Networking Working Group
Internet-Draft
Intended status: Informational
Expires: March 3, 2009

J. Martocci, Ed.
Johnson Controls Inc.
Pieter De Mil
Ghent University - IBCN
W. Vermeylen
Arts Centre Vooruit
September 3, 2008

Commercial Routing Requirements in Low Power and Lossy Networks
draft-martocci-roll-building-routing-reqs-00

Status of this Memo

Copyright Notice

Abstract

The ROLL Working Group was recently chartered by the IETF to define routing characteristics for low power embedded devices. ROLL would like to serve the Industrial, Commercial (Building), Home and Urban markets. Pursuant to this effort, this document defines the

functional requirements for installing integrated facility management systems in commercial facilities. The body of this document defines the routing requirements for commercial building application. Other commercial building requirements such as cost and installation requirements have been included in Appendix A for reference.

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 Error! Reference source not found..

Table of Contents

1. Terminology

Access Point: The access point is an infrastructure device that connects the low power and lossy network system to the Internet, possibly via a customer premises local area network (LAN).

Actuator: A field device that controls and/or modulates a flow of a gas or liquid; or controls electricity distribution.

ASHRAE: American Society of Heating, Refrigerating and Air-Conditioning Engineers

BAS: Building Automation System. This term is synonymous with Facility Management System (FMS).

BMS: Building Automation System. This term is synonymous

with Facility Management System (FMS).

Channel: Radio frequency sub-band used to transmit a modulated signal carrying packets.

Channel Hopping An algorithm by which field devices synchronously change channels during operation

Commissioning Tool: Any physical or logical device temporarily added to the network for the expressed purpose of setting up the network and device operational parameters.

Controller: A field device that can receive sensor input and automatically change the environment in the facility by manipulating digital or analog actuators.

Downstream: Data direction traveling from a Local Area Network (LAN) to a Personal Area Network (PAN) device.

Field Device: Physical devices placed in the plant's operating environment (both RF and environmental). Field devices include sensors and actuators as well as network routing devices and access points

Fire: The term used to describe building equipment used to monitor, control and evacuate an internal space in case of a fire situation. Equipment includes smoke detectors, pull boxes, sprinkler systems and evacuation control.

FFD: Full Function Device. An 802.15.4 device that can route messages across the mesh in addition to providing an end application. Most FFD are line powered since they must always be ready to forward messages.

FMS: Facility Management System. A global term applied across all the vertical designations within a building

including, HVAC, Fire, Security, Lighting and Elevator control.

HVAC: Heating, Ventilation and Air Conditioning. A term applied to the comfort level of an internal space.

IETF: Internet Engineering Task Force

Intrusion Protection: A term used to protect resources from external infiltration. Intrusion protection systems utilize door locks, window tampers and card readers.

LAN: Local Area Network.

PAN: Personal Area Network.
A geographically limited wireless network based on e.g. 802.15.4 or Z-Wave radio.

ROLL: Routing Over Low-power and Lossy networks

ROLL device: A ROLL network node with constrained CPU and memory resources; potentially constrained power resources.

Sensor: A PAN device that measures data and/or detects an event.

Upstream: Data direction traveling from a PAN to a LAN device.

LLN: Low power and Lossy networks (LLNs) are typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4, Bluetooth, Low Power WiFi

Lighting: The term used to describe building equipment used to monitor and control an internal or external lighted space. Equipment includes occupancy sensors, light switches and ballasts.

LLN: Low power and Lossy Network.

PAN: Personnel Area Network

RF: Radio Frequency

RFD: Reduced Function Device. An 802.15.4 device that can send messages on the network; receive messages from the network; but cannot route messages across the network. In most cases these devices are edge devices of the network.. RFDs may be line powered, but also can be battery powered since they play no role on the mesh.

ROLL: Routing over Low power and Lossy networks. This IETF working group will develop routing characteristics and rules for supporting LLNs utilizing 6LoWPAN.

Security: The term used to describe building equipment used to monitor and control occupant and equipment safety inside a building. Equipment includes window tamper switches, door access systems, infrared detection systems, and video cameras.

Sensors: A field device that monitors an environmental condition in a building and reports its findings to higher order devices for control and alarming operations.

Superframe: A collection of timeslots repeating at a constant rate.

TC: Trust Center. A logical device on the network that is trusted by the network members. The TC administers security policy.

Timeslot: A fixed time interval that may be used for the transmission or reception of a packet between two field devices. A timeslot used for communications is associated with a slotted-link

Upstream: Data direction travelling from the field device to the host application.

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 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; 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. Each section describes the basic functionality of the layer, its networking model, power requirements and a brief description of the communication requirements.

2.1. 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.

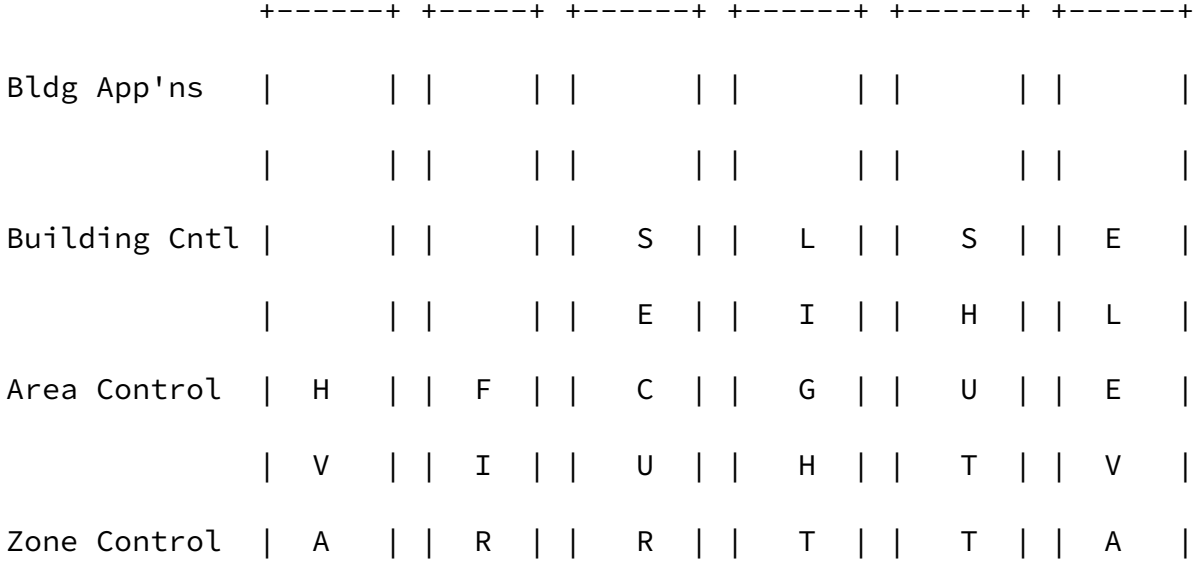

Figure 1 - Building Systems and Devices

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. As noted in Figure 1 the HVAC, Security and Lighting functions within a building address area or room level applications. 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.

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 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 and controllers spaced about 50ft apart. In most cases there is a 3:1 ratio of sensors to controllers. That is, for each room there is an installed temperature sensor, flow sensor and damper controller 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. 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 1mbps data rates per camera as contrasted by the few kbps needed by most other FMS sensing equipment. To date, camera systems have been deployed on a proprietary wired high speed network or on enterprise VLAN. Camera compression technology now supports full-frame video over wireless media.

2.2.2.5. 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. Wireless installation will necessarily need to keep the same work flow. The electrician will install the products as before and run continuity 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 366 different rooms including a concert hall, theater hall, several bars, etc. About 2000 activities take place at Vooruit on a yearly basis, some activities simultaneously with a total maximum of 3500 visitors. 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.

This use case is also useful in the home automation scenario, although the requirement about preventing the "popcorn effect" [REF HOME AUTOMATION] 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 areas with transparent walls execute the command around 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 366 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. Making the control of the building management system wireless (e.g. over a PDA) would be an advantage as you do not have to cross the complete building to the control room to change the temperature of a single room.

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-resisted 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 would heavily cut into working hours.

3.4. Life Cycle of Smoke Detectors

A smoke detector must be replaced periodically. A secure mechanism

is needed to remove the old device and install the new device. During construction work, the safety can be augmented by temporarily adding extra sensing and/or actuating devices.

This life cycle management use case is valid for each type of device we wish to add or to replace. What is the maximum of the time we allow for each task (adding a new device, removal of a device, replacement of a device)? The negative impact on the functionality of the network should be minimal.

3.5. Surveillance

To protect the building against burglary a guard must be able to monitor and control all entrances (open/close, latch moved) and lights (activated outside the opening hours). It should also be possible to view video streams from several security cameras either from the control room or on a PDA of an in-the-field security person. The arriving and exiting visitors also must be monitored from the control room to guarantee their security.

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 internal mobile telephone system and/or PDAs. 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 and 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. This is also the case for wireless camera surveillance which is monitored via PDA.

3.7. Public Address

It should be possible to send video, audio and text messages to the visitors in the building. These messages can be very diverse, e.g. commercials on televisions in the bar, ASCII text boards displaying the name of the event in a room, video screens with an outline of the upcoming events at Vooruit, audio announcements such as delays in the

program, lost and found children, evacuation orders, etc.

3.8. Positioning

Person localization / equipment theft: 2s - room accuracy required - high responsiveness required to cope with movement Interaction positioning: detect vicinity of two nodes (people or equipment): 1s - sub-room accuracy - high responsiveness required to cope with movement Equipment localization: 2-4s Or Asset Management - room accuracy required - medium responsiveness.

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 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 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. Computer-free installation

It MUST be possible to fully commission devices without requiring any additional commissioning device (e.g. laptop). The device MAY be completely configured for network operation by setting a bank of switches. The number of switches MUST not exceed 16 switches.

4.1.2. Fixed addressing

The device network address MUST be settable and henceforth fixed for the device without the need for other system devices such as DHCP servers.

4.1.3. Network Setup Time

Network setup MUST support device commissioning times of no more than 15 minutes per sensor/controller pair.

4.1.4. Battery Powered devices

Sensing devices must be able to utilize battery power yet still be viable devices on a ROLL network. Batteries must be operational for at least 5 years when the sensing device is transmitting its data (64 bytes) once per minute.

4.1.5. 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.

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

A network MUST operationally support at least 1000 routing and 1000 non-routing devices.

Subnetworks (e.g. rooms, primary equipment) within the network must support upwards to 255 sensors and/or actuators.

Subnetworks MUST seamlessly merge into networks. Networks MUST seamlessly merge into internetworks.

4.2.2. 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.

4.2.3. Automatic Gain Control

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

4.2.4. Peer-to-peer Communication

Network devices MUST be able to communicate in a peer-to-peer manner with all other devices on the network without being subject to intermediate bridge or gating devices.

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 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 algorithms must therefore be tailored to fit these resource constrained devices.

4.4.1. 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.

4.4.2. 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 application).

4.4.3. 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 application)

4.4.4. Parenting for Constrained Devices

The routing algorithms must support in-bound packet caches for sensor and actuator devices when these devices are not accessible on the network. The cached packets need to be delivered to its destination when the device is accessible on the network.

4.4.5. Adjustable System Table Sizes

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

4.5. 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.

4.5.1. QoS

Routers MUST support quality of service prioritization to assure timely response for critical FMS packets (e.g. Fire and Security events).

4.6. 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. Devices operating within a specified locale

such as a room will need to multicast to all devices within the room.

4.6.1. Unicast/Multicast/Anycast

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

4.6.2. Unique Addresses

Sensor/Actuator/Controller addressability MUST be unique site-wide. All addressable nodes MUST be accessible to all other nodes in the internetwork.

4.7. Manageability

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

4.7.1. Device Replacement

Replacement devices must be plug-n-play with no additional setup than what is normally required for a new device. No bound information from other nodes MUST need be reconfigured.

4.7.2. Firmware Upgrades

To support high speed code downloads, a mechanism MUST be defined to download firmware to devices in parallel yet support guaranteed delivery. Devices receiving a high speed download MAY cease normal operation, but upon completion of the download MUST automatically resume normal operation.

4.7.3. 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.

4.7.4. Trace Route

Network diagnostics such as PING and Trace Route SHOULD be supported with extensions in Trace Route describing wireless parameter information when applicable.

4.8. 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. The ROLL routing algorithms 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.

4.8.1. IPv4 Compatibility

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

4.8.2. Maximum Packet Size

Routing algorithms must support packet sizes to 1526 octets.

4.9. 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. Route adaptation

also reduces latency if the new route costs consider hop count as a cost attribute.

4.9.1. Path Cost

Path selection MUST be based on path quality, rather than signal strength only. Path quality includes signal strength, available bandwidth, hop count and communication error rates.

4.9.2. Path Adaptation

Communication paths MUST adapt toward signal quality optimality in time.

4.9.3. 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

4.9.4. Route Preference

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

4.9.5. 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. The default MUST be asymmetric routes.

4.9.6. Path Persistence

Devices SHOULD optionally persist communication paths across boots

4.10. Reliability

4.10.1. 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.

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:

Need to complete the Acknowledgement section below and develop Reference and Normative Reference sections.

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

TBD

10.1. Normative References

TBD

10.2. Informative References

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
?
?
?

Phone: ?
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

Intellectual Property Statement

this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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

11. APPENDIX A - Additional Building Requirements (Informative)

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 industrial will be considered.

11.1. Additional Commercial Product Requirements

11.1.1. Wired and Wireless Imlementations

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 Building Protocol - BACnet

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

11.1.4. Support of Building Protocol - LON

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.

11.2. 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 20kbps is the lowest acceptable operational data rate acceptable on the network.

11.3.3. 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.

11.3.4. 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.

11.3.5. 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% App?n layer errors on all messages.

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