



Manufacturer Usage Descriptions

Automated device classification and policy discovery

Eliot Lear
Principal Engineer
14. Nov. 2019

Today's latest threat: printers

Study cites multi-function printers as some of the most dangerous members of the IoT family



Bitdefender.com, 28 February 2019

What Sort of Access Do These Printers Require?

| From | To | Protocol | Source Port | Destination Port(s) |
|---------|----------------------|----------|-------------|---------------------|
| Printer | xmpp009.hpeprint.com | TCP | | 80, 443, 5222,5223 |
| Printer | DNS Server | UDP | | 53 |
| Printer | chat.hpeprint.com | TCP | | 80,443 |
| Printer | 224.0.0.251/32 | UDP | | 5353 |
| Printer | 220.0.0.252/32 | UDP | | 5355 |
| Printer | h10141.www1.hp.com | TCP | | 80 |
| Printer | Local Networks | UDP | 5353 | |
| Printer | Local Networks | TCP | 80 | |

Source: University of New South Wales, using mudgee

(not shown: L2 packets)

The possibilities are endless



Infusion pumps



Smart lighting



Printers



Industrial Equipment



Parking meters



Security cameras



Refrigerators



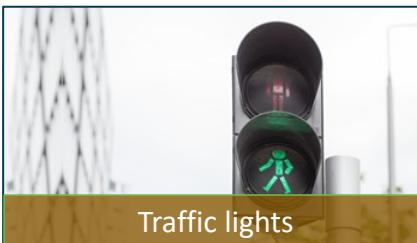
Smart thermostat



HVAC system



Baby monitor



Traffic lights



Point of sale

Assumptions and Assertions

| Assumptions | Assertions |
|---|---|
| A Thing has a single use or a small number of uses. | Because a Thing has a single or a small number of intended uses, all other uses must be unintended. |
| Things are tightly constrained. Very little CPU, memory, and battery. | Any intended use can be clearly identified. |
| Network administrators are the ultimate arbiters of how their networks will be used | Manufacturers are in a generally good position to provide guidance to administrators. |
| Even those Things that can protect themselves today may not be able to do so tomorrow | A mechanism is needed to protect devices that may have vulnerabilities. |

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



Introducing Manufacturer Usage Descriptions (MUD)

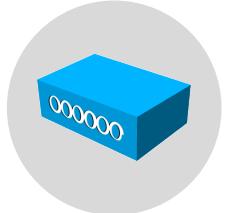
A URL:

<https://manufacturer.example.com/mydevice.json>

A MUD File:

```
...  
  "ace": [ {  
    "name": "cl0-todev",  
    "matches": {  
      "ietf-mud:mud": {  
        "controller": "my-controller"  
      },  
      "actions": {  
        "forwarding": "accept"  
      } } ]  
...  
  ]
```

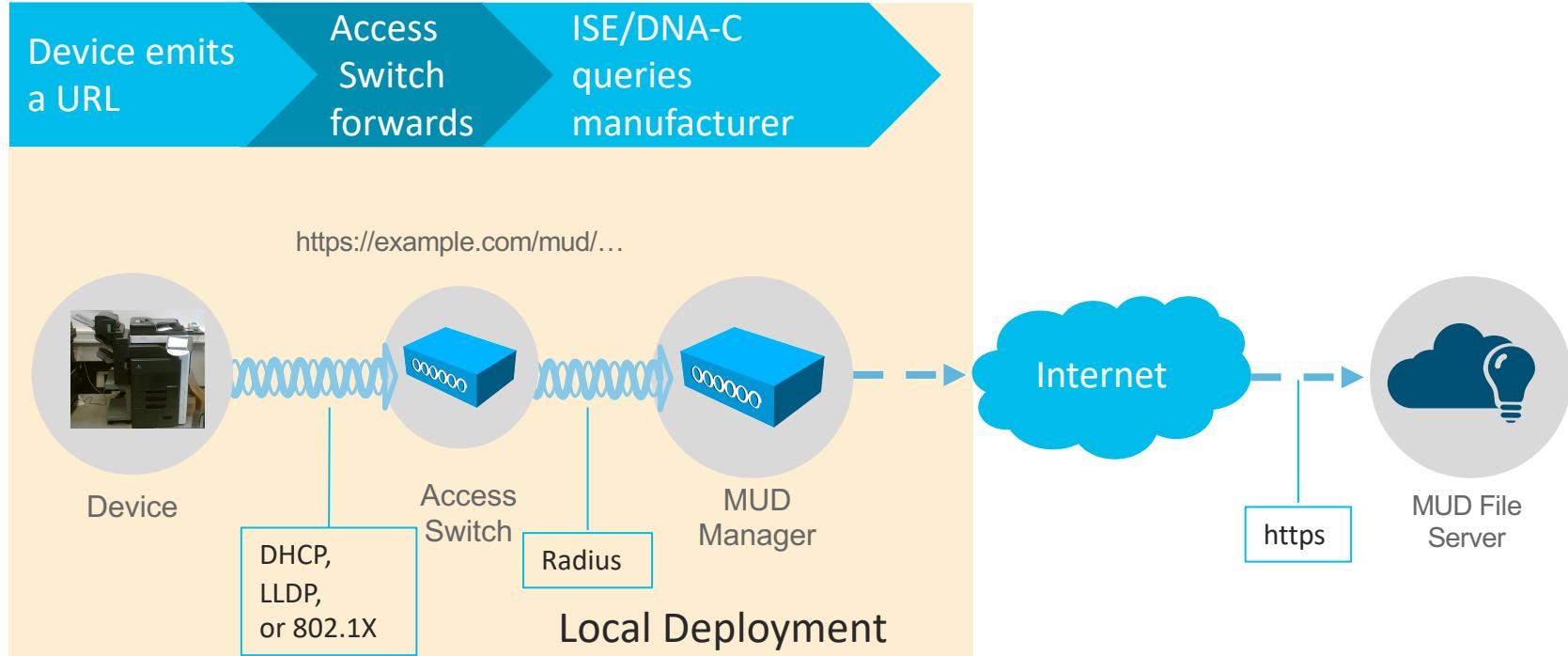
The MUD Manager:



The MUD File Server:

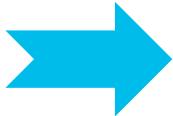


Expressing Manufacturer Usage Descriptions



Getting from the MUD file to deployment config

```
... "acl": [
  {
    "name": "mud-76228-v4to",
    "type": "ipv4-acl-type",
    "aces": {
      "ace": [
        {
          "name": "myctl0-todev",
          "matches": {
            "ietf-mud:mud": {
              "my-controller": [
                null
              ]
            }
          },
          "actions": {
            "forwarding": "accept"
          }
        }
      ]
    }
  }
]
```

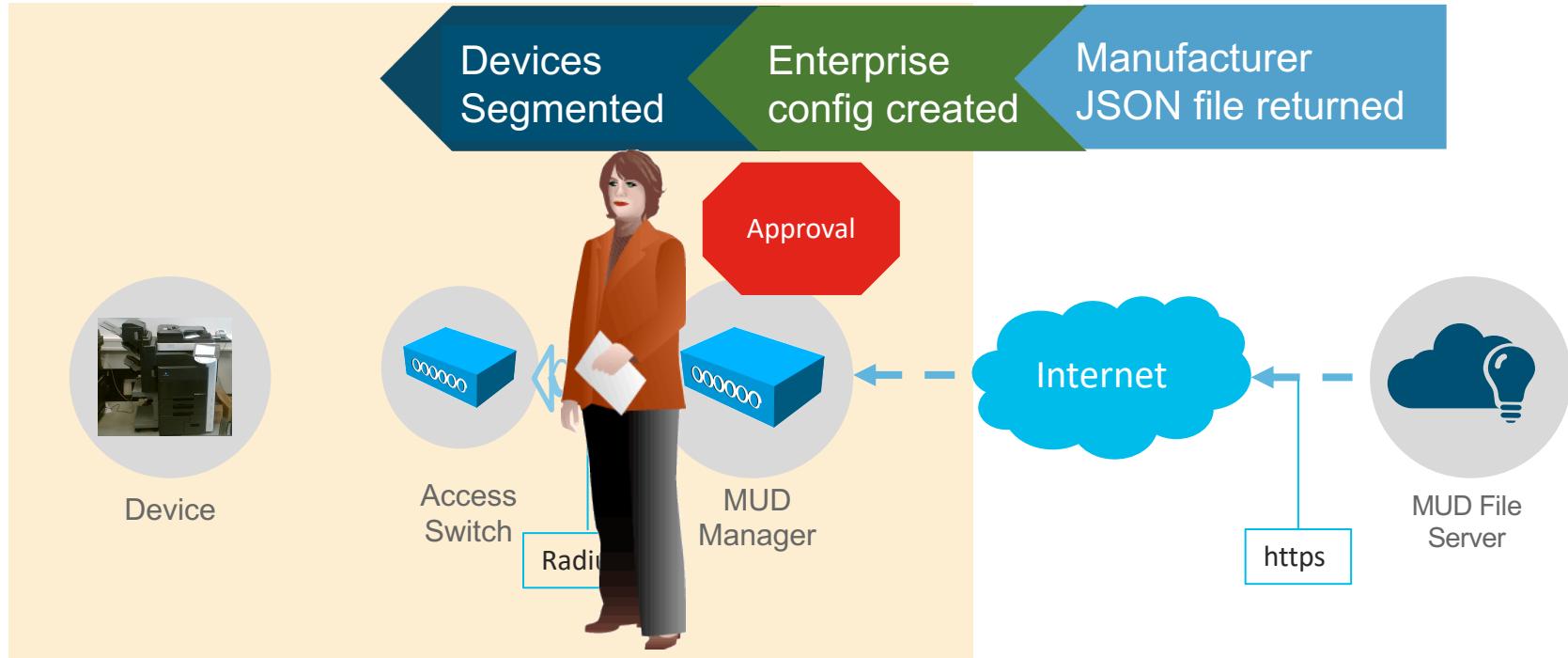


Whatever is appropriate in
the local deployment.

**10.1.2.3
10.4.5.6**

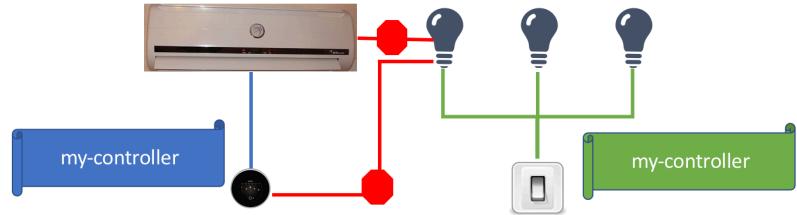
<https://mudmaker.org>

Expressing Manufacturer Usage Descriptions

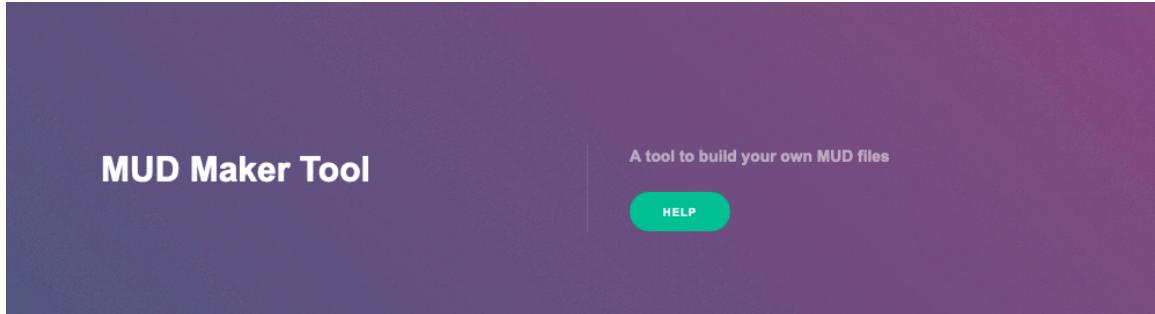


Results

- Devices are automatically segmented based on what sort of access they were designed to have
- Administrator didn't play guessing games



For Device Developers: Authoring Tooling



Please enter host and model the intended MUD-URL for this device: [?](#)

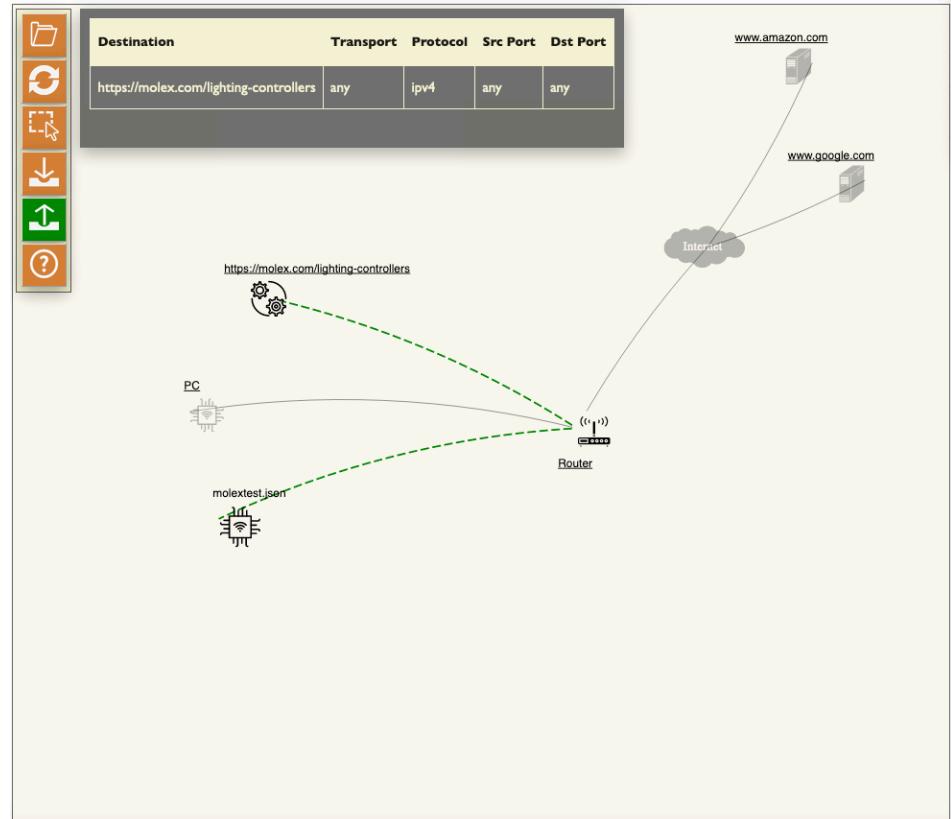
/ (model name here->)

Manufacturer Name

Please provide a URL to documentation about this device:

Please enter a short description for this device:

For Device Developers: Policy Visualization



For Admins: Simple GUI for Approval

CISCO MUD

Device Management

| Sr No. | MAC Address | Endpoint Profile | IP Address | MUD URL |
|--------|----------------|------------------|------------|---|
| 1 | aabb.cddd.eefa | - | | |
| 2 | aabb.cddd.eefe | - | | |
| 3 | aabb.cddd.eeff | - | | http://10.64.69.209:8080 /blindv1.json |

Devices

Group Based Policy Matrix

ACL

Network Elements

CISCO MUD

Policies Associated With http://10.64.69.209:8080/blindv1.json

Approve **Not Approve**

| Sr No. | Pretty Printed Policies | Deployment Policies |
|--------|---|---|
| 1 | permit https://www.example.com/blind-controllers ip | Group Based Policy SGT Click to Add SGT [Device], [Device] Click to Add SGT with ip |
| 2 | permit https://www.example.com/light-controllers ip | ACL Policy permit ip any Click to Add IP 0.0.0.0 |

Group Based Policy
SGT [Device], [Device] [Click to Add SGT](#) with ip

ACL Policy
permit ip any 0.0.0.0

Some MUD characteristics

- MUD configures **the network, and not devices.**
 - Devices require no semantic understanding of MUD or MUD files
 - Almost no additional processing by devices required (just output a MUD URL)
 - MUD makes no promises to device as to what network resources it will be granted access to
- It is a component architecture
 - Use what you want, discard the rest
 - If you only want to classify, take MUD URL, maybe additional “header” information
 - If device doesn’t output MUD URL, it can be associated in other ways
 - Label scan
 - BOM import
 - Imported SBOM component
 - MUD can provide no more than whatever underlying network capabilities exist. It is merely a management function.

Next steps

- Focus has primarily been on L3 Access
 - Work needed to automate controller selection
 - SP/CPE gear integration would help
 - Reporting tooling
- Today MUD can function well on 802.3, 802.11 networks
- MUD can also provide lower level network characteristics in extensions:
 - Expected b/w / frequency profile to test against (important for 3G/5G)
 - DETNET / TSN characteristics

References

- RFC 8520 – Manufacturer Usage Descriptions
- MUD file authoring tool and visualizer
<https://mudmaker.org>
- DACL-based MUD manager
<https://github.com/CiscoDevNet/MUD-Manager>
- Openflow-based MUD Manager
<https://github.com/usnistgov/nist-mud>
- More coming