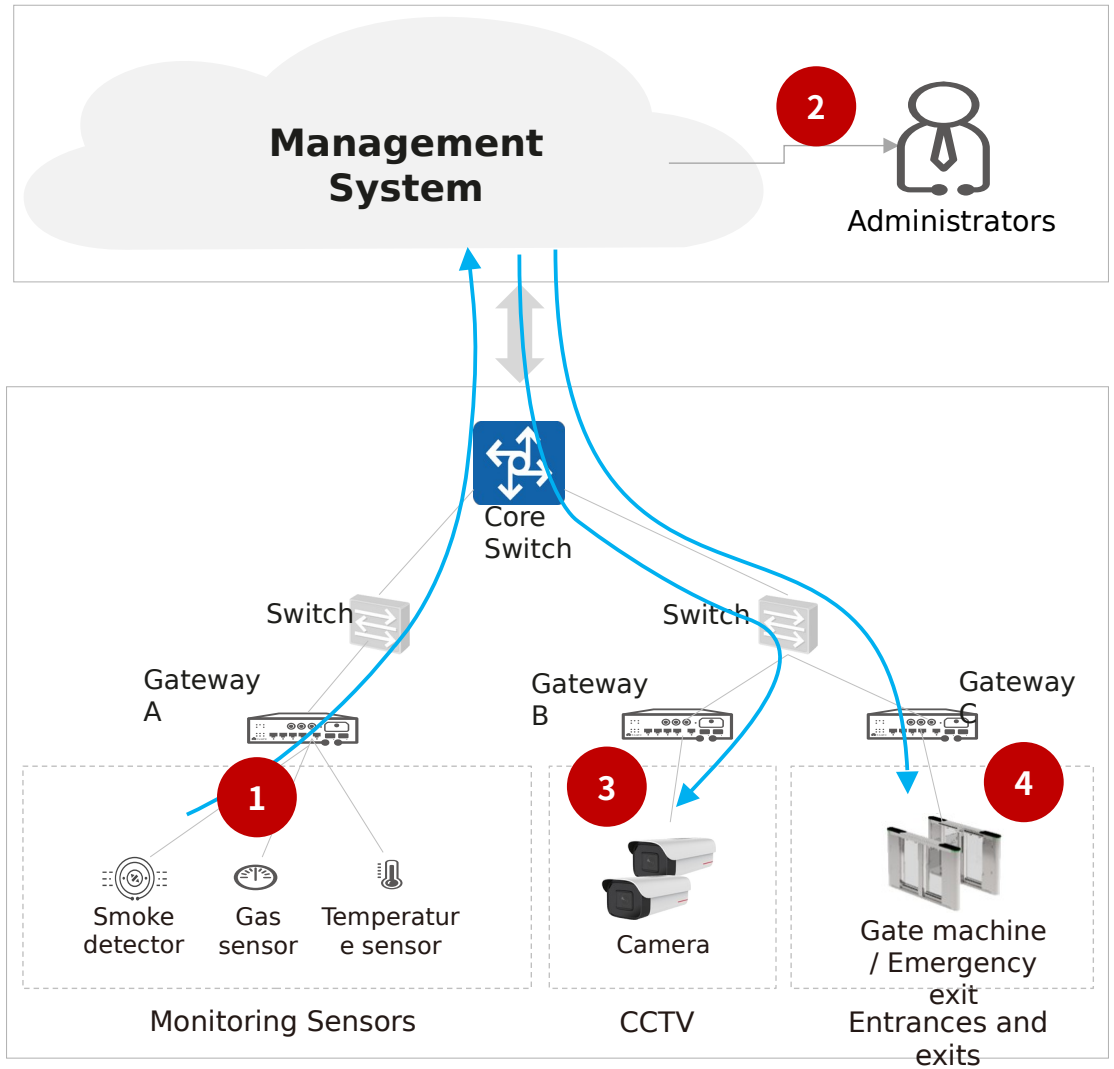
# Inter-Gateway Discovery and Communications in Building Automation Systems

# Current Fire Alert Scenario




**Typical resolution process:**

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

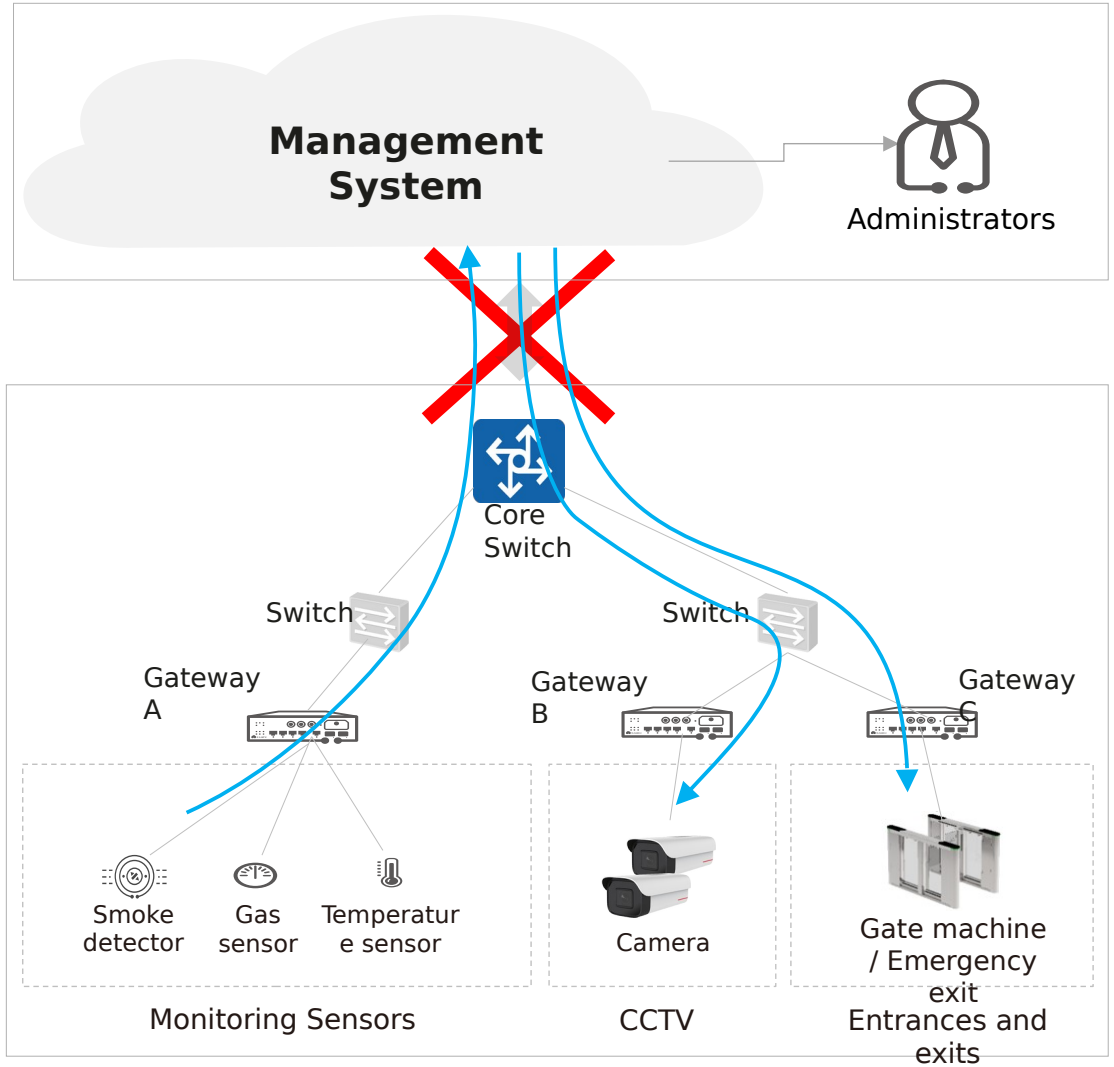
2. The administrator identifies the alarm detail, such as which building and which floor.

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.

# Disadvantages of Current Solution

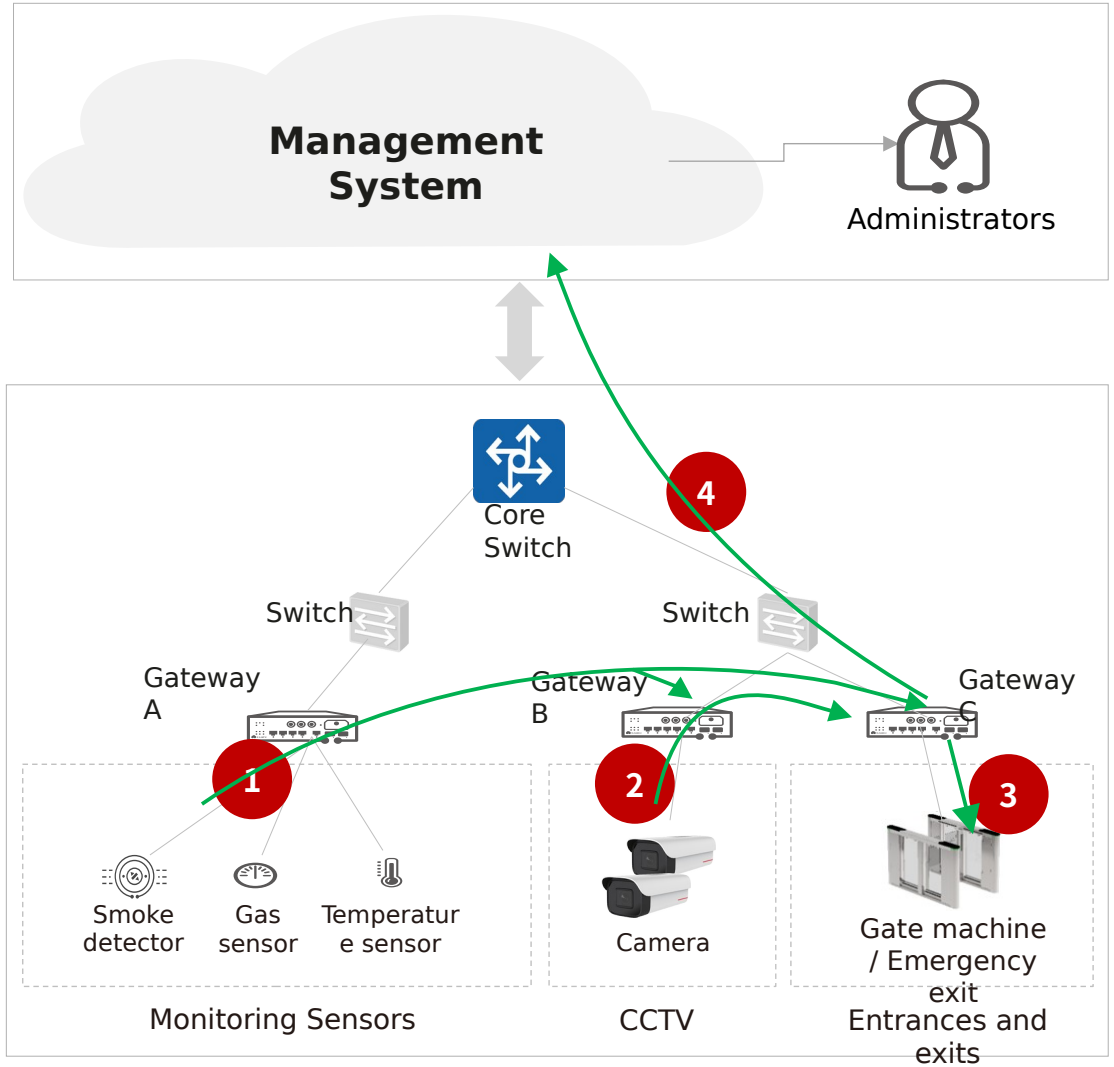



1. The whole process totally relies on the involvement of the data center side administrators, and they need to remotely trigger all commands. If the **network between the data center and the end devices is down**, which is very likely in a disaster situation, then this process won't be available.

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

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

# Expected resolution process



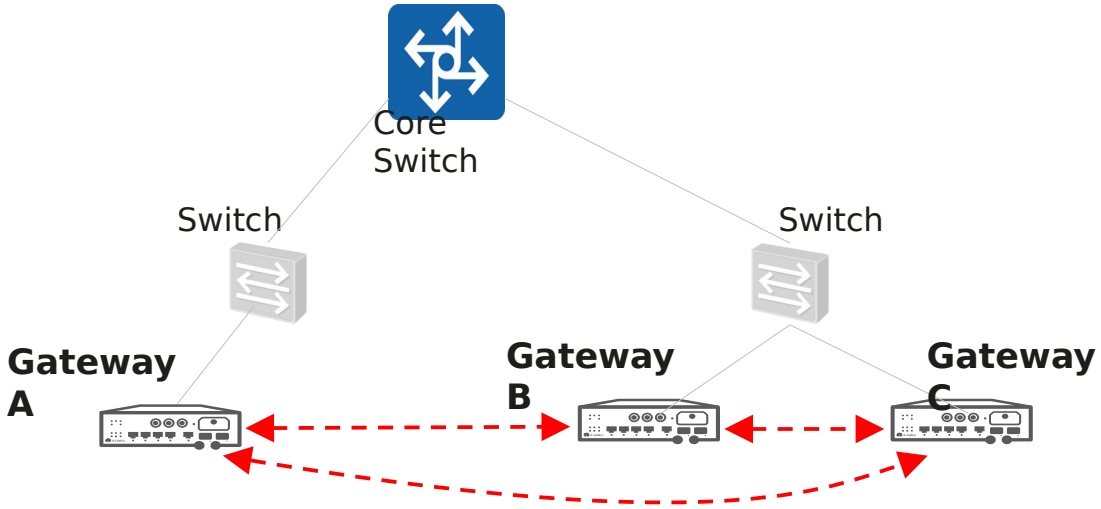

1. The sensors detect exceptions and trigger alarms. Gateway A receives these alarms and spreads them to other Gateways.

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.

# Gateway-to-Gateway Communications




As shown in the expected process and the left diagram, the gateways are not connected directly but need to communicate with each other.

1. The gateways need to discover other gateways and their services.

2. The gateways need to choose the protocols to communicate.

3. The communication between gateways need to be secured, i.e., the authentication of the peer and other security requirements should be met.

# Service Discovery

The gateways not only transfer the data from end devices to management system, they now need to communicate with each other and deal with the data. So, the gateways need to discover other gateways and the services provided by these gateways.

**Candidate mechanisms of service discovery:**

1st: SSDP (Simple Service Discovery Protocol)
Origin: draft-cai-ssdp-v1 “Simple Service Discovery Protocol/1.0”

2nd: mDNS + DNS-SD
Origin: RFC 6762 “Multicast DNS”, RFC 6763 “DNS-Based Service Discovery”

3rd: CoAP Discovery
Origin: RFC 7252 “The Constrained Application Protocol (CoAP)”

# Data Exchange Protocol

The data including alarms and notifications need to be communicated between gateways.

**Candidate protocols to exchange data:**

1st: CoAP

Origin: RFC 7252 “The Constrained Application Protocol (CoAP)”

2nd: MQTT

Origin: OASIS

3rd: MQTT-SN (MQTT for Sensor Networks)

Origin: OASIS

# Lightweight Identity Credential

The security basis for the communications between the gateways and end devices and among the gateways is to authenticate each peer's identity. Therefore, an appropriate cryptographic identity mechanism is needed. Considering the end devices may be constrained IoT devices, the identity credential should be a lightweight mechanism.

**Candidate mechanisms of lightweight credential:**

1 Symmetric Key (PSK)
2 Asymmetric Key (Public / Private keys)
**3 Lightweight Certificate** (PKI)
4 ...

**Candidate technologies of lightweight certificate:**

1st: Profiled X.509 Certificates
Origin: RFC 7925 “TLS / DTLS Profiles for the Internet of Things”

2nd: Certificate Compression
Origin: RFC 8879 “TLS Certificate Compression”

**3rd: C509 Certificates**
Origin: draft-ietf-cose-cbor-encoded-cert “CBOR Encoded X.509 Certificates”

# Lightweight Certificate Request Mechanism

If certificate is chosen as the type of identity credential, a lightweight certificate request mechanism should also be considered.

**Candidate mechanisms:**

1st: CMC (Certificate Management over CMS)
Origin: RFC 5272 “Certificate Management over CMS (CMC)”, RFC 6402 “Certificate Management over CMS (CMC) Updates”

2nd: CMP (Certificate Management Protocol)
Origin: RFC 4210 “Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)”

3rd: Lightweight CMP
Origin: draft-ietf-lamps-lightweight-cmp-profile “Lightweight Certificate Management Protocol (CMP) Profile”

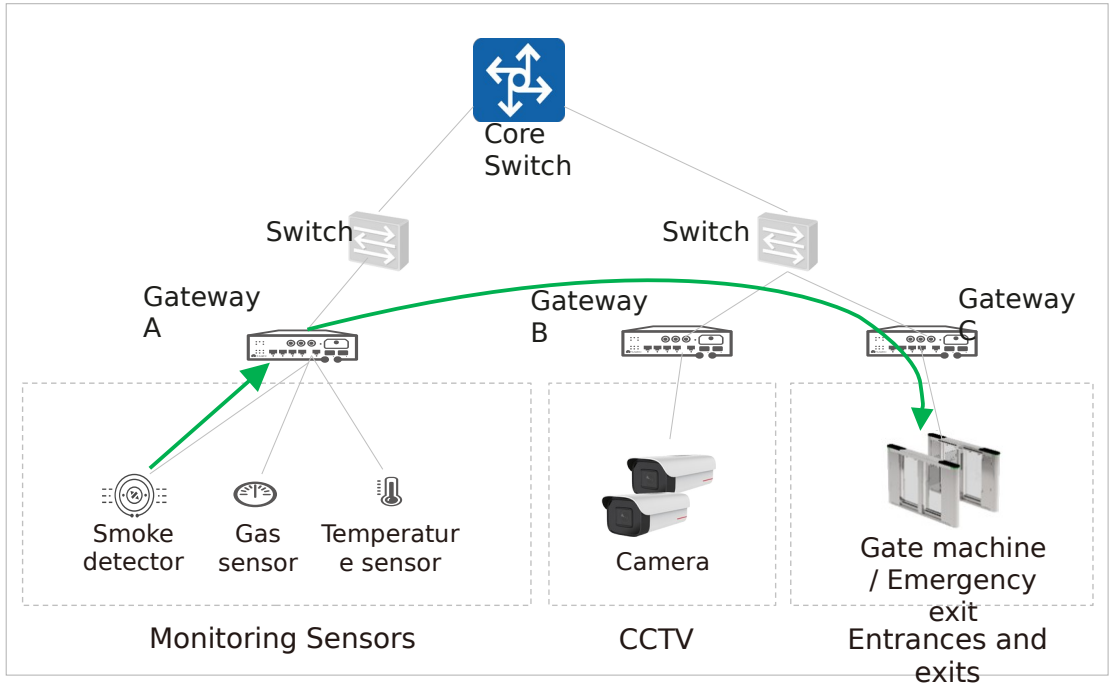
4th: EST (Enrollment over Secure Transport)
Origin: RFC 7030 “Enrollment over Secure Transport”

5th: EST-CoAP
Origin: RFC 9148 “EST-coaps: Enrollment over Secure Transport with the Secure Constrained Application Protocol”

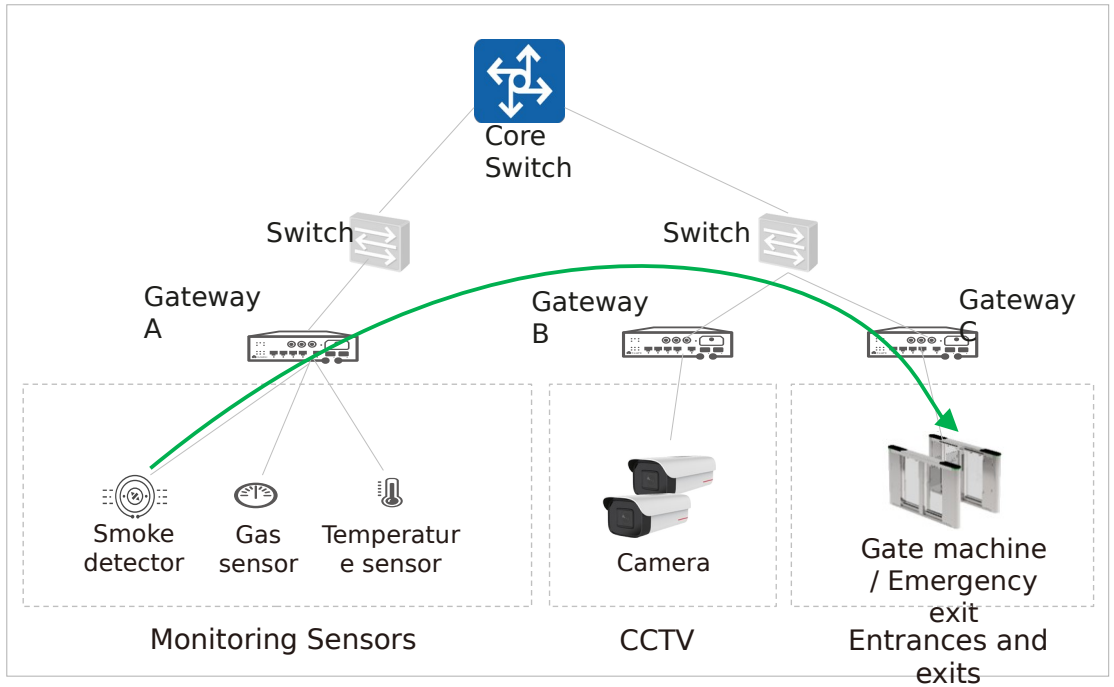
6th: CMP-CoAP
Origin: draft-ietf-ace-cmpv2-coap-transport “CoAP Transfer for the Certificate Management Protocol”

7th: C509 CSR over CoAP
Origin: draft-ietf-cose-cbor-encoded-cert “CBOR Encoded X.509 Certificates”

# Future Evolution of Coordination Solutions




**Gateway A can communicate with end devices connected to other Gateways**




**End devices can directly communicate with each other**

Thank you.