RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **MBS-R01**

Putting Access Management for the Internet of Things into Practice with MUD

MODERATOR: **Eliot Lear**
Principal Engineer
Cisco Systems
@eliotlear

PANELISTS:

L Jean Camp
Professor of Informatics
Indiana University

Drew Cohen
CEO
Masterpiece Solutions, Inc.

Darshak Thakore
Principal Architect
Cable Labs

Mudumbai Ranganathan
Engineer
National Institutes of Standards and Technology

#RSAC

Let’s talk about an oven

Today’s enterprise threat: printers

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

Bitdefender.com, 28 February 2019

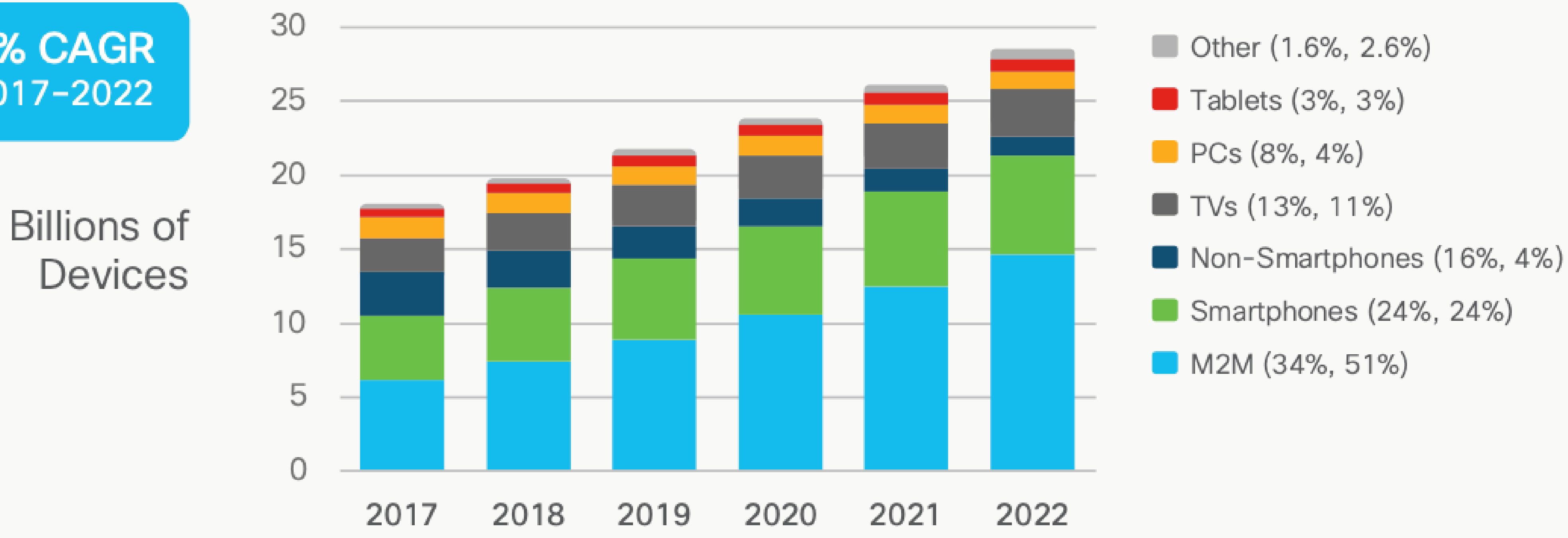
What Sort of Access Do These Printers Require?

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 Internet is already all about IoT

10% CAGR
2017–2022



* Figures (n) refer to 2017, 2022 device share

Source: Cisco VNI Global IP Traffic Forecast, 2017–2022

Ask the Audience!

- What percentage of devices in your network are IoT?
  - A: less than 20%
  - B: greater than 20%
  - C: don’t know

  - Go To The Poll

Scaling Problem: Number of Types of Things

Why is this important to NIST and what’s going on?

Why NIST?

- NIST is concerned with protecting our critical IT infrastructure.
  - Unsecured / unrestricted IOT devices can have a large impact on our critical infrastructure.
  - Secured IOT identified as key component for resilience against botnet attacks (DOC/DHS report May 2017).
  - NIST is involved with evaluating and promoting standards for IOT Cybersecurity.

Sample of NIST Activities

- Publications to provide security guidance for device manufacturers.
- Practice guides for technology deployment.
- Early prototyping of emerging standards.
- Participation in standards activities.
- Research on how emerging standards can be utilized in improving IOT Cybersecurity.
- Workshops and industry outreach.

- NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
- NISTIR 8259: Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers
- NIST SPECIAL PUBLICATION 1800-15A,B,C : Securing Small-Business and Home Internet of Things (IoT) Devices Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

RSAConference2020

What Is Manufacturer Usage Descriptions (MUD)?

Delivering device intent

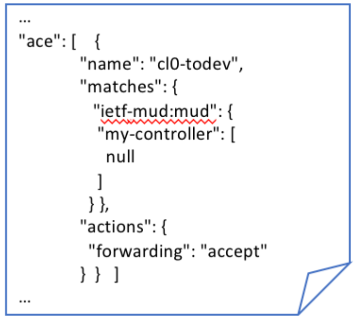
MUD: A component architecture

A URL:

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

The MUD Manager:

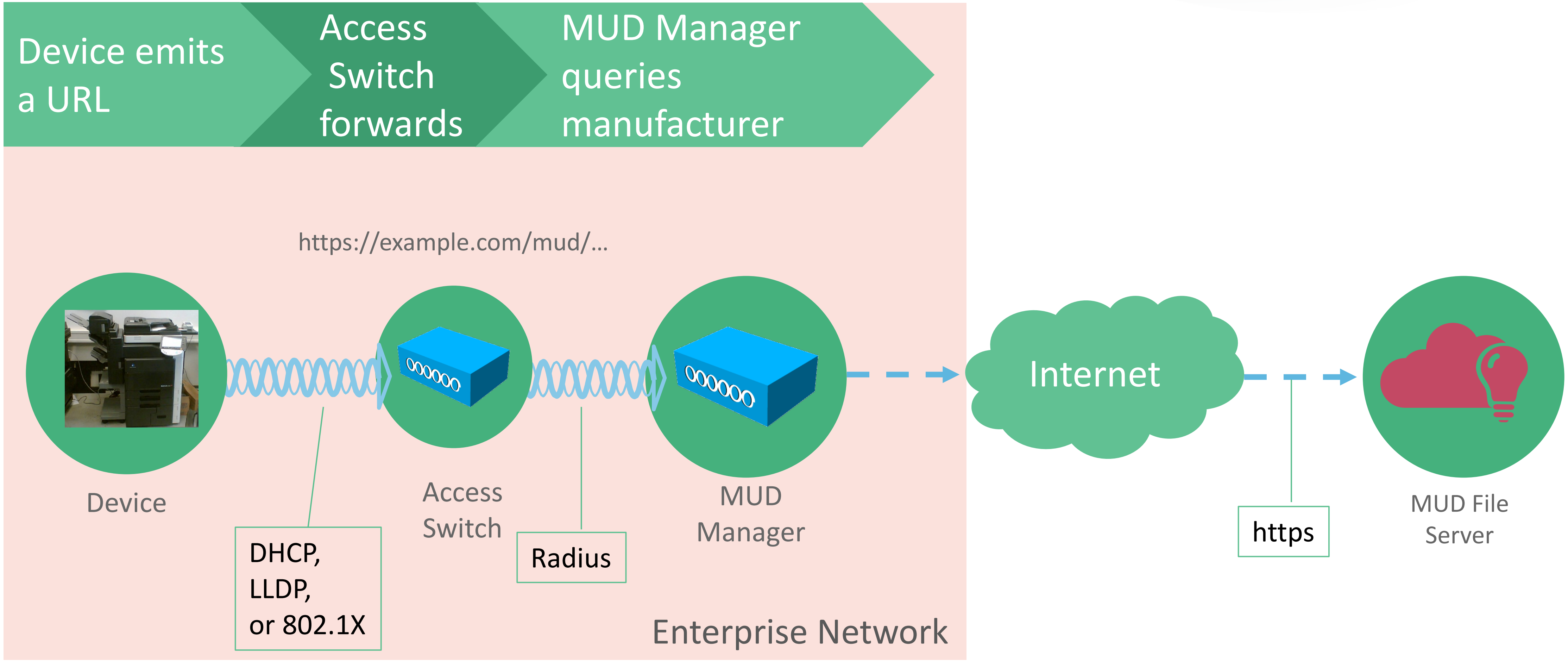
A MUD File:



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

The MUD File Server:

Expressing Manufacturer Usage Descriptions



Device emits a URL

Access Switch forwards

MUD Manager queries manufacturer

https://example.com/mud/...

Device

Access Switch

MUD Manager

Internet

MUD File Server

DHCP,
LLDP,
or 802.1X

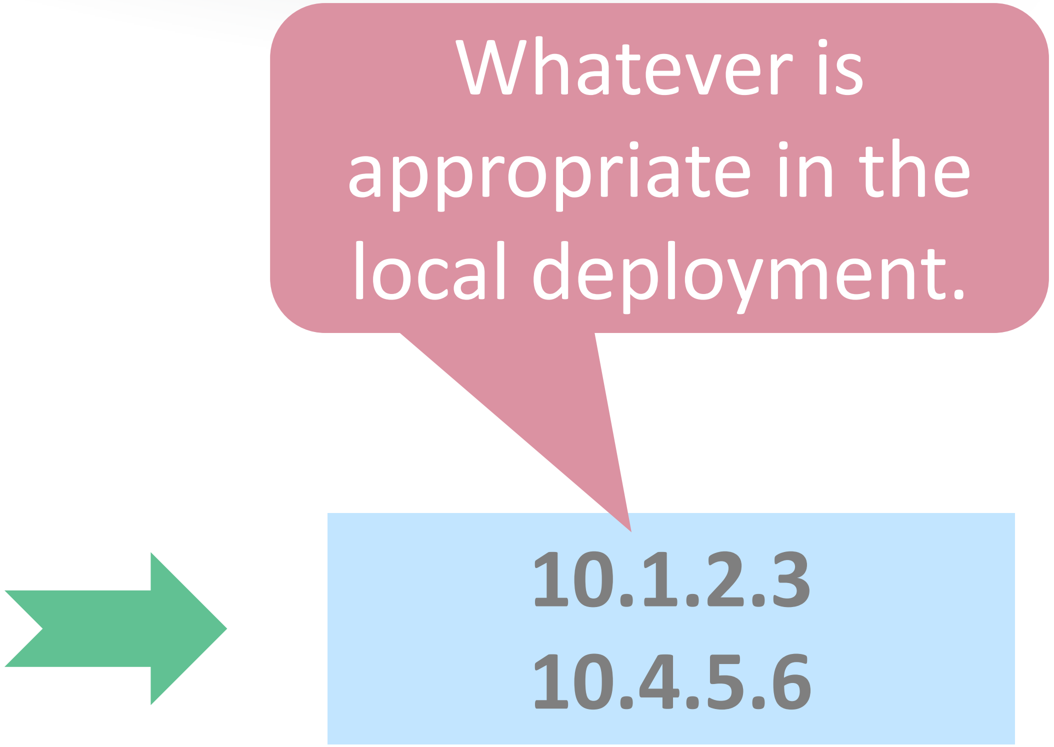
Radius

https

Enterprise Network

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"
            } ...
```

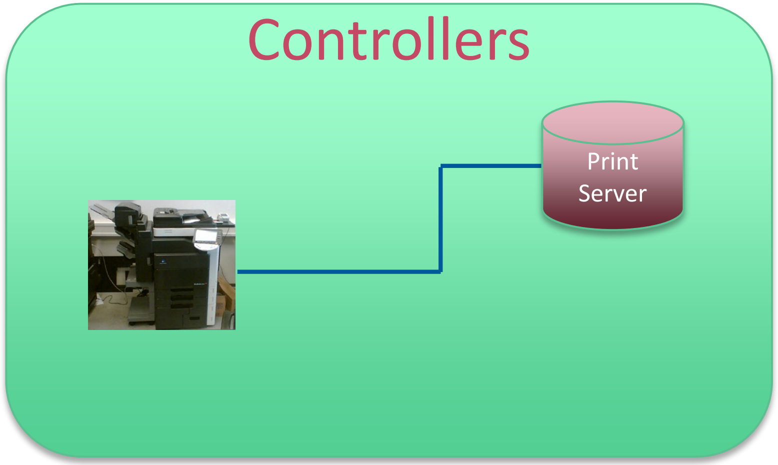


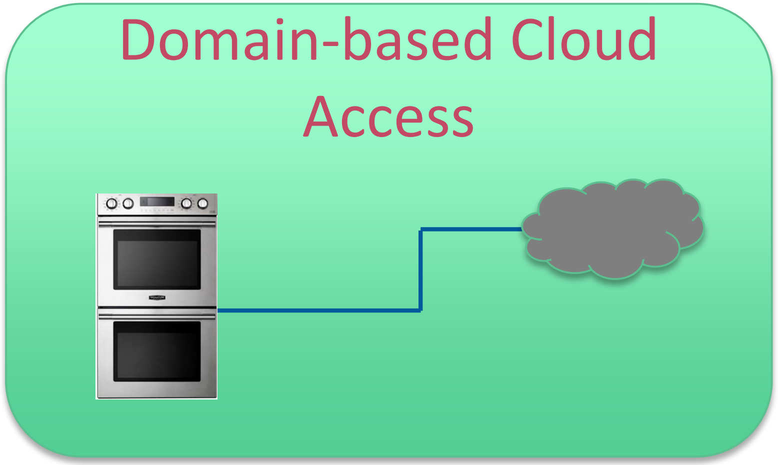
Whatever is appropriate in the local deployment.

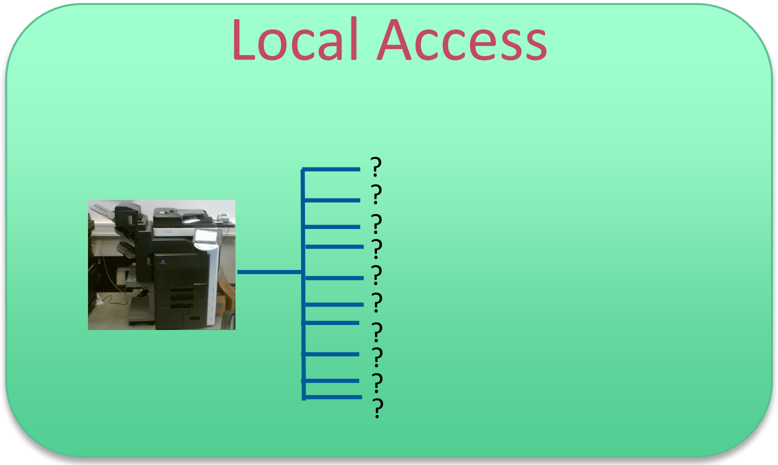
10.1.2.3
10.4.5.6

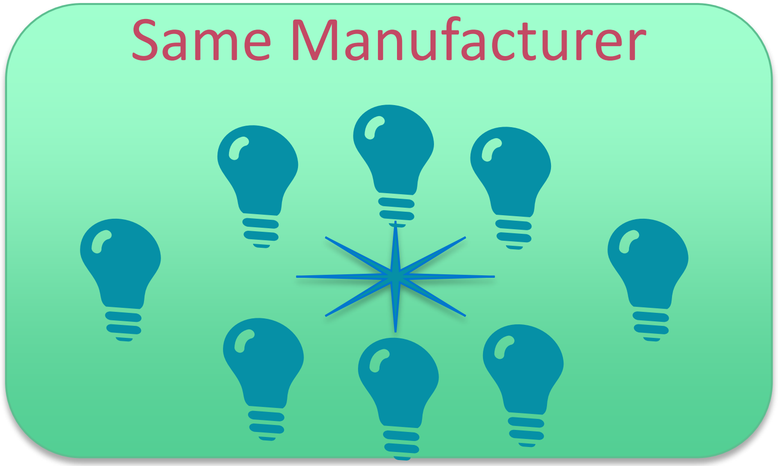
https://mudmaker.org

What Classes of Endpoints MUD provides access to

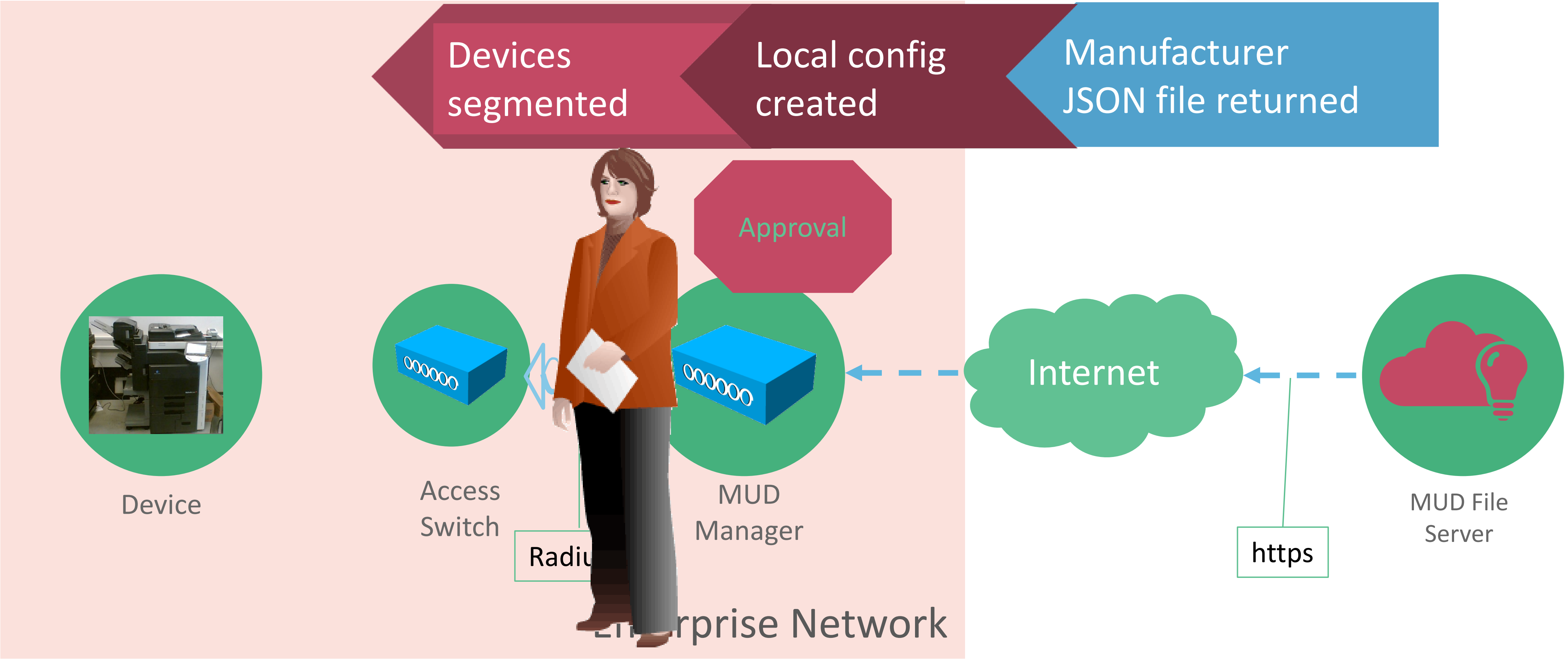

Controllers


Domain-based Cloud Access

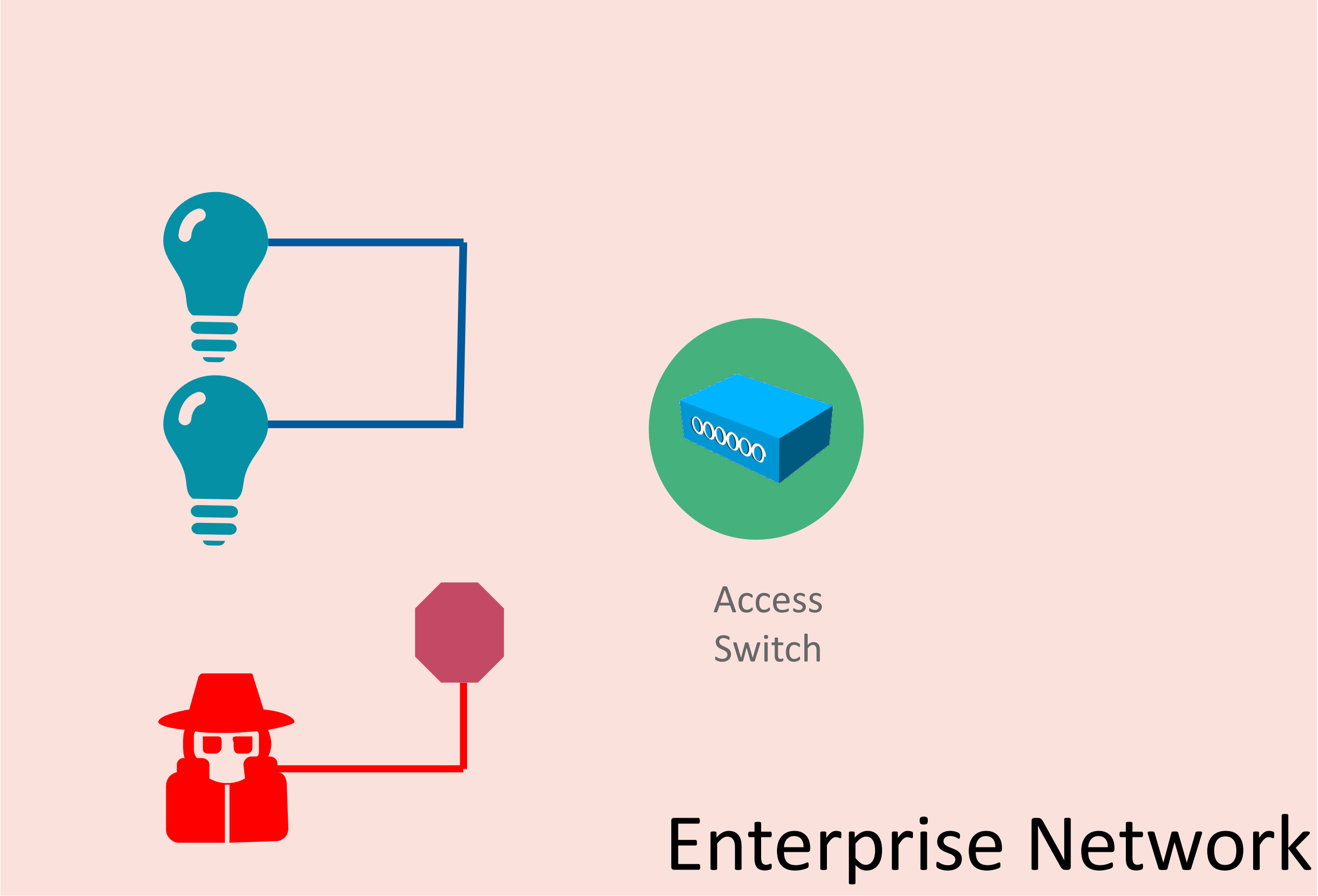

Local Access


Same Manufacturer

Expressing Manufacturer Usage Descriptions



Results: Micro-segmentation of that Thing



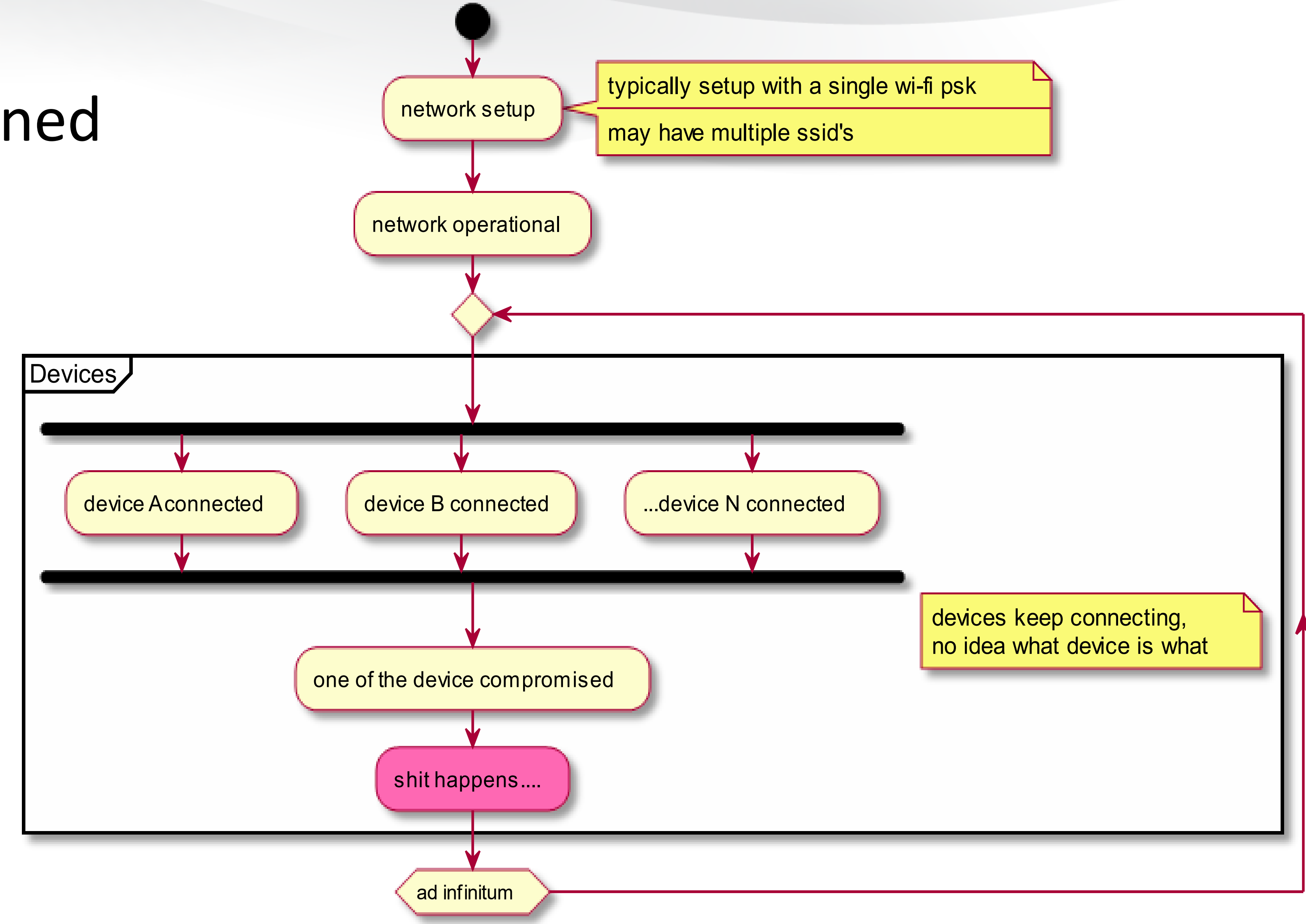
- Visibility of what’s on the network
- Access limited to devices based on manufacturer recommendations
- Policy choices easily identified by MUD file
- Hacked devices can’t probe for holes
- An additional layer of security
  - BUT- manufacturers should still **always** secure their devices

RSA Conference2020

What are the economic incentives?

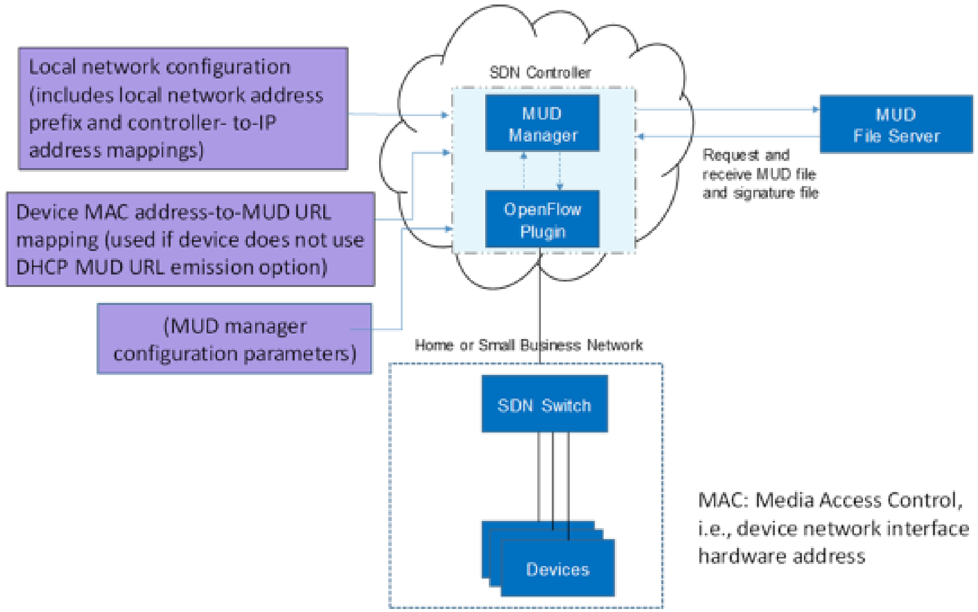
Network's viewpoint

- Network is a constrained resource
- Today's vicious cycle



What does this mean for enterprises and consumers? An implementor’s perspective

NIST-MUD:
Scalable Software-Defined Access Control for IOT



Local network configuration (includes local network address prefix and controller- to-IP address mappings)
Device MAC address-to-MUD URL mapping (used if device does not use DHCP MUD URL emission option)
(MUD manager configuration parameters)
SDN Controller
MUD Manager
OpenFlow Plugin
MUD File Server
Request and receive MUD file and signature file
Home or Small Business Network
SDN Switch
Devices

MAC: Media Access Control, i.e., device network interface hardware address

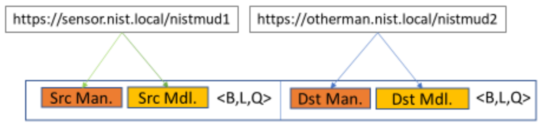
Research Questions

- Can the standard be implemented in a memory scalable fashion using SDN?
- What are the performance impacts?

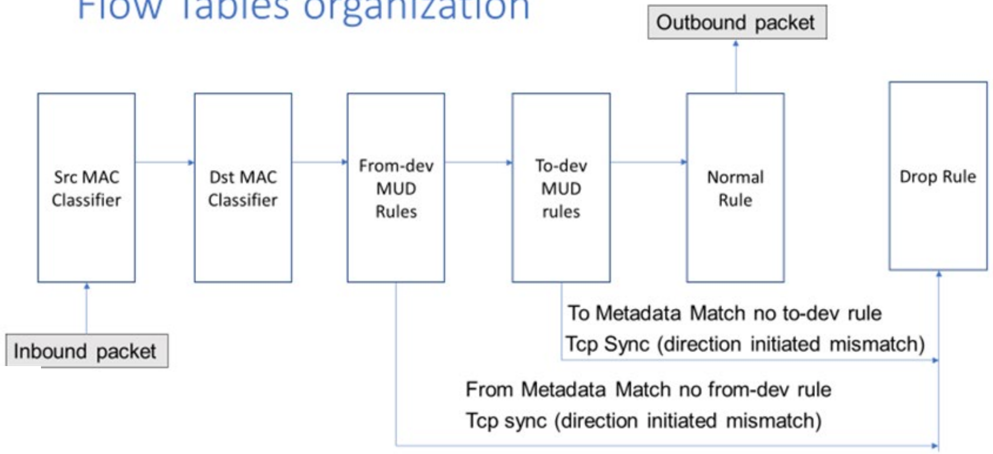
Multi-table design for memory scalability

Metadata Organization

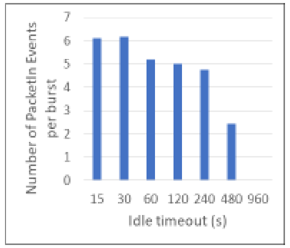
B = "Blocked" bit
L= "Local Networks bit
Q="Quarantine" bit

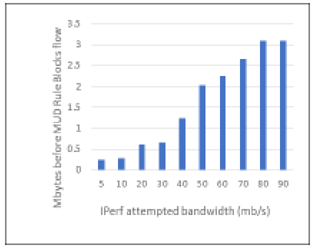

https://sensor.nist.local/nistmud1
https://otherman.nist.local/nistmud2
Src Man.
Src Mdl.
<B,L,Q>
Dst Man.
Dst Mdl.
<B,L,Q>

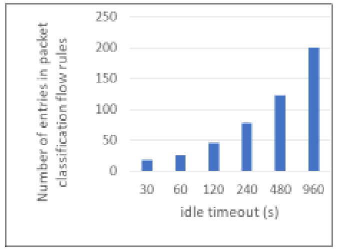
Flow Tables organization


Outbound packet
Src MAC Classifier
Dst MAC Classifier
From-dev MUD Rules
To-dev MUD rules
Normal Rule
Drop Rule
Inbound packet
To Metadata Match no to-dev rule
Tcp Sync (direction initiated mismatch)
From Metadata Match no from-dev rule
Tcp sync (direction initiated mismatch)

Performance Measurements

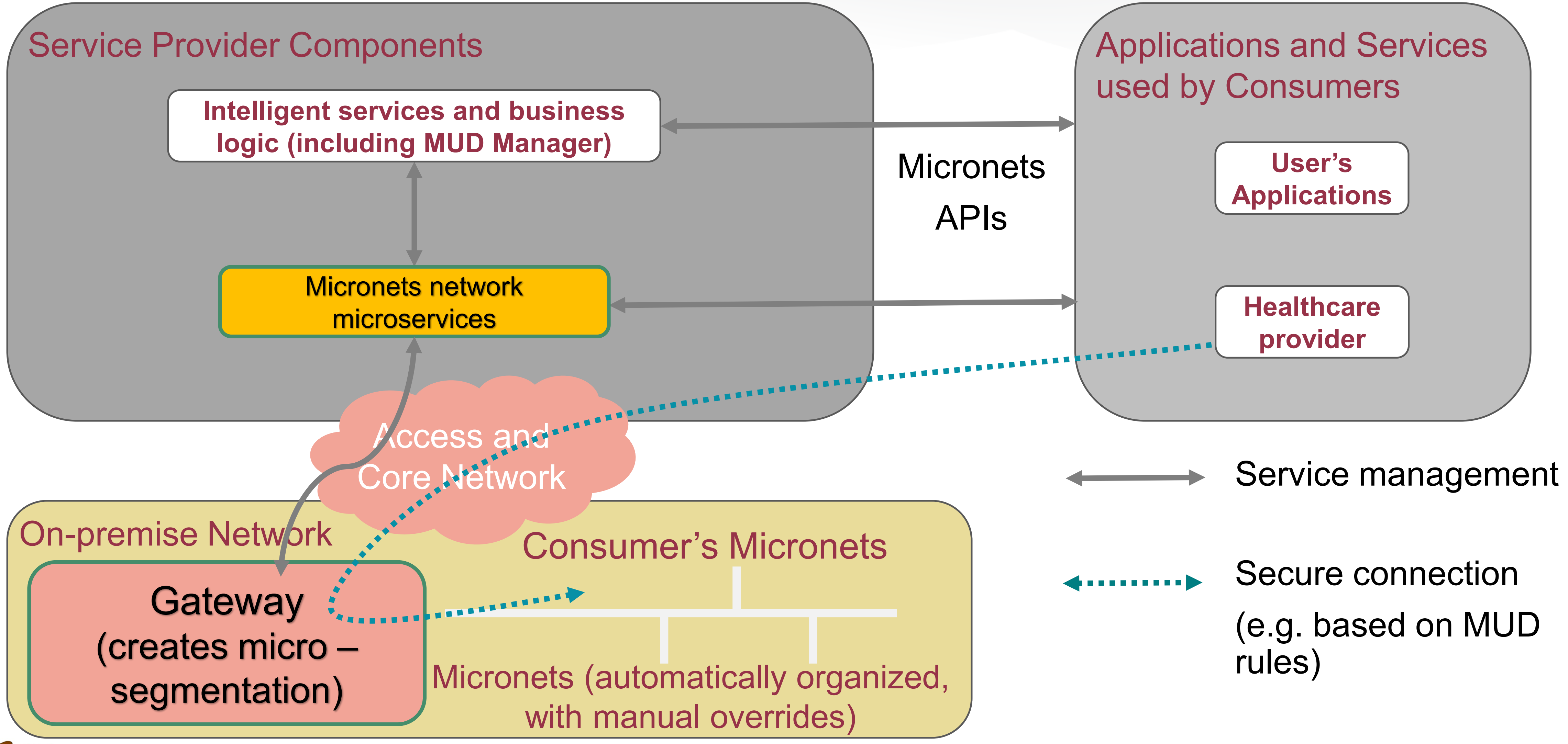






Ranganathan M., Montgomery D., El-Mimouni O., "Soft-MUD: Implementing Manufacturer Usage Descriptions on OpenFlow SDN Switches," Int. Conf. Networks, 2019.

Micronets Reference Architecture

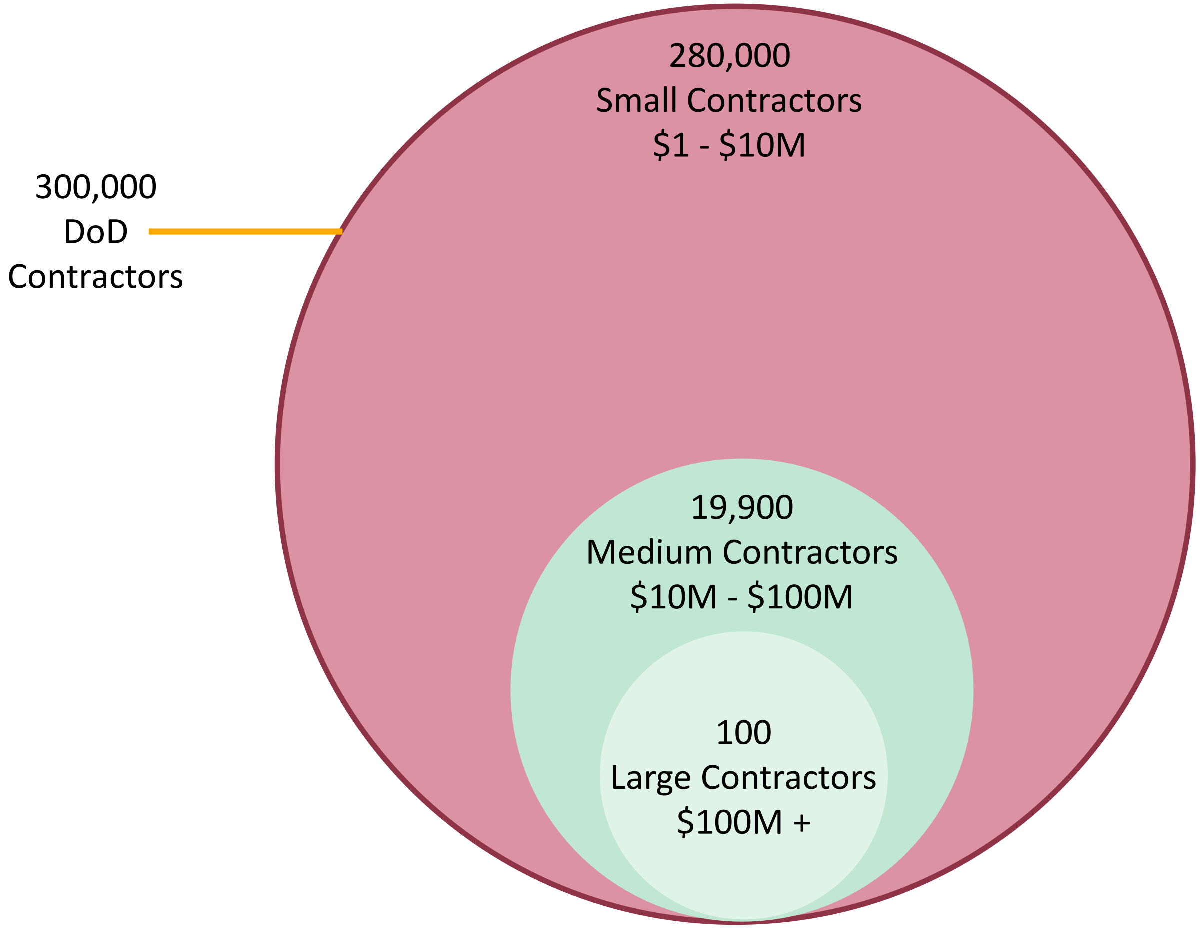

Service Provider Components
Intelligent services and business logic (including MUD Manager)
Micronets network microservices
Micronets APIs
Applications and Services used by Consumers
User's Applications
Healthcare provider
Access and Core Network
On-premise Network
Gateway (creates micro – segmentation)
Consumer's Micronets
Micronets (automatically organized, with manual overrides)
Service management
Secure connection (e.g. based on MUD rules)

Findings

- OpenFlow provides a convenient platform for implementing the standard.
- Standard may be implemented efficiently even on limited memory devices.
  - O(N) flow rules for N devices at the switch.
- Normal (non-IOT) traffic can co-exist with IOT traffic.
  - Can be isolated using SDN flow rules without needing VLANs.
- Eventually consistent behavior results in least performance impact.

DIB Small Businesses

The Largest Threat Vector & Most Challenged by CMMC



- To meet CMMC requirements, DIB contractors will require investment in a suite of cybersecurity products.
- The costs and effort of achieving CMMC is disproportionally higher for Small Businesses.
  - Large businesses can amortize CMMC costs over a larger contract base
  - Large businesses typically have better IT support than small businesses
  - The top Cyber products are focused on large businesses, making them costly and difficult to implement on Small Business infrastructure (often a single, consumer grade Wi-Fi router)
  - ***There is a gap in cost effective small business network defense***
- *Yikes!* is a low-cost, easy to implement option for small businesses **to achieve level 4/5 CMMC** compliance.

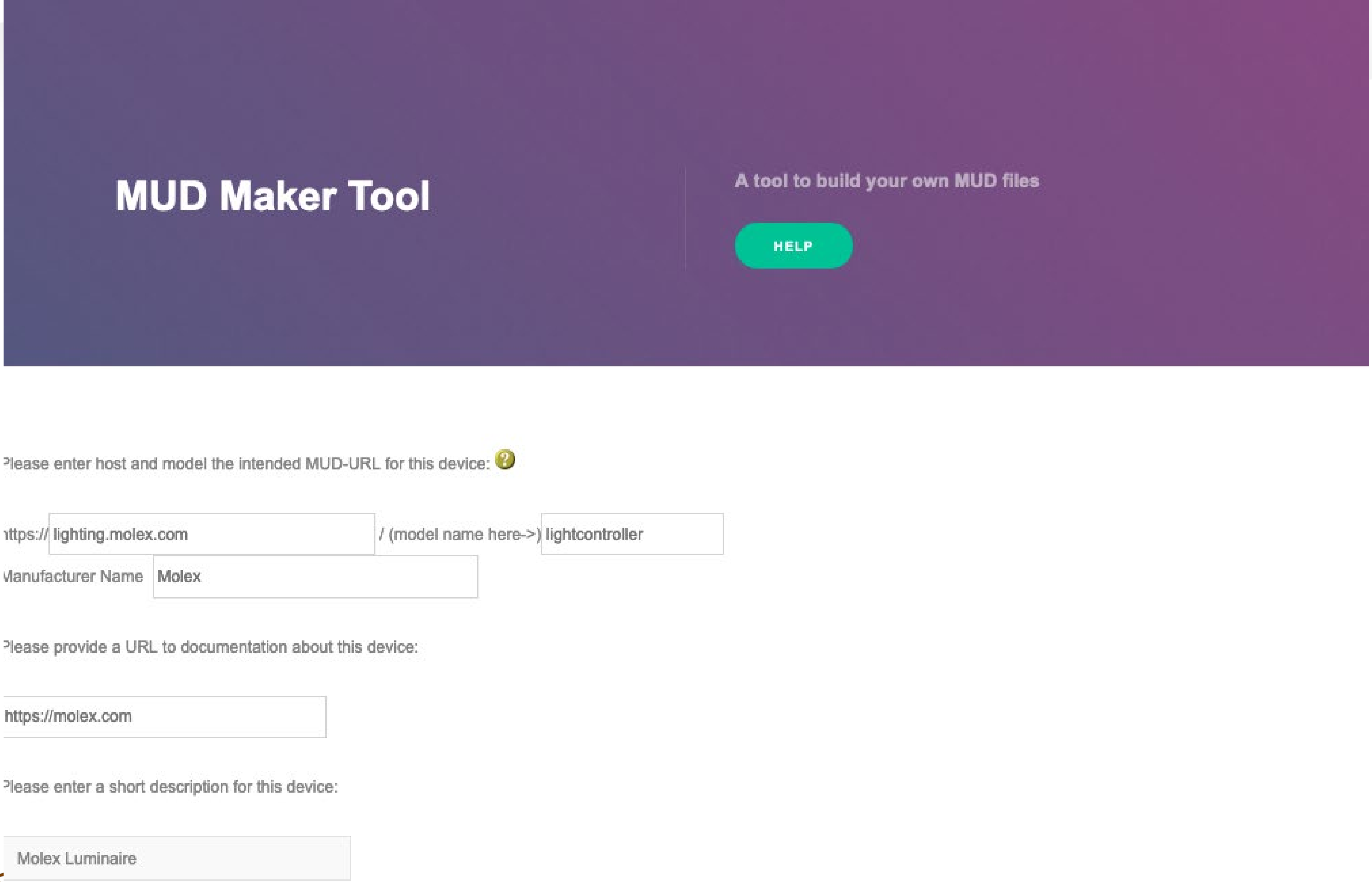
MUD

The *Yikes!* Solution

- Easy to Install – Built on consumer grade equipment and setup requires no specialized IT or Cyber knowledge
- Employs virtualized software defined network (SDN) architecture for unparalleled flexibility and integration.
- Automatic device identification and device isolation to facilitate appropriate behavior, automatically blocking/mitigating many threat vectors by default.
- Automatically detects device and traffic anomalies, performs DNS trust checks, and monitors threat signals.

Mobile Application + Cloud Service + Router Software

What Tooling Is There?



MUD Maker Tool

A tool to build your own MUD files

Please enter host and model the intended MUD-URL for this device: ?

https:// lighting.molex.com / (model name here->) lightcontroller

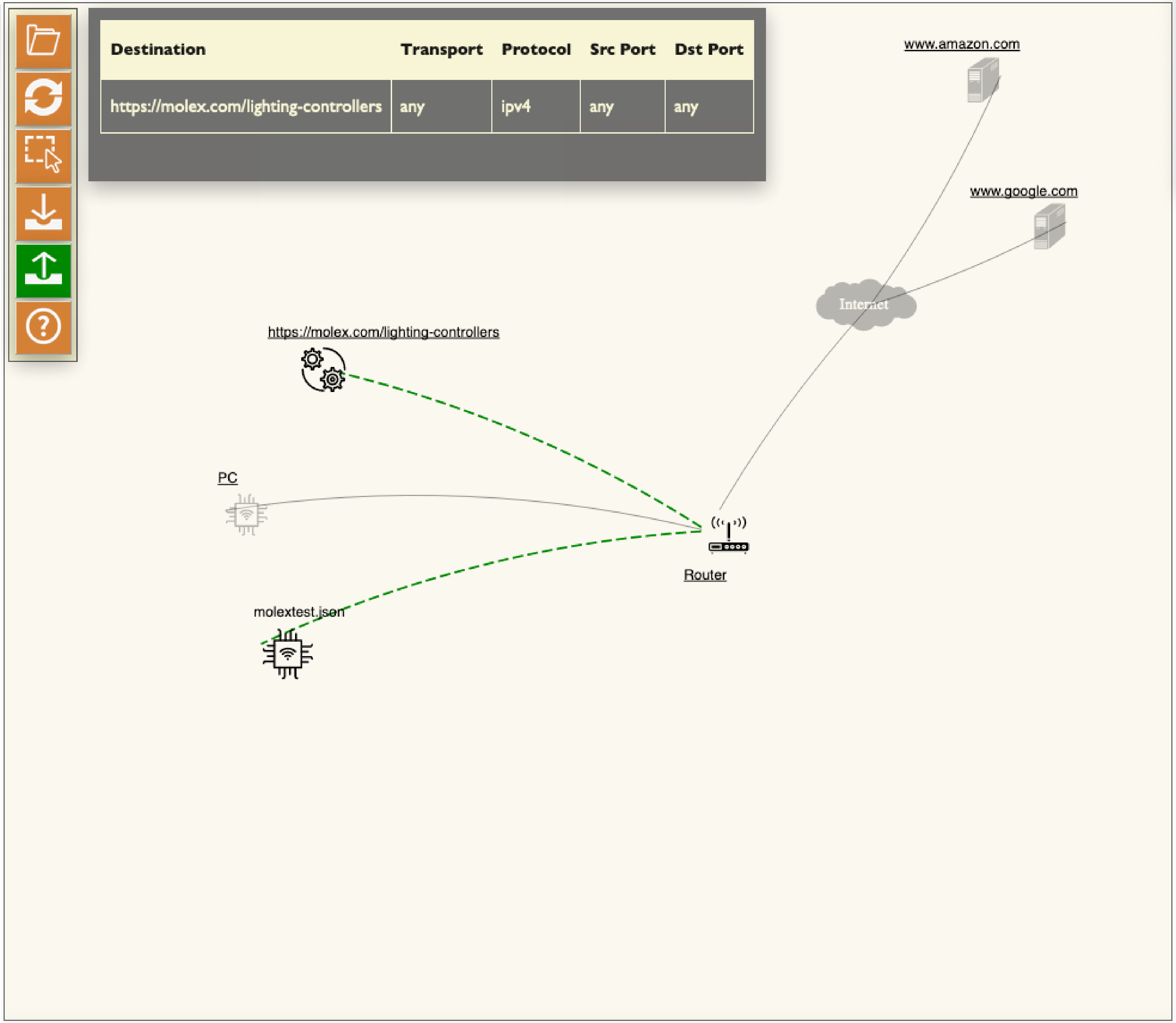
Manufacturer Name Molex

Please provide a URL to documentation about this device:

https://molex.com

Please enter a short description for this device:

Molex Luminaire



Destination	Transport	Protocol	Src Port	Dst Port
https://molex.com/lighting-controllers	any	ipv4	any	any

What should you be doing…

- Demand that manufacturers create MUD files
  - The tooling is there
  - Requires and demonstrates that they understand their own devices' communications needs
- Read up on MUD
  - RFC 8520
  - NIST 1800-15, Parts A-D: a practice guide
  - www.mudmaker.org