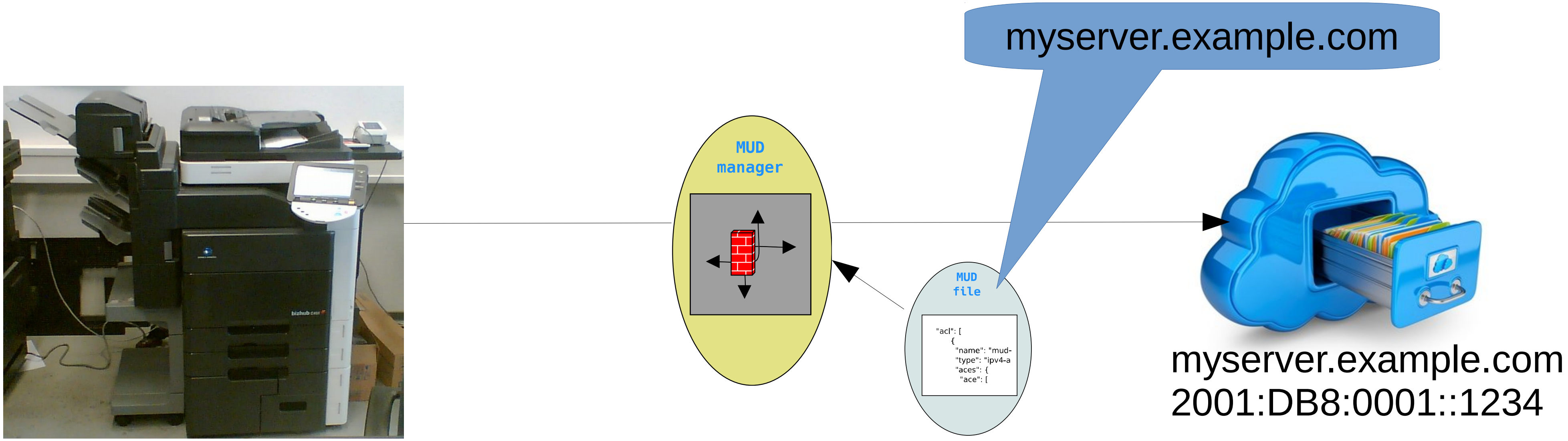
Operational Considerations for use of DNS in IoT devices

Michael Richardson
IETF107 OPSAWG meeting
April 7, 2020

`draft-richardson-opsawg-mud-iot-dns-considerations-02`

What is the problem?



myserver.example.com

MUD manager

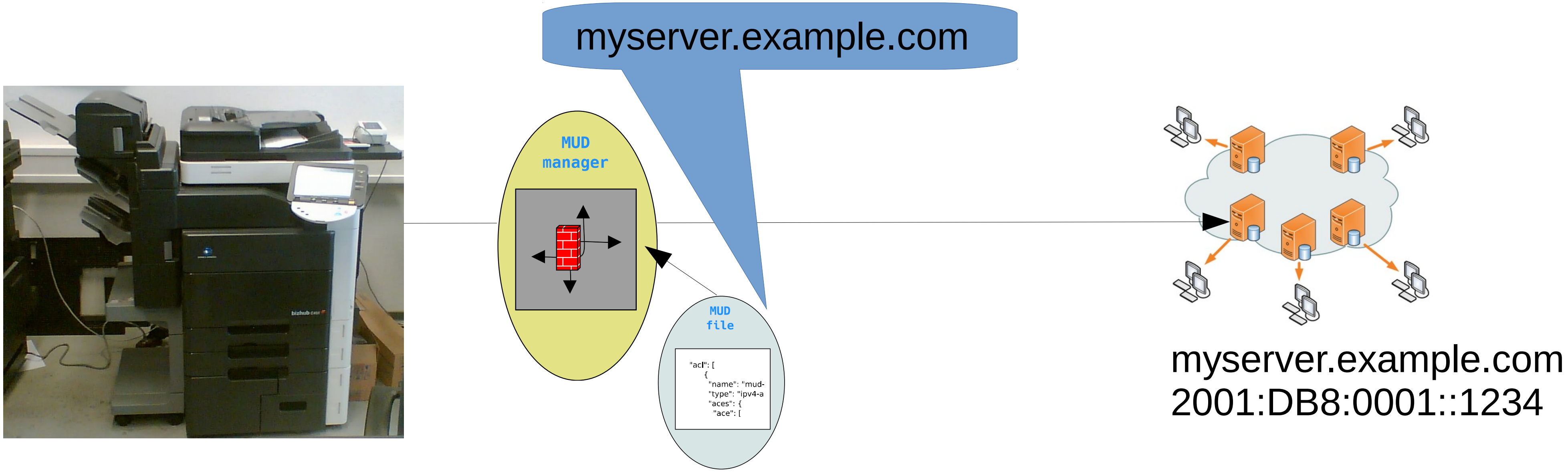
MUD file

```
"acl": [
      {
        "name": "mud-
        "type": "ipv4-a
        "aces": {
          "ace": [
```

myserver.example.com
2001:DB8:0001::1234

- IoT devices makes legit connection to network service
  - myserver.example.com is some resource

Add in A Content Distribution Network

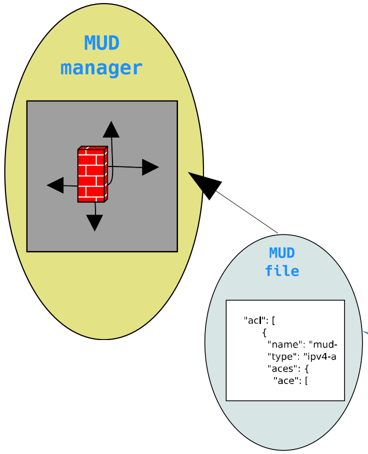


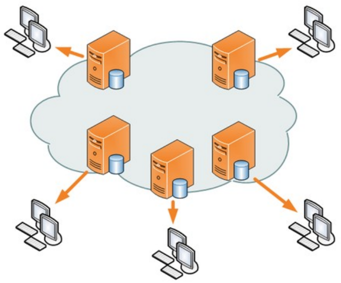
```
"acl": [
    {
      "name": "mud-
      "type": "ipv4-a
      "aces": {
        "ace": [
```

myserver.example.com
2001:DB8:0001::1234

- IoT devices looks up cloud resource, gets appropriate IP address, and connects
- MUD manager looks up cloud resource from MUD file, gets same IP address, has authorized connection
  - NOTE: MUD manager resolves names to IPs and installs ACLs.
  - Going from IP to name is not reliable, and the same IP could support many names.

Add in off-site DNS server (Do53, DoT, DoH)

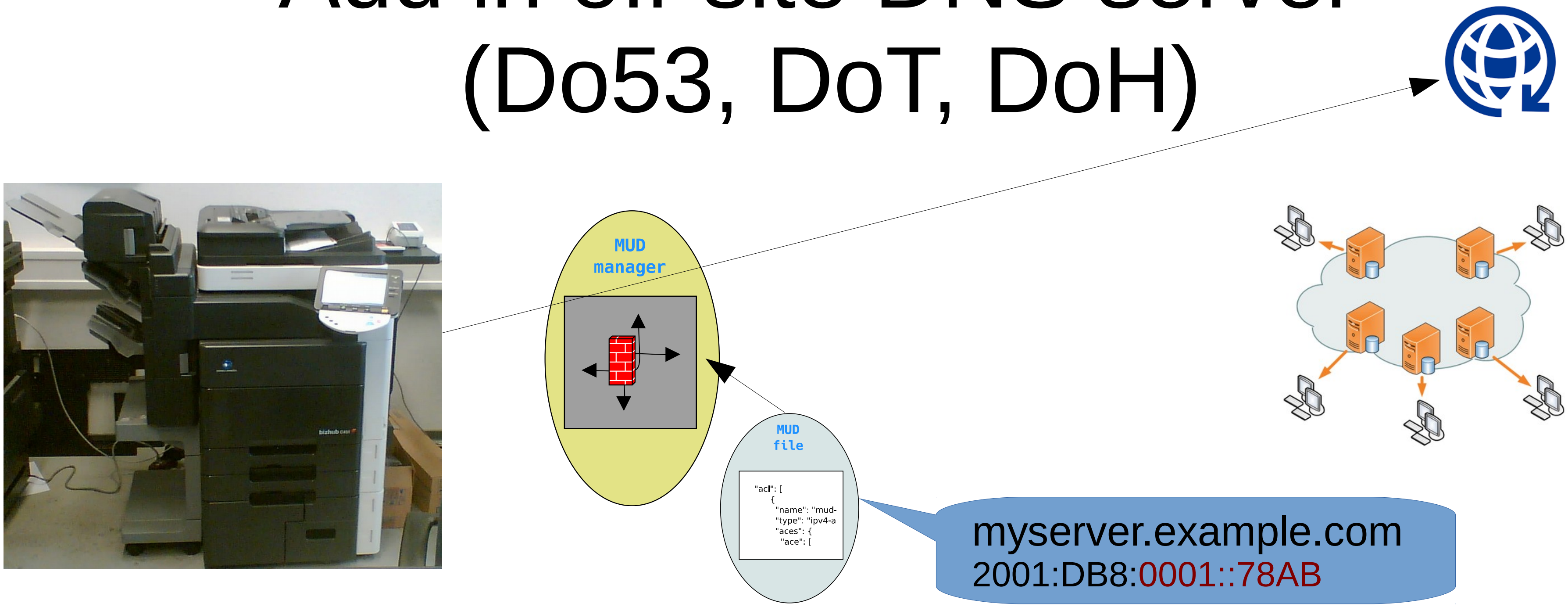




myserver.example.com
2001:DB8:0001::78AB

- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

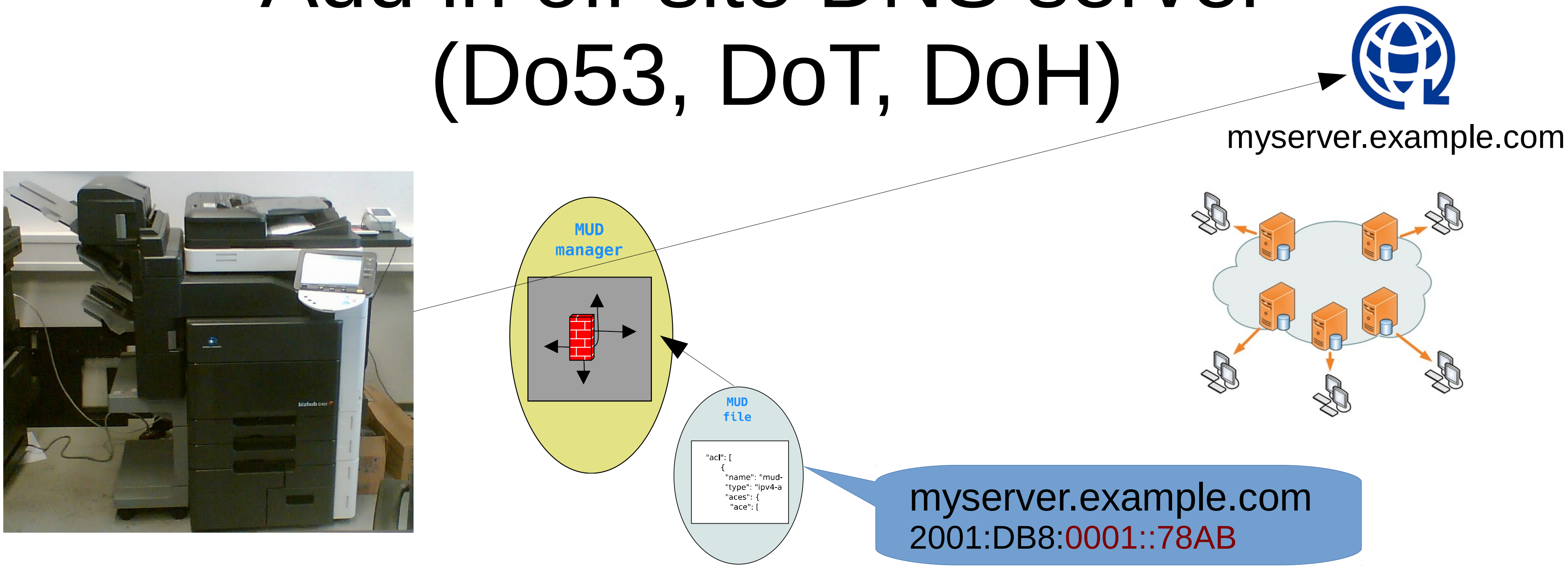
Add in off-site DNS server (Do53, DoT, DoH)



myserver.example.com
2001:DB8:0001::78AB

- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

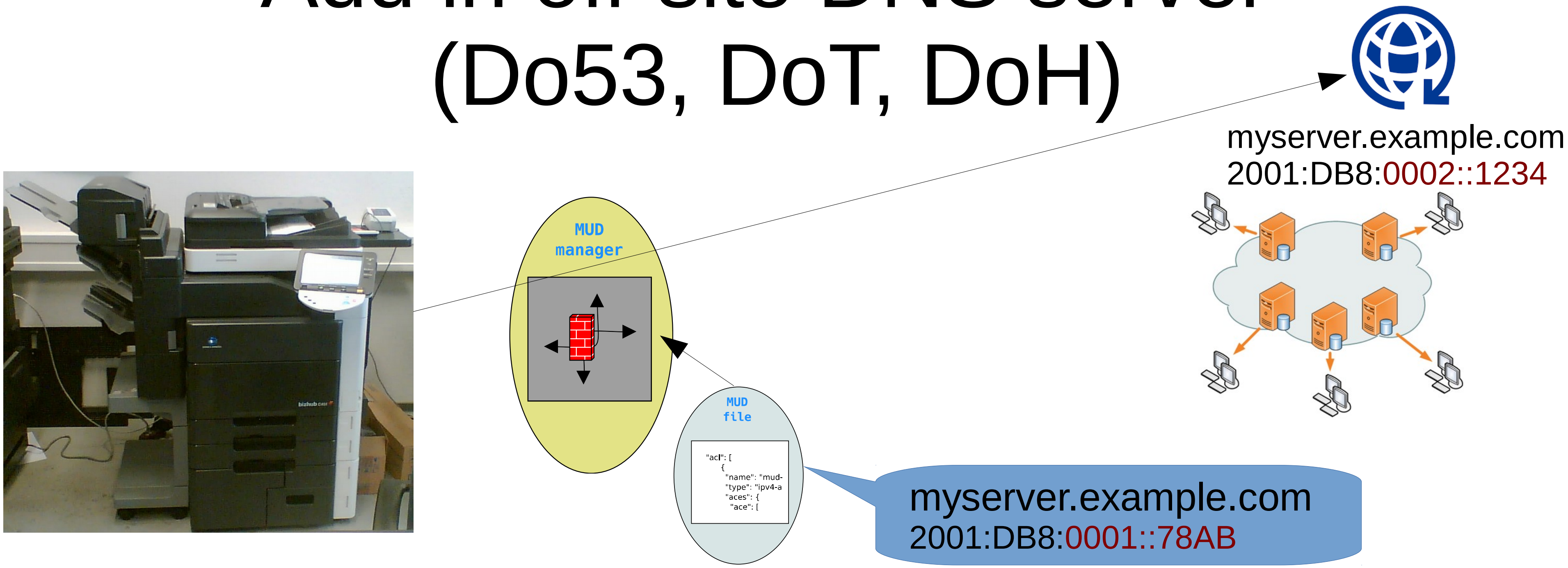
Add in off-site DNS server (Do53, DoT, DoH)



myserver.example.com
2001:DB8:0001::78AB

- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

Add in off-site DNS server (Do53, DoT, DoH)

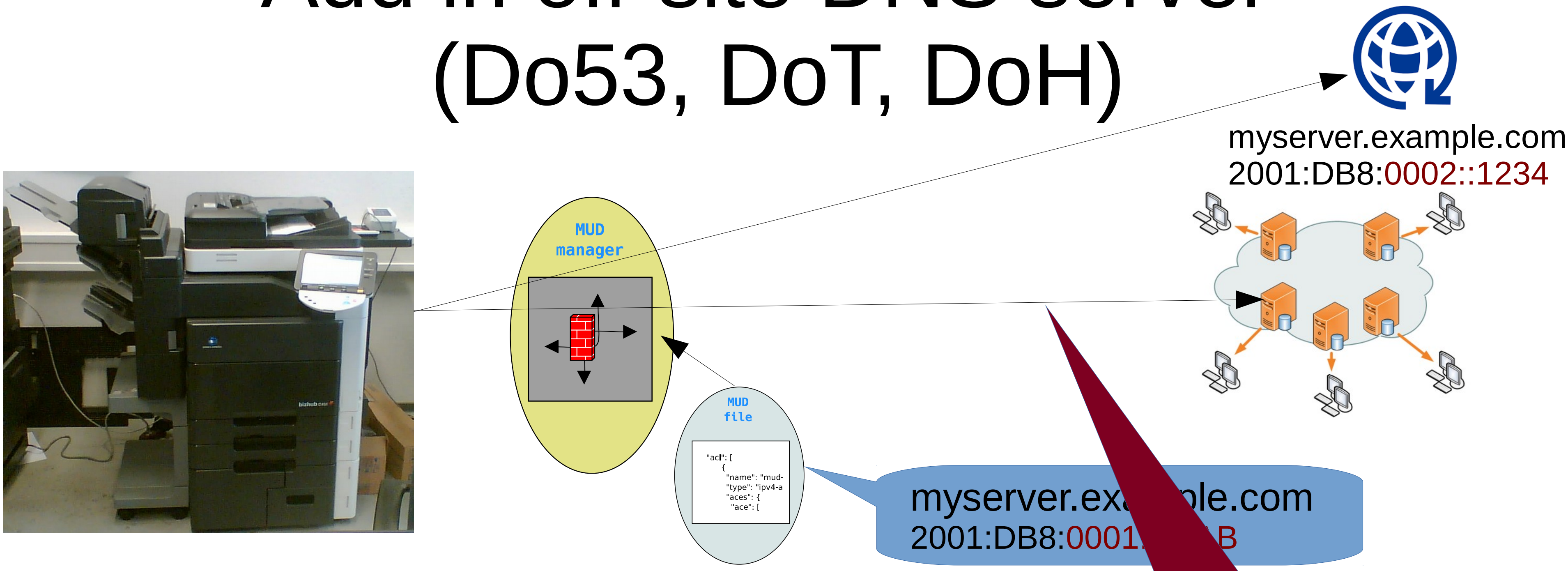


myserver.example.com
2001:DB8:0002::1234

myserver.example.com
2001:DB8:0001::78AB

- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

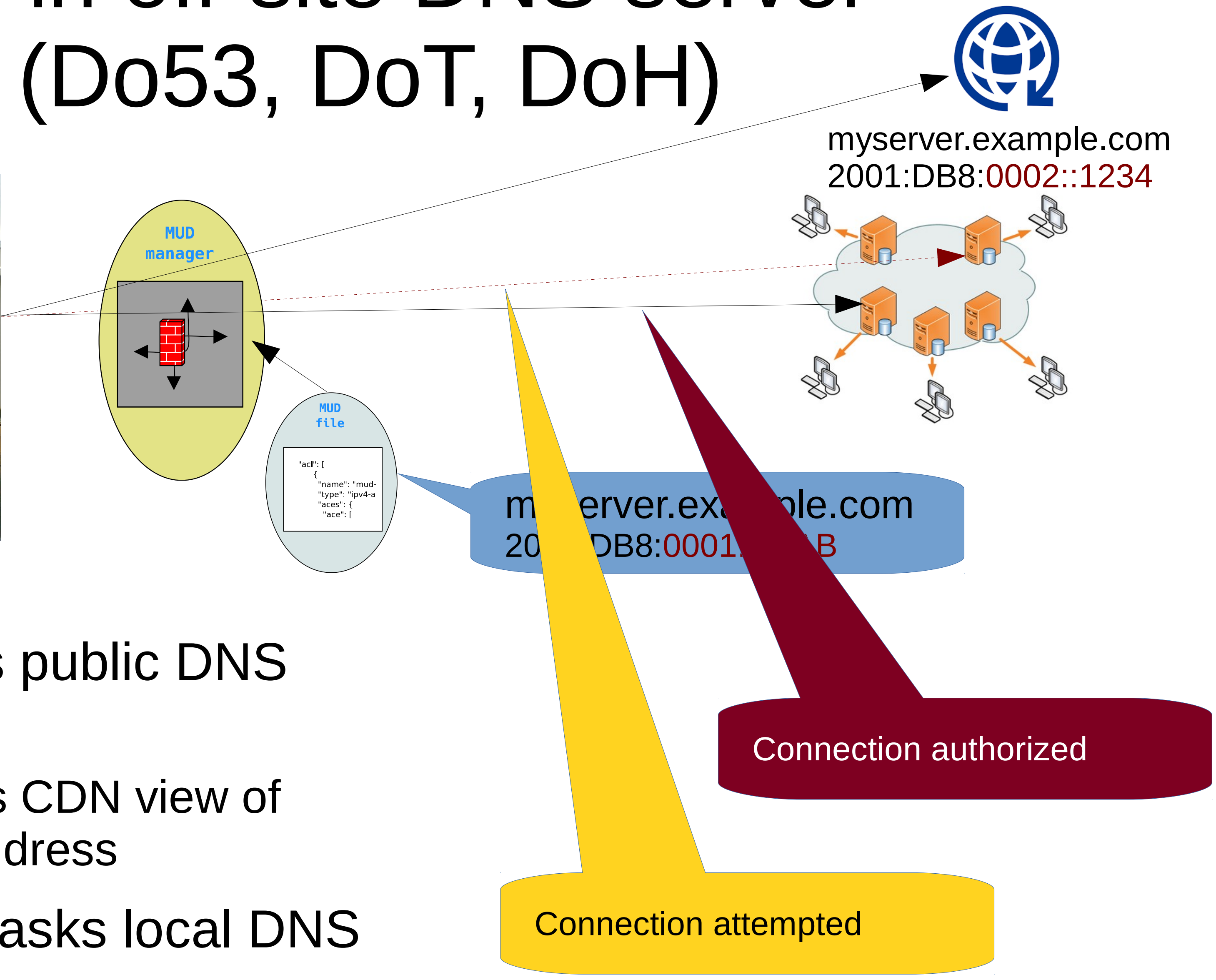
Add in off-site DNS server (Do53, DoT, DoH)



Connection authorized

- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

Add in off-site DNS server (Do53, DoT, DoH)



- IoT device asks public DNS server
  - IoT device gets CDN view of best/closest address
- MUD manager asks local DNS server
  - MUD managers get different view of best/closest address

Other problems include

- IP address literals in protocol
  - One can put it in the MUD file, but it’s a bad thing to bake in.
  - Must include IPv4 and IPv6 versions
  - Hard to coordinate updates
- Non-deterministic IPs or DNS in protocol
  - Such as asking an update server where to get the update, and the answering being a random S3 bucket or cloud instance name
- Using a too inclusive name!

Advice

1) Don’t do this!

   Always use names
   from the manufacturer

2) Always use DNS provided by DHCP

3) If using external DNS, then arrange for all possible records to be returned

Use of Round Robin DNS vs geo-fenced DNS

- Two ways of answering DNS.
  - Return just the A/AAAA to be used
  - *Return all A/AAAA, but sort it so that first one is desired one.*

What to do next

- This is aimed at being a BCP for MUD
- Adopt?
- More examples needed, and there are likely some other BCP references that would significantly help.
- Seems to be no agreed upon term “quadX”
- QUESTIONS?

Image Credits:

- Slides from Cisco
- Images from IoT-DIR IETF GITHUB
- https://en.wikipedia.org/wiki/Content_delivery_network#/media/File:NCDN_-_CDN.png
- https://starecat.com/content/wp-content/uploads/what-seems-to-be-the-problem-mary-doctor-it-hurts-when-i-do-this-then-dont-do-that.jpg