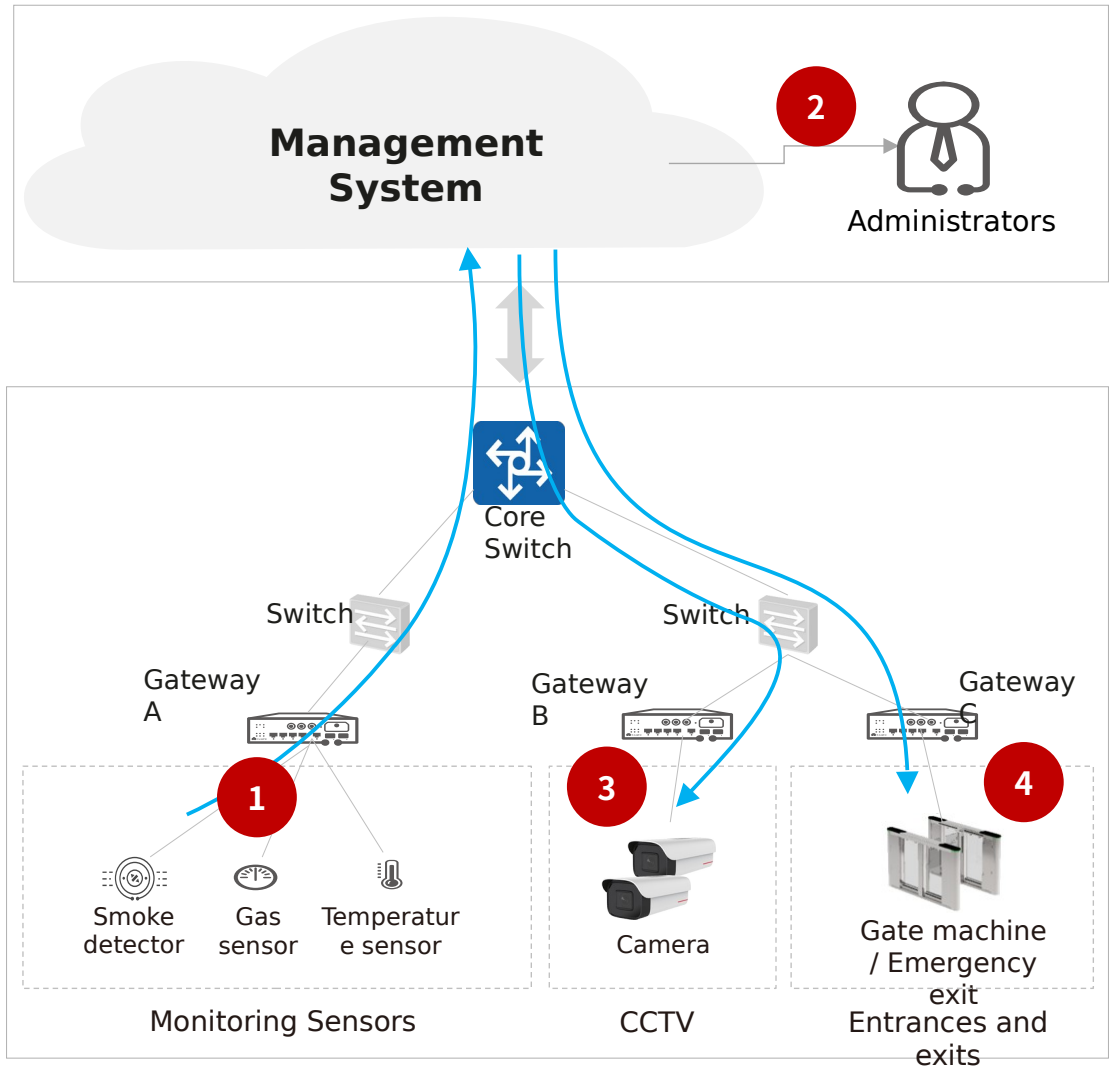
Resiliency and Emergency Communication in Building Automation Systems

Panwei (William)
<william.panwei@huawai.com>
Michael Richardson
<mcr+ietf@sandelman.ca>

Current Fire Alert Scenario



Typical disposal process:

1. The sensors detect exceptions and send alarms to the Management System.

2. The administrator identifies the alarm detail, such as which building and which floor.

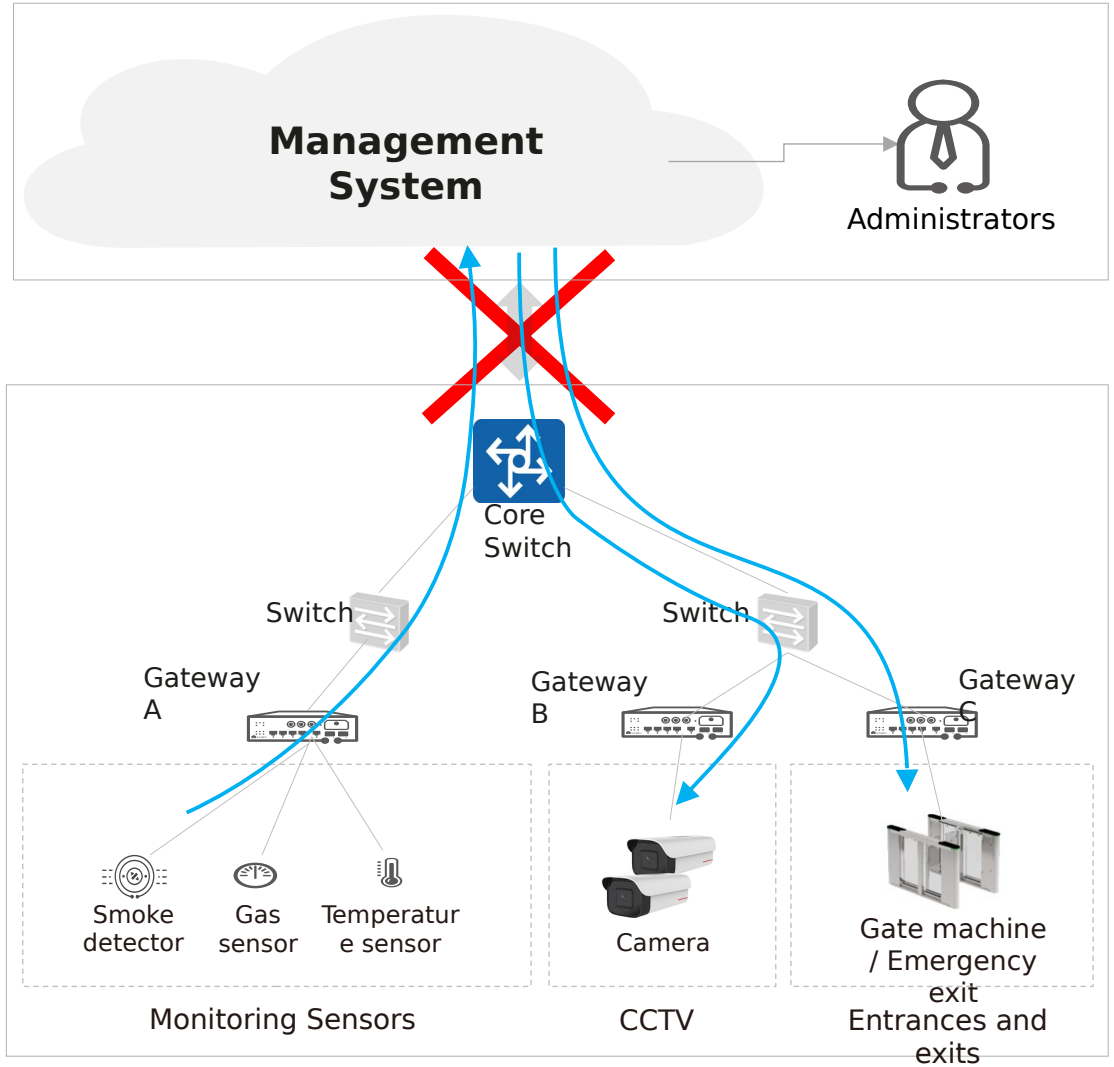
3. The administrator (may notify other administrators to) check the CCTV live video of the corresponding building and floor.

4. The administrator (may notify other administrators to) open the gate machine and unlock the emergency exit.

Gateways are deployed in different locations (such as different floors).

Gateways are installed at different stages/different times, by different vendors

Disadvantages of Current Solution

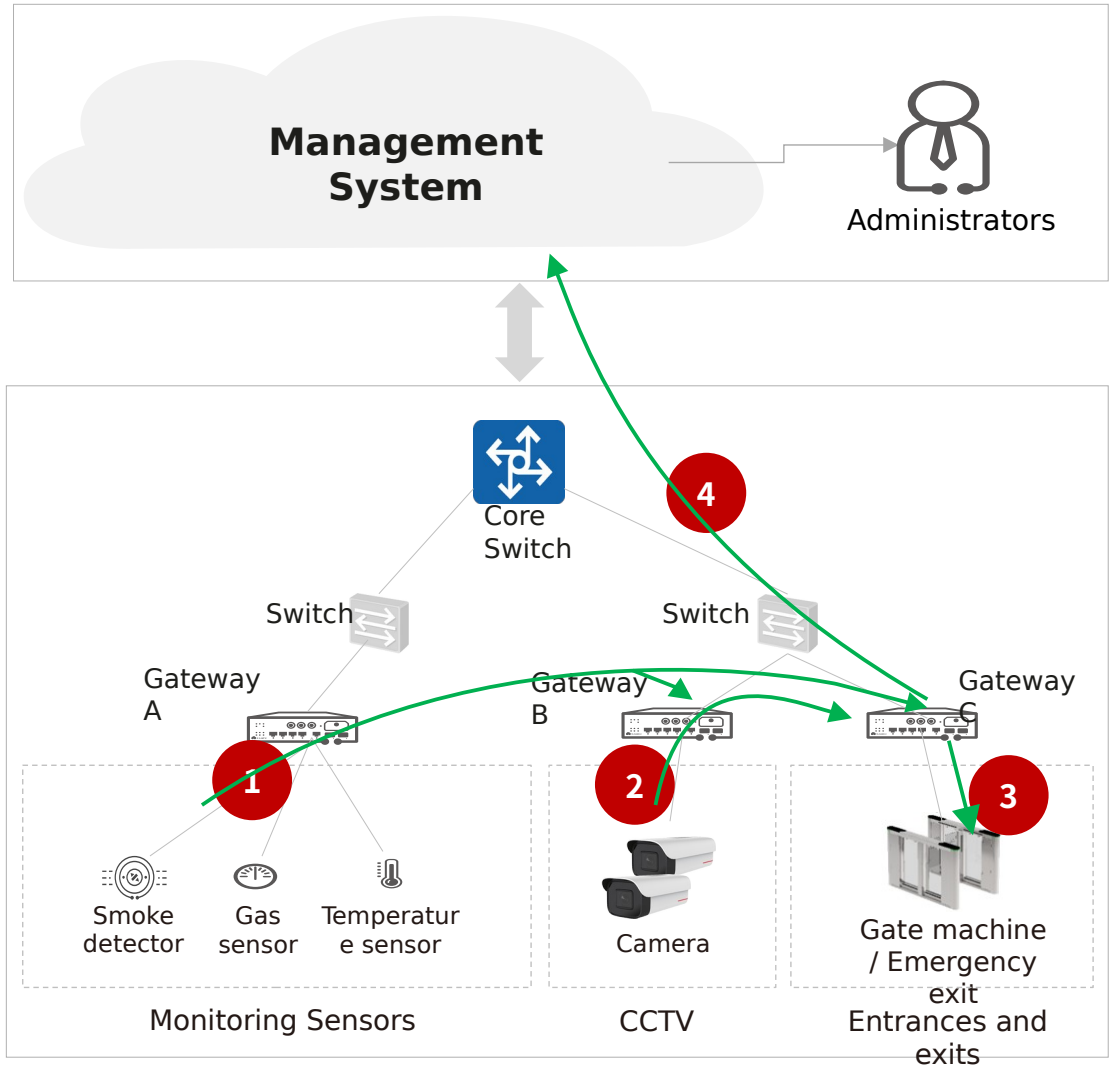


1. The whole process totally relies on the involvement of the data center side administrators, and they need to remotely trigger all commands. If the **network between the data center and the end devices is down**, which is very likely in a disaster situation, then this process won't be available.

2. The rate of **false alarm** is relatively high.

3. **Administrator distractions** may cause untimely responses.

Gateway-to-Gateway Communications



Expect disposal process:

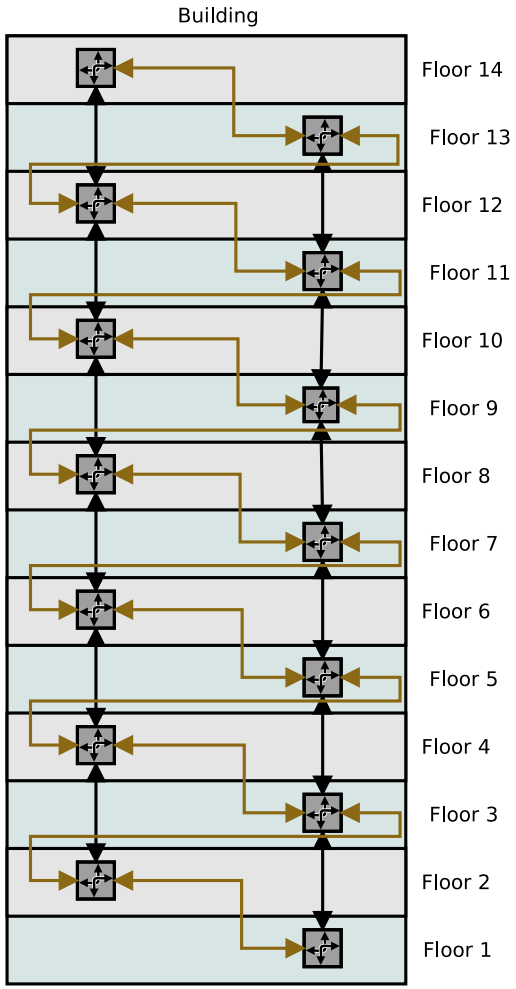
1. The sensors detect exceptions and trigger alarms, and these alarms will be spread to other Gateways by Gateway A.

2. Some cameras can use AI technologies to analyze images and videos, for example, detecting the movement of people. In this case, Gateway B can receive such a notification from the cameras, and spread it to Gateway C.

3. In response to Gateway A's alarm and Gateway B's notification, Gateway C gives commands to open the gate machine and unlock the emergency exit.

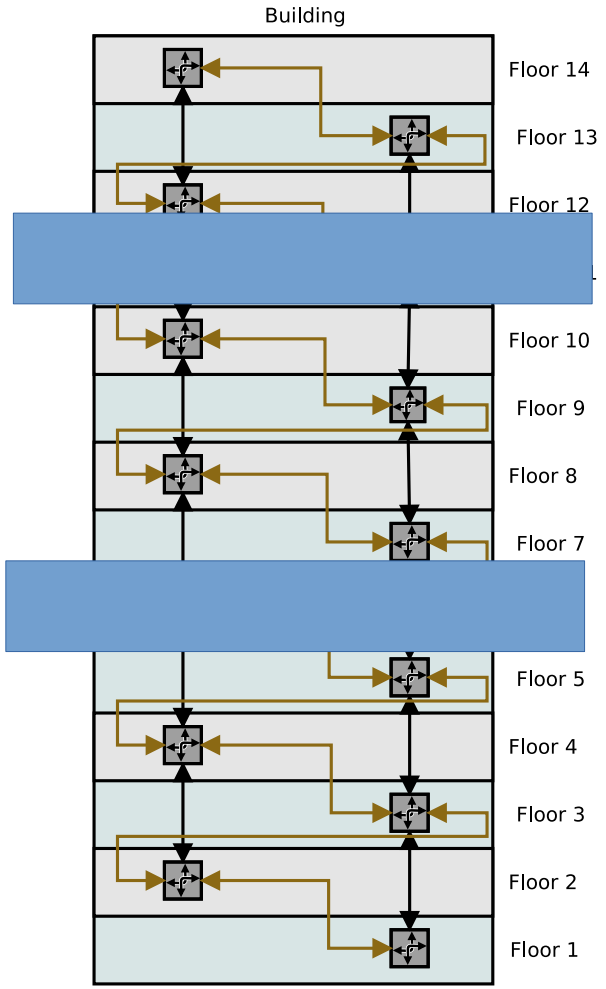
4. Gateway C may report this event disposal back to the management system and the administrators.

Generalize Problem to Multi-Storey Buildings



- A gateway on each floor
  - linked to gateway one floor up and one floor down
- Redundancy provided by a second link to a gateway two floors away
  - via a diverse path
  - bigger buildings might have multiple gateways per floor
- IPv4-think… form an L2 metro-ethernet ring.
  - or SDN can do stuff
- IPv6-think: OSPFv3? ROLL? SNAC?
  - ROLL (RFC6550) actually pretty good fit
- During a failure, communications between floors for coordination is important
  - system is distributed, but needs awareness

SNAC'ing during a failure



- network isolation reduces network to small groups of gateways
- SNAC method lets' adjacent floors communicate with other's sensors
- gateway devices may have significant intelligences (routers with VMs), but might have to turn that off when on battery
- alternate solutions with ungrounded RPL (RFC6550) are possible
  - RFC6550 also could be a SNAC solution

Conclusions and Discussion

- this is a kind of edge between managed and unmanaged networks
  - management can do some activities like pre-deploying credentials
- this might not be close enough to home problem as described in SNAC problem statement to have anything in common
  - or may be there are some interesting synergies

- these slides are about the L3/routing problem in the building situation
- there are L4→L9 problems as well
  - come to our side meeting, Tuesday 18:00 in room Philadelphia South