Networking Working Group
Internet-Draft
Intended status: Informational
Expires: April 29, 2009

J. Martocci, Ed.
Johnson Controls Inc.
Pieter De Mil
Ghent University IBCN
W. Vermeylen
Arts Centre Vooruit
Nicolas Riou
Schneider Electric
October 29, 2008

Building Automation Routing Requirements in Low Power and Lossy Networks

draft-ietf-roll-building-routing-reqs-01

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. Pursuant to this effort, this document defines the 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 RFC-2119.

Table of Contents

1. Terminology

For description of the terminology used in this specification, please see the Terminology ID referenced in Section 10.1.

2. Introduction

Commercial buildings have been fitted with pneumatic and subsequently electronic communication pathways 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. 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. Sensing devices may be battery or mains powered. Actuators and area controllers will be mains powered.

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.

The following sections describe the sensor, actuator, area controller and zone controller layers of the topology. (NOTE: The Building Controller and Enterprise layers of the FMS are excluded from this discussion since they typically deal in communication rates requiring WLAN communication technologies).

2.1. Facility Management System (FMS) Topology

2.1.1. 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 horizontally layered system of sensors, actuators, controllers and user interface devices. Additionally, an FMS may also be divided vertically across alike, but different building subsystems such as 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.

```
              +------+ +-----+ +------+ +------+ +------+ +------+

Bldg App'ns   |      | |     | |      | |      | |      | |      |

              |      | |     | |      | |      | |      | |      |

Building Cntl |      | |     | |  S   | |  L   | |  S   | |  E   |

              |      | |     | |  E   | |  I   | |  H   | |  L   |

Area Control  |  H   | |  F  | |  C   | |  G   | |  U   | |  E   |
```

```
              |  V   | |  I  | |   U  | |   H  | |   T  | |  V   |
Zone Control  |  A   | |  R  | |   R  | |   T  | |   T  | |  A   |
              |  C   | |  E  | |   I  | |   I  | |   E  | |  T   |
Actuators     |      | |     | |   T  | |   N  | |   R  | |  O   |
              |      | |     | |   Y  | |   G  | |   S  | |  R   |
Sensors       |      | |     | |      | |      | |      | |      |
              +------+ +-----+ +------+ +------+ +------+ +------+
```

Figure 1: Building Systems and Devices

2.1.2. 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 the leaves of the network tree structure providing environmental data into the system. The actuators are the sensors counterparts modifying the characteristics of the system based on the input sensor data and the applications deployed.

2.1.3. 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.

2.1.4. 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.

2.2. Installation Methods

2.2.1. Wired Communication Media

Commercial controllers are traditionally deployed in a facility using twisted pair serial media following the EIA-485 electrical standard operating nominally at 38400 to 76800 baud. This allows runs to 5000 ft without a repeater. With the maximum of three repeaters, a single communication trunk can serpentine 15000 ft. EIA-485 is a multi-drop media allowing upwards to 255 devices to be connected to a single trunk.

Most sensors and virtually all actuators currently used in commercial buildings are "dumb", non-communicating hardwired devices. However, sensor buses are beginning to be deployed by vendors which are used for smart sensors and point multiplexing. The Fire industry deploys addressable fire devices, which usually use some form of proprietary communication wiring driven by fire codes.

2.2.2. 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.

2.2.2.1. 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.

2.2.2.2. 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.

2.2.2.3. 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 typically tether many lights together into a single zone. Wireless systems configure each fixture independently to increase flexibility and reduce installation costs.

2.2.2.4. 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.

2.2.3. Installation Procedure

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.

Most FMS equipment is 24 VAC equipment that can be installed by a low-voltage electrician. He/she arrives on-site during the construction of the building prior to the sheet wall and ceiling installation. This allows him/her to allocate wall space, easily land the equipment and run the wired controller and sensor networks. The Building Controllers and Enterprise network are not normally installed until months later. The electrician completes his task by running a wire verification procedure that shows proper continuity between the devices and proper local operation of the devices.

Later in the installation cycle, 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 operable. The Building Controllers are completely commissioned using a crossover cable or a temporary IP switch together with static IP addresses.

Once the IP network is operational, the FMS may optionally be added to the enterprise network. The wireless installation process must follow the same work flow. The electrician will install the products as before and run local functional tests between the wireless devices to assure operation before leaving the job. The electrician does not carry a laptop so the commissioning must be built into the device operation.

3. Building Automation Applications

Vooruit is an arts centre in a restored monument which dates from 1913. This complex monument consists of over 350 different rooms including a meeting rooms, large public halls and theaters serving as many as 2500 guests. A number of use cases regarding Vooruit are described in the following text. The situations and needs described in these use cases can also be found in all automated large buildings, such as airports and hospitals.

3.1. Locking and Unlocking the Building

The member of the cleaning staff arrives first in the morning unlocking the building (or a part of it) from the control room. This means that several doors are unlocked; the alarms are switched off; the heating turns on; some lights switch on, etc. Similarly, the last person leaving the building has to lock the building. This will lock all the outer doors, turn the alarms on, switch off heating and lights, etc.

The ''building locked'' or ''building unlocked'' event needs to be delivered to a subset of all the sensors and actuators. It can be beneficial if those field devices form a group (e.g. ''all-sensors-actuators-interested-in-lock/unlock-events). Alternatively, the area and zone controllers could form a group where the arrival of such an event results in each area and zone controller initiating unicast or multicast within the LLN.

This use case is also described in the home automation, although the requirement about preventing the "popcorn effect" draft [I-D.ietf-roll-home-routing-reqs] can be relaxed a little bit in building automation. It would be nice if lights, roll-down shutters and other actuators in the same room or area with transparent walls execute the command around (not 'at') the same time (a tolerance of 200 ms is allowed).

3.2. Building Energy Conservation

A room that is not in use should not be heated, air conditioned or ventilated and the lighting should be turned off. In a building with a lot of rooms it can happen quite frequently that someone forgets to switch off the HVAC and lighting. This is a real waste of valuable energy. To prevent this from happening, the janitor can program the building according to the day's schedule. This way lighting and HVAC is turned on prior to the use of a room, and turned off afterwards. Using such a system Vooruit has realized a saving of 35% on the gas and electricity bills.

3.3. Inventory and Remote Diagnosis of Safety Equipment

Each month Vooruit is obliged to make an inventory of its safety equipment. This task takes two working days. Each fire extinguisher (100), fire blanket (10), fire-resistant door (120) and evacuation plan (80) must be checked for presence and proper operation. Also the battery and lamp of every safety lamp must be checked before each public event (safety laws). Automating this process using asset

tracking and low-power wireless technologies would heavily cut into working hours.

It is important that these messages are delivered very reliably and that the power consumption of the sensors/actuators attached to this safety equipment is kept at a very low level.

3.4. Life Cycle of Field Devices

Some field devices (e.g. smoke detectors) must be replaced periodically. Devices must be easily added and deleted from the network to support augmenting sensors/actuators during construction.

A secure mechanism is needed to remove the old device and install the new device. New devices need to be authenticated before they can participate in the routing process of the LLN. After the authentication, zero-configuration of the routing protocol is necessary.

3.5. Surveillance

Ingress and egress are real-time applications needing response times below 500msec. Each door must support local programming to restrict use on a per person basis with respect to time-of-day and person entering. While much of the application is localized at the door, tamper, door ajar, forced entry must be routed to one or more fixed or mobile user devices within 5 seconds.

3.6. Emergency

In case of an emergency it is very important that all the visitors be evacuated as quickly as possible. The fire and smoke detectors have to set off an alarm, and alert the mobile personnel on their user device (e.g. PDA). All emergency exits have to be instantly unlocked and the emergency lighting has to guide the visitors to these exits. The necessary sprinklers have to be activated and the electricity grid has to be monitored if it becomes necessary to shut down some parts of the building. Emergency services have to be notified instantly.

A wireless system could bring in some extra safety features. Locating fire fighters and guiding them through the building could be a life-saving application.

These life critical applications must take routing precedence over other network traffic. Commands entered during these emergencies must be properly authenticated by device, user, and command request.

3.7. Public Address

It should be possible to send audio and text messages to the visitors in the building. These messages can be very diverse, e.g. ASCII text boards displaying the name of the event in a room, audio announcements such as delays in the program, lost and found children, evacuation orders, etc.

The control network must be able to readily sense the audience in an area and deliver applicable message content.

4. Building Automation Routing Requirements

Following are the building automation routing requirements for a network used to integrate building sensor actuator and control products. These requirements have been limited to routing requirements only. These requirements are written not presuming any preordained network topology, physical media (wired) or radio technology (wireless). See Appendix A for additional requirements that have been deemed outside the scope of this document yet will pertain to the successful deployment of building automation systems.

4.1. Installation

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. There is never an IP network in place during this installation.

In retrofit applications, pulling wires from sensors to controllers can be costly and in some applications (e.g. museums) not feasible.

Local (ad hoc) testing of sensors and room controllers must be completed before the tradesperson can complete his/her work. 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 IP network may or may not be in place at this time. Following are the installation routing requirements.

4.1.1. Zero-Configuration installation

It MUST be possible to fully commission network devices without requiring any additional commissioning device (e.g. laptop). The device MAY support up to sixteen integrated switches to uniquely identify the device on the network.

4.1.2. Sleeping devices

Sensing devices must be able to utilize battery power or Energy Harvesting techniques for power. This presumes a need for devices that most often sleep. Routing must support these catatonic devices to assure that established routes do not utilize sleeping devices. It must also define routing rules when these devices need to access the network. Communication to these devices must be bidirectional. Routing must support proxies that can cache the inbound data for the sleeping device until the device awakens. Routing must understand the selected proxy for the sleeping device.

Batteries must be operational for at least 5 years when the sensing device is transmitting its data (e.g. 64 bytes) once per minute. This requires that sleeping devices must have minimal network access time when they awake and transmit onto the network.

4.1.3. Local Testing

The local sensors and requisite actuators and controllers must be testable within the locale (e.g. room) to assure communication connectivity and local operation without requiring other systemic devices. Routing must allow for temporary ad hoc paths to be established that are updated as the network physically and functionally expands.

4.1.4. Device Replacement

Replacement devices must be plug-and-play with no additional setup compared to what is normally required for a new device. Devices referencing data in the replaced device MUST not need to be reconfigured to the new device.

4.2. 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.

4.2.1. Network Domain

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

.

4.2.2. 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.

Network devices must be able to communicate in a peer-to-peer manner with all other devices on the network. Thus the routing protocol MUST provide routes to any other devices without being subject to a constrained path via a gating device.

4.3. 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.

4.3.1. Mobile Device Association

Mobile devices SHOULD be capable of unjoining (handing-off) from an old network joining onto a new network within 15 seconds.

4.4. 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.

4.4.1. Limited Processing Power Sensors/Actuators

The software stack requirements for sensors and actuators MUST be implementable in 8-bit devices with no more than 128KB of flash memory (including at least 32KB for the application code) and no more than 8KB of RAM (including at least 1KB RAM available for the application).

4.4.2. Limited Processing Power Controllers

The software stack requirements for room controllers SHOULD be implementable in 8-bit devices with no more than 256KB of flash memory (including at least 32KB for the application code) and no more than 8KB of RAM (including at least 1KB RAM available for the application)

4.5. Addressing

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

As with any network communication, broadcasting should be minimized. This is especially a problem for small embedded devices with limited network bandwidth. In many cases a global broadcast could be replaced with a multicast since the application knows the application domain. Broadcasts and multicasts are typically used for network joins and application binding in embedded systems.

4.5.1. Unicast/Multicast/Anycast

Routing MUST support anycast, unicast, multicast and broadcast services (or IPv6 equivalent).

4.6. Manageability

In addition to the initial installation of the system (see Section 4.1), it is equally important for the ongoing maintenance of the system to be simple and inexpensive.

4.6.1. Firmware Upgrades

To support high speed code downloads, routing MUST support parallel downloads to targeted devices yet guarantee packet delivery.

4.6.2. Diagnostics

To improve diagnostics, the network layer 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 packets sent, packets received, number of failed communication attempts, neighbor table and routing table entries.

4.6.3. Route Tracking

Route diagnostics SHOULD be supported providing information such as path quality; number of hops; available alternate active paths with associated costs.

4.7. Compatibility

The building automation industry adheres to application layer protocol standards to achieve vendor interoperability. These standards are BACnet and LON. It is estimated that fully 80% of the customer bid requests received world-wide will require compliance to one or both of these standards. ROLL routing will therefore need to dovetail to these application protocols to assure acceptance in the building automation industry. These protocols have been in place for over 10 years. Many sites will require backwards compatibility with the existing legacy devices.

4.7.1. IPv4 Compatibility

The routing protocol MUST define a communication scheme to assure compatibility of IPv4 and IPv6 devices.

4.7.2. Maximum Packet Size

Routing MUST support packet sizes to 1526 octets (to be backwards compatible with 802.3 subnetworks)

4.8. Route Selection

Route selection determines reliability and quality of the communication paths among the devices. Optimizing the routes over time resolve any nuances developed at system startup when nodes are asynchronously adding themselves to the network. Path adaptation will reduce latency if the path costs consider hop count as a cost attribute.

4.8.1. Path Cost

The routing protocol MUST support a range of metrics and optimize (constrained) path according to these metrics. These metrics SHOULD include signal strength, available bandwidth, hop count and communication error rates.

4.8.2. Path Adaptation

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

4.8.3. Route Redundancy

To reduce real-time latency, the network layer SHOULD be configurable to allow secondary and tertiary paths to be established and used upon failure of the primary path.

4.8.4. Route Discovery Time

Route discovery occurring during packet transmission MUST not exceed 120 msecs.

4.8.5. Route Preference

The route discovery mechanism SHOULD allow a source node (sensor) to dictate a configured destination node (controller) as a preferred routing path.

4.8.6. Path Symmetry

The network layer SHOULD support both asymmetric and symmetric routes as requested by the application layer. When the application layer selects asymmetry the network layer MAY elect to find either asymmetric or symmetric routes. When the application layer requests symmetric routes, then only symmetric routes MUST be utilized.

4.8.7. Path 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.

5. Traffic Pattern

The independent nature of the automation systems within a building plays heavy onto the network traffic patterns. Much of the real-time sensor data stays within the local environment. Alarming and other event data will percolate to higher layers.

Systemic data may be either polled or event based. Polled data systems will generate a uniform packet load on the network. This architecture has proven not scalable. Most vendors have developed event based systems which passes 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 the initial 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 need to reference peers occasionally for sensor data or to coordinate across systems. Normally, though, data will migrate from the sensor level upwards through the local, area then supervisory level. Bottlenecks will typically form at the funnel point from the area controllers to the supervisory controllers.

6. Open issues

Other items to be addressed in further revisions of this document include:

All known open items completed

7. Security Considerations

Security policies, especially wireless encryption and overall device authentication need to be considered. These issues are out of scope for the routing requirements, but could have an impact on the processing capabilities of the sensors and controllers.

As noted above, the 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.

8. IANA Considerations

This document includes no request to IANA.

9. Acknowledgments

J. P. Vasseur, Ted Humpal and Zach Shelby are gratefully acknowledged for their contributions to this document.

This document was prepared using 2-Word-v2.0.template.dot.

10. References

10.1. Normative References

draft-ietf-roll-home-routing-reqs-03

draft-ietf-roll-terminology-00.txt

10.2. Informative References

''RS-485 EIA Standard: Standard for Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multipoint Systems'', April 1983

''BACnet: A Data Communication Protocol for Building and Automation Control Networks'' ANSI/ASHRAE Standard 135-2004'', 2004

''LON: OPEN DATA COMMUNICATION IN BUILDING AUTOMATION, CONTROLS AND BUILDING MANAGEMENT - BUILDING NETWORK PROTOCOL - PART 1: PROTOCOL STACK'', 11/25/2005

11. Appendix A: Additional Building Requirements

Appendix A contains additional building requirements that were deemed out of scope for the routing document yet provided ancillary informational substance to the reader. The requirements will need to be addressed by ROLL or other WGs before adoption by the building automation industry will be considered.

11.1. Additional Commercial Product Requirements

11.1.1. Wired and Wireless Implementations

Solutions MUST support both wired and wireless implementations.

11.1.2. 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.

11.1.3. Support of the BACnet Building Protocol

Devices implementing the ROLL features MUST be able to support the BACnet protocol.

11.1.4. Support of the LON Building Protocol

Devices implementing the ROLL features MUST be able to support the LON protocol.

11.1.5. Energy Harvested Sensors

RFDs SHOULD target for operation using viable energy harvesting techniques such as ambient light, mechanical action, solar load, air pressure and differential temperature.

11.1.6. Communication Distance

A source device may be upwards to 1000 feet from its destination. Communication MUST be established between these devices without needing to install other intermediate 'communication only' devices such as repeaters

11.1.7. 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.

11.1.8. Cost

The total installed infrastructure cost including but not limited to the media, required infrastructure devices (amortized across the number of devices); labor to install and commission the network MUST not exceed $1.00/foot for wired implementations.

Wireless implementations (total installed cost) must cost no more than 80% of wired implementations.

11.2. Additional Installation and Commissioning Requirements

11.2.1. Device Setup Time

Network setup by the installer MUST take no longer than 20 seconds per device installed.

11.2.2. Unavailability of an IT network

Product commissioning MUST be performed by an application engineer prior to the installation of the IT network.

11.3. Additional Network Requirements

11.3.1. TCP/UDP

Connection based and connectionless services MUST be supported

11.3.2. Data Rate Performance

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

11.3.3. High Speed Downloads

Devices receiving a download MAY cease normal operation, but upon completion of the download MUST automatically resume normal operation.

11.3.4. Interference Mitigation

The network MUST automatically detect interference and migrate the network to a better 802.15.4 channel to improve communication. Channel changes and nodes response to the channel change MUST occur within 60 seconds.

11.3.5. 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.

11.3.6. Packet Reliability

Reliability MUST 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.

11.3.7. 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.

11.3.8. Adjustable System Table Sizes

Routing MUST support adjustable router table entry sizes on a per node basis to maximize limited RAM in the devices.

11.4. Prioritized Routing

Network and application routing prioritization is required to assure that mission critical applications (e.g. Fire Detection) cannot be deferred while less critical application access the network.

11.4.1. Packet Prioritization

Routers MUST support quality of service prioritization to assure timely response for critical FMS packets.

11.5. Constrained Devices

The network may be composed of a heterogeneous mix of full, battery and energy harvested devices. The routing protocol must support these constrained devices.

11.5.1. Proxying for Constrained Devices

Routing MUST support in-bound packet caches for low-power (battery and energy harvested) devices when these devices are not accessible on the network.

These devices MUST have a designated powered proxying device to which packets will be temporarily routed and cached until the constrained device accesses the network.

11.6. Reliability

11.6.1. Device 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. Network routers SHOULD maintain previous packet flow information temporally to minimize overall network overhead.

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

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.