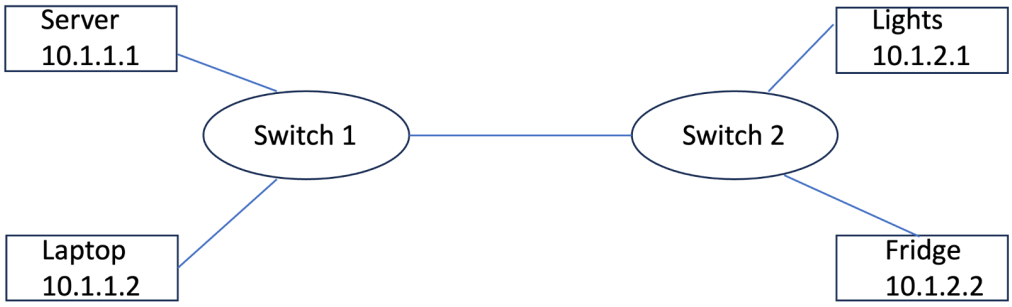
References:

- **Firewalls**
  - Computer Networking: Section 4.3 “Inspecting Datagrams: Firewalls and Intrusion Detection Systems”
- **Mininet:**
  - On the Mininet site, the API Reference will be an excellent resource for figuring out how to run pings or open the command prompt in between the `net.start()` and `net.stop()` lines.
  - A Mininet Walkthrough can be found on this page
- **POX Controller/ OpenFlow:**
  - https://noxrepo.github.io/pox-doc/html/#
  - POX WIKI
  - Inside your VM, the `pox/pox/forwarding/l2_learning.py` example file

  Sending OpenFlow messages with POX
  - **Link to OpenFlow Tutorial**: here
  - OpenFlow 1.3 specification
- **IP Header**
  - Protocol Numbers in IP Header (Protocol Field)



Topology 1

Requirement: In your code use the naming convention below:

Device	Required Naming Convention
Laptop	‘laptop’
Server	‘server’
Fridge	‘Fridge’
Lights	‘Lights’

Switch 1	‘s1’
Switch 2	‘s2’

Table 1: Naming convention

High-level rules:

1. **General Connectivity:** Allow all ARP and ICMP traffic across the network to facilitate general network connectivity.
2. **Web Traffic:** Allow all TCP traffic between the laptop and the server.
3. **Access to IoT devices:** Allow all TCP traffic between the laptop and the lights. Allow all UDP traffic between the laptop and the fridge. Note: server does not access IoT devices
4. **Laptop/Server General Management:** Allow all UDP traffic between the laptop and the server.
5. **Default Deny**: Block all traffic that does not match the above criteria.

Rule #	Src Host	Src IP	Dst Host	Dst IP	Protocol	Action
1		any		any	ARP	accept
2		any		any	ICMP	accept
3	laptop		server		TCP	accept
4	server		laptop		TCP	accept
5	laptop		Lights		TCP	accept
6	Lights		laptop		TCP	accept
7	laptop		Fridge		UDP	accept
8	laptop		server		UDP	accept
9		any		any	ANY	drop

Table 2 - Basic Firewall Rules