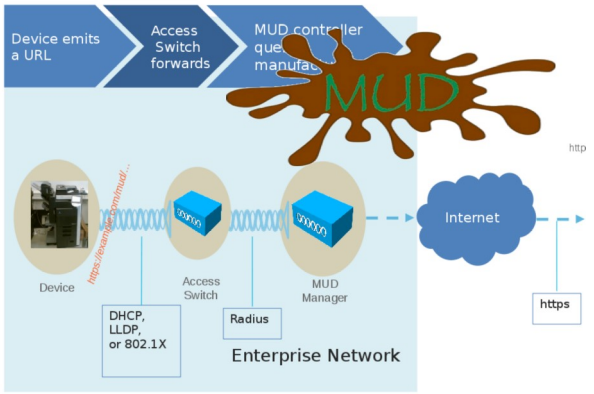
STUFF


Device emits a URL
Access Switch forwards
MUD
http
Internet
Device
Access Switch
MUD Manager
https
DHCP, LLDP, or 802.1X
Radius
Enterprise Network

MUD (RFC8520) overview

Manufacturer Usage Description RFC8520

These slides adapted
From a set from Eliot Lear

Manufacturer Usage Description addresses four questions:

Manufacturer Usage Description addresses four questions:

What is this Thing?

Manufacturer Usage Description addresses four questions:

What is this Thing?

- The MUD URL identifies the device to the network. It can provide it's model name/type!
  - [BRSKI can provide the serial number]
- Informs the NOC or resident what is on their network

Manufacturer Usage Description addresses four questions:

What is this Thing?

Who is responsible for it?

Manufacturer Usage Description addresses four questions:

What is this Thing?

Who is responsible for it?

- If something breaks, who should be called?

Manufacturer Usage Description addresses four questions:

Manufacturer Usage Description addresses four questions:

- With which devices should it communicate?

Manufacturer Usage Description addresses four questions:

Manufacturer Usage Description addresses four questions:

What is this Thing?

Who is responsible for it?

What access does it need?

Is it doing what it should be doing?

- With which devices is it actually communicating?
- Is it behaving as designed?

Background Assumptions and Assertions

Assumptions

Assertions

Background Assumptions and Assertions

Assumptions

Assertions

Background Assumptions and Assertions

Assumptions

Assertions

Background Assumptions and Assertions

Assumptions

A Thing has a single use or a small number of uses.

Assertions

Background 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.

Background 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.	

Background 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.

Background 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	

Background 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.

Background 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	

Background 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 become vulnerable.

Background 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 become vulnerable.

Not true
For desktops, Phones, and Devices that Learn skills

Background 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 become vulnerable.

Third parties Can provide Additional advice

Background 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 become vulnerable.

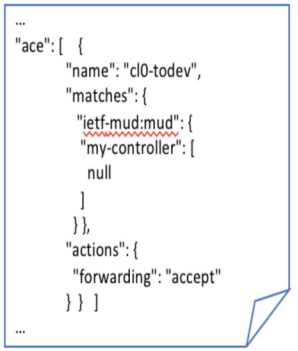
Positive Identification Of each Device Enables Additional controls

Introducing
Manufacturer Usage Descriptions (MUD)

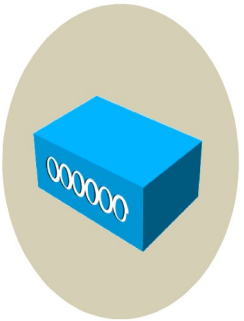
A URL:

The MUD File Server:

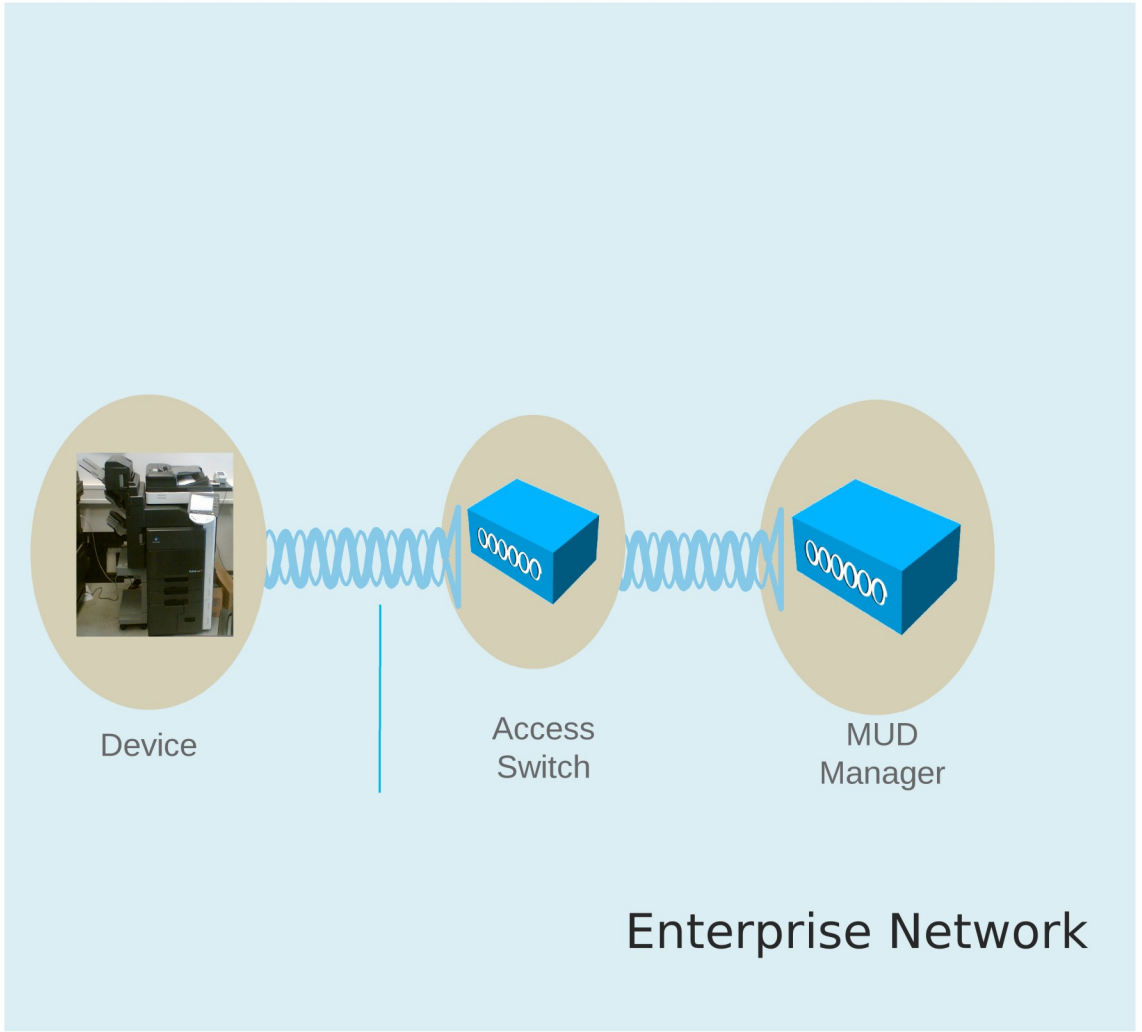
A MUD File:



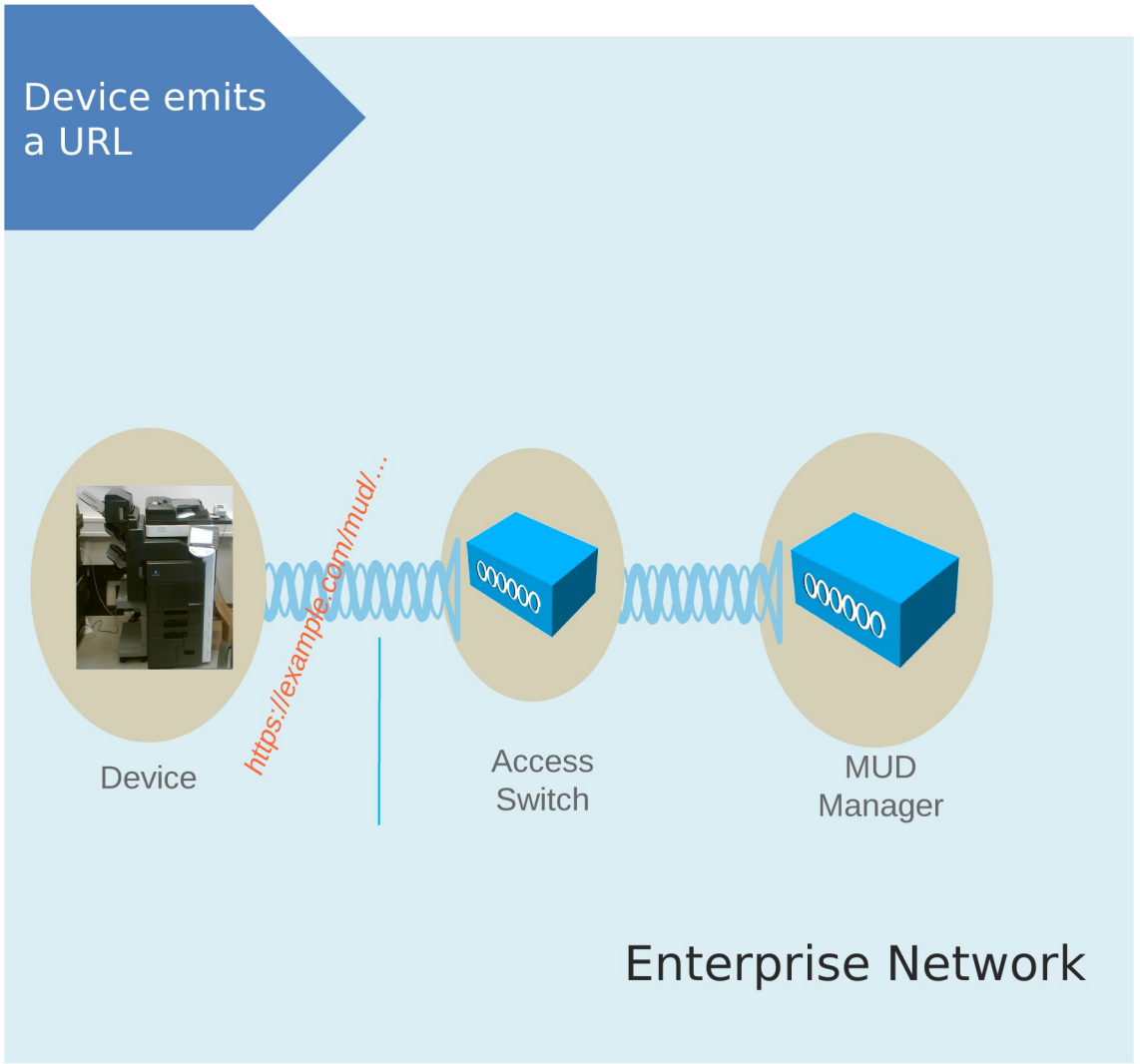
The MUD Manager:



Expressing Manufacturer Usage Descriptions

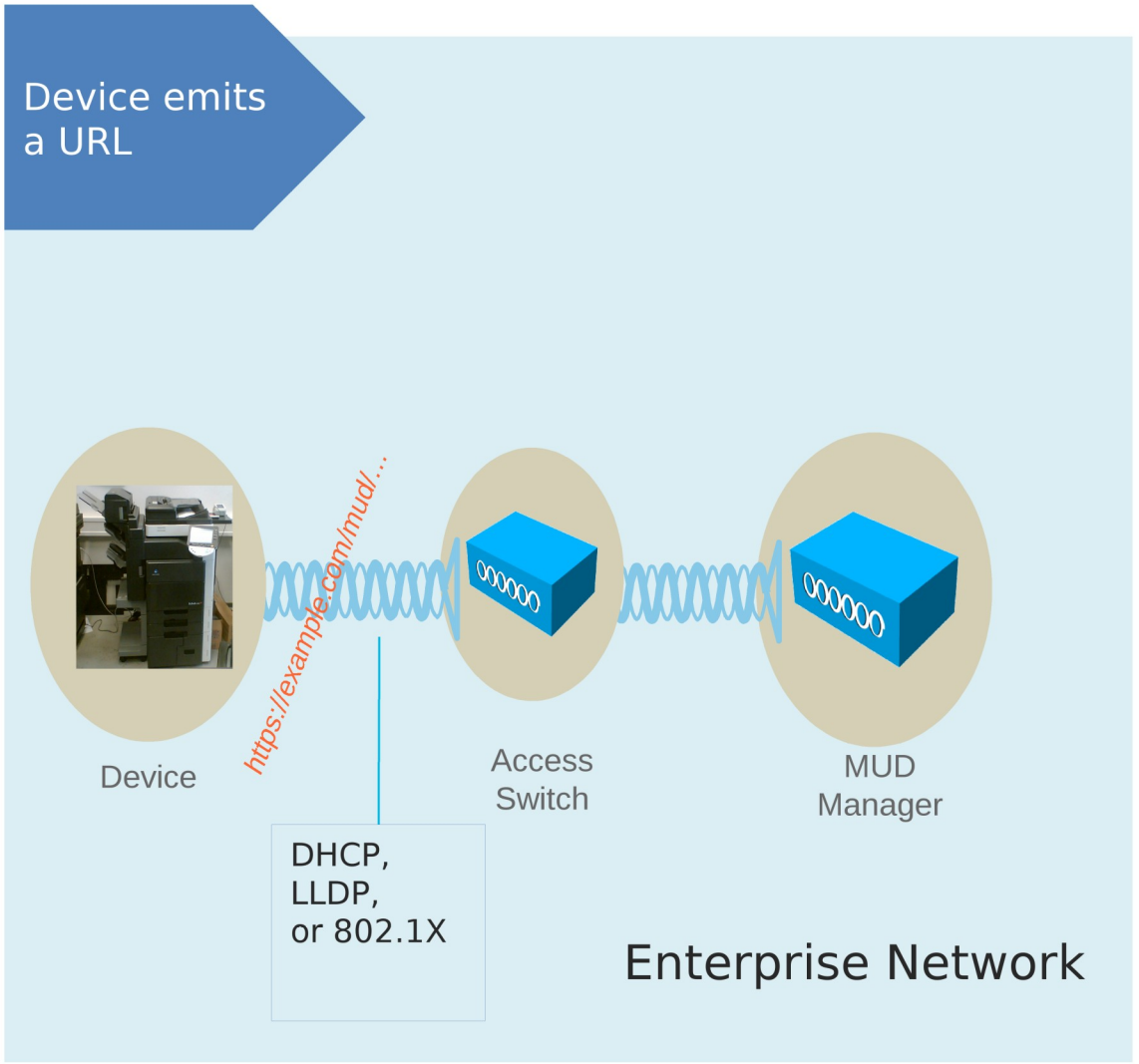


Expressing Manufacturer Usage Descriptions



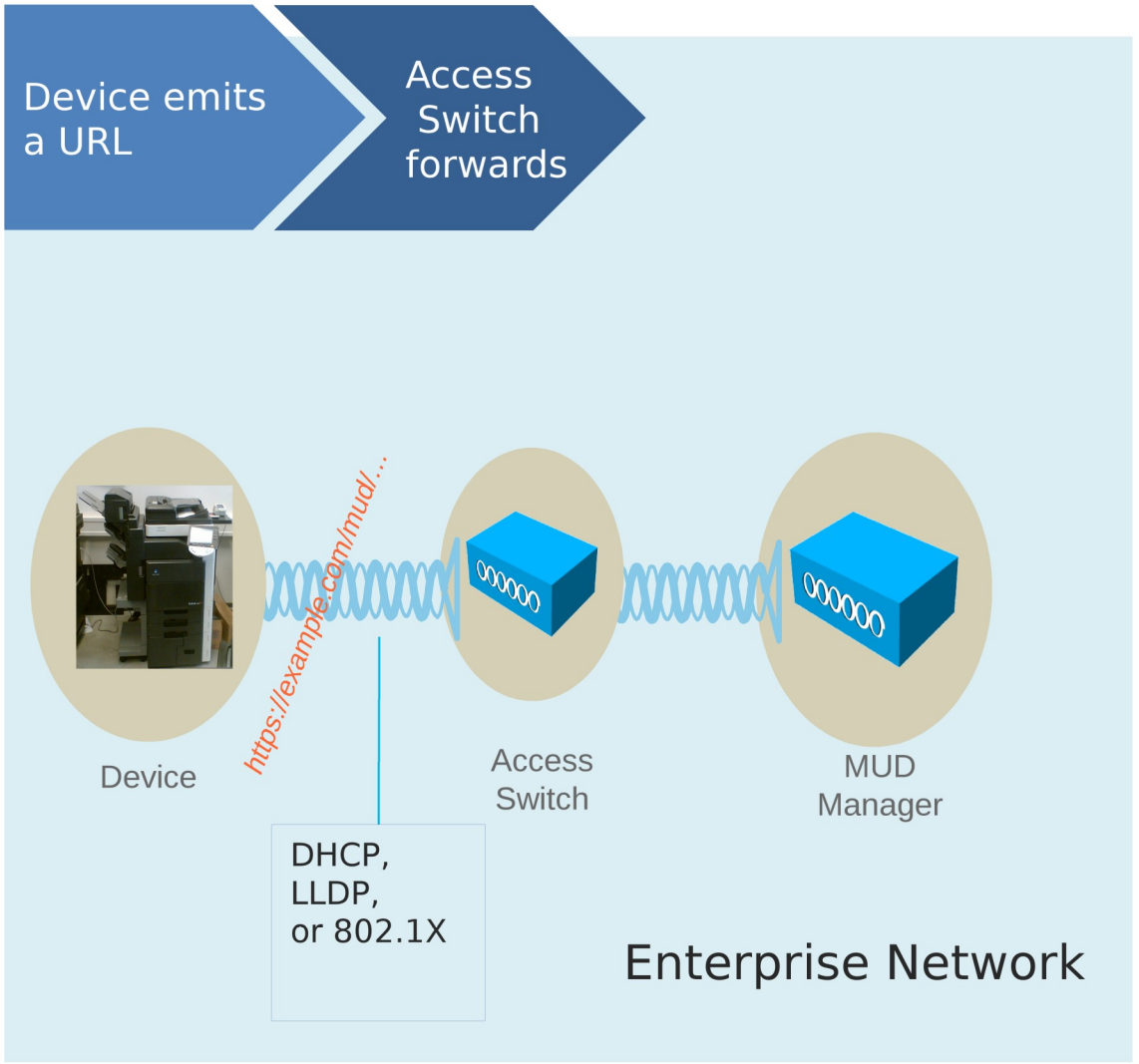
MUD File
Server

Expressing Manufacturer Usage Descriptions



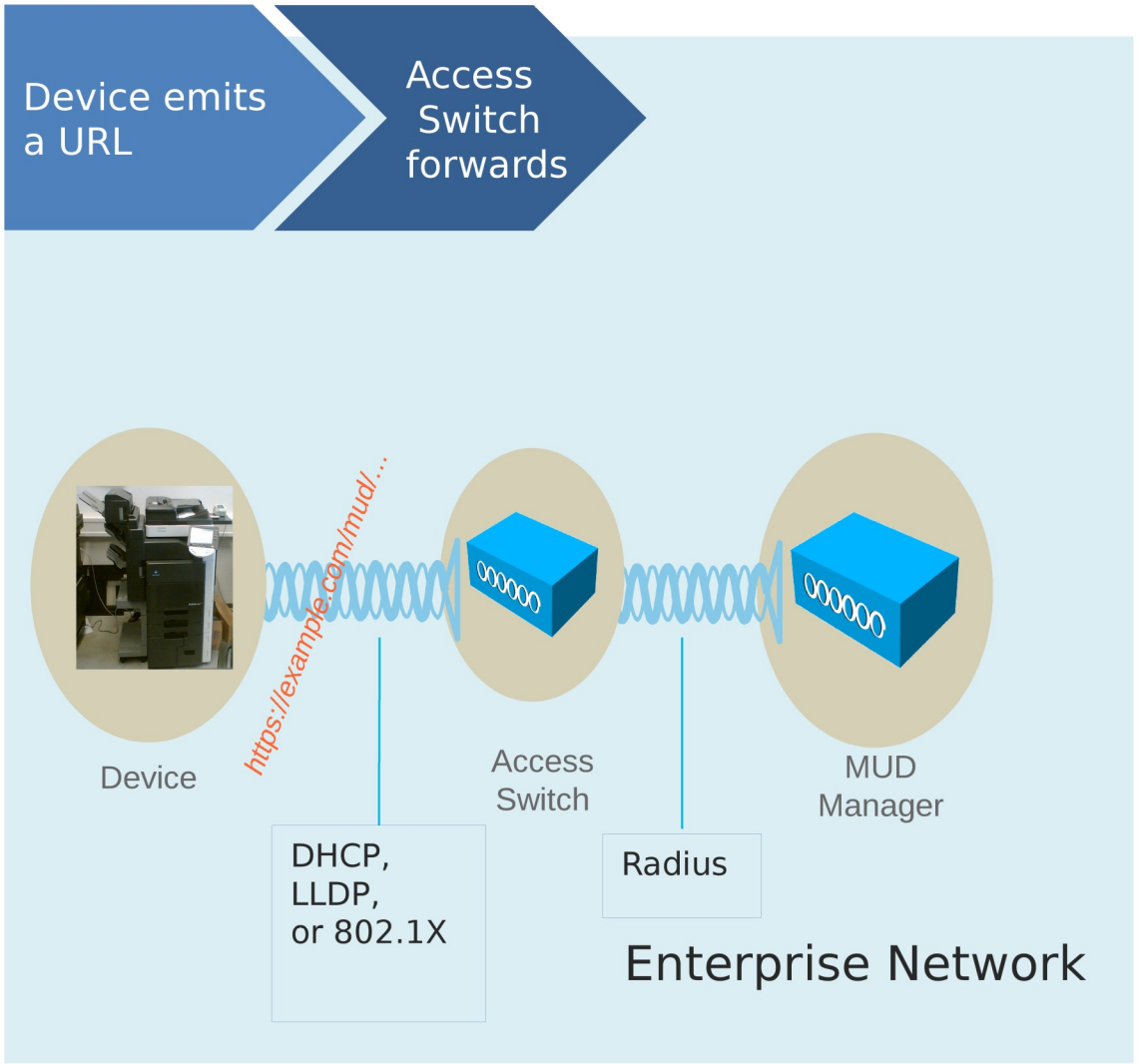
MUD File
Server

Expressing Manufacturer Usage Descriptions



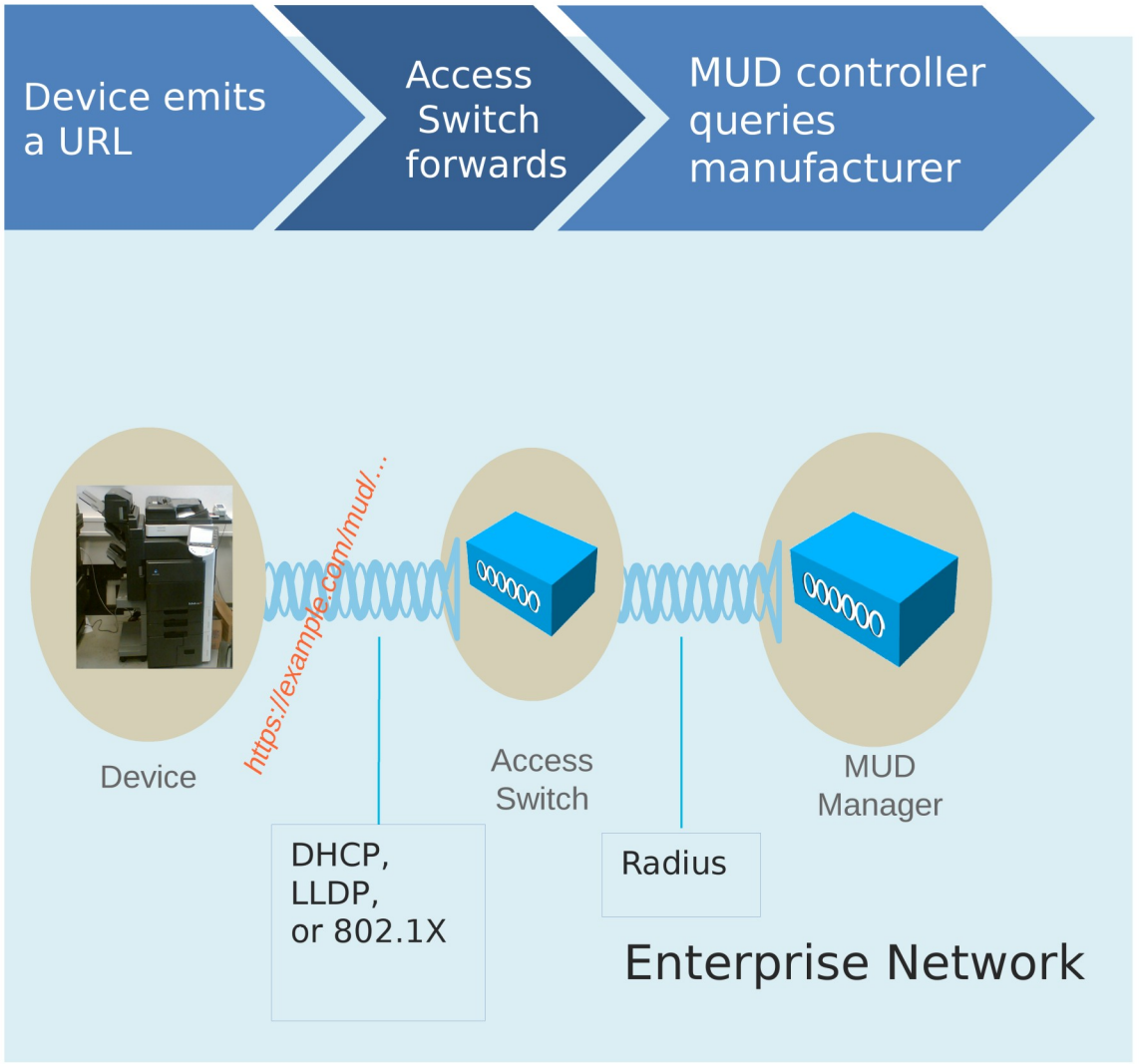
MUD File Server

Expressing Manufacturer Usage Descriptions



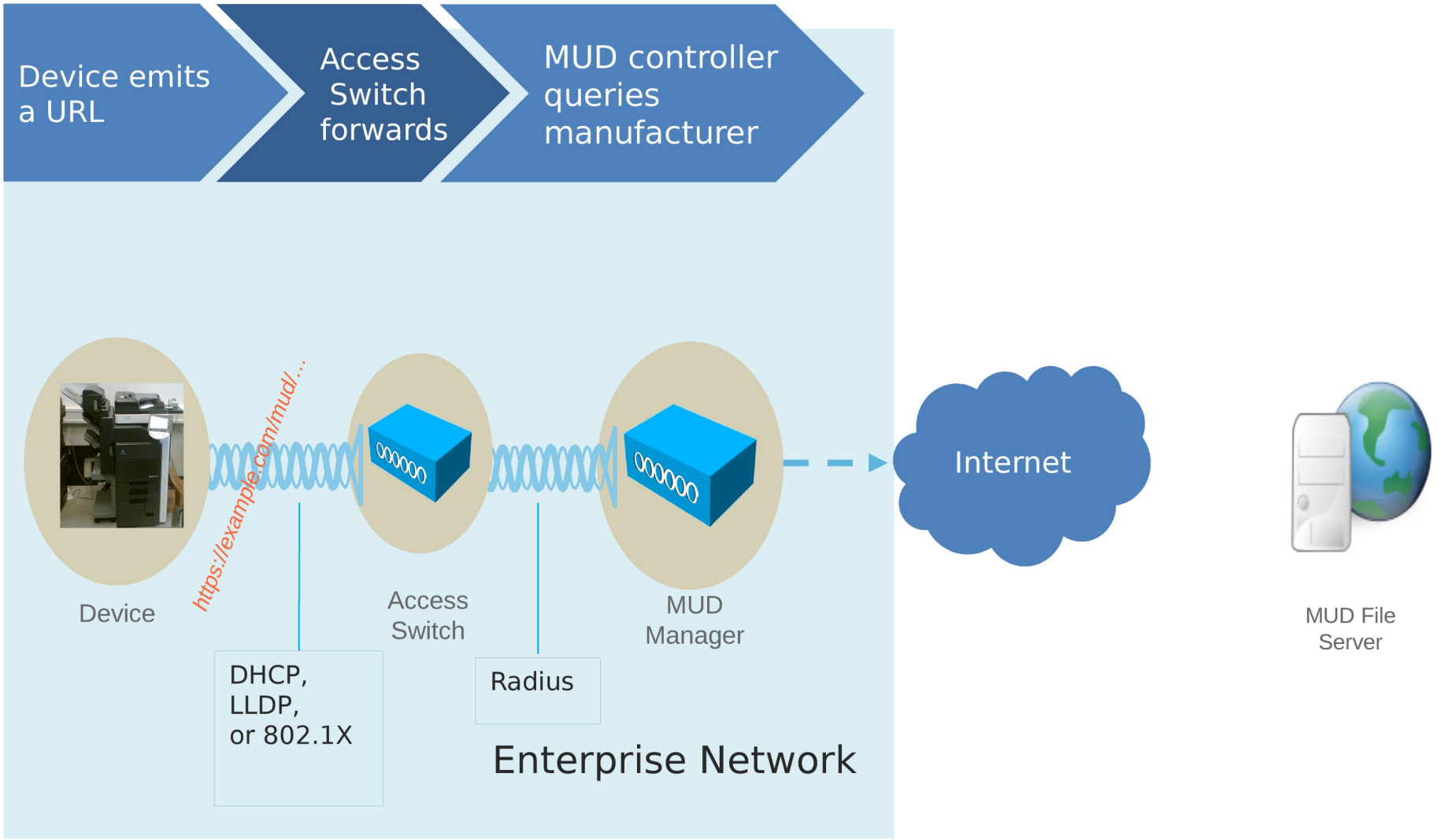
MUD File Server

Expressing Manufacturer Usage Descriptions

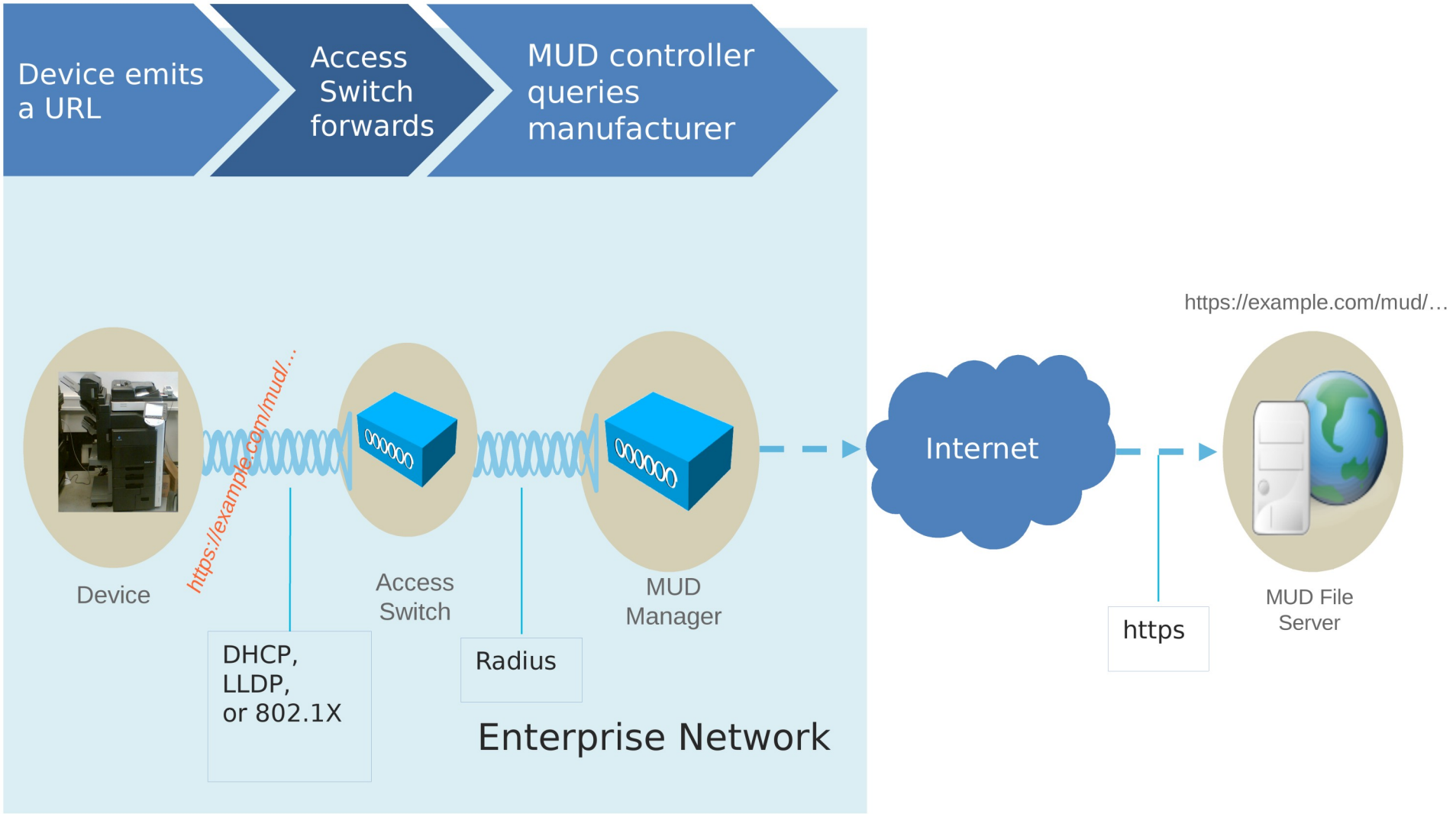


MUD File Server

Expressing Manufacturer Usage Descriptions



Expressing Manufacturer Usage Descriptions



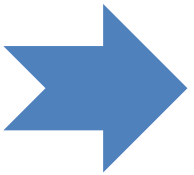
Getting from the MUD file to deployment config

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

https://mudmaker.org

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"
          } ...
```

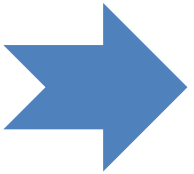


10.1.2.3
10.4.5.6

https://mudmaker.org

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"
          } ...
```

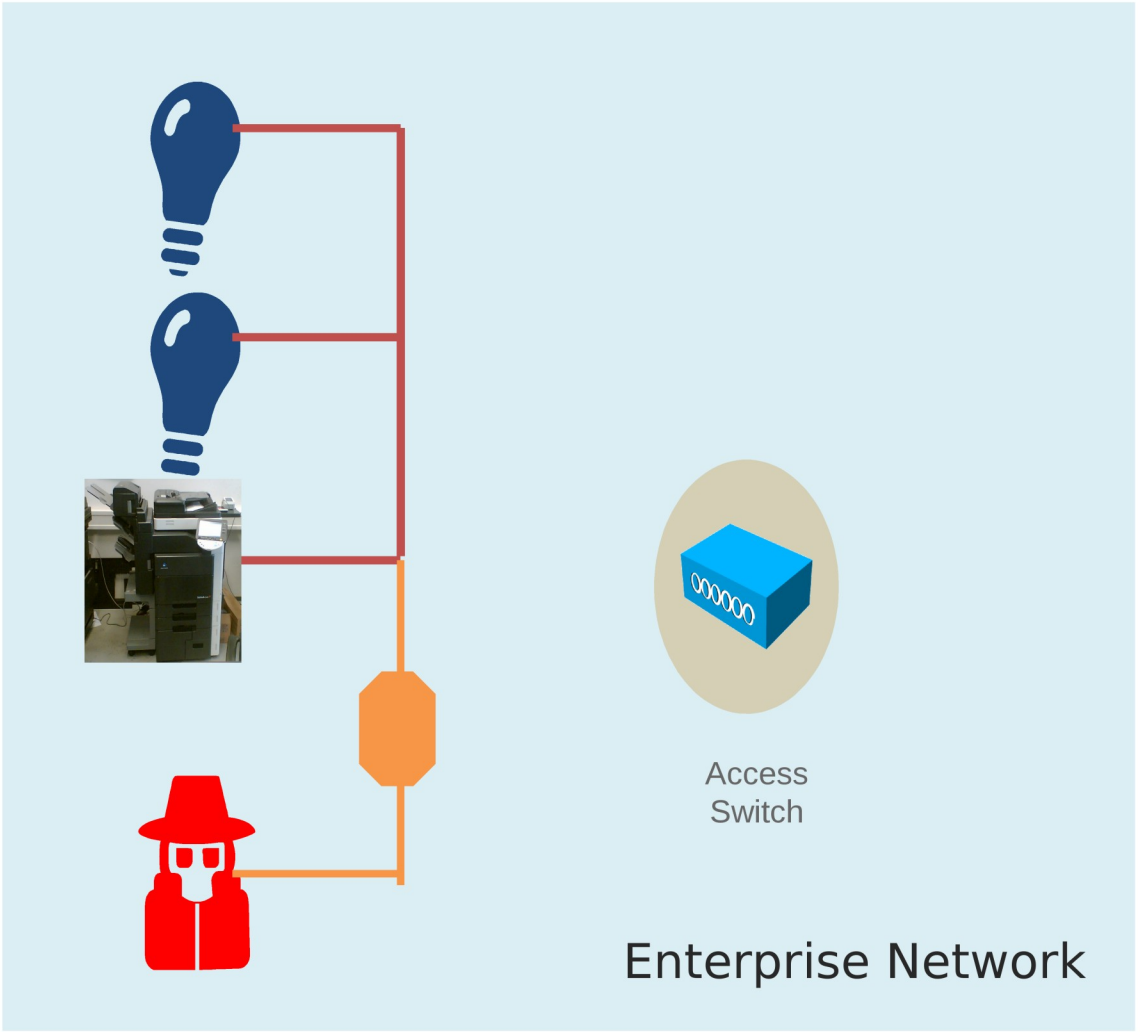


Whatever is appropriate in the local deployment.

10.1.2.3
10.4.5.6

https://mudmaker.org

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

When not to use MUD

- Multi-purpose systems
- Systems where the software is from third parties
  - Uncooperative third parties
- Pretty much anything that is browser based, probably is too hard to describe