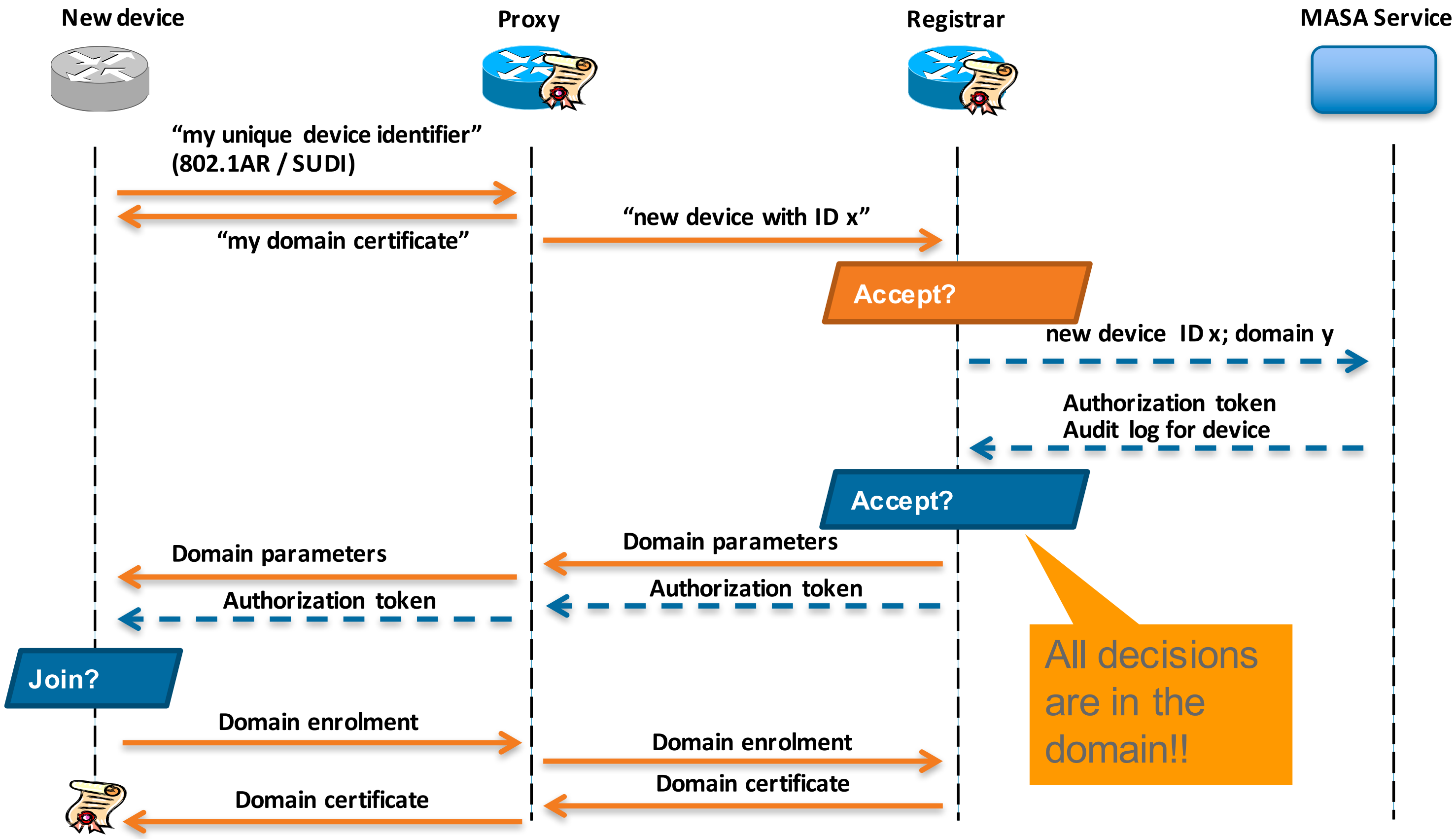
Enrol a new device into the correct network:

- Zero-touch (device is "factory default")
- "Secure":
  - authenticate new device
  - authenticate network

these are a MUST for large scale → IoT

- Philosophy: bootstrap a key infrastructure (LDevID) from IDevIDs, the rest is easy

Secure Enrolment Process



New device

Proxy

Registrar

MASA Service

"my unique device identifier"
(802.1AR / SUDI)

"my domain certificate"

"new device with ID x"

Accept?

new device ID x; domain y

Authorization token
Audit log for device

Accept?

Domain parameters

Domain parameters

Authorization token

Authorization token

Join?

Domain enrolment

Domain enrolment

Domain certificate

Domain certificate

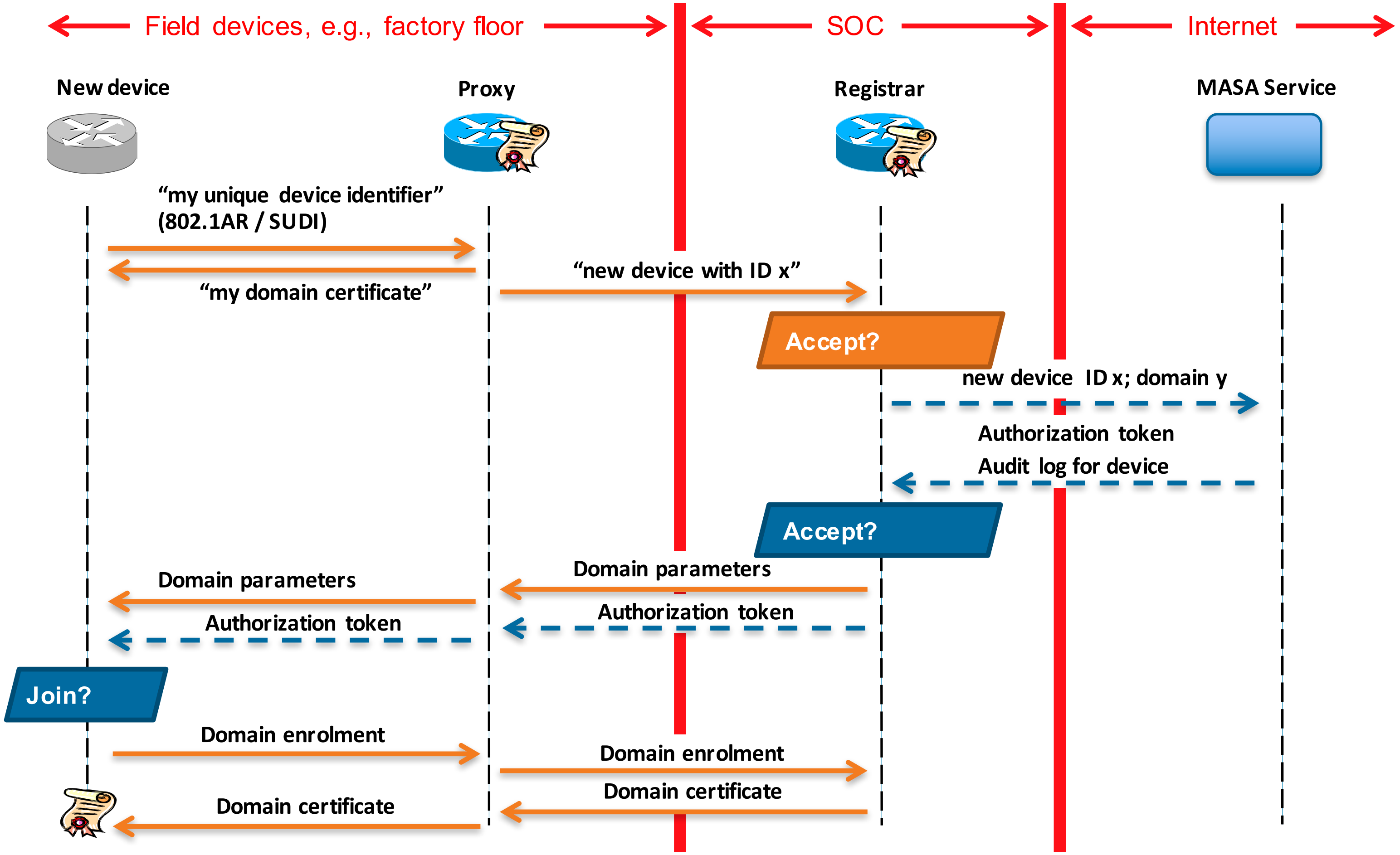
All decisions are in the domain!!

Features

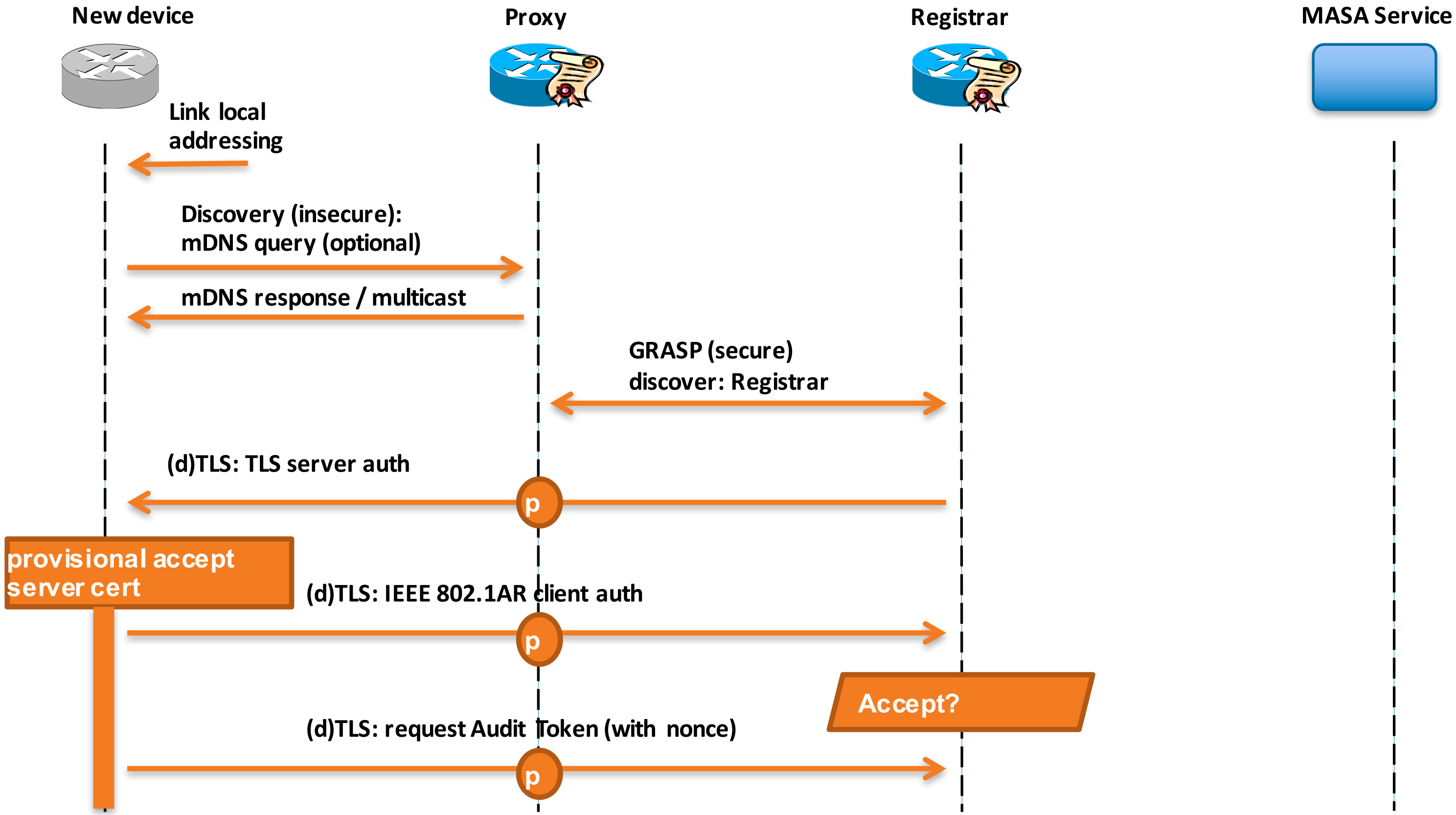
- New device has only link local connectivity
  - Can only attack first hop
- New device can be cryptographically authenticated
- New device can authenticate network
  - Join only the authorized network

- Applicability: Potentially anywhere, network devices, sensors, etc.

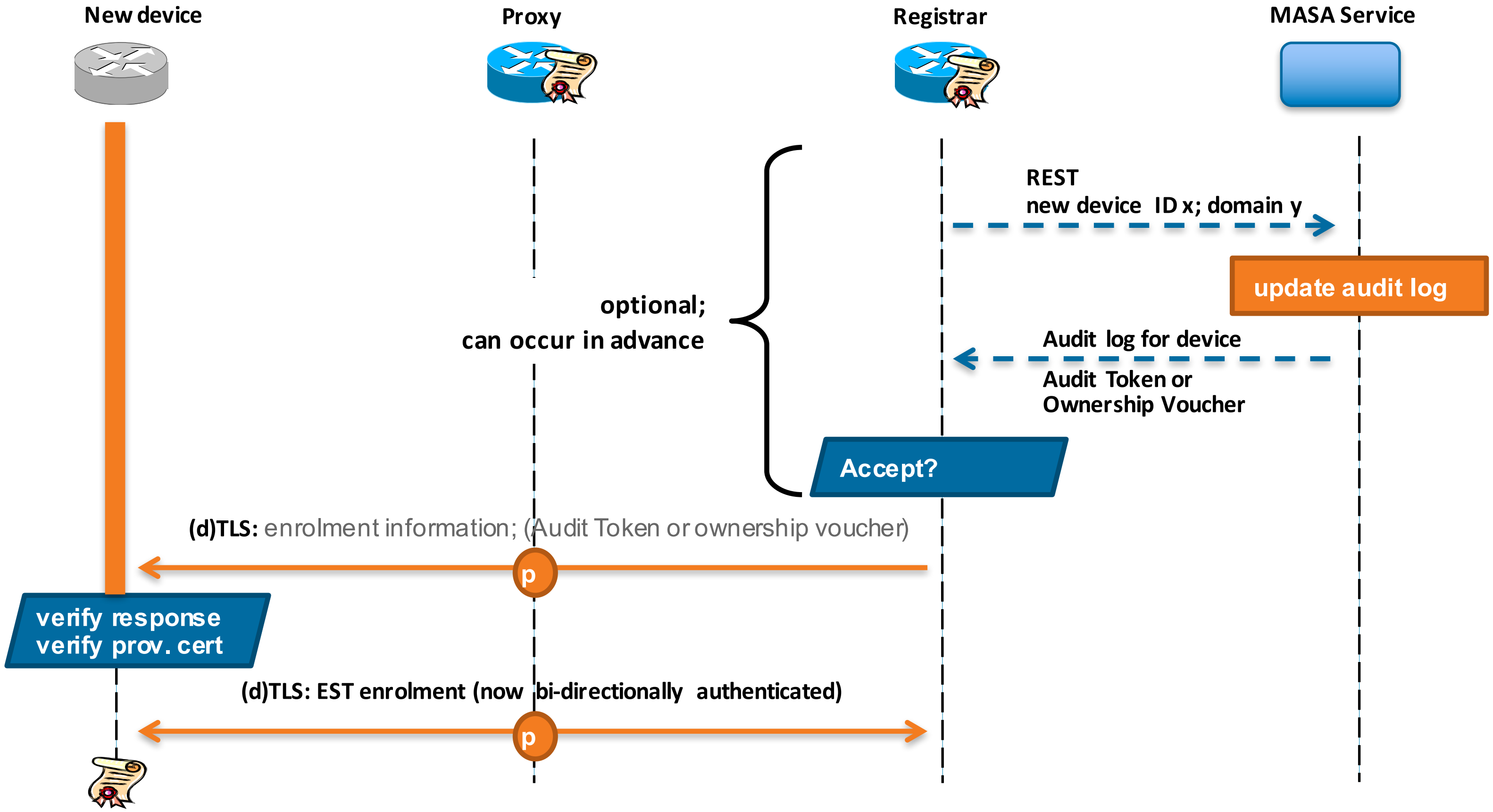
Possible Security Zones



Protocols
Disclaimer: Work in Progress


New device
Proxy
Registrar
MASA Service
Link local addressing
Discovery (insecure): mDNS query (optional)
mDNS response / multicast
GRASP (secure) discover: Registrar
(d)TLS: TLS server auth
p
provisional accept server cert
(d)TLS: IEEE 802.1AR client auth
p
Accept?
(d)TLS: request Audit Token (with nonce)
p

Protocols
Disclaimer: Work in Progress



Other Approaches

- 6TISCH:
  - dTLS / CoAP / 6top transport
  - uses IDevID to derive LDevID (for link security)
  - Goal: transport YANG (ANIMA goal: derive LDevID)
- NETCONF:
  - Goal: transport YANG (ANIMA goal: derive LDevID)
  - Many protocols supported: http, https, DNS, mDNS, DHCP, removable storage, ...
  - Uses IDevID directly (ANIMA uses IDevID to derive LDevID)
- 802.1x / EAP / PANA:
  - Needs to “know” which network to join.

How should the network protect a Thing?

Assumptions and Assertions

Assumptions	Assertions
A Thing has a single or small number of uses.	Because a Thing has a single or a small number of intended uses, it all other uses must be unintended
Start simple, but allow for richer approaches LATER	Any intended use can be clearly identified by the manufacturer
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 by the manufacturer
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to make the distinction

Drug Facts

Active Ingredient (in each tablet) **Purpose**
Aspirin 81 mg...Pain reliever

Uses
for 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 Reye's syndrome, a rare but serious illness.

Ask a doctor before use if you have ·stomach problems (such as heartburn, upset 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 occurs

If pregnant or breast-feeding ask a health professional
It is espcially important not to use aspirin during th
of pregnancy unless definitely directed to do so
because it may cause problems in the unborn
complications during delivery.

Keep out of the reach of children. In case of
help or contact a Poison Control Center imme

Directions
·drink a full glass of water with each dose. ·A
12 years of age and over: take 4 to 8 tablets e
exceed 48 tablets in 24 hours unless directed
·Children under 12 years: consult a doctor

Other Information ·store at room temperature

Inactive Ingredients collodial silicon dioxide
sodium, FD&C Yellow #10 al lake, FD&C Yel
methacrylic and copolymer, microcrystalline
acid, talc, titanium dioxide, triethyl citrate

GOODSENSE
For Adults
Safe Pain Relief Plus Lifesaving Benefits**
Aspirin
Pain Reliever/Fever Reducer (NSAID)
Fast, Safe Pain Relief
• Headaches
• Everyday Aches & Pains
Compare to active ingredient of Bayer® Aspirin
500 Coated Tablets - 325 mg

Translating intent into config

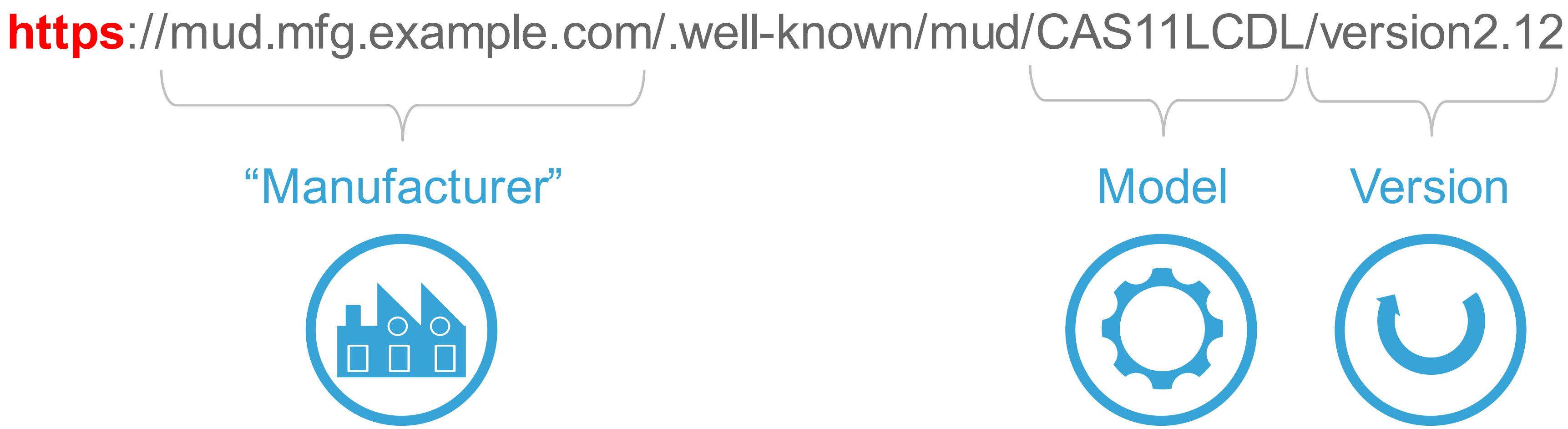
Any intended use can be clearly identified by the manufacturer

```
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
```

How to locate the policy? A URI



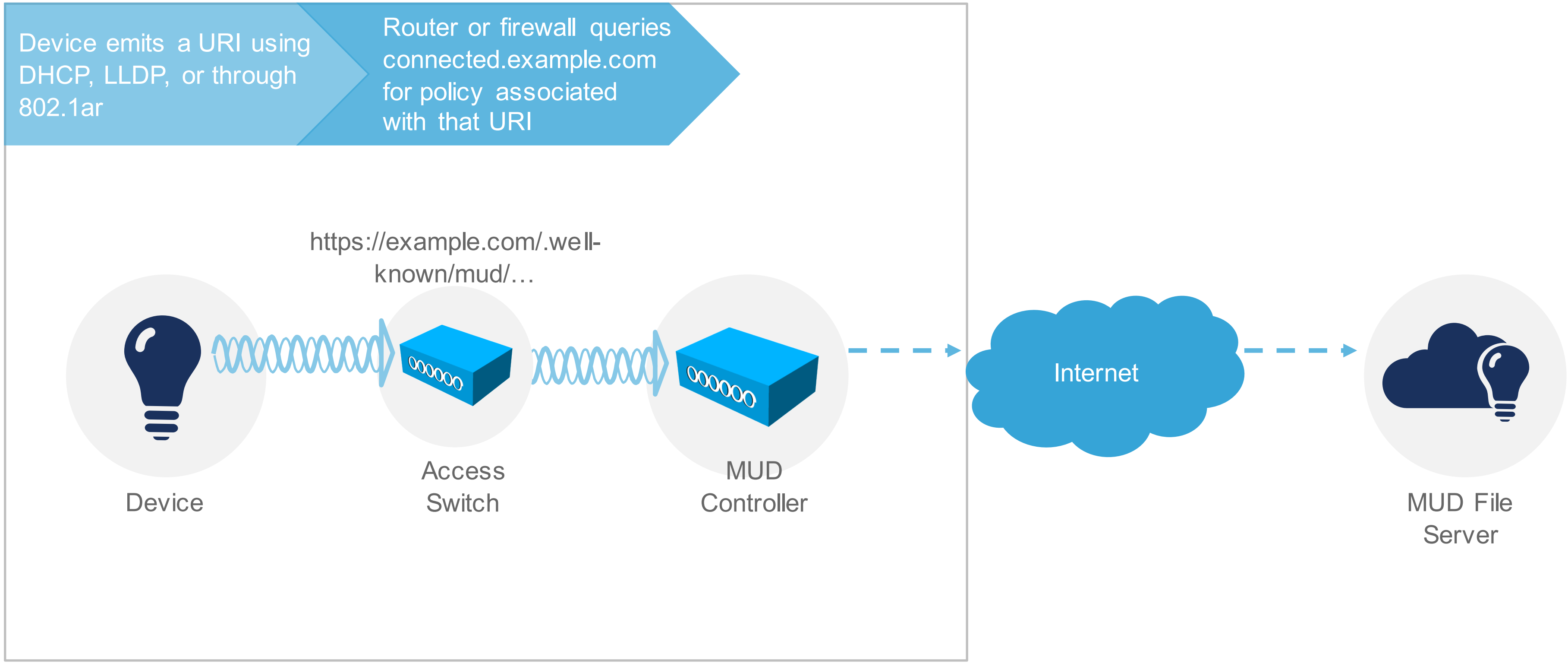
https://mud.mfg.example.com/.well-known/mud/CAS11LCDL/version2.12

“Manufacturer”

Model

Version

Expressing Manufacturer Usage Descriptions



Device emits a URI using DHCP, LLDP, or through 802.1ar

Router or firewall queries connected.example.com for policy associated with that URI

https://example.com/.well-known/mud/…

Device

Access Switch

MUD Controller

Internet

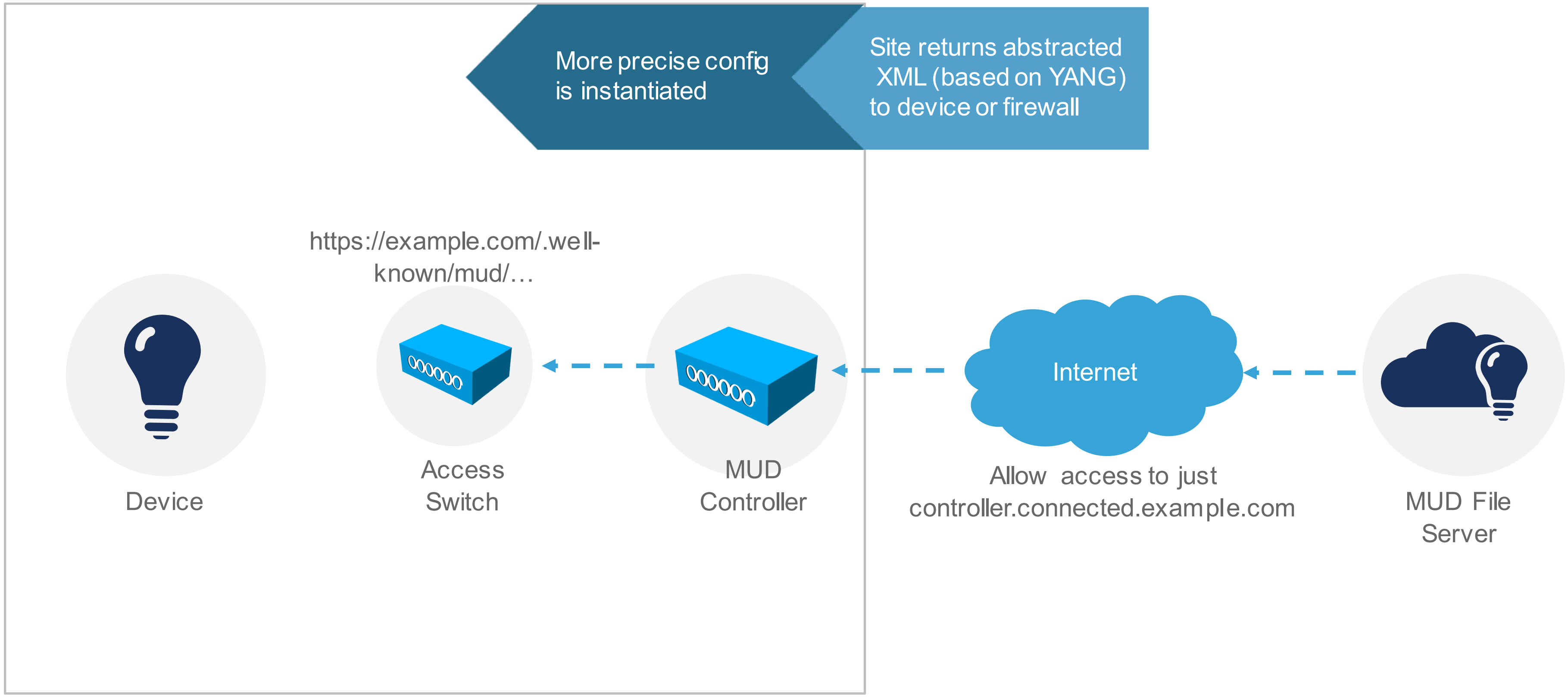
MUD File Server

Makes use of YANG-based XML

```
<?xml version = '1.0' encoding = 'UTF-8'? >
<edit-config
 xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
 xmlns:inet="urn:ietf:params:xml:ns:yang:ietf-inet-types"
 xmlns:mud="urn:ietf:params:xml:ns:yang:cisco-manpolicy"
 xmlns:acl="urn:ietf:params:xml:ns:yang:ietf-acl">
 <mud:supportInformation>
 <mud:lastUpdate>2015-05-12T20:00:50Z</mud:lastUpdate>
 <mud:cacheValidity>1440</mud:cacheValidity>
 </mud:supportInformation>
 <config>
 <top>
 <acl:access-list>
 <acl:access-list-entries>
                 <acl:access-list-entry>
                  <acl:rule-name>access-thermostat-controller</acl:rule-name>
                  <acl:matches>
                  <inet:hostname>controller.example.com</inet:hostname>
                  </acl:matches>
                  <acl:actions>
                  <acl:permit/>
                  </acl:actions>
 </acl:access-list-entry>
                 <acl:access-list-entry>
                  <acl:rule-name>let-me-talk-to-other-thermostats</acl:rule-name>
                  <acl:matches>
                  <mud:sameManufacturer/>
                  </acl:matches>
                  <acl:actions>
                  <acl:permit/>
                  </acl:actions>
                 </acl:access-list-entry>
                 <acl:access-list-entry>
                  <acl:rule-name>deny-other</acl:rule-name>
                  <acl:actions>
                  <acl:deny/>
                  </acl:actions>
                 </acl:access-list-entry>
 </acl:access-list-entries>
 </acl:access-list>
 </top>
 </config>
</edit-config>
```

Only the text in red would have to change with the proposed standardization

Expressing Manufacturer Usage Descriptions



More precise config is instantiated

Site returns abstracted XML (based on YANG) to device or firewall

https://example.com/.well-known/mud/…

Allow access to just controller.connected.example.com

So what do we need to do this?

A way to communicate identifiers	IEEE 802.1AR & IEEE 802.1X, DHCP, LLDP
A way to express network configuration	YANG
A way to retrieve the policy	HTTP/TLS
An access-list model	draft-ietf-netmod-acl-model
A URI to point at the policy	draft-lear-ietf-netmod-mud
Use of DNS Names in ACLs	draft-lear-ietf-acl-dnsname-00
A new PKIX constraint for the URI	draft-lear-ietf-pkix-mud-extension-00
A DHCP option for the URI (2nd best)	draft-lear-ietf-dhc-mud-option-01
An LLDP TLV	(later)

X.509 Constraint or DHCP option?

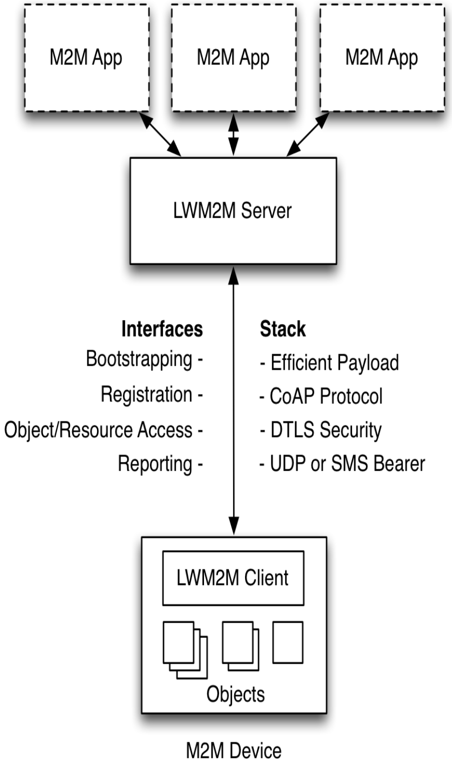
- IEEE 802.1AR has stronger security properties
- DHCP is the **2nd choice** to deliver the MUD URI
- DHCP is still useful - assertion is from the device for **its protection**.
- No code impact for systems already implementing 802.1AR
- Very easy to implement and deploy for any system already implementing DHCP
- Need to think about software variations and attestation

Open Issues & Questions

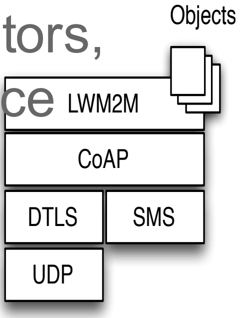
- Serialization of the MUD File needs to be more fully specified.
- Extensibility is a challenge
- Given the scale of risk, configuration generated by these models really MUST be signed.
  - Advice needed
- Looking for more eyes on draft MUD constraint
  - ANIMA work is currently leveraging MUD for discovery. Should we write another constraint?
- Protocol review of ANIMA

Standardizing device security models

Device Management for Security



- **OMA LWM2M** reuses IETF technologies, such as CoAP, DTLS, and Resource Directory.
- Servers are deployable on gateways and in the cloud. Authorized may get access to the data.
- Objects allow to determine device status and to configure device.
- Various objects specified providing information about sensors/actuators, software/firmware versions, device meta-data, and ACLs.
- LWM2M tutorial is available.



Questions?