Workgroup: Network Working Group
Internet-Draft:
draft-richardson-snac-building-use-case-00
Published: 26 June 2022
Intended Status: Standards Track
Expires: 28 December 2022
Authors: M. Richardson
Sandelman Software Works
W. Pan
Huawei Technologies

# Inter-Gateway Discovery and Communications in Building Automation Systems

## Abstract

This document describes a use case where gateways need to discover each other in order to maintain building safety systems

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 December 2022.

**Table of Contents**


1. Introduction
   1.1. Building Network Topology
   1.2. Scope of problem
2. Privacy Considerations
3. Security Considerations
4. IANA Considerations
5. Acknowledgements
6. Changelog
7. References
   7.1. Normative References
   7.2. Informative References

Authors' Addresses


## 1. Introduction

XXX - Intra-Gateway or Inter-Gateway?

This document describes a scenario where gateway to gateway discovery is needed in order to maintain a series of building safety systems.

New Buildings are being built with digitally controlled automation, and existing buildings are being retrofitted with new automation systems. While some buildings can and do leverage legacy wiring systems such as BACnet, and able to deploy technology like [RFC8163] to turn existing twisted pair control systems into IPv6 networks, other buildings are using various combinations of 802.15.4, Powerline ethernet, etc. as an alternative to explicit wiring.

Whether wired or wireless passing of a signal through re-inforced concrete floors presents a challenge, particularly in the retrofit situation.

### 1.1. Building Network Topology

The sheer height of many buildings means that even per-floor gateways may be more than 100m away (copper ethernet distance) from the control room. The distance issue then requires that fiber be used to connect the building, or that sub-control rooms be established at regular intervals.

As an alternative to this resulting star topology, with many critical points, a daisy-chain topology can be established, where the gateways on adjacent floors (or areas) are directly connected. To provide redundancy an additional cable can connect alternating floors, ideally via a different conduit. A routing protocol such as [RFC6550] can be used, or a metro-ethernet topology can be used to connect the gateways.

This deals with the Layer 1 and Layer 2 resiliency in face of destruction of the control room, or the conduits leading to the control room. But what about the resiliency at layer 4 and at the application layer? Regulations often say that when a smoke detector is tripped in one area that some or all adjacent areas need also to signal for occupants to leave. Emergency doors and stairwells need to be unlocked, emergency lighting and communications systems activated.

### 1.2. Scope of problem

Many industrial settings can assume a competent operator to plan and manage the network. On the other hand, the HOMENET problem description assumes that there is no such operator [RFC7368].

In the building case there is a hybrid situation. For most of the regular, boring operation of the building there is a central point of control, a human operator is reachable, and maintenance people or processes can be deployed.

It is during an emergency that the problems arise. The central point of control and the humans involved may become unavailable due to network partition, or because there are other things occupying their attention.

This document presents the problem of having (network) adjacent gateways being able discover each other and interoperate with each other's sensor network from a just powered on situation. The criteria of just powered on does not imply a factory default situation. This criteria is to acknowledge that the power situation might be unstable: batteries and backup generators might not come on immediately, but there could be some short duration when power is unstable. As a result, any kind of configuration or network convergence that depends upon connectivity that would exist during regular operation can not be assumed.

A key point about the just powered-on situation is that it assumes that any mesh network (whether [RFC6550] or Metro-Ring) may not have formed yet, and may never form.

A network forming with [RFC6550] would normally do address assignment from the PIOs contained in the DODAGs. For stability, resiliency, and ease of deployment, the Gateway devices would likely number their sensors using either a ULA locally generated, or via an IPv6 prefix allocated via DHCPv6-PD using an extremely long (essentially infinite) lifetime.

The Gateways could advertise their prefixes into a [RFC6550] mesh using DAO messages. (On a network built using a metro-ring protocol,

then the entire gateway network is a single L2 domain, and a single OSPF area could be created)

Note that [RFC6550] includes support for non-Grounded DODAGs (no DODAG root) which would permit adjacent nodes to communicate and form a DAG, it is unclear yet if that mechanism can be used for this.

## 2. Privacy Considerations

To be considered.

## 3. Security Considerations

Something about building networks and physical security.

## 4. IANA Considerations

None.

## 5. Acknowledgements

Hello.

## 6. Changelog

## 7. References

### 7.1. Normative References


**[BCP14]** Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.


### 7.2. Informative References


**[diehard]** McTiernan, J., McTiernan, J., and Twentieth Century Fox, "Die Hard", 1988.

**[RFC6550]** Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

**[RFC7368]** Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC

7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

**[RFC8163]** Lynn, K., Ed., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks", RFC 8163, DOI 10.17487/RFC8163, May 2017, <https://www.rfc-editor.org/info/rfc8163>.

## Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Wei Pan
Huawei Technologies

Email: william.panwei@huawei.com