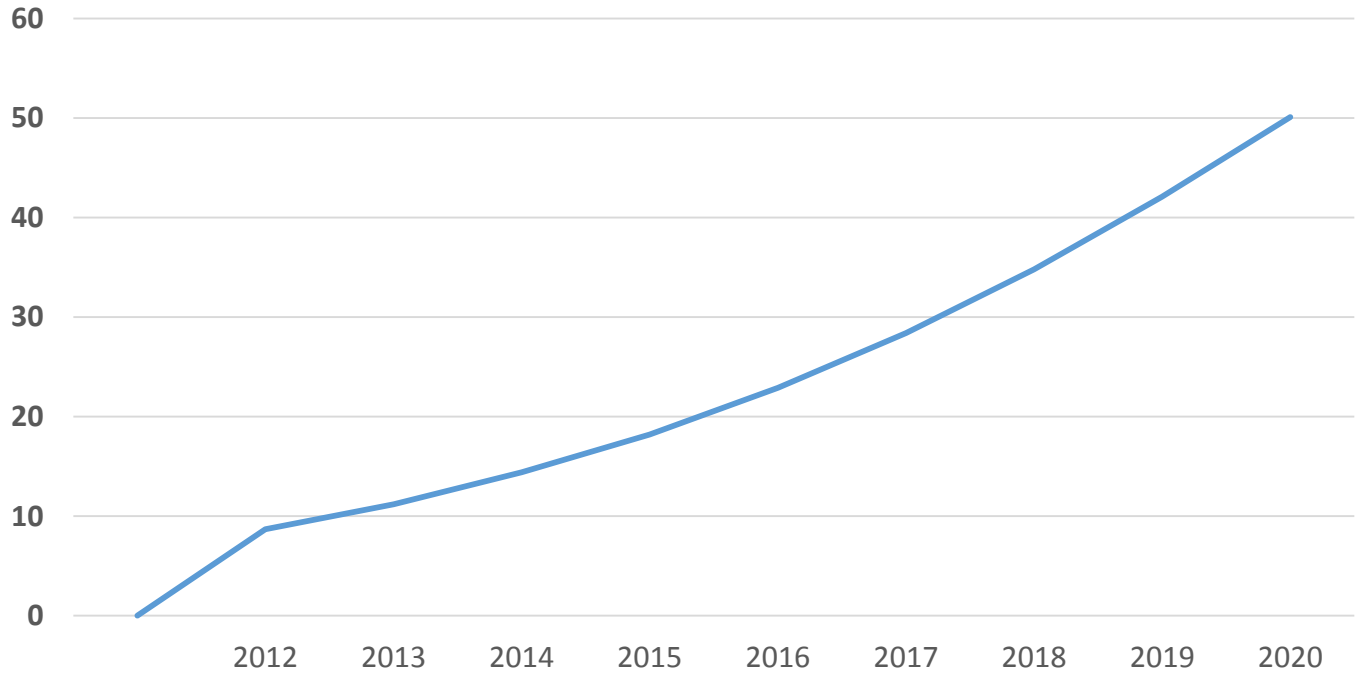
Manufacturer Usage Descriptions

draft-lear-mud-framework-01

Eliot Lear

6 April 2016

Number of connected devices (Billions)



The Real Problem

- We don’t know how to manage larger numbers of **types** of devices
- We don’t even know how to count how many types of devices there are

When this matters

Static environments

Dynamic systems

The Network Needs Two Pieces of Information

- What the device is
- **How the network should protect it**

We have some constraints

- Devices have very few resources to devote to security.
- The larger the footprint on the endpoint, the larger the threat surface (more code = more bugs)
- Strong security will not be possible in some instances.

How Should the Network Protect the Device?

Assumptions	Assertions
A thing has an IP stack and a use or a single number of uses.	Because a Thing has a single or a small number of intended uses, it all other uses must be unintended
With many **types of things**, it will not be possible for security vendors to profile them all.	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 in the future	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

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

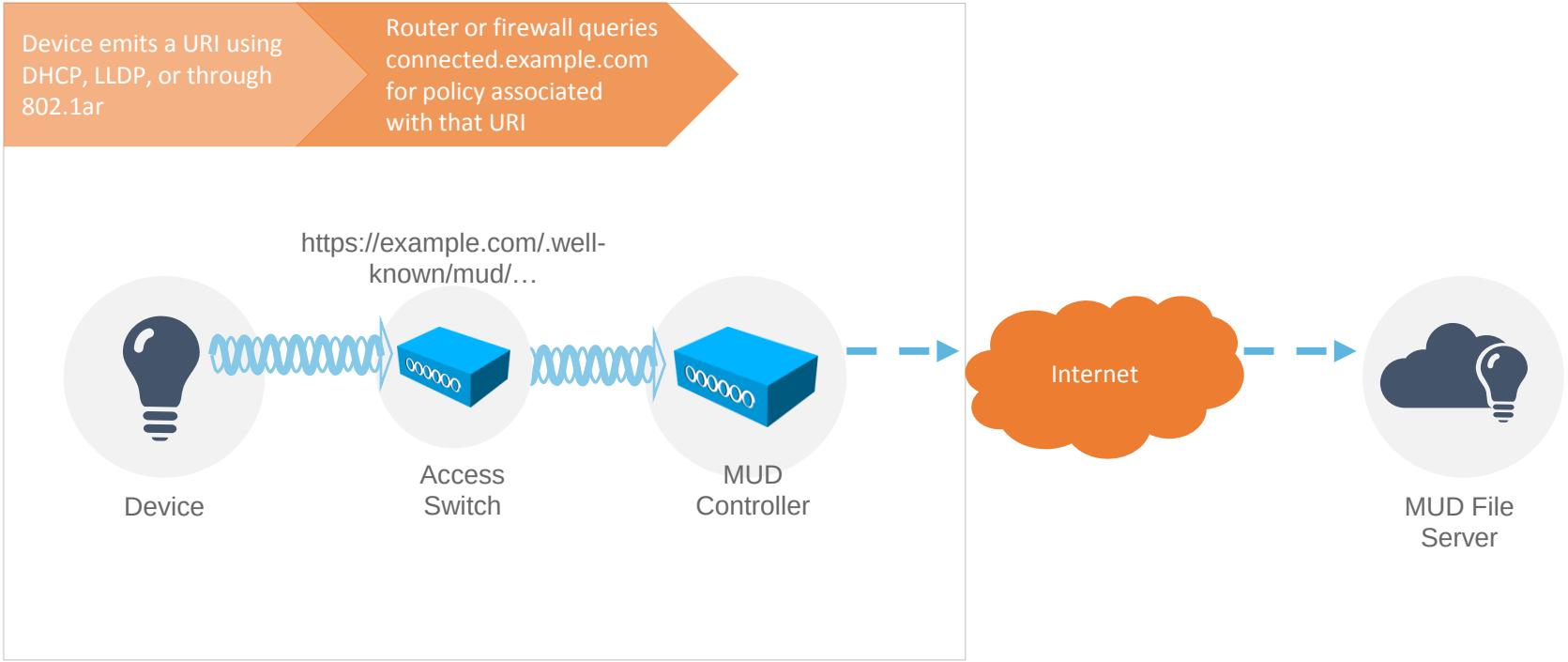
https://mud.mfg.example.com/.well-known/mud/CAS11LCDL/version2.12

"Manufacturer"

Model

Version

Expressing Manufacturer Usage Descriptions



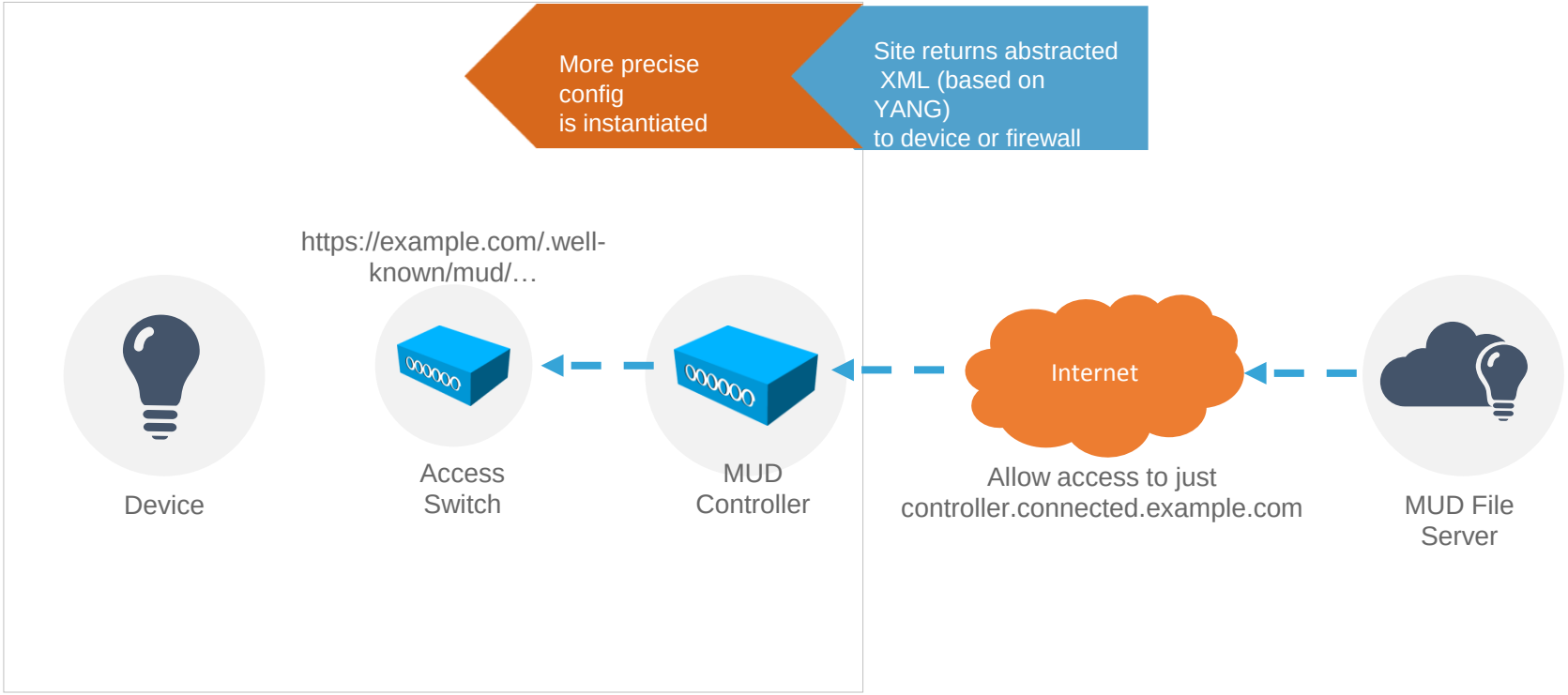
Makes use of YANG-based XML

```
<?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



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

Some comments

- New use of YANG model
  - Not tied to NETCONF
  - MUD files need to be signed
  - Extensibility is a little tricky (no capabilities exchange)
  - Perhaps some challenges around input versus output policies
  - Only covers access – not QoS (yet)
- Manufacturers have an operational role in this model (but this only mirrors a need for them to support their products)

What is needed…

- Feedback!
- Would like more eyes on the draft and the concept
- What to do with this draft?


CISCO