Networking Working Group
Internet-Draft
Intended status: Informational
Expires: March 14, 2010

J. Martocci, Ed.
Johnson Controls Inc.
Pieter De Mil
Ghent University IBCN
W. Vermeylen
Arts Centre Vooruit
Nicolas Riou
Schneider Electric
September 14, 2009

Building Automation Routing Requirements in Low Power and Lossy Networks
draft-ietf-roll-building-routing-reqs-07

Status of this Memo

Copyright Notice

Abstract

The Routing Over Low power and Lossy network (ROLL) Working Group has been chartered to work on routing solutions for Low Power and Lossy networks (LLN) in various markets: Industrial, Commercial (Building), Home and Urban networks. Pursuant to this effort, this document defines the IPv6 routing requirements for building automation.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in (RFC2119).

Table of Contents

1. Terminology....4
2. Introduction....4
3. Overview of Building Automation Networks....5
3.1. Introduction....5
3.2. Building Systems Equipment....6
3.2.1. Sensors/Actuators....6
3.2.2. Area Controllers....7
3.2.3. Zone Controllers....7
3.3. Equipment Installation Methods....7
3.4. Device Density....8
3.4.1. HVAC Device Density....8
3.4.2. Fire Device Density....9
3.4.3. Lighting Device Density....9
3.4.4. Physical Security Device Density....9
4. Traffic Pattern....9
5. Building Automation Routing Requirements....11
5.1. Device and Network Commissioning....11
5.1.1. Zero-Configuration Installation....12
5.1.2. Local Testing....12
5.1.3. Device Replacement....12
5.2. Scalability....12
5.2.1. Network Domain....12
5.2.2. Peer-to-Peer Communication....13
5.3. Mobility....13
5.3.1. Mobile Device Requirements....13
5.4. Resource Constrained Devices....14
5.4.1. Limited memory footprint on host devices....14
5.4.2. Limited Processing Power for routers....14
5.4.3. Sleeping Devices....14
5.5. Addressing....15
5.6. Manageability....15

5.6.1. Diagnostics.....15
5.6.2. Route Tracking.....15
5.7. Route Selection.....16
5.7.1. Route Cost.....16
5.7.2. Route Adaptation.....16
5.7.3. Route Redundancy.....16
5.7.4. Route Discovery Time.....16
5.7.5. Route Preference.....16
5.7.6. Real-time Performance Measures.....17
5.7.7. Prioritized Routing.....17
5.8. Security Requirements.....17
5.8.1. Authentication.....17
5.8.2. Encryption.....18
5.8.3. Disparate Security Policies.....18
5.8.4. Routing Security Policies To Sleeping Devices.....18
6. IANA Considerations.....18
7. Acknowledgments.....19
8. References.....19
8.1. Normative References.....19
8.2. Informative References.....19
9. Appendix A: Additional Building Requirements.....19
9.1. Additional Commercial Product Requirements.....19
9.1.1. Wired and Wireless Implementations.....19
9.1.2. World-wide Applicability.....19
9.2. Additional Installation and Commissioning Requirements...20
9.2.1. Unavailability of an IP network.....20
9.3. Additional Network Requirements.....20
9.3.1. TCP/UDP.....20
9.3.2. Interference Mitigation.....20
9.3.3. Packet Reliability.....20
9.3.4. Merging Commissioned Islands.....20
9.3.5. Adjustable Routing Table Sizes.....21
9.3.6. Automatic Gain Control.....21
9.3.7. Device and Network Integrity.....21
9.4. Additional Performance Requirements.....21
9.4.1. Data Rate Performance.....21
9.4.2. Firmware Upgrades.....21
9.4.3. Route Persistence.....21

1. Terminology

For description of the terminology used in this specification, please see [I-D.ietf-roll-terminology].

2. Introduction

The Routing Over Low power and Lossy network (ROLL) Working Group has been chartered to work on routing solutions for Low Power and Lossy networks (LLN) in various markets: Industrial, Commercial (Building), Home and Urban networks. Pursuant to this effort, this document defines the IPv6 routing requirements for building automation.

Commercial buildings have been fitted with pneumatic and subsequently electronic communication routes connecting sensors to their controllers for over one hundred years. Recent economic and technical advances in wireless communication allow facilities to increasingly utilize a wireless solution in lieu of a wired solution; thereby reducing installation costs while maintaining highly reliant communication.

The cost benefits and ease of installation of wireless sensors allow customers to further instrument their facilities with additional sensors; providing tighter control while yielding increased energy savings.

Wireless solutions will be adapted from their existing wired counterparts in many of the building applications including, but not limited to Heating, Ventilation, and Air Conditioning (HVAC), Lighting, Physical Security, Fire, and Elevator systems. These devices will be developed to reduce installation costs; while increasing installation and retrofit flexibility, as well as increasing the sensing fidelity to improve efficiency and building service quality.

Sensing devices may be battery-less; battery or mains powered. Actuators and area controllers will be mains powered. Due to building code and/or device density (e.g. equipment room), it is envisioned that a mix of wired and wireless sensors and actuators will be deployed within a building.

Facility Management Systems (FMS) are deployed in a large set of vertical markets including universities; hospitals; government

facilities; Kindergarten through High School (K-12); pharmaceutical manufacturing facilities; and single-tenant or multi-tenant office buildings. These buildings range in size from 100K sqft structures (5 story office buildings), to 1M sqft skyscrapers (100 story skyscrapers) to complex government facilities such as the Pentagon. The described topology is meant to be the model to be used in all these types of environments, but clearly must be tailored to the building class, building tenant and vertical market being served.

Section 3 describes the necessary background to understand the context of building automation including the sensor, actuator, area controller and zone controller layers of the topology; typical device density; and installation practices.

Section 4 defines the traffic flow of the aforementioned sensors, actuators and controllers in commercial buildings.

Section 5 defines the full set of IPv6 routing requirements for commercial buildings.

Appendix A documents important commercial building requirements that are out of scope for routing yet will be essential to the final acceptance of the protocols used within the building.

Sections 3 and Appendix A are mainly included for educational purposes.

The expressed aim of this document is to provide the set of IPv6 routing requirements for LLNs in buildings as described in Section 5.

3. Overview of Building Automation Networks

3.1. Introduction

To understand the network systems requirements of a facility management system in a commercial building, this document uses a framework to describe the basic functions and composition of the system. An FMS is a hierarchical system of sensors, actuators, controllers and user interface devices that interoperate to provide a safe and comfortable environment while constraining energy costs.

An FMS may is divided functionally across alike, but different building subsystems such as heating, ventilation and air conditioning (HVAC); Fire; Security; Lighting; Shutters and Elevator control systems as denoted in Figure 1.

Much of the makeup of an FMS is optional and installed at the behest of the customer. Sensors and actuators have no standalone functionality. All other devices support partial or complete standalone functionality. These devices can optionally be tethered to form a more cohesive system. The customer requirements dictate the level of integration within the facility. This architecture provides excellent fault tolerance since each node is designed to operate in an independent mode if the higher layers are unavailable.

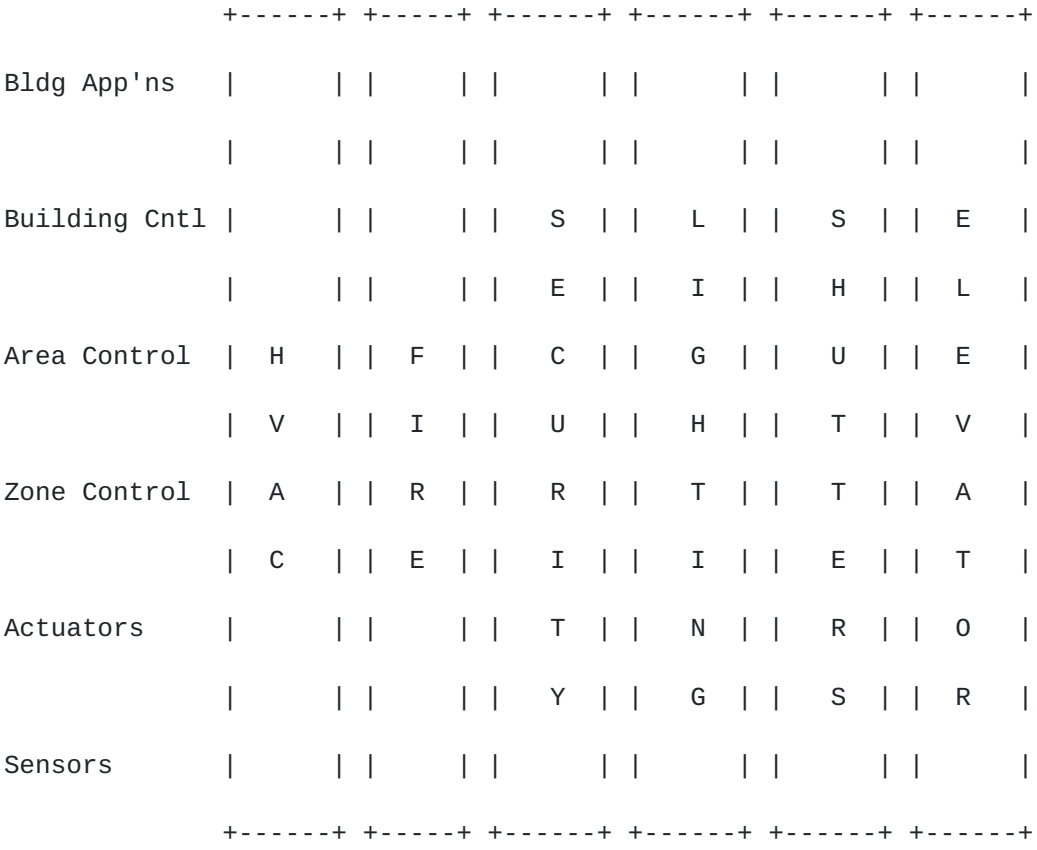

Figure 1: Building Systems and Devices

3.2. Building Systems Equipment

3.2.1. Sensors/Actuators

As Figure 1 indicates an FMS may be composed of many functional stacks or silos that are interoperably woven together via Building

Applications. Each silo has an array of sensors that monitor the environment and actuators that effect the environment as determined by the upper layers of the FMS topology. The sensors typically are at the edge of the network structure providing environmental data into the system. The actuators are the sensors' counterparts modifying the characteristics of the system based on the sensor data and the applications deployed.

3.2.2. Area Controllers

An area describes a small physical locale within a building, typically a room. HVAC (temperature and humidity) and Lighting (room lighting, shades, solar loads) vendors oft times deploy area controllers. Area controls are fed by sensor inputs that monitor the environmental conditions within the room. Common sensors found in many rooms that feed the area controllers include temperature, occupancy, lighting load, solar load and relative humidity. Sensors found in specialized rooms (such as chemistry labs) might include air flow, pressure, CO2 and CO particle sensors. Room actuation includes temperature setpoint, lights and blinds/curtains.

3.2.3. Zone Controllers

Zone Control supports a similar set of characteristics as the Area Control albeit to an extended space. A zone is normally a logical grouping or functional division of a commercial building. A zone may also coincidentally map to a physical locale such as a floor.

Zone Control may have direct sensor inputs (smoke detectors for fire), controller inputs (room controllers for air-handlers in HVAC) or both (door controllers and tamper sensors for security). Like area/room controllers, zone controllers are standalone devices that operate independently or may be attached to the larger network for more synergistic control.

3.3. Equipment Installation Methods

Commercial controllers have been traditionally deployed in a facility using serial media following the EIA-485 electrical standard operating nominally at 76800 baud with distances upward to 15000 feet. EIA-485 is a multi-drop media allowing upwards to 255 devices to be connected to a single trunk.

Wired FMS installation is a multifaceted procedure depending on the extent of the system and the software interoperability requirement.

However, at the sensor/actuator and controller level, the procedure is typically a two or three step process.

The installer arrives on-site during the construction of the building prior to drywall and ceiling installation. The installer allocates wall space installs the controller and sensor networks. The Building Controllers and Enterprise network are not normally installed until months later. The electrician completes the task by running a verification procedure that verifies proper wired or wireless continuity between the devices.

Months later, the higher order controllers are installed, programmed and commissioned together with the previously installed sensors, actuators and controllers. In most cases the IP network is still not in place. The Building Controllers are completely commissioned using a crossover cable or a temporary IP switch together with static IP addresses.

After occupancy, when the IP network is operational, the FMS often connects to the enterprise network. Dynamic IPs replace static IPs. VLANs oft time segregate the facility and IT systems. For multi-building multi-site facilities VPNs, NATs and firewalls are also introduced.

3.4. Device Density

Device density differs depending on the application and as dictated by the local building code requirements. The following sections detail typical installation densities for different applications.

3.4.1. HVAC Device Density

HVAC room applications typically have sensors/actuators and controllers spaced about 50ft apart. In most cases there is a 3:1 ratio of sensors/actuators to controllers. That is, for each room there is an installed temperature sensor, flow sensor and damper actuator for the associated room controller.

HVAC equipment room applications are quite different. An air handler system may have a single controller with upwards to 25 sensors and actuators within 50 ft of the air handler. A chiller or boiler is also controlled with a single equipment controller instrumented with 25 sensors and actuators. Each of these devices would be individually addressed since the devices are mandated or optional as defined by the specified HVAC application. Air handlers typically

serve one or two floors of the building. Chillers and boilers may be installed per floor, but many times service a wing, building or the entire complex via a central plant.

These numbers are typical. In special cases, such as clean rooms, operating rooms, pharmaceuticals and labs, the ratio of sensors to controllers can increase by a factor of three. Tenant installations such as malls would opt for packaged units where much of the sensing and actuation is integrated into the unit. Here a single device address would serve the entire unit.

3.4.2. Fire Device Density

Fire systems are much more uniformly installed with smoke detectors installed about every 50 feet. This is dictated by local building codes. Fire pull boxes are installed uniformly about every 150 feet. A fire controller will service a floor or wing. The fireman's fire panel will service the entire building and typically is installed in the atrium.

3.4.3. Lighting Device Density

Lighting is also very uniformly installed with ballasts installed approximately every 10 feet. A lighting panel typically serves 48 to 64 zones. Wired systems tether many lights together into a single zone. Wireless systems configure each fixture independently to increase flexibility and reduce installation costs.

3.4.4. Physical Security Device Density

Security systems are non-uniformly oriented with heavy density near doors and windows and lighter density in the building interior space. The recent influx of interior and perimeter camera systems is increasing the security footprint. These cameras are atypical endpoints requiring upwards to 1 megabit/second (Mbit/s) data rates per camera as contrasted by the few Kbits/s needed by most other FMS sensing equipment. Previously, camera systems had been deployed on proprietary wired high speed network. More recent implementations utilize wired or wireless IP cameras integrated to the enterprise LAN.

4. Traffic Pattern

The independent nature of the automation subsystems within a building plays heavy onto the network traffic patterns. Much of the real-time

sensor environmental data and actuator control stays within the local LLN environment; while alarming and other event data will percolate to higher layers.

Each sensor in the LLN unicasts P2P about 200 bytes of sensor data to its associated controller each minute and expects an application acknowledgement unicast returned from the destination. Each controller unicasts messages at a nominal rate of 6kB/min to peer or supervisory controllers. 30% of each node's packets are destined for other nodes within the LLN. 70% of each node's packets are destined for an aggregation device (MP2P)and routed off the LLN. These messages also require a unicast acknowledgement from the destination. The above values assume direct node-to-node communication; meshing and error retransmissions are not considered.

Multicasts (P2MP) to all nodes in the LLN occur for node and object discovery when the network is first commissioned. This data is typically a one-time bind that is henceforth persisted. Lighting systems will also readily use multicasting during normal operations to turn banks of lights 'on' and 'off' simultaneously.

FMS systems may be either polled or event based. Polled data systems will generate a uniform and constant packet load on the network. Polled architectures, however have proven not scalable. Today, most vendors have developed event based systems which pass data on event. These systems are highly scalable and generate low data on the network at quiescence. Unfortunately, the systems will generate a heavy load on startup since all initial sensor data must migrate to the controller level. They also will generate a temporary but heavy load during firmware upgrades. This latter load can normally be mitigated by performing these downloads during off-peak hours.

Devices will also need to reference peers periodically for sensor data or to coordinate operation across systems. Normally, though, data will migrate from the sensor level upwards through the local, area then supervisory level. Traffic bottlenecks will typically form at the funnel point from the area controllers to the supervisory controllers.

Initial system startup after a controlled outage or unexpected power failure puts tremendous stress on the network and on the routing algorithms. An FMS system is comprised of a myriad of control algorithms at the room, area, zone, and enterprise layers. When these control algorithms are at quiescence, the real-time data rate is small and the network will not saturate. An overall network traffic load of 6KBps is typical at quiescence. However, upon any power loss, the control loops and real-time data quickly atrophy. A

ten minute power outage may require many hours to regain building control. Traffic flow may increase ten-fold until the building control stabilizes.

Power disruptions are unexpected and in most cases will immediately impact lines-powered devices. Power disruptions however, are transparent to battery powered devices. These devices will continue to attempt to access the LLN during the outage. Battery powered devices designed to buffer data that has not been delivered will further stress the network operation when power returns.

Upon restart, lines-powered devices will naturally dither due to primary equipment delays or variance in the device self-tests. However, most lines-powered devices will be ready to access the LLN network within 10 seconds of power up. Empirical testing indicates that routes acquired during startup will tend to be very oblique since the available neighbor lists are incomplete. This demands an adaptive routing protocol to allow for route optimization as the network stabilizes.

5. Building Automation Routing Requirements

Following are the building automation routing requirements for networks used to integrate building sensor, actuator and control products. These requirements are written not presuming any preordained network topology, physical media (wired) or radio technology (wireless).

5.1. Device and Network Commissioning

Building control systems typically are installed and tested by electricians having little computer knowledge and no network knowledge whatsoever. These systems are often installed during the building construction phase before the drywall and ceilings are in place. For new construction projects, the building enterprise IP network is not in place during installation of the building control system. For retrofit applications, the installer will still operate independently from the IP network so as not to affect network operations during the installation phase.

In traditional wired systems correct operation of a light switch/ballast pair was as simple as flipping on the light switch. In wireless applications, the tradesperson has to assure the same operation, yet be sure the operation of the light switch is associated to the proper ballast.

System level commissioning will later be deployed using a more computer savvy person with access to a commissioning device (e.g. a laptop computer). The completely installed and commissioned enterprise IP network may or may not be in place at this time. Following are the installation routing requirements.

5.1.1. Zero-Configuration Installation

It MUST be possible to fully commission network devices without requiring any additional commissioning device (e.g. laptop).

5.1.2. Local Testing

During installation, the room sensors, actuators and controllers SHOULD be able to route packets amongst themselves without requiring any additional routing infrastructure or routing configuration.

5.1.3. Device Replacement

To eliminate the need to reconfigure the application upon replacing a failed device in the LLN; the replaced device must be able to advertise the old IP address of the failed device in addition to its new IP address. The routing protocols MUST support hosts and routers that advertise multiple IPv6 addresses.

5.2. Scalability

Building control systems are designed for facilities from 50000 sq. ft. to 1M+ sq. ft. The networks that support these systems must cost-effectively scale accordingly. In larger facilities installation may occur simultaneously on various wings or floors, yet the end system must seamlessly merge. Following are the scalability requirements.

5.2.1. Network Domain

The routing protocol MUST be able to support networks with at least 2000 nodes where 1000 nodes would act as routers and the other 1000 nodes would be hosts. Subnetworks (e.g. rooms, primary equipment) within the network must support upwards to 255 sensors and/or actuators.

5.2.2. Peer-to-Peer Communication

The data domain for commercial FMS systems may sprawl across a vast portion of the physical domain. For example, a chiller may reside in the facility's basement due to its size, yet the associated cooling towers will reside on the roof. The cold-water supply and return pipes serpentine through all the intervening floors. The feedback control loops for these systems require data from across the facility.

A network device MUST be able to communicate in a point-to-point manner with any other device on the network. Thus, the routing protocol MUST provide routes between arbitrary hosts within the appropriate administrative domain.

5.3. Mobility

Most devices are affixed to walls or installed on ceilings within buildings. Hence the mobility requirements for commercial buildings are few. However, in wireless environments location tracking of occupants and assets is gaining favor. Asset tracking applications, such as tracking capital equipment (e.g. wheel chairs) in medical facilities, require monitoring movement with granularity of a minute. This soft real-time performance requirement is reflected in the performance requirements below.

5.3.1. Mobile Device Requirements

To minimize network dynamics, mobile devices should not be allowed to act as forwarding devices (routers) for other devices in the LLN. Network configuration should allow devices to be configured as routers or hosts.

5.3.1.1. Device Mobility within the LLN

An LLN typically spans a single floor in a commercial building. Mobile devices may move within this LLN. For example, a wheel chair may be moved from one room on the floor to another room on the same floor.

A mobile LLN device that moves within the confines of the same LLN SHOULD reestablish end-to-end communication to a fixed device also in the LLN within 5 seconds after it ceases movement. The LLN network convergence time should be less than 10 seconds once the mobile device stops moving.

5.3.1.2. Device Mobility across LLNs

A mobile device may move across LLNs, such as a wheel chair being moved to a different floor.

A mobile device that moves outside its original LLN SHOULD reestablish end-to-end communication to a fixed device also in the new LLN within 10 seconds after the mobile device ceases movement. The network convergence time should be less than 20 seconds once the mobile device stops moving.

5.4. Resource Constrained Devices

Sensing and actuator device processing power and memory may be 4 orders of magnitude less (i.e. 10,000x) than many more traditional client devices on an IP network. The routing mechanisms must therefore be tailored to fit these resource constrained devices.

5.4.1. Limited memory footprint on host devices.

The software size requirement for non-routing devices (e.g. sleeping sensors and actuators) SHOULD be implementable in 8-bit devices with no more than 128KB of memory.

5.4.2. Limited Processing Power for routers

The software size requirements for routing devices (e.g. room controllers) SHOULD be implementable in 8-bit devices with no more than 256KB of flash memory.

5.4.3. Sleeping Devices

Sensing devices will, in some cases, utilize battery power or energy harvesting techniques for power and will operate mostly in a sleep mode to maintain power consumption within a modest budget. The routing protocol MUST take into account device characteristics such as power budget.

Typically, sensor battery life (2000mah) needs to extend for at least 5 years when the device is transmitting its data (200 octets) once per minute over a low power transceiver (25ma) and expecting a application acknowledgement. This requires a highly efficient routing protocol that minimizes hops and hence latency in end-to-end communication. The routing protocol MUST take into account node properties such as 'Low-powered node' which produce efficient low latency routes that minimize radio 'on' time for these devices.

Proxies with unconstrained power budgets often times are used to cache the inbound data for a sleeping device until the device awakens. In such cases, the routing protocol MUST discover the capability of a node to act as a proxy during route calculation; then deliver the packet to the assigned proxy for later delivery to the sleeping device upon its next awakened cycle.

5.5. Addressing

Facility Management systems require different communication schemes to solicit or post network information. Multicasts or anycasts need be used to resolve unresolved references within a device when the device first joins the network.

As with any network communication, multicasting should be minimized. This is especially a problem for small embedded devices with limited network bandwidth. Multicasts are typically used for network joins and application binding in embedded systems. Routing MUST support anycast, unicast, and multicast.

5.6. Manageability

In addition to the initial installation of the system, it is equally important for the ongoing maintenance of the system to be simple and inexpensive.

5.6.1. Diagnostics

To improve diagnostics, the routing protocol SHOULD be able to be placed in and out of 'verbose' mode. Verbose mode is a temporary debugging mode that provides additional communication information including at least total number of routed packets sent and received, number of routing failures (no route available), neighbor table members, and routing table entries.

5.6.2. Route Tracking

Route diagnostics SHOULD be supported providing information such as route quality; number of hops; available alternate active routes with associated costs. Route quality is the relative measure of 'goodness' of the selected source to destination route as compared to alternate routes. This composite value may be measured as a function of hop count, signal strength, available power, existing active routes or any other criteria deemed by ROLL as the route cost differentiator.

5.7. Route Selection

Route selection determines reliability and quality of the communication among the devices by optimizing routes over time and resolving any nuances developed at system startup when nodes are asynchronously adding themselves to the network.

5.7.1. Route Cost

The routing protocol MUST support a metric of route quality and optimize selection according to such metrics within constraints established for links along the routes. These metrics SHOULD reflect metrics such as signal strength, available bandwidth, hop count, energy availability and communication error rates.

5.7.2. Route Adaptation

Communication routes MUST adapt toward the chosen metric(s) (e.g. signal quality) optimality in time.

5.7.3. Route Redundancy

The routing layer SHOULD be configurable to allow secondary and tertiary routes to be established and used upon failure of the primary route.

5.7.4. Route Discovery Time

Mission critical commercial applications (e.g. Fire, Security) require reliable communication and guaranteed end-to-end delivery of all messages in a timely fashion. Application layer time-outs must be selected judiciously to cover anomalous conditions such as lost packets and/or route discoveries; yet not be set too large to over damp the network response. If route discovery occurs during packet transmission time (proactive routing), it SHOULD NOT add more than 120ms of latency to the packet delivery time.

5.7.5. Route Preference

The routing protocol SHOULD allow for the support of manually configured static preferred routes.

5.7.6. Real-time Performance Measures

A node transmitting a 'request with expected reply' to another node must send the message to the destination and receive the response in not more than 120 msec. This response time should be achievable with 5 or less hops in each direction. This requirement assumes network quiescence and a negligible turnaround time at the destination node.

5.7.7. Prioritized Routing

Network and application packet routing prioritization must be supported to assure that mission critical applications (e.g. Fire Detection) cannot be deferred while less critical applications access the network. The routing protocol MUST be able to provide routes with different characteristics, also referred to as "QoS" routing.

5.8. Security Requirements

Security policies, especially wireless encryption and device authentication needs to be considered, especially with concern to the impact on the processing capabilities and additional latency incurred on the sensors, actuators and controllers.

FMS systems are typically highly configurable in the field and hence the security policy is most often dictated by the type of building to which the FMS is being installed. Single tenant owner occupied office buildings installing lighting or HVAC control are candidates for implementing low or even no security on the LLN. Antithetically, military or pharmaceutical facilities require strong security policies. As noted in the installation procedures, security policies must be facile to allow for no security policy during the installation phase (prior to building occupancy), yet easily raise the security level network wide during the commissioning phase of the system.

5.8.1. Authentication

Authentication SHOULD be optional on the LLN. Authentication SHOULD be fully configurable on-site. Authentication policy and updates MUST be routable over-the-air. Authentication SHOULD occur upon joining or rejoining a network. However, once authenticated devices SHOULD NOT need to reauthenticate with any other devices in the LLN. Packets may need authentication at the source and destination nodes,

however, packets routed through intermediate hops should not need reauthentication at each hop.

5.8.2. Encryption

5.8.2.1. Encryption Types

Data encryption of packets MUST optionally be supported by use of either a network wide key and/or application key. The network key would apply to all devices in the LLN. The application key would apply to a subset of devices on the LLN.

The network key and application keys would be mutually exclusive. The routing protocol MUST allow routing a packet encrypted with an application key through forwarding devices that without requiring each node in the route to have the application key.

5.8.2.2. Packet Encryption

The encryption policy MUST support encryption of the payload only or the entire packet. Payload only encryption would eliminate the decryption/re-encryption overhead at every hop providing more real-time performance.

5.8.3. Disparate Security Policies

Due to the limited resources of an LLN, the security policy defined within the LLN MUST be able to differ from that of the rest of the IP network within the facility yet packets MUST still be able to route to or through the LLN from/to these networks.

5.8.4. Routing Security Policies To Sleeping Devices

The routing protocol MUST gracefully handle routing temporal security updates (e.g. dynamic keys) to sleeping devices on their 'awake' cycle to assure that sleeping devices can readily and efficiently access then network.

6. IANA Considerations

This document includes no request to IANA.

7. Acknowledgments

In addition to the authors, J. P. Vasseur, David Culler, Ted Humpal and Zach Shelby are gratefully acknowledged for their contributions to this document.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.ietf-roll-terminology]Vasseur, J., "Terminology in Low power And Lossy Networks", draft-ietf-roll-terminology-00 (work in progress), October 2008.

9. Appendix A: Additional Building Requirements

Appendix A contains additional building requirements that were deemed out of scope for ROLL, yet provided ancillary substance for the reader.

9.1. Additional Commercial Product Requirements

9.1.1. Wired and Wireless Implementations

Vendors will likely not develop a separate product line for both wired and wireless networks. Hence, the solutions set forth must support both wired and wireless implementations.

9.1.2. World-wide Applicability

Wireless devices must be supportable at the 2.4Ghz ISM band. Wireless devices should be supportable at the 900 and 868 ISM bands as well.

9.2. Additional Installation and Commissioning Requirements

9.2.1. Unavailability of an IP network

Product commissioning must be performed by an application engineer prior to the installation of the IP network (e.g. switches, routers, DHCP, DNS).

9.3. Additional Network Requirements

9.3.1. TCP/UDP

Connection based and connectionless services must be supported

9.3.2. Interference Mitigation

The network must automatically detect interference and seamlessly migrate the network hosts channel to improve communication. Channel changes and nodes response to the channel change must occur within 60 seconds.

9.3.3. Packet Reliability

In building automation, it is required for the network to meet the following minimum criteria :

< 1% MAC layer errors on all messages; After no more than three retries

< .1% Network layer errors on all messages;

After no more than three additional retries;

< 0.01% Application layer errors on all messages.

Therefore application layer messages will fail no more than once every 100,000 messages.

9.3.4. Merging Commissioned Islands

Subsystems are commissioned by various vendors at various times during building construction. These subnetworks must seamlessly

merge into networks and networks must seamlessly merge into internetworks since the end user wants a holistic view of the system.

9.3.5. Adjustable Routing Table Sizes

The routing protocol must allow constrained nodes to hold an abbreviated set of routes. That is, the protocol should not mandate that the node routing tables be exhaustive.

9.3.6. Automatic Gain Control

For wireless implementations, the device radios should incorporate automatic transmit power regulation to maximize packet transfer and minimize network interference regardless of network size or density.

9.3.7. Device and Network Integrity

Commercial Building devices must all be periodically scanned to assure that the device is viable and can communicate data and alarm information as needed. Router should maintain previous packet flow information temporally to minimize overall network overhead.

9.4. Additional Performance Requirements

9.4.1. Data Rate Performance

An effective data rate of 20kbits/s is the lowest acceptable operational data rate acceptable on the network.

9.4.2. Firmware Upgrades

To support high speed code downloads, routing should support transports that provide parallel downloads to targeted devices yet guarantee packet delivery. In cases where the spatial position of the devices requires multiple hops, the algorithm should recurse through the network until all targeted devices have been serviced. Devices receiving a download may cease normal operation, but upon completion of the download must automatically resume normal operation.

9.4.3. Route Persistence

To eliminate high network traffic in power-fail or brown-out conditions previously established routes should be remembered and

invoked prior to establishing new routes for those devices reentering the network.

Authors' Addresses

Jerry Martocci
Johnson Control
507 E. Michigan Street
Milwaukee, Wisconsin, 53202
USA
Phone: 414.524.4010
Email: jerald.p.martocci@jci.com

Nicolas Riou
Schneider Electric
Technopole 38TEC T3
37 quai Paul Louis Merlin
38050 Grenoble Cedex 9
France
Phone: +33 4 76 57 66 15
Email: nicolas.riou@fr.schneider-electric.com

Pieter De Mil
Ghent University - IBCN
G. Crommenlaan 8 bus 201
Ghent 9050
Belgium
Phone: +32-9331-4981
Fax: +32--9331--4899
Email: pieter.demil@intec.ugent.be

Wouter Vermeylen
Arts Centre Vooruit
???
Ghent 9000
Belgium

Phone: ???
Fax: ???
Email: wouter@vooruit.be