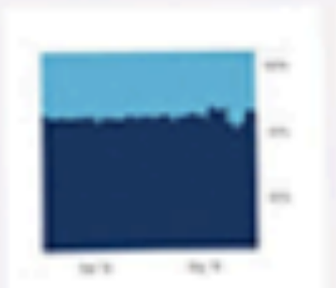
Securing the Internet of Things

Elmer Lastdrager

3 June 2021

.nl stats and data



Stichting Internet Domeinregistratie Nederland (SIDN)

Critical infrastructure services

- Lookup IP address of a domain name (almost every interaction)
- Registration of all .nl domain names
- Manage fault-tolerant and distributed infrastructure

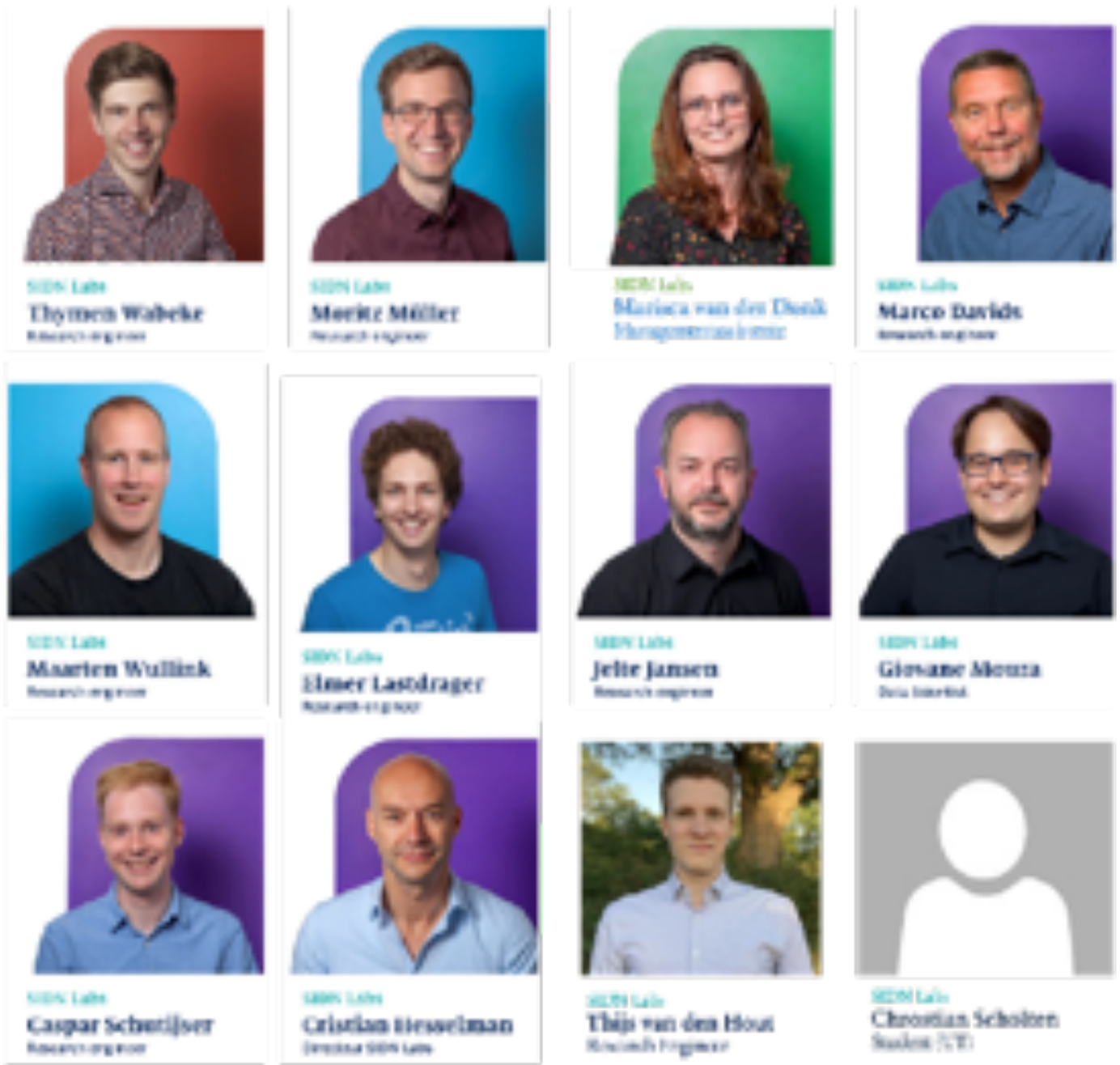
.nl = the Netherlands
17M inhabitants
6.2M domain names
3.4M DNSSEC-signed
2.5B DNS queries/day
8.6B NTP queries/day

Increase the value of the Internet in the Netherlands and elsewhere

- Enable safe and novel use of the Internet
- Improve the security and resilience of the Internet itself

SIDN LABS

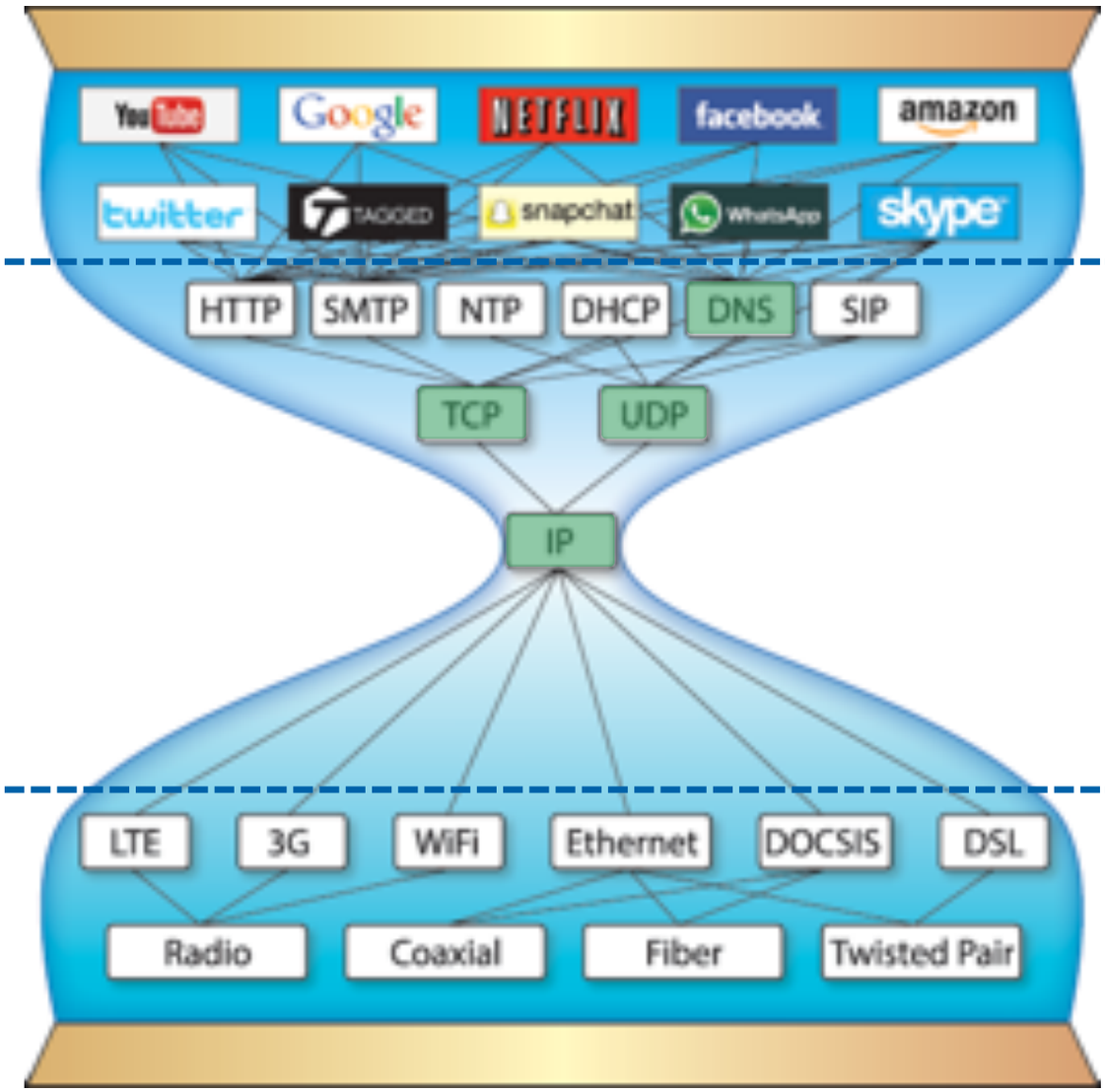
SIDN Labs



- Technical experts, divers in seniority and nationality
- Help SIDN teams, write open-source software, analyze large amounts of data, conduct experiments, write articles, collaborate with universities
- M.Sc students help us advance specific areas

Most people

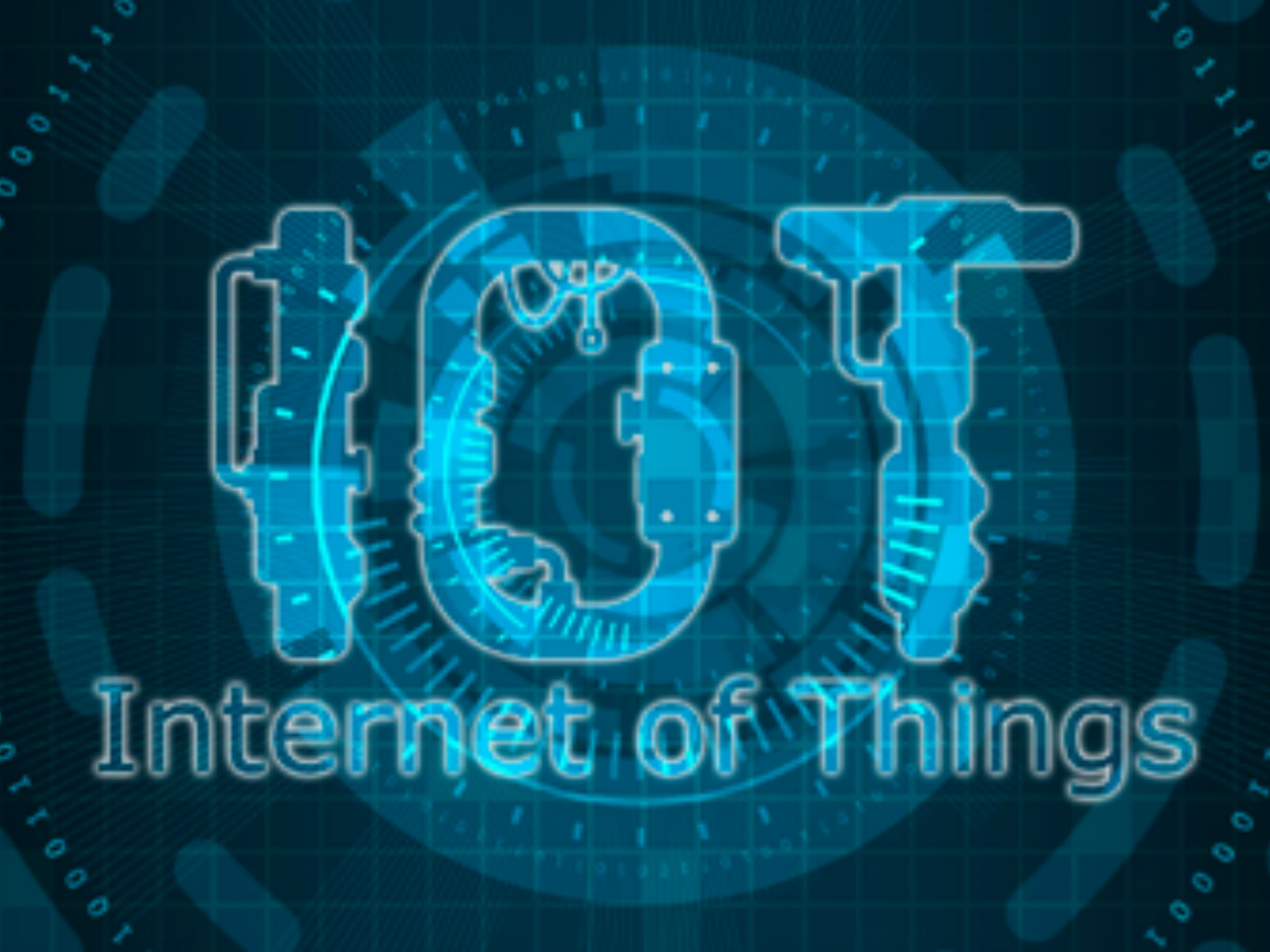
Us



Services

Transmission

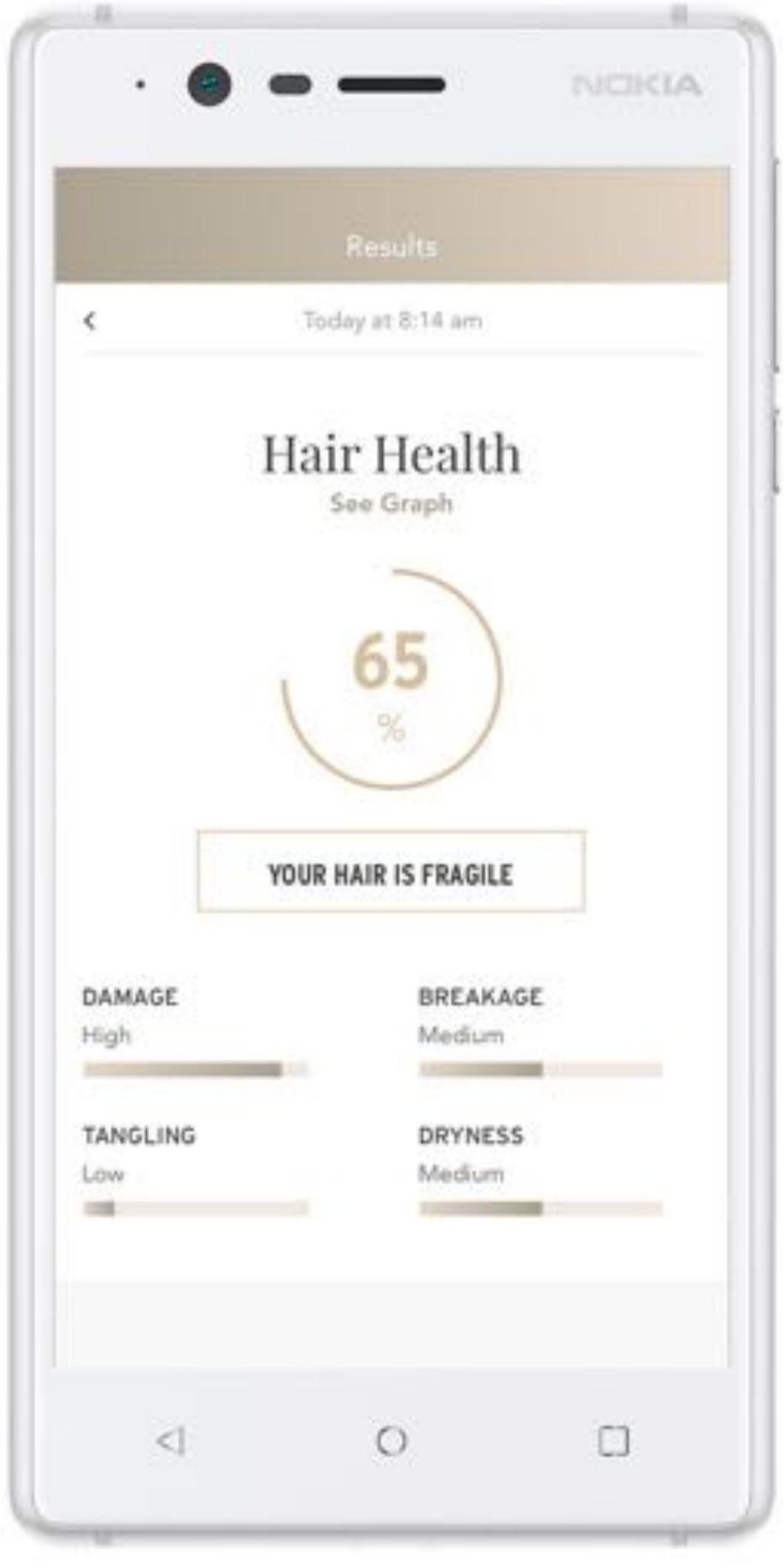
SDN LABS


IoT
Internet of Things

Smart Devices

"**A smart device is an electronic device**, [snip], **that can operate to some extent interactively and autonomously.**"

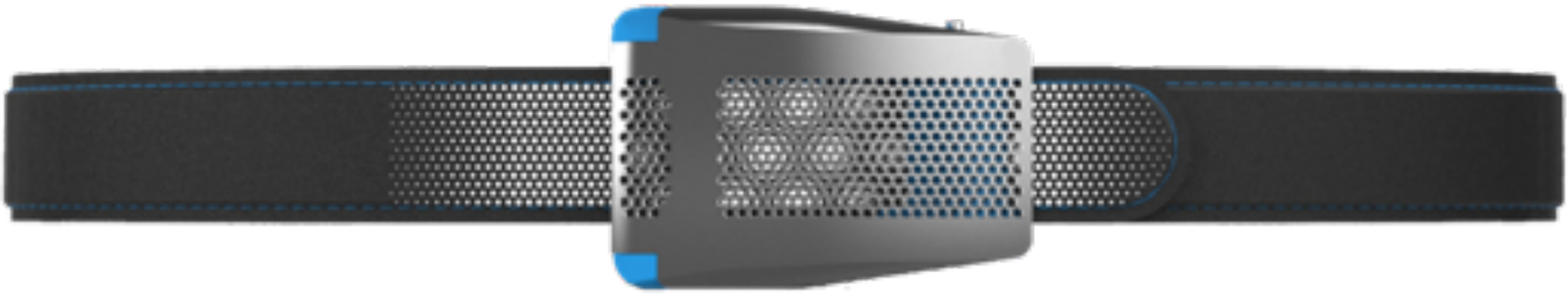
According to Wikipedia


NOKIA
Results
Today at 8:14 am
Hair Health
See Graph
65
%
YOUR HAIR IS FRAGILE
DAMAGE
High
BREAKAGE
Medium
TANGLING
Low
DRYNESS
Medium

This is GeniCan.

Como Huggies TweetPee funciona

Design ergonómico



Welcome to U by Moen
Demo the Controller and learn how easy it is to precisely control temperature, select shower outlets, and save your perfect shower as a preset for later.
100°
Demo the Smartphone App to see how the same easy controls are available in the palm of your hand, along with up to 10 additional presets.

SMALT with voice

Connect SMALT with Amazon Echo and simply say “Alexa, dispense half a teaspoon of salt".

Bring the flavor

SMALT dispenses salt with a shake/pinch of your smartphone screen or simply turning the dial manually.

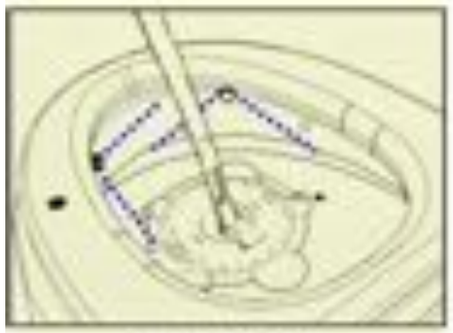
i.Con
i.Con

What does i.Con do with its data? Can I use it anonymously?

“Absolutely! All data will be kept anonymous but users will have the option to share their recent data with friends, or, indeed the world. You will be able to anonymously access stats that you can compare with i.Con users worldwide.”

(i) Pressure sensor
(ii) Motion sensor (PIR)
(iii) Urinalysis strip
(iv) Stool camera
(v) Anus camera
(vi) Uroflow camera

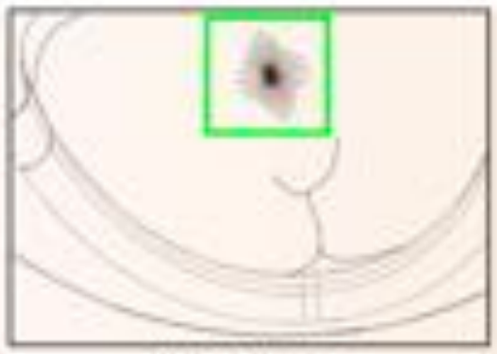
Urinalysis



Uroflowmetry

Bristol stool form scale

Seating time
defecation time



Analprint scan

Fingerprint scan

Cloud-based
health portal

YOU GET CONNECTED!
AND YOU GET CONNECTED!
EVERYTHING GETS CONNECTED!

What is the IoT?

Wikipedia definition:

"*The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.*"

Global Standards Initiative definition:

“a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[3] and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".”

Towards a definition of the Internet of Things (IoT)

Revision 1 – Published 27 MAY 2015

A simpler definition:

“Stuff that did not use to be networked”

HOW LONG YOU'VE HAD YOUR SMART APPLIANCE

6 MONTHS | 1 YEAR | 5 YEARS | 10 YEARS

BEST-CASE

YOU'RE CONSTANTLY BEING RESCUED FROM PERIL BY A FACELESS TEAM OF ENGINEERS WHO COULD WANDER AWAY AT ANY TIME

YOUR APPLIANCE IS PART OF A BOTNET RUN BY ORGANIZED CRIME

WORST-CASE

SLIDESHOW

The internet of insecure things: Thousands of internet-connected devices are a security disaster in the making

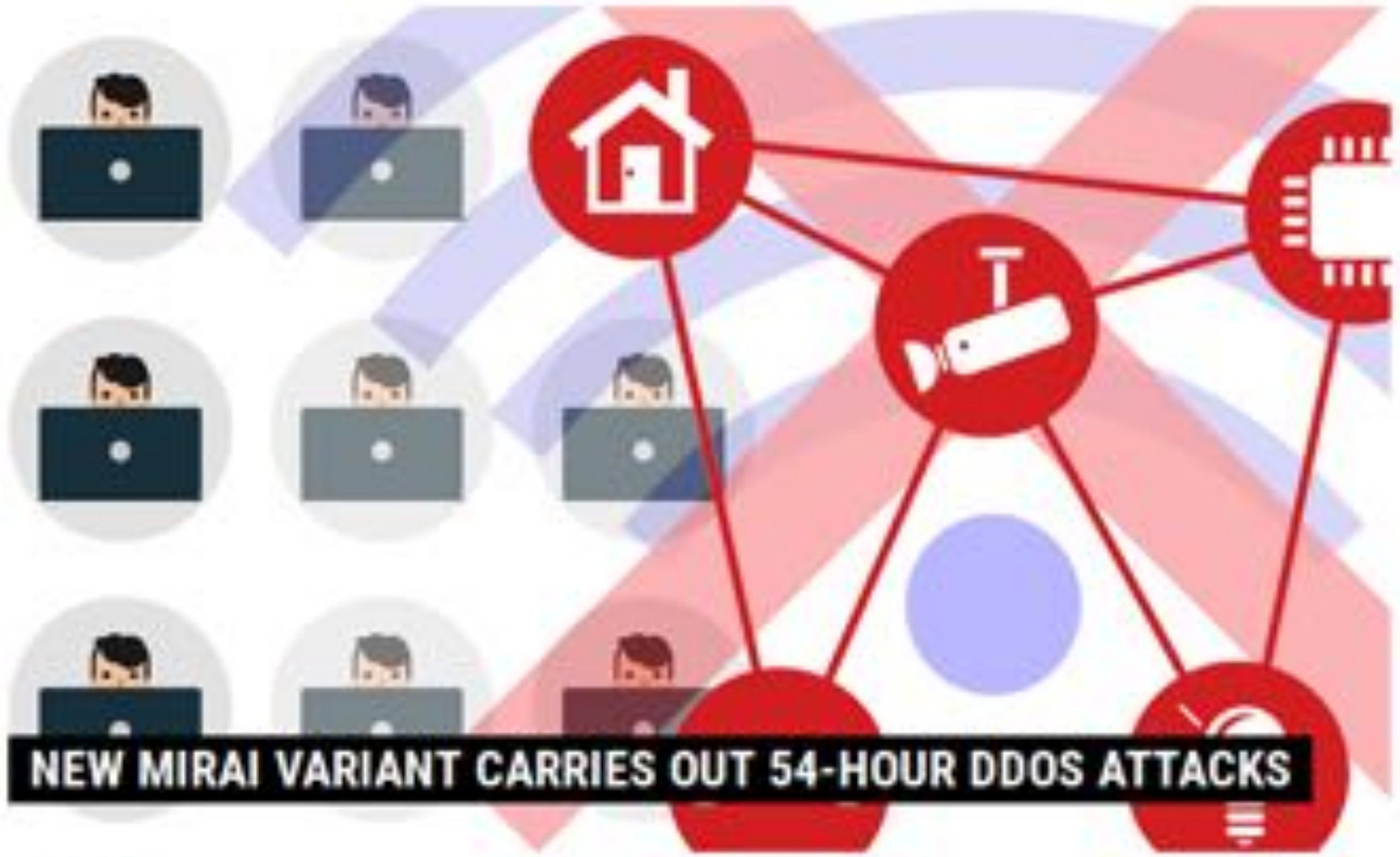
By Josh Fruhlinger, CSO | Oct 12, 2016 4:00 AM PT

The "S" in IoT
stands for
SECURITY

Why?

Why?

- Security is hard
- Security is expensive
- In some cases: security is not ‘user-friendly’
- Security is not a feature that sells devices
  - But time to market and price are
- Security is invisible



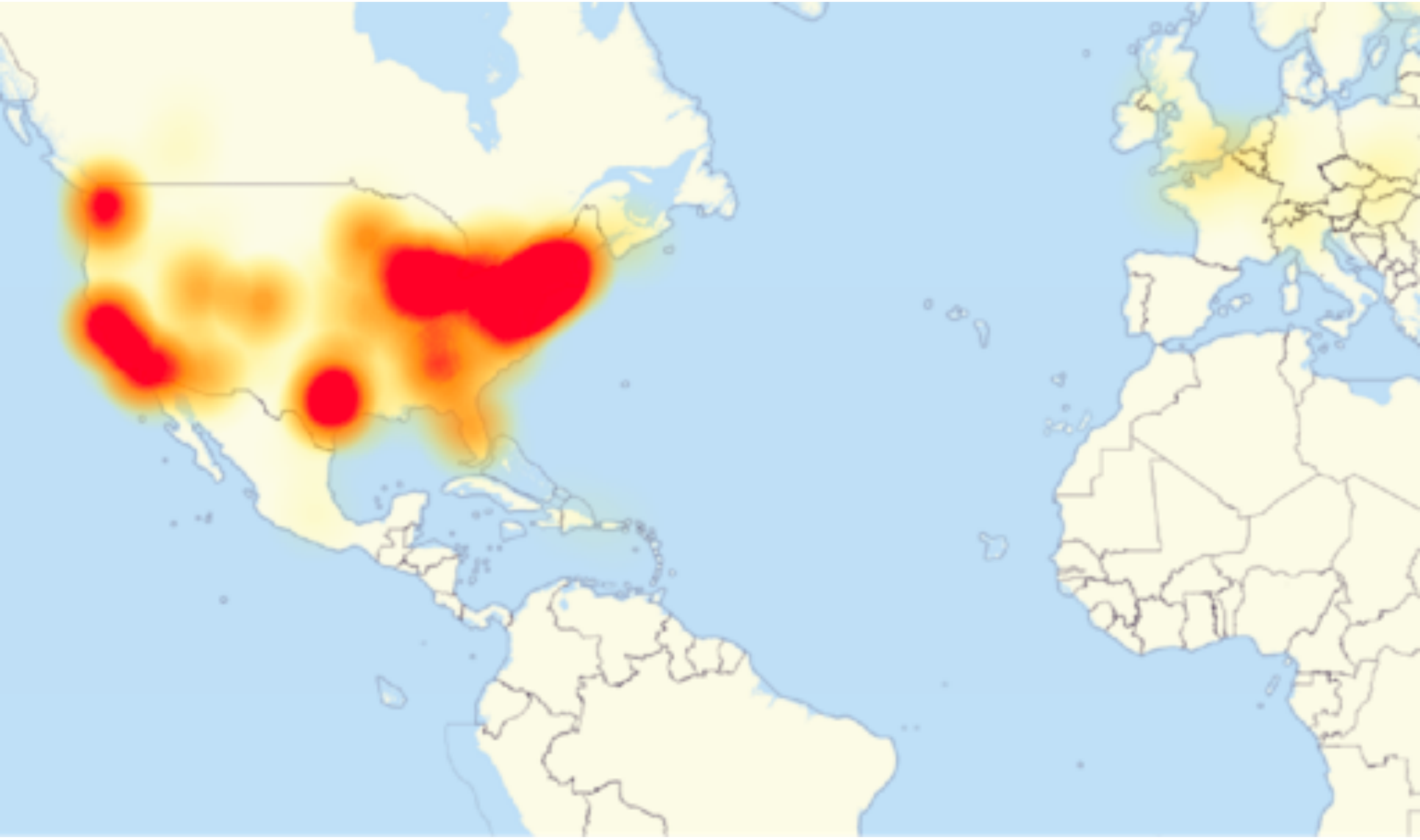
by **Tom Spring** March 30, 2017 , 2:50 pm

A variant of the Mirai malware pummeled a U.S. college last month with a marathon 54-hour long attack. Researchers say this latest Mirai variant is a more potent version of the notorious Mirai malware that made headlines in October, targeting DNS provider Dyn and the Krebs on Security website.

Mirai vs Dyn SM

1.2 Tbps

From ‘only’ 100.000 devices



A: Market (vendors)

B: Government

C: Consumers

This guy's light bulb performed a DoS attack on his entire smart house

Kashmir Hill

3/03/15 9:41am | Filed to: REAL FUTURE

RISK ASSESSMENT —

BrickerBot, the permanent denial-of-service botnet, is back with a vengeance

New botnet squadrons wage fiercer, more intense attacks on unsecured IoT devices.

DAN GOODIN - 4/24/2017, 10:43 PM

SECURITY IS SEXY
By Darlene Storm, Computerworld | FEB 2, 2015 12:09 PM PT

About
Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

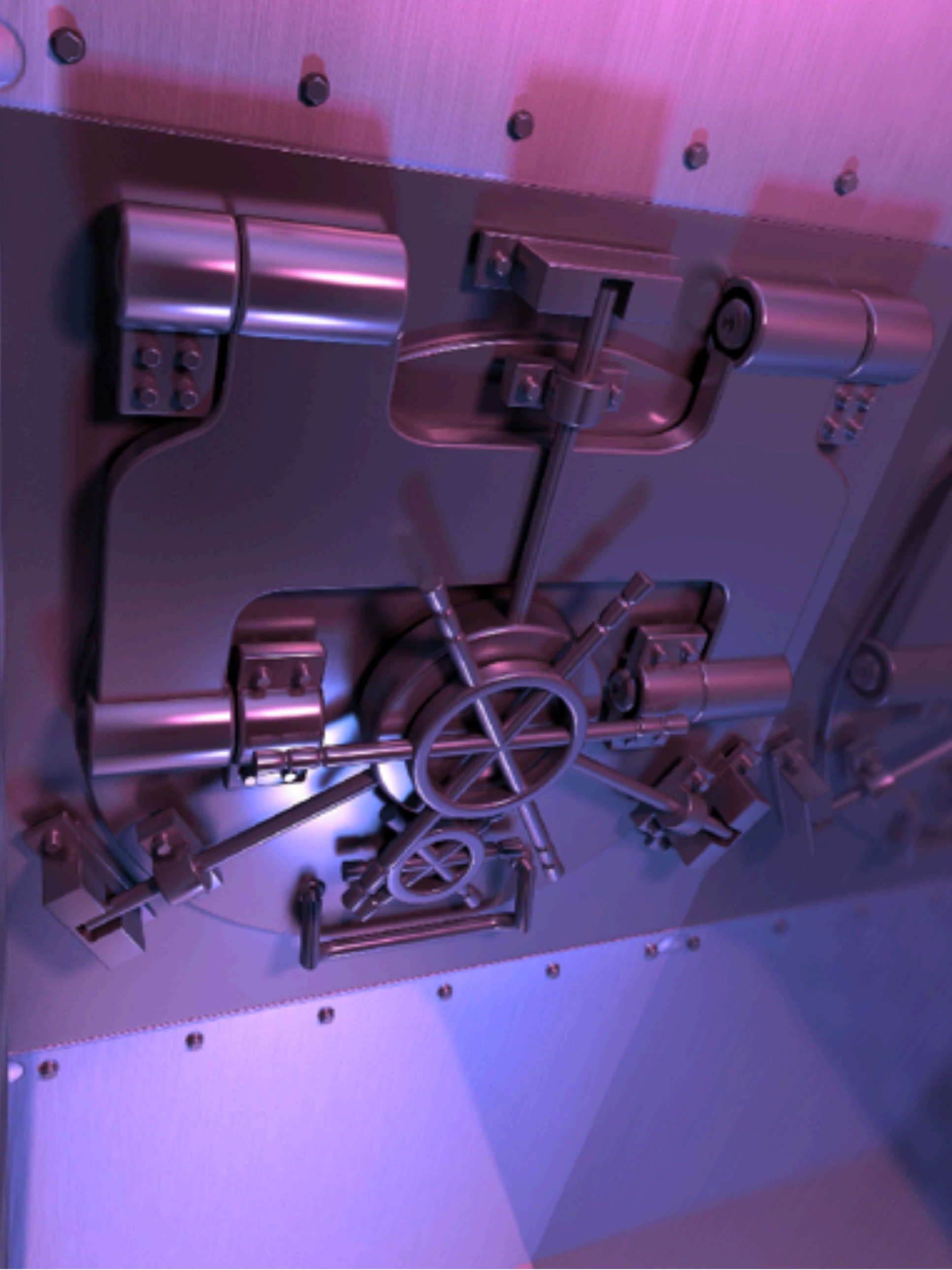
This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!

MORE LIKE THIS

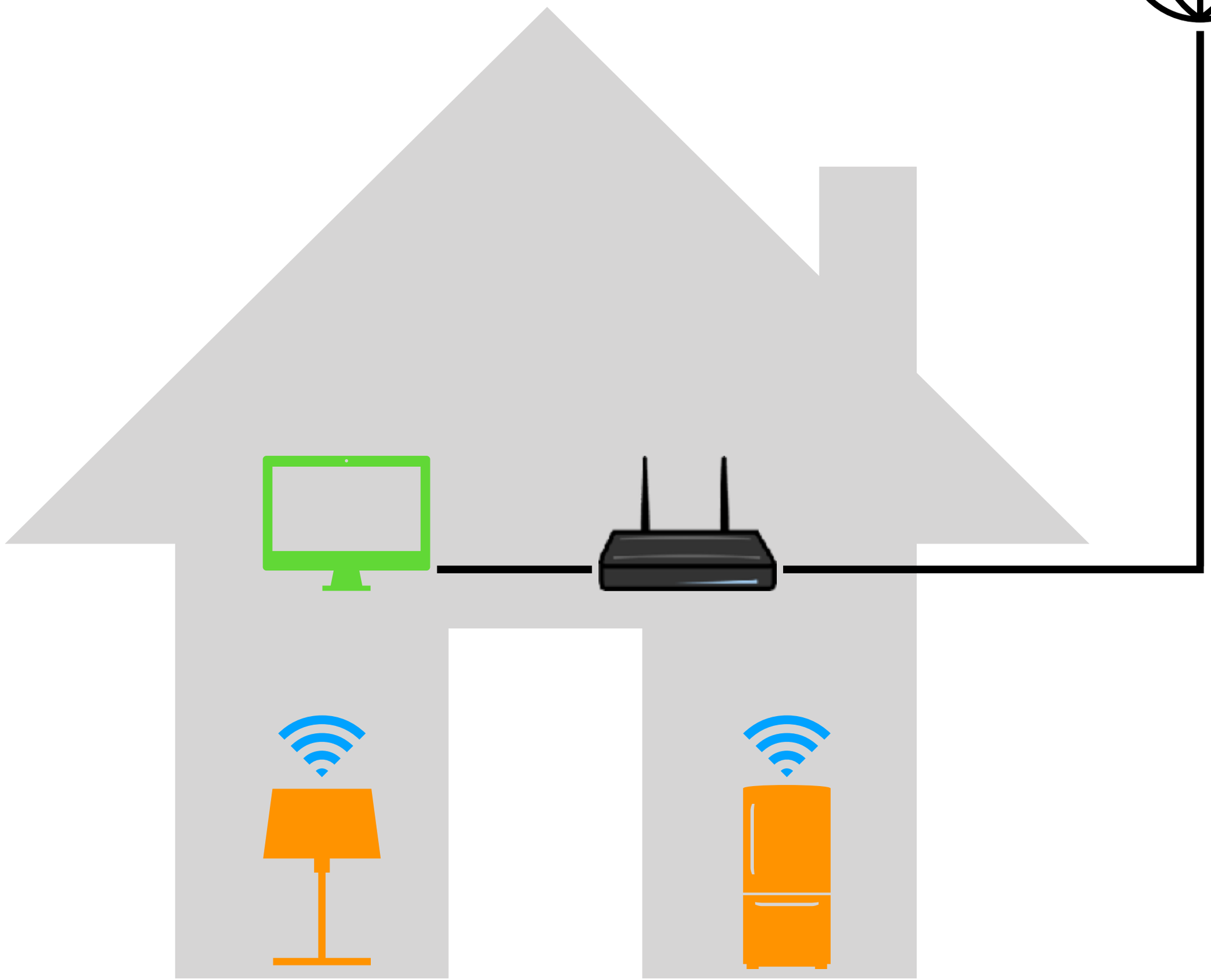
Hacker strikes again: Creep hijacks baby monitor to scream at infant and...

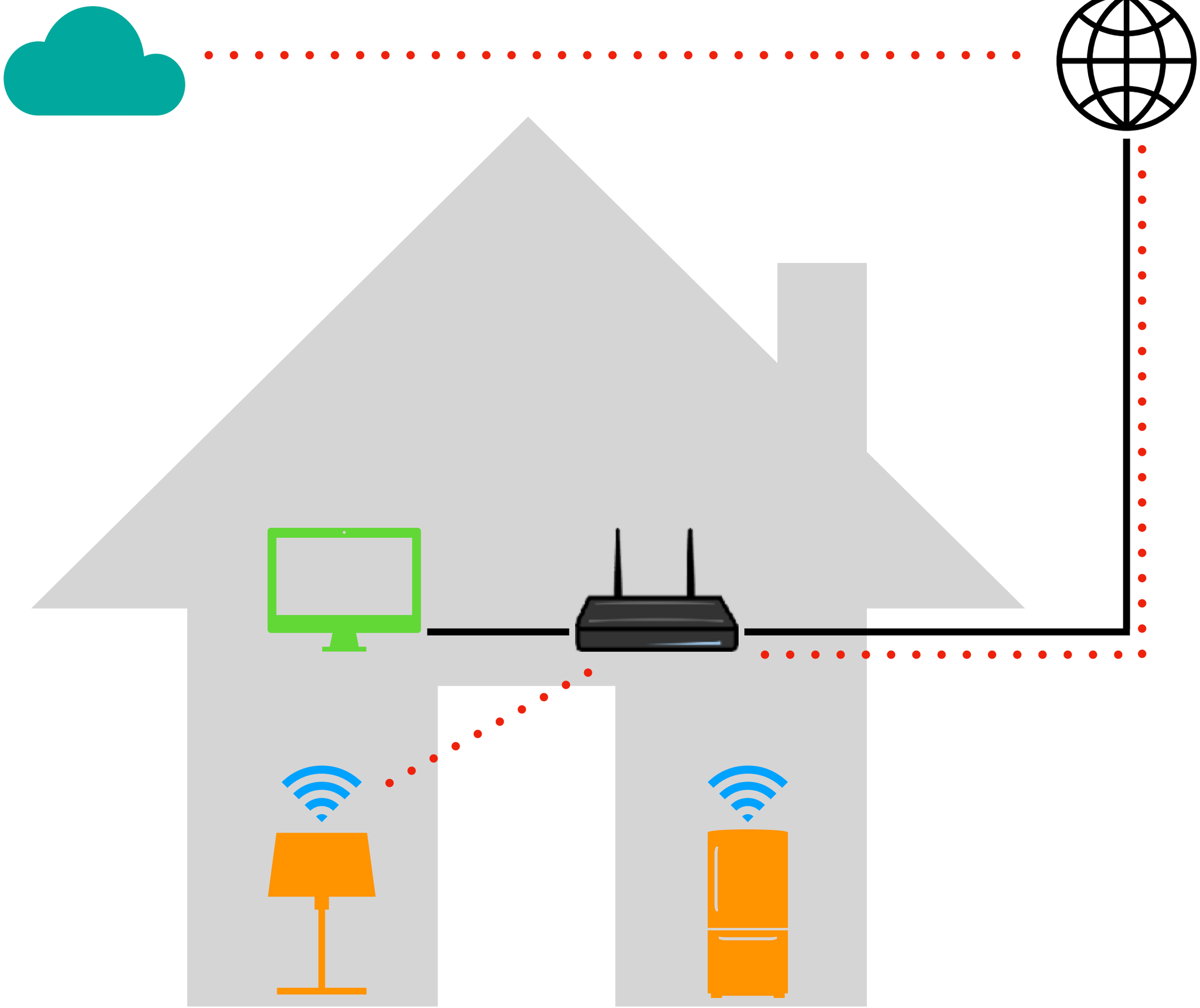
2 more wireless baby monitors hacked: Hackers remotely spied on babies and...

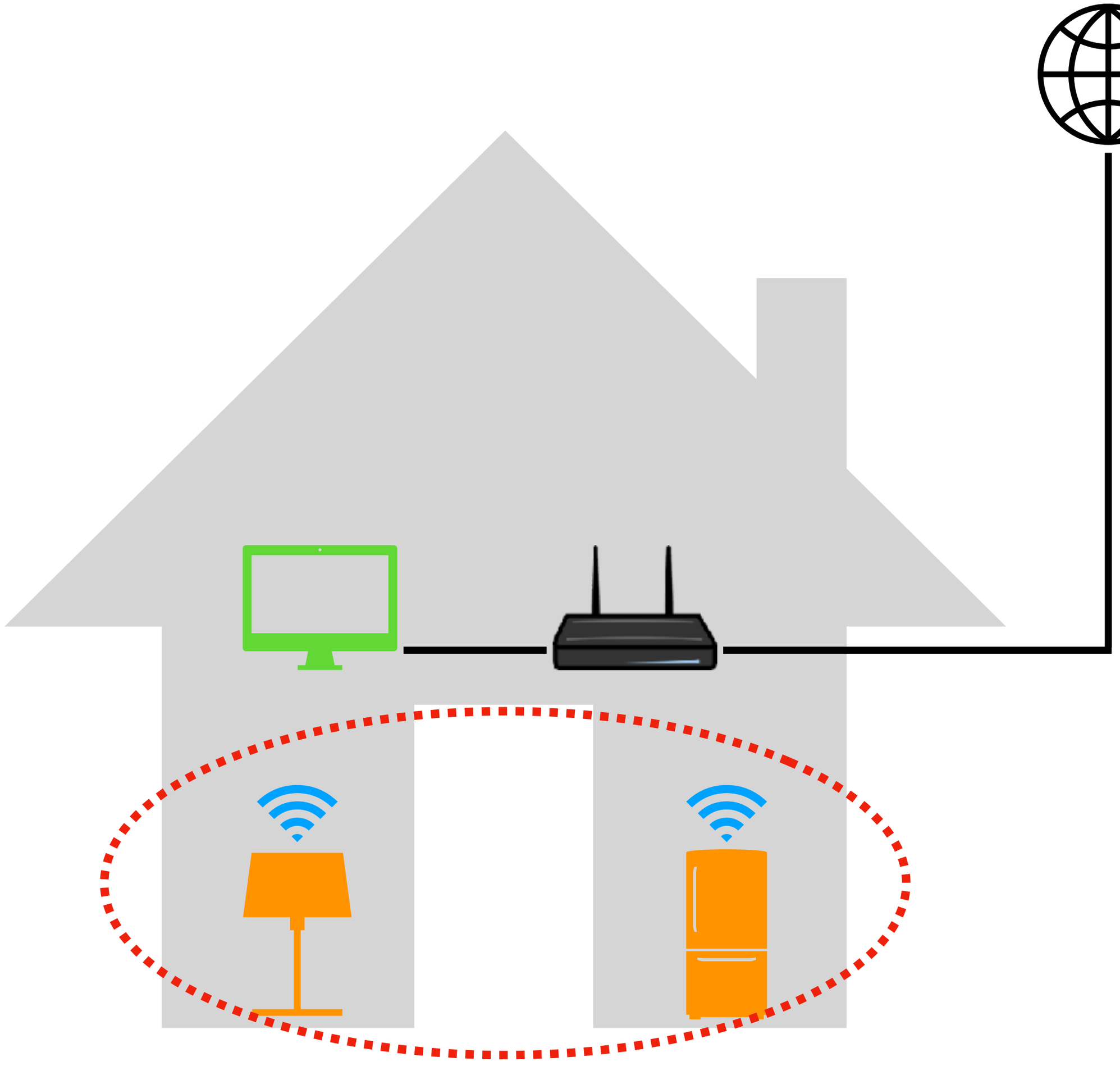
Eerie music coming from wireless baby cam; is it a

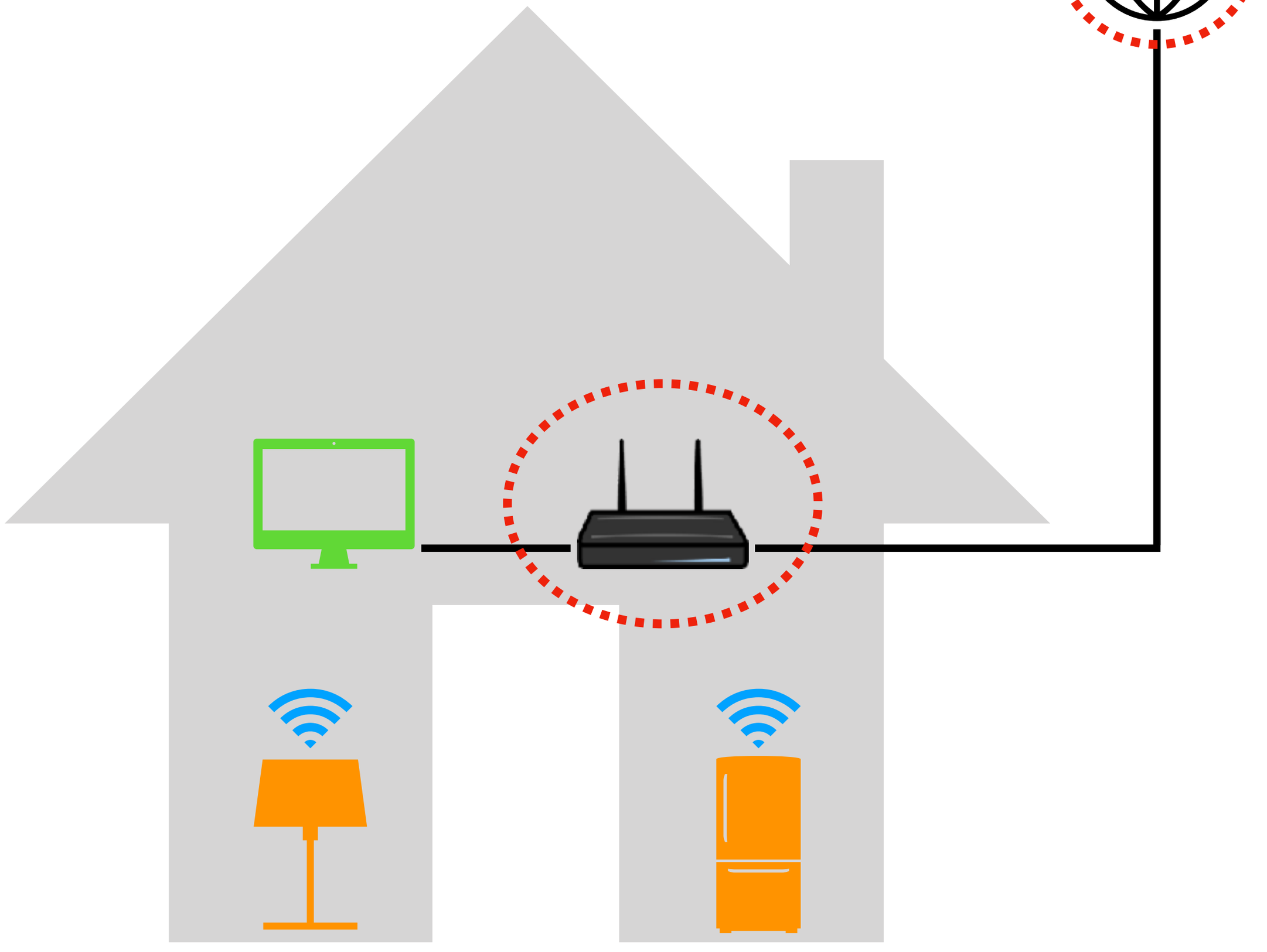


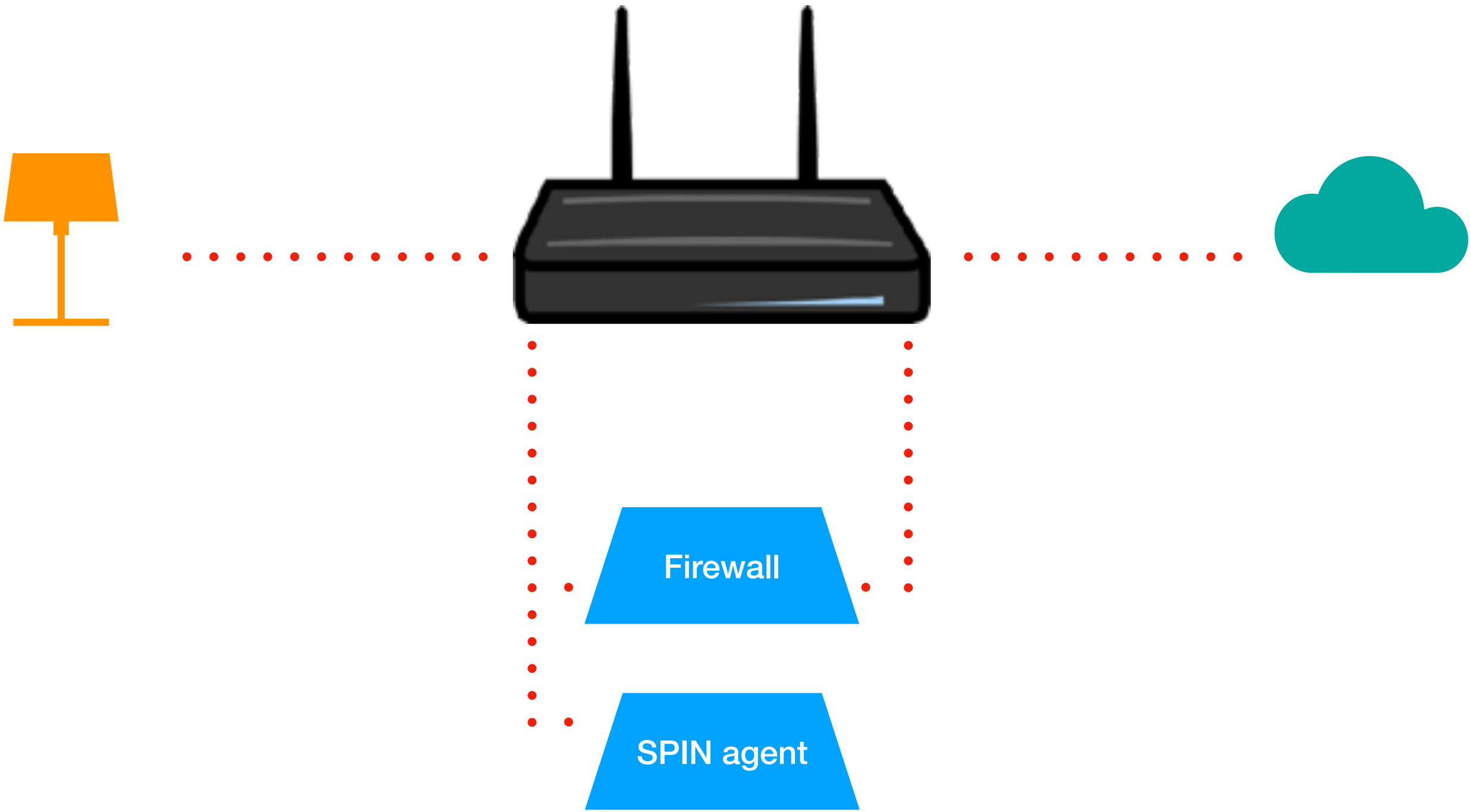
DETECT SMOKE AND CO
CONTROL SWITCHES AND OUTLETS
CONTROL LIGHTING
CONTROL SHADES AND BLINDS
ADJUST CLIMATE
UNLOCK AND LOCK DOORS
OPEN AND CLOSE GARAGE DOORS
MONITOR YOUR HOME

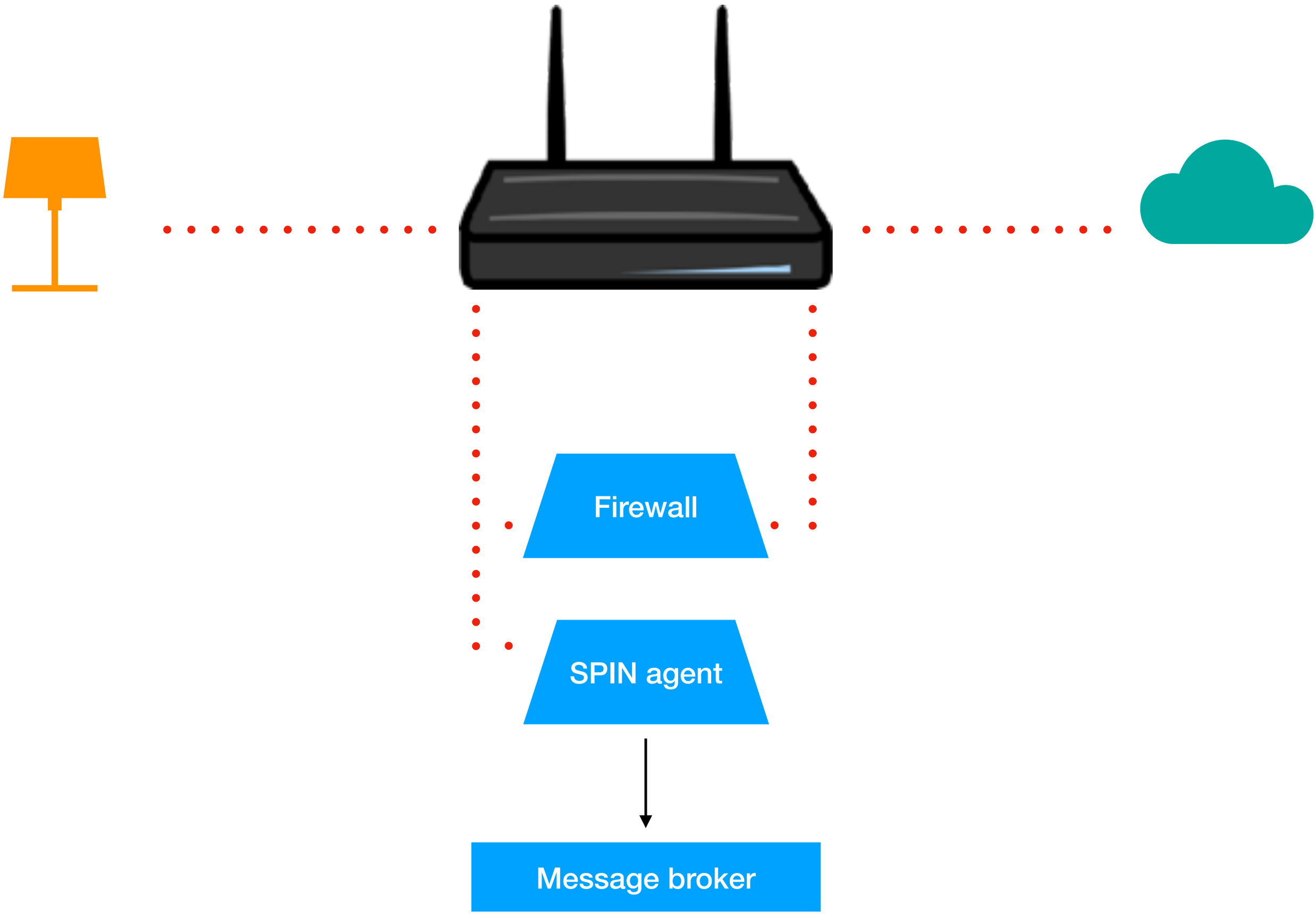


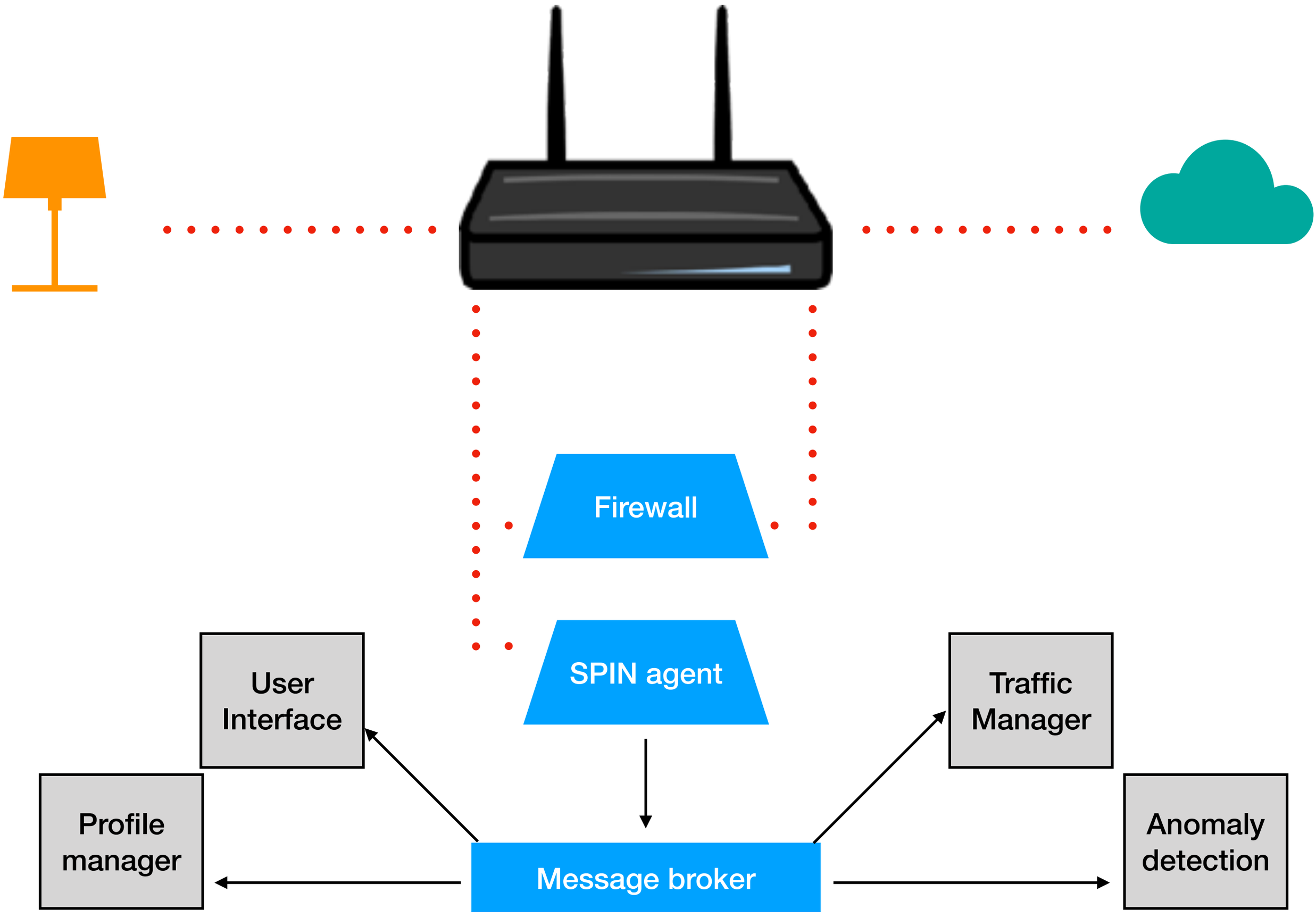


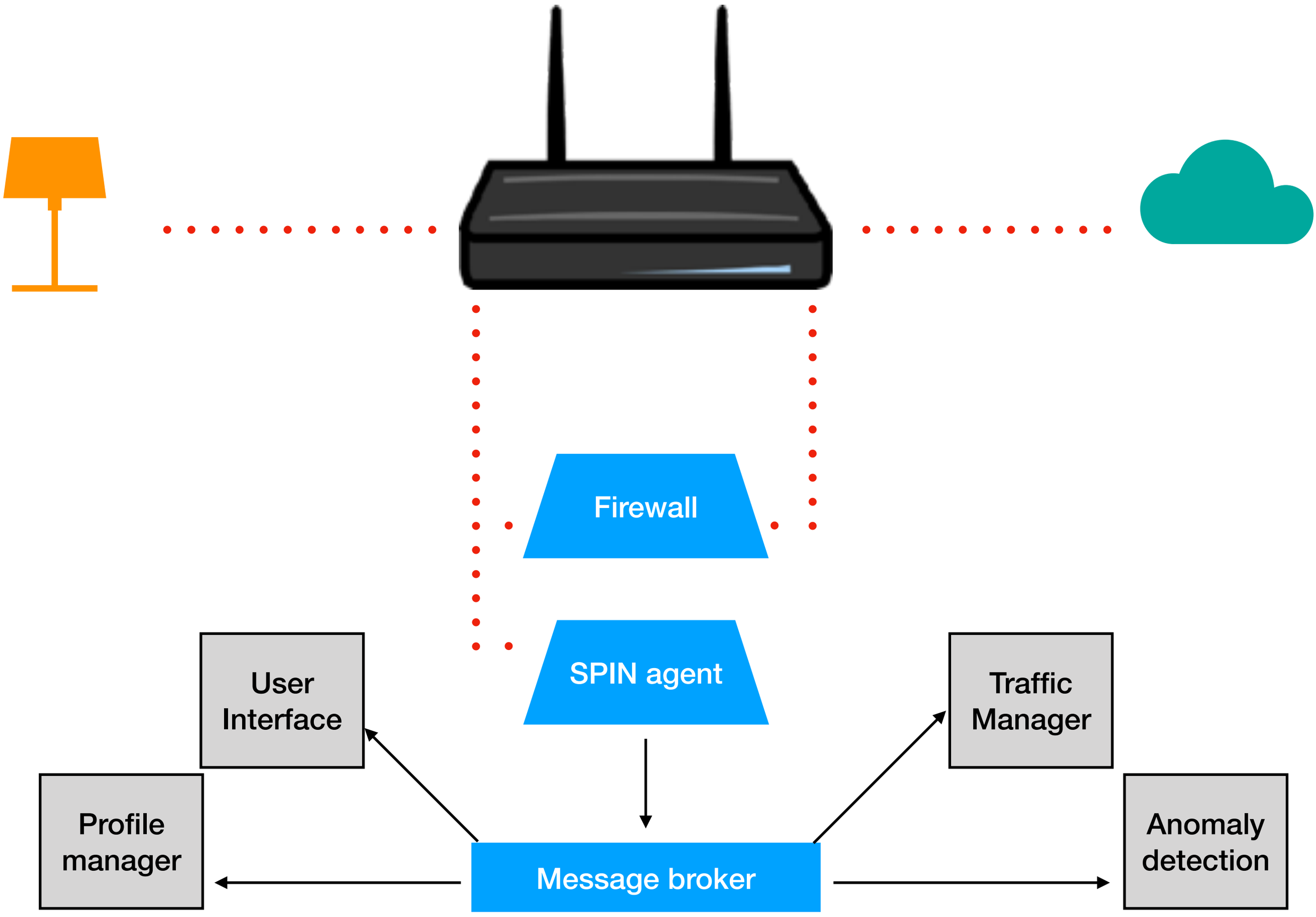


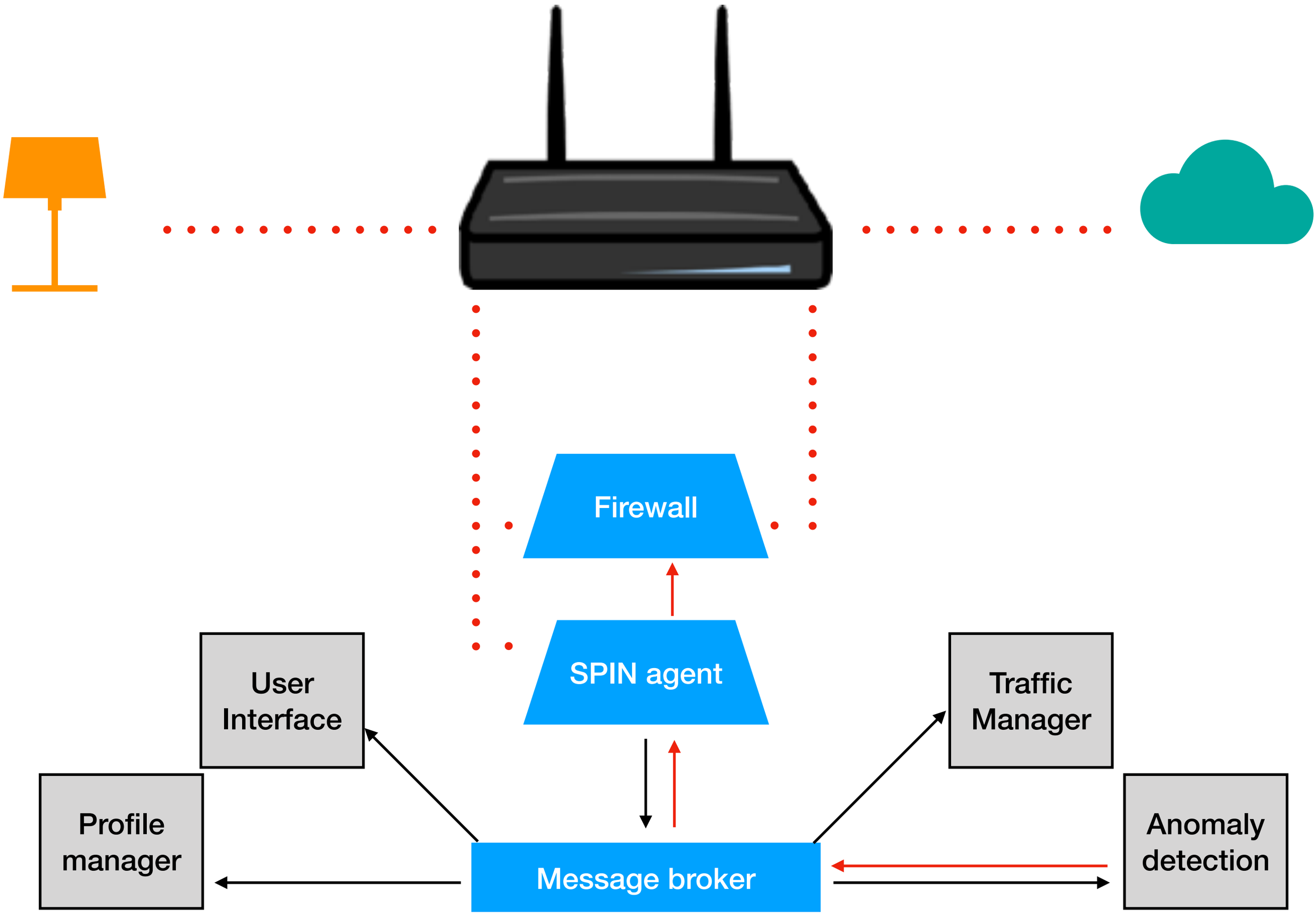



Firewall
SPIN agent


Firewall
SPIN agent
Message broker


Firewall
SPIN agent
User Interface
Profile manager
Message broker
Traffic Manager
Anomaly detection


Firewall
SPIN agent
User Interface
Profile manager
Message broker
Traffic Manager
Anomaly detection


Firewall
SPIN agent
User Interface
Profile manager
Message broker
Traffic Manager
Anomaly detection

ANOMALY
VALUE
TIME

[Docs] [txt|pdf] [draft-ietf-opsa...] [Tracker] [Diff1] [Diff2] [Errata]

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 8520
Category: Standards Track
ISSN: 2070-1721

E. Lear
Cisco Systems
R. Droms
Google
D. Romascanu
March 2019

Manufacturer Usage Description Specification

Abstract

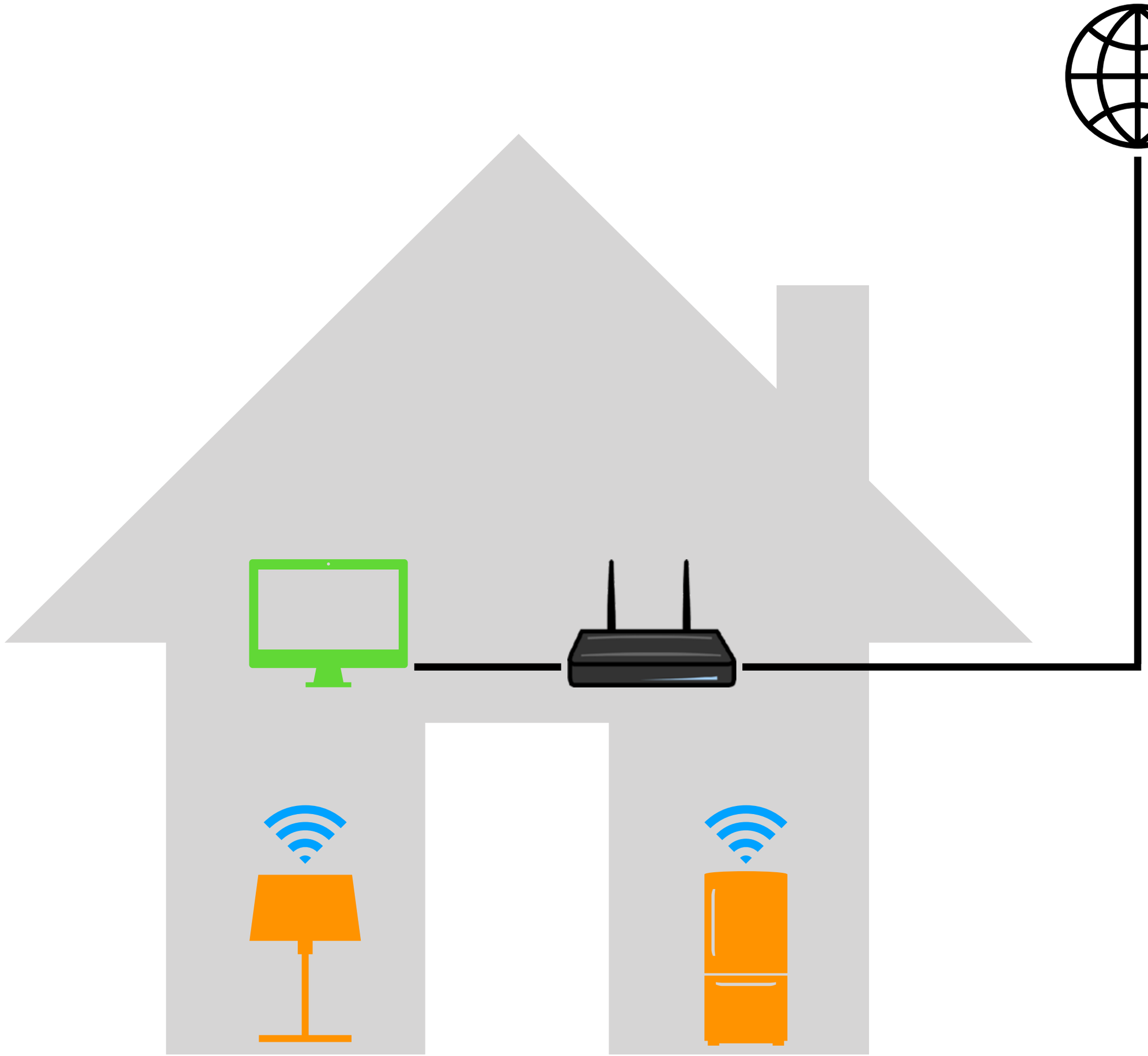
This memo specifies a component-based architecture for Manufacturer Usage Descriptions (MUDs). The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. Later work can delve into other aspects.

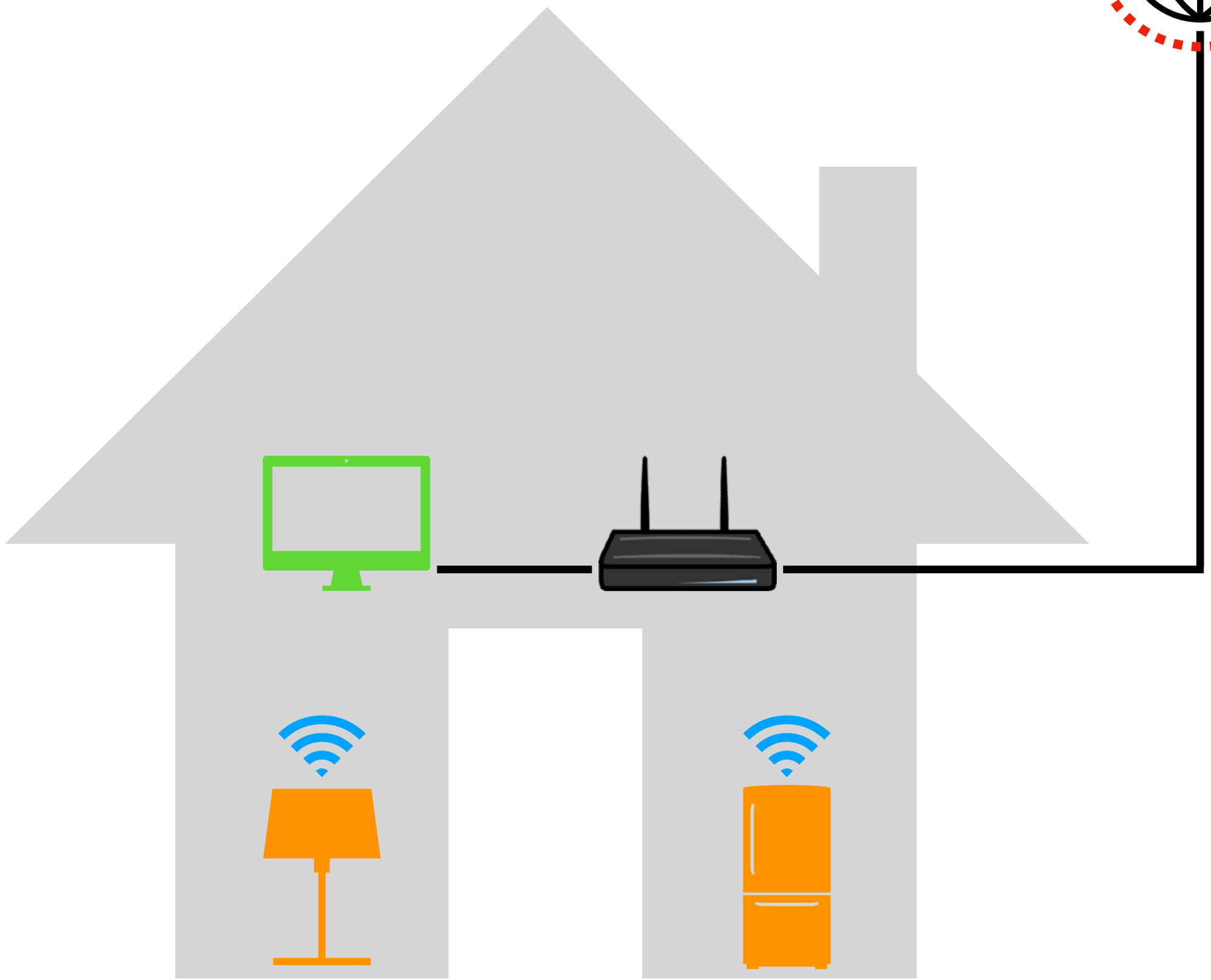
This memo specifies two YANG modules, IPv4 and IPv6 DHCP options, a Link Layer Discovery Protocol (LLDP) TLV, a URL, an X.509 certificate extension, and a means to sign and verify the descriptions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

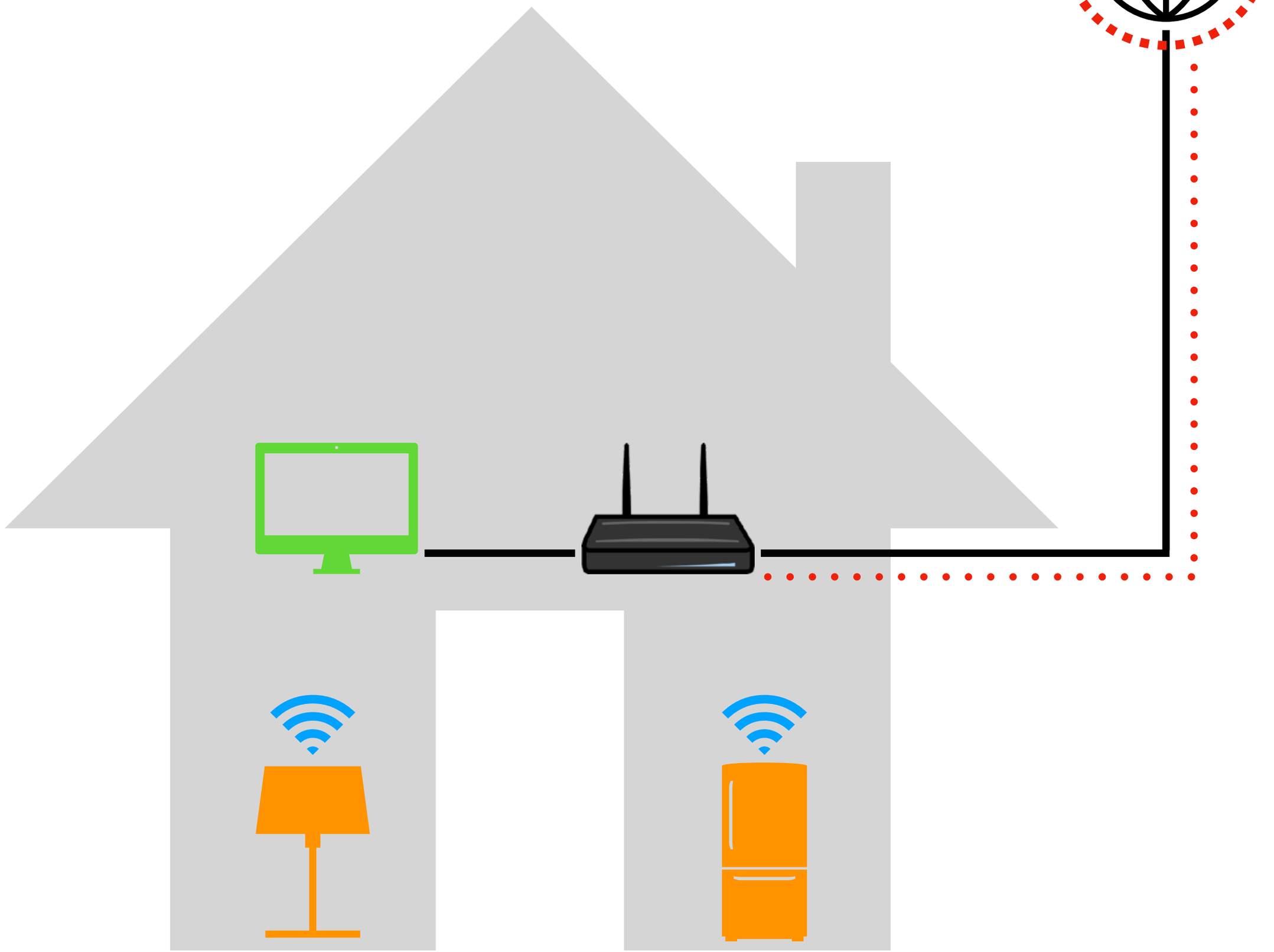


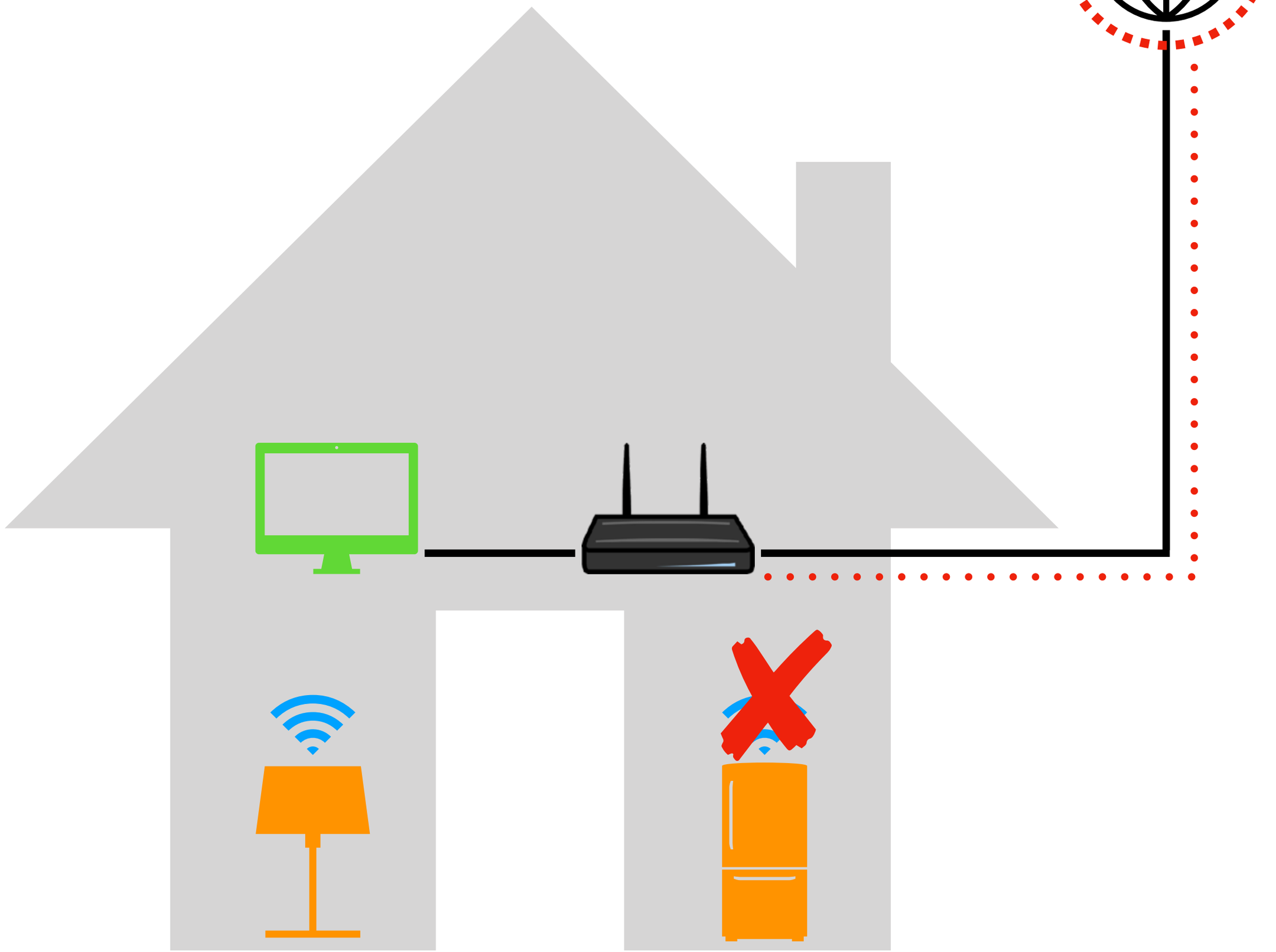


CAUTION

KEEP OUT

QUARANTINE

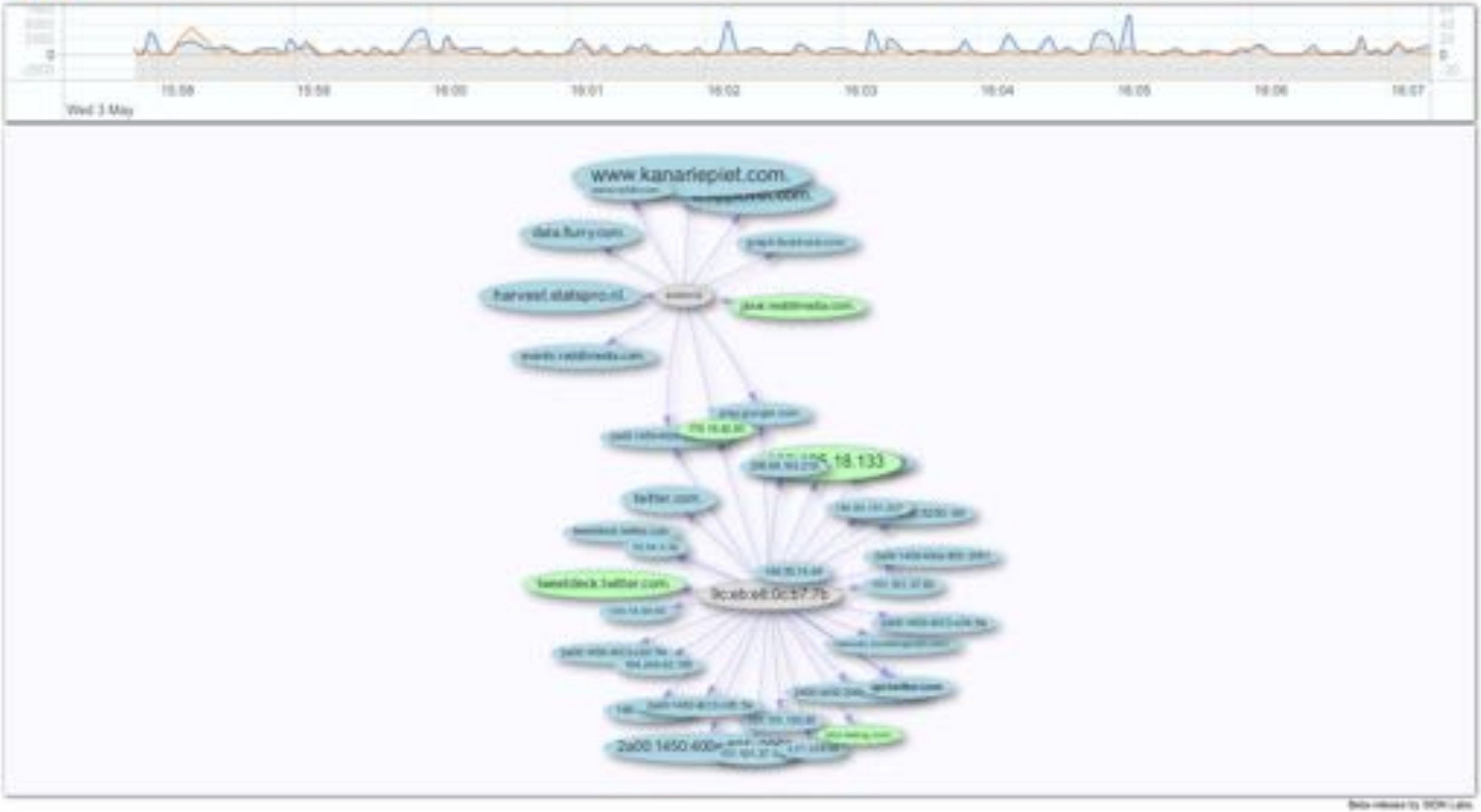


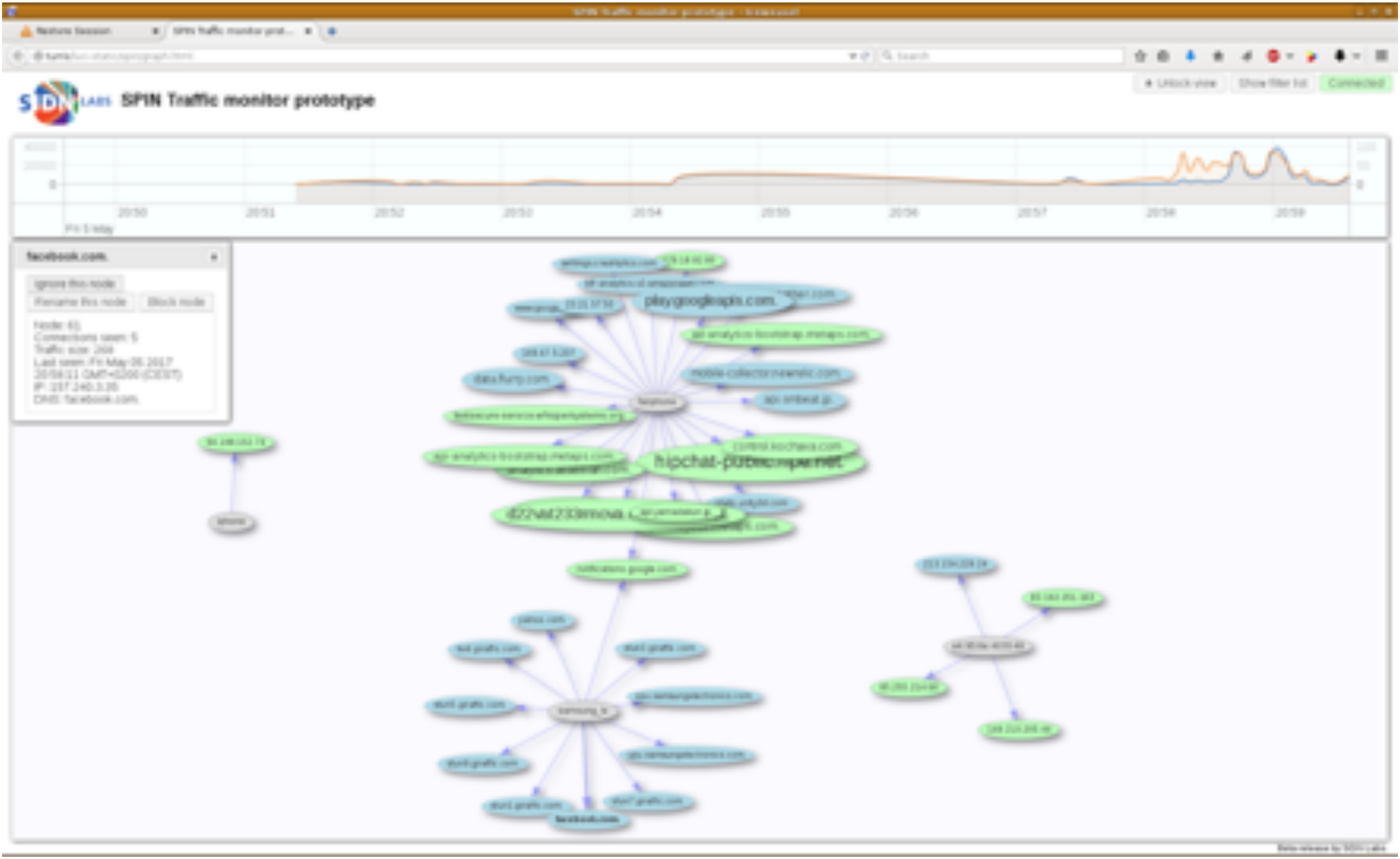


Demo in Images

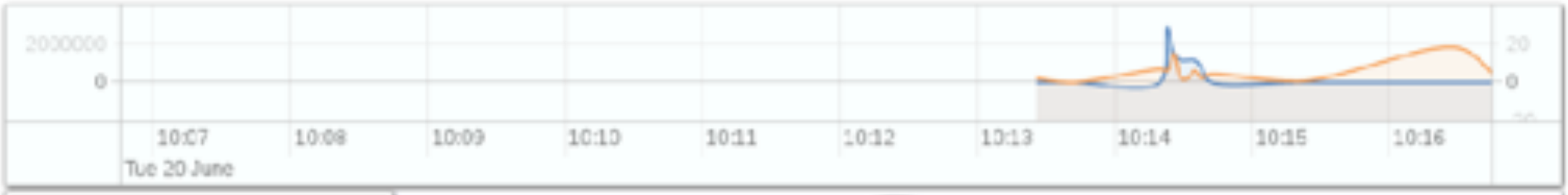
Security and Privacy for In-home Networks (SPIN)

SPIN Traffic monitor prototype




SPIN Traffic monitor prototype
facebook.com
Ignore this node
Rename this node
Block node
playgoogleapis.com
hipchat-public.net

SPIN Traffic monitor prototype



twitter.com

Ignore this node

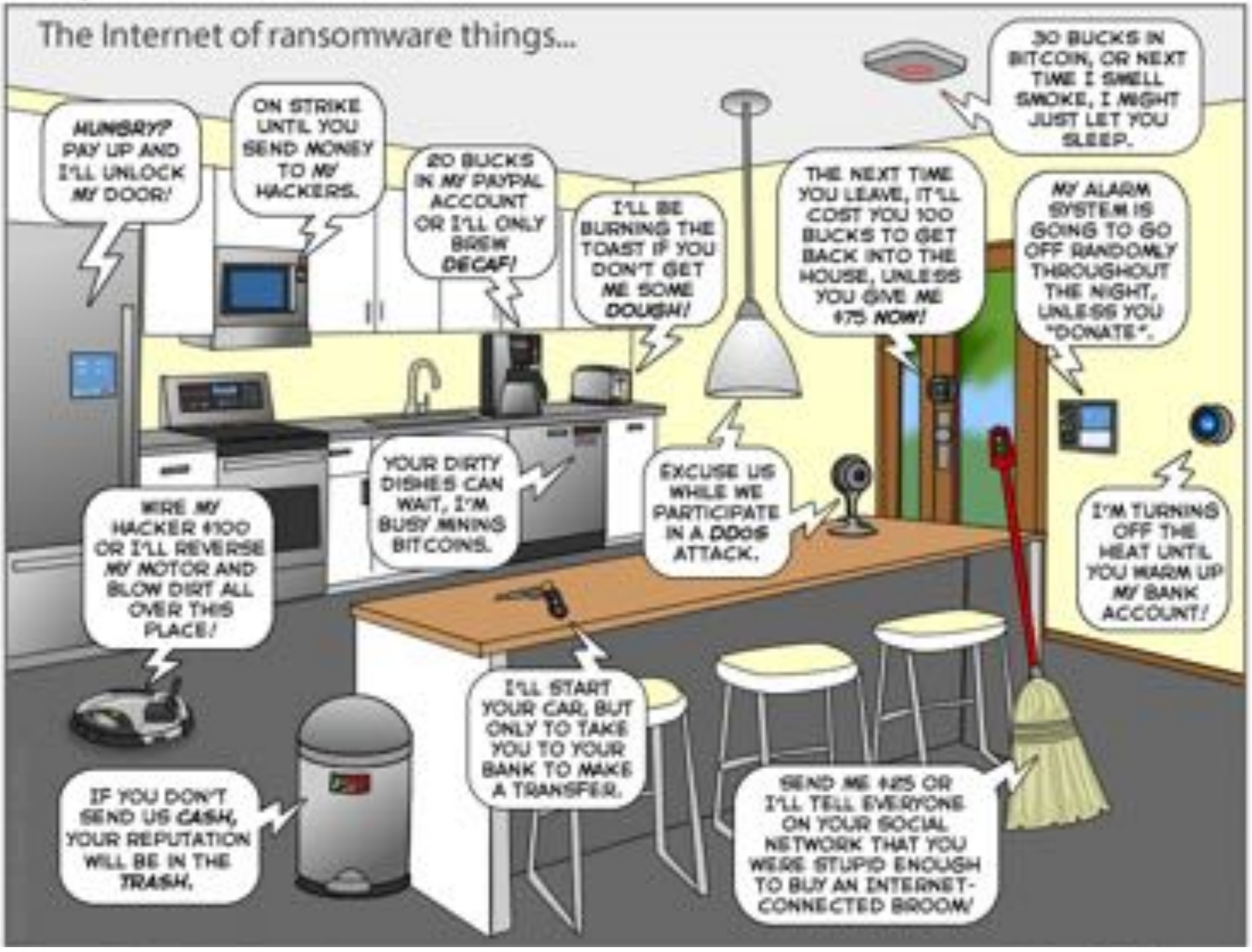
Rename this node | Block node

Node: 35
Connections seen: 2
Traffic size: 1950
Last seen: Tue Jun 20 2017 10:14:36 GMT+0200 (CEST)
IP: 104.244.42.129,104.244.42.193,104.2
DNS: twitter.com,www.twitter.com

sobo

LoRaWAN™

IOT FACTORY



elmer.lastdrager@sidn.nl
https://spin.sidnlabs.nl

Q&A

https://spin.sidnlabs.nl
https://github.com/sidn/spin

Elmer Lastdrager
Research Engineer
elmer.lastdrager@sidn.nl
@elmerlastdrager