Manufacturer Usage Descriptions

Eliot Lear

4 April 2016

This presentation covers two drafts

- draft-lear-ietf-netmod-mud-00.txt
- draft-lear-ietf-netmod-acl-dnsname-00.txt

The overall concept will be presented in OPSAWG and SAAG.

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

The Network Needs Two Pieces of Information

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

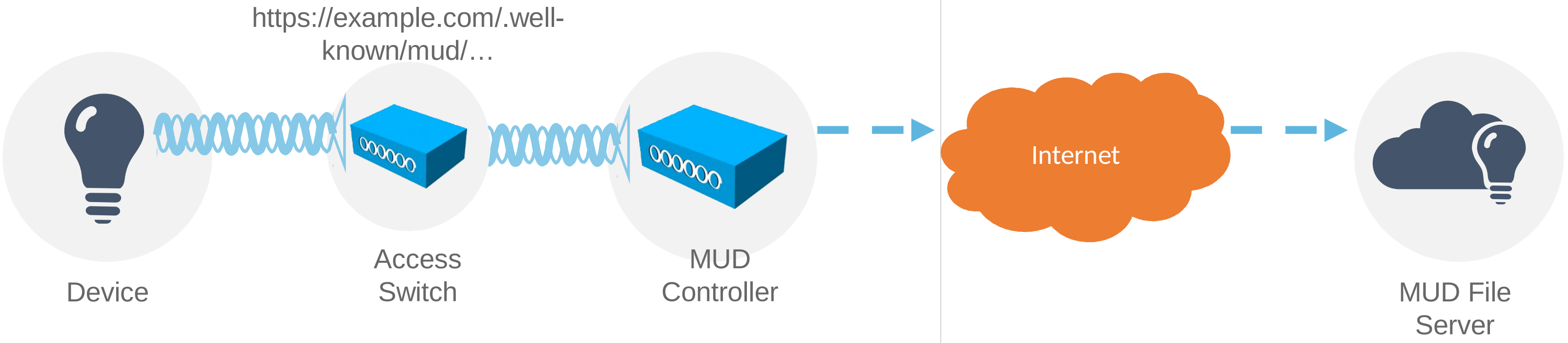
We have some assumptions and constraints

- Things serve a single- or limited number of uses
  - (this solution is not intended for all devices)
- Things 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.
- This approach requires a **file server** and not a semantically-aware NETCONF server serve **files** (or pages).

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

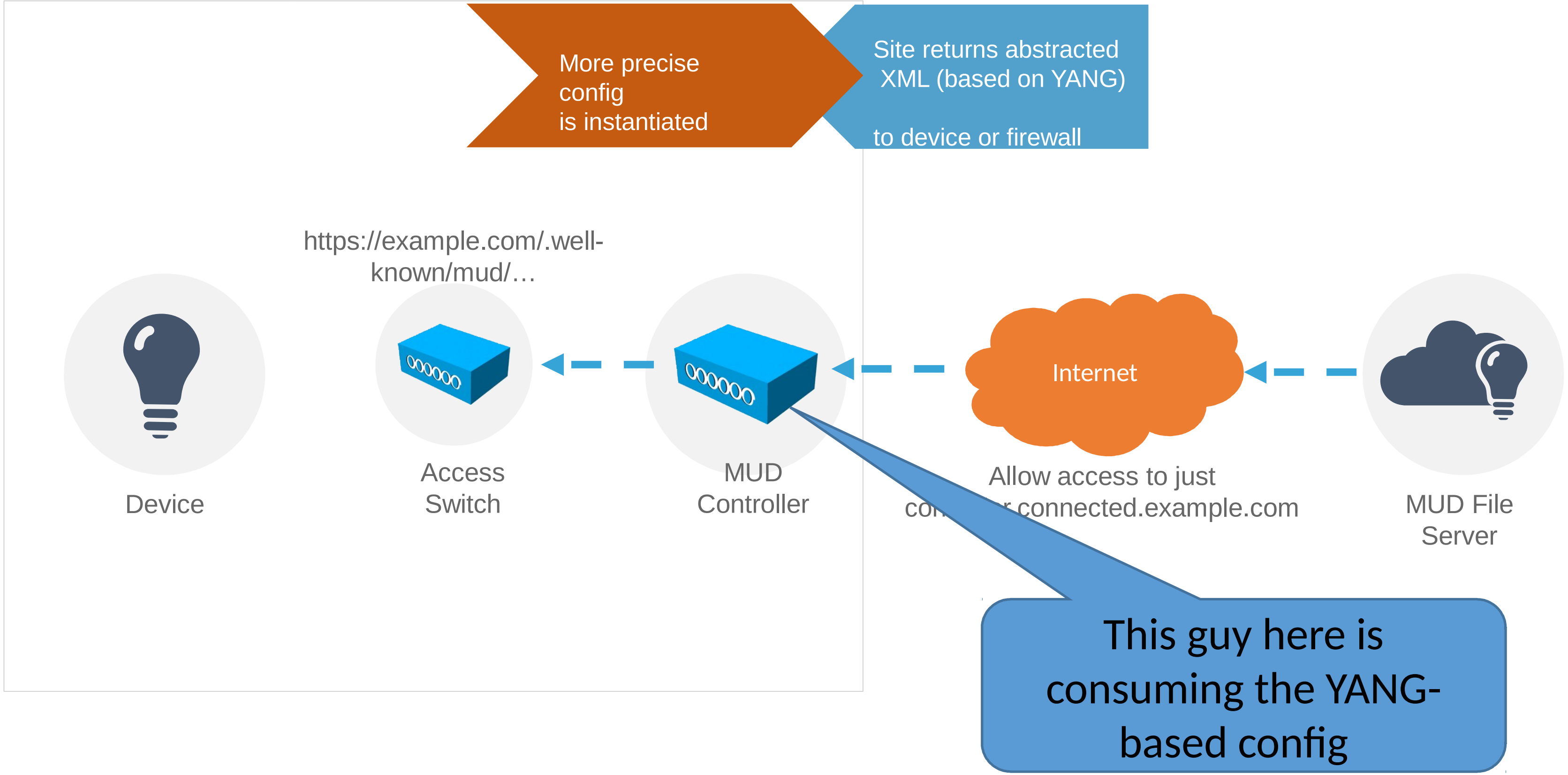
Access Switch

MUD Controller

Internet

MUD File Server

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/…
Device
Access Switch
MUD Controller
Internet
Allow access to just co[illegible]r.connected.example.com
MUD File Server

This guy here is consuming the YANG-based config

Need a way to specify the recommendations

- This is **network configuration information** (access-lists)
- Don’t want to reinvent the wheel (this group is producing access lists)
- The configuration is meant for **millions** of devices in a wide variety of deployments
- We need a way to abstract out certain aspects
  - What controllers a Thing should speak to
  - What is “local”
  - Maybe the notion of a “manufacturer”
  - We need to know how often a MUD controller should query for description updates
  - Some additional meta-information (like linking to ANIMA)

What Controllers a Thing may speak to

- They may be local network management stations
- They may be cloud-based services
  - iPhones speak to Apple for their management
  - Android devices speak to Google for their management

Other functions can be (mostly) described with the existing model.

draft-lear-ietf-netmod-mud-00

- Augments ACL draft
- Adds some meta information
  - When to check for updates
  - MASA server
  - When was file touched last
  - Is the device still supported by the vendor?
- Abstracts away IP addresses
  - manufacturer/same-manufacturer
  - manufacturer, model
  - controller
  - local-networks

draft-lear-ietf-acl-dnsname-00

- Augments the ietf-acl model
- “Just” adds DNS names as a filter
- Approach was based on discussion on the list
- Needs more review

Open Issues & Questions

- Access-lists can be applied both inbound and outbound
  - Let this device (not) transmit to {some set of devices or services}
  - Let this device (not) receive from {some set of devices or services}
  - The existing ACL model does not address this. Should we?
- Given the scale of risk, configuration generated by these models really MUST be signed.
  - There needs to at least be normative reference to how this should be done. Where?
- Normal extensibility mechanisms can't be used. Currently versioning the URI (simplest approach)
  - (Remember, no NETCONF?)

What is needed…

- Would like more eyes on the drafts and the concept
    - **Including co-authors/editors!**
- Can these drafts be adopted as WG drafts?

cisco