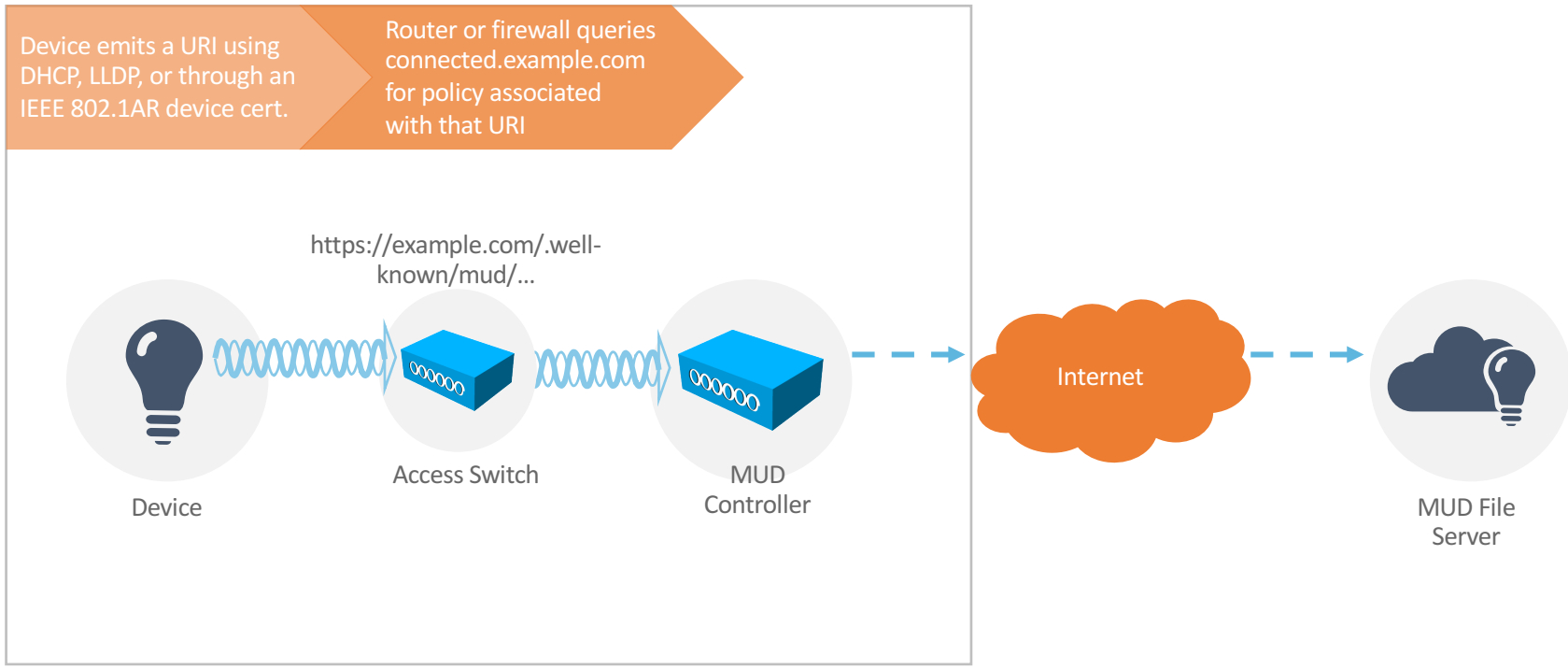
Slinging MUD (an update)

Brian Weis, Eliot Lear

Summary: Manufacturer Usage Descriptions

- A URI sent by a device
- 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

Expressing Manufacturer Usage Descriptions



How to locate the policy? A URL

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

"Manufacturer"

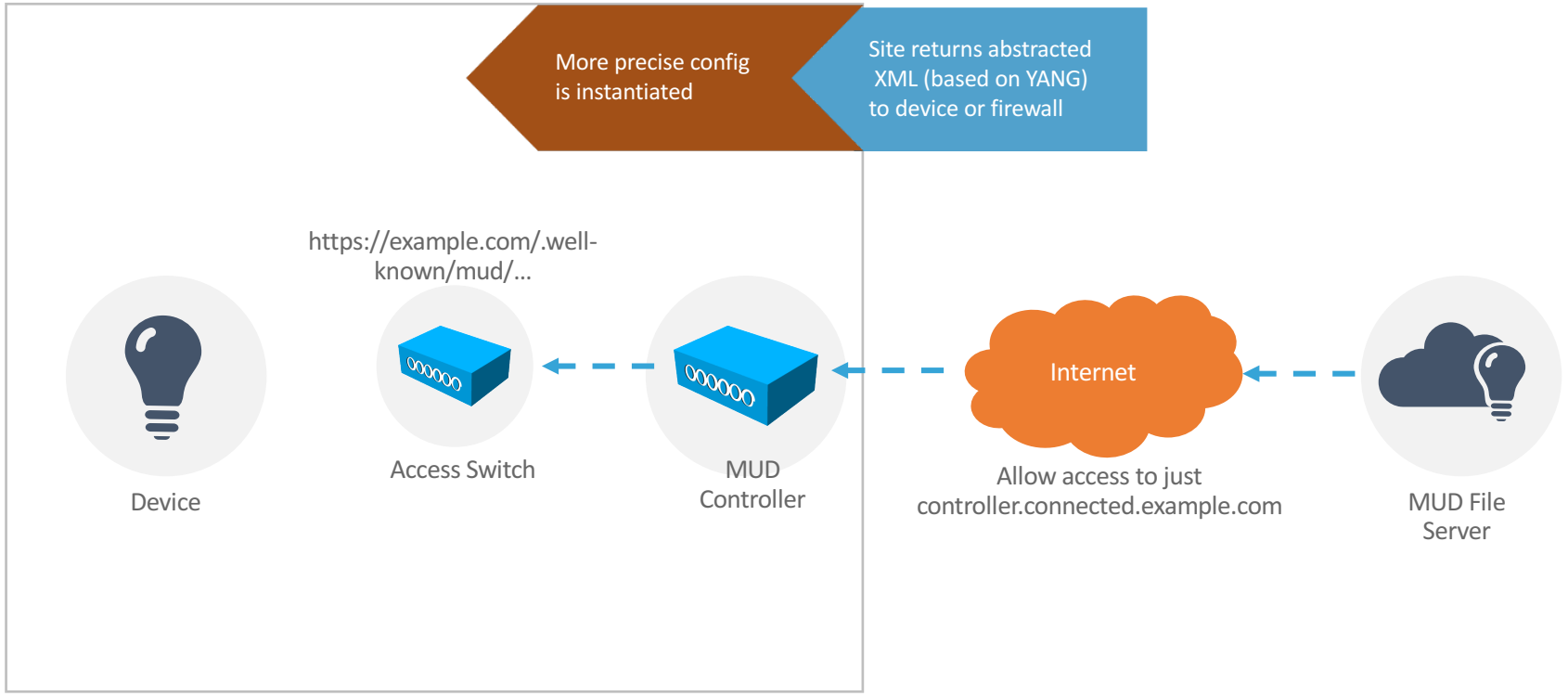
Model

The MUD File

```
{
"ietf-acl:access-lists": {
  "ietf-acl:access-list": [
    {
     "acl-name": "mud-10387-v4in",
     "acl-type": "ipv4-acl",
    "ietf-mud:packet-direction": "to-device",
    "access-list-entries": {
      "ace": [
       {
        "rule-name": "clout0-in",
        "matches" : {
         "ietf-mud:direction-initiated" : "from-device"
          },
        "actions": {
         "permit": [
          null
         ]
        }
       },
       {
        "rule-name": "entin0-in",
        "matches": {
         "ietf-mud:controller":
          "http://dvr264.example.com/controller",
          "ietf-mud:direction-initiated" : "to-device"
         },
         "actions": {
          "permit": [
           null
          ]

         }
        }
       ]
      }
    },
    {
     "acl-name": "mud-10387-v4out",
     "acl-type": "ipv4-acl",
    "ietf-mud:packet-direction": "from-device",
....
```

Expressing Manufacturer Usage Descriptions



Since Last IETF

- WG draft adopted: draft-ietf-opsawg-mud-01 (one update)
- systeminfo: non normative description of the device
- Shortened some of the YANG element names
- A URN for standard controller functions: currently two are envisioned (DNS and NTP)
- Signing and verification updated
- A few more references
- Requested early IANA assignment of namespaces

There's code

- Today, simple MUD controller implementation on Github
  - https://github.com/elear/mud
- MUD file generator
  - https://www.ofcourseimright.com/mudmaker
    (code also available on Github)
- Very shortly, some code for DNS-based ACLs for Linux
  - based on dnscap, observes queries and responses, pairs them up, and generates appropriate iptables rules

A new related draft

- **draft-weis-radext-mud-00**
  - A RADIUS option used by a network element sniffing DHCP or LLDP to relay the MUD URI to a RADIUS server
  - Includes a brief discussion on how the MUD URI is handled by the network element and the RADIUS server

Next steps

- We need more eyes on the YANG model
- We need more eyes on security considerations
  - What happens when…
- We need more experience using MUD
- More code needed (and more code will be provided)