Device Quarantine definition for Manufacturer Usage Descriptions (RFC8520)

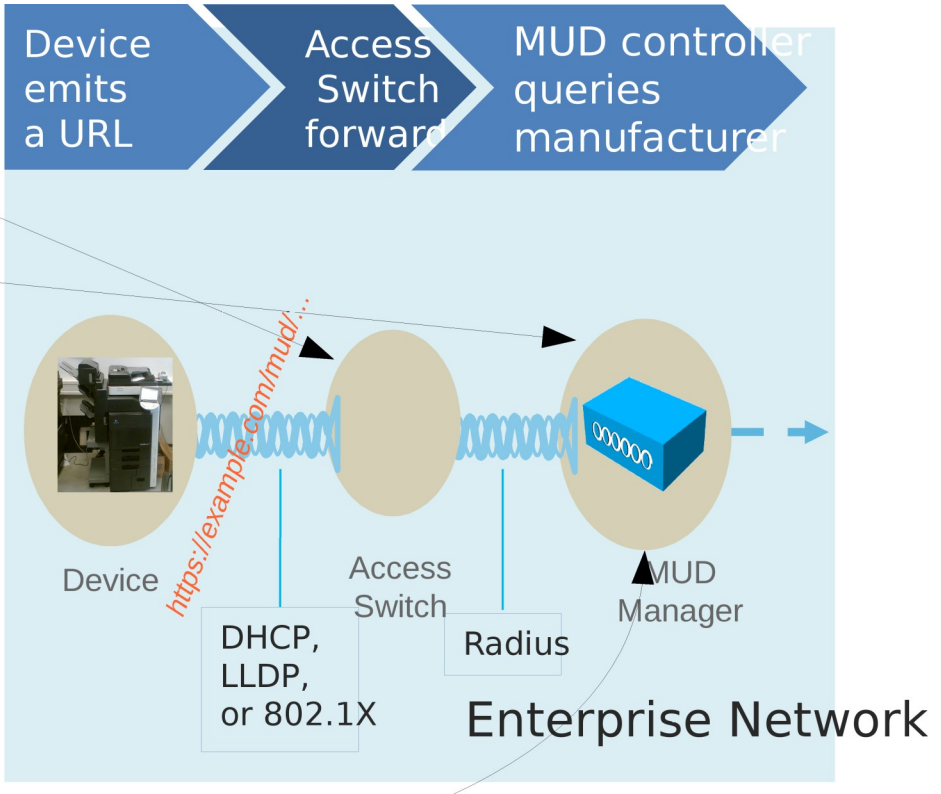
Draft-richardson-shg-mud-quarantined-access

IETF107 - OPS Area Working Group (opsawg)
2020-03-24 Vancouver

Michael Richardson (Sandleman Software Works)
Mudumbai Ranganathan (NIST)

What puts a device into Quarantine?

- Device violates its MUD specification
- External vulnerability report identifying a vulnerability in the device firmware
- Network administrator decides to place device into quarantine (e.g. runs an automated vulnerability scan on the device and discovers vulnerability)

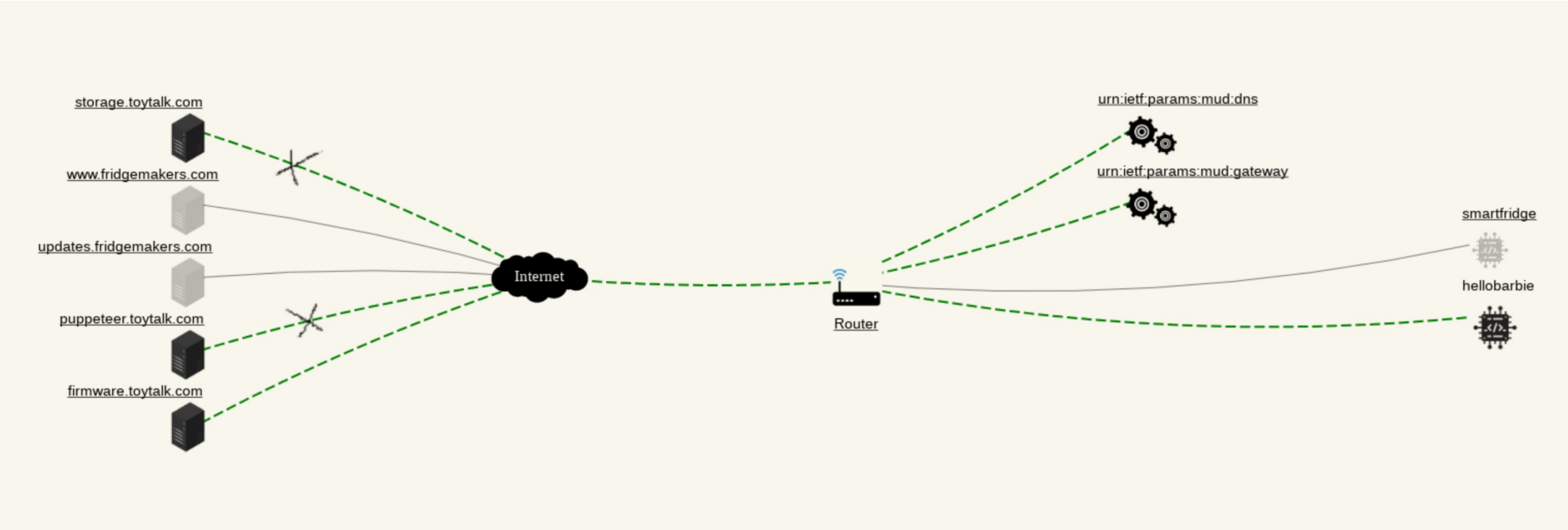


Critical ACEs

- Complete isolation from network may not be advisable.
  - Device can’t update itself.
  - May be connected to critical equipment.
- Critical Access Control Entries
  - ACEs that should not be blocked when device goes into quarantine

Example

hellobarbie may only access firmware.toytalk.com under quarantine
– subset of allowable ACEs under non-quarantine operation



MUD Extension for Quaranitne ACEs

```
augment "/m:mud" {
  description
    "Adds leaf nodes appropriate MUD usage in the
     Secure Home Gateway";

  container quarantine-device-policy {

    list enabled-ace-names {
      key ace-name;
      leaf ace-name {
        type leafref {
          Path "/acl:acls/acl:acl/acl:aces/acl:ace/acl:name";
        }

  }
```

The policies that should be enforced on traffic coming from the device when it is under quarantine. These policies are usually a subset of operational policies and are intended to permit firmware updates only.

They are intended to keep the device safe (and the network safe from the device) when the device is suspected of being out-of-date, but still considered sufficiently intact to be able to do a firmware update.