Roll
Internet-Draft
Intended status: Informational
Expires: November 14, 2013

A. Brandt
Sigma Designs
E. Baccelli
INRIA
R. Cragie
Gridmerge
P. van der Stok
Consultant

May 13, 2013

Applicability Statement: The use of the RPL protocol set in Home Automation and Building Control
draft-brandt-roll-rpl-applicability-home-building-04

Abstract

The purpose of this document is to provide guidance in the selection and use of RPL protocols to implement the features required in building and home environments.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 14, 2013.

Copyright Notice

Table of Contents

1. Introduction

TODO: Adapt to new template

Home automation and building control application spaces share a substantial number of properties. The purpose of this document is to give guidance in the use of RPL-P2P to provide the features required by the requirements documents "Home Automation Routing Requirements in Low-Power and Lossy Networks" [RFC5826] and "Building Automation Routing Requirements in Low-Power and Lossy Networks" [RFC5867].

1.1. 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.

1.2. Overview of requirements

Applicable requirements are described in [RFC5826] and [RFC5867].

1.3. Out of scope requirements

The considered network diameter is limited to a max diameter of 10 hops and a typical diameter of 5 hops, which captures the most common cases in home automation and building control networks.

This document does not consider the applicability of RPL-related specifications for urban and industrial applications [RFC5548], [RFC5673], which may exhibit significantly larger network diameters.

2. Deployment Scenario

Networking in buildings is essential to satisfy the energy saving regulations. Comfort of buildings is adapted to the presence of individuals. When no one is present, energy consumption can be reduced. Cost is the main driving factor behind wireless networking in buildings. Especially for retrofit, wireless connectivity saves cabling costs.

A typical home automation network is less than 100 nodes. Large building deployments may span 10,000 nodes but to ensure uninterrupted service of light and air conditioning systems in individual zones of the building, nodes are organized in subnetworks. Each subnetwork in a building automation deployment typically contains contains tens to hundreds of nodes.

The main purpose of the network is to provide control over light and heating/cooling resources. User intervention may be enabled via wall controllers combined with movement, light and temperature sensors to enable automatic adjustment of window blinds, reduction of room temperature, etc.

People expect immediate and reliable responses to their presence or actions. A light not switching on after entry into a room leads to confusion and a profound dissatisfaction with the light product.

The surveillance of the correct functioning is at least as important. Devices communicate regularly their status and send alarm messages announcing a dysfunction of equipment or network.

In building control the infrastructure of the building management network can be shared with the security/access, the IP telephony, and the fire/alarm networks. This approach has a strong impact on the operation and cost of the network.

2.1. Network Topologies

The typical home automation network or building control subnetwork can consist of a wired and one or more wireless subnetworks. Especially in large buildings the wireless network is connected to an IP backbone network where all infrastructure services are located, such as DNS, automation servers, etc. The wireless subnetwork is a mesh network with a border router located at a convenient place in the home (building).

In a building control network there may be several redundant border routers to each subnetwork. Subnetworks often overlap geographically (and from a wireless perspective). Due to the two purposes of the network, (i) direct control and (ii) surveillance, there may exist two types of routing topologies in a given subnetwork (i) a tree-shaped collection of routes spanning from a central building controller via the border router, on to destination nodes in the subnetwork, and/or (ii) a flat, un-directed collection of intra-network routes between functionally related nodes in the subnetwork.

Nodes in Home and Building automation networks are typically inexpensive devices with very low memory capacity, such as individual

wall switches. Only a few nodes (such as multi-purpose remote controls) are more expensive devices, which can afford more memory capacity.

2.2. Traffic Characteristics

Traffic may enter the network from a central controller or it may originate from an intra-network node. The majority of traffic is light-weight point-to-point control style; e.g. Put-Ack or Get-Response. There are however exceptions. Bulk data transfer is used for firmware update and logging. Multicast is used for service discovery or to control groups of nodes, such as light fixtures. Firmware updates enter the network while logs leave the network. Often, there is a direct relation between a controlling sensor and the controlled equipment. The bulk of senders and receivers are separated by a distance that allows one-hop direct path communication. A graph of the communication will show several fully connected subsets of nodes. However, due to interference, multipath fading, reflection and other transmission mechanisms, the one-hop direct path may be temporally disconnected. For reliability purposes, it is therefore essential that alternative n-hop communication routes exist for quick error recovery. Looking over time periods of a day, the networks are very lightly loaded. However, bursts of traffic can be generated by the entry of several persons simultaneously, the occurrence of a defect, and other unforeseen events. Under those conditions, the timeliness must nevertheless be maintained. Therefore, measures are necessary to remove any unnecessary traffic. Short routes are preferred. Long multi-hop routes via the edge router, should be avoided whenever possible. Group communication is essential for lighting control. For example, once the presence of a person is detected in a given room, all involved lights in the room and no other lights should be dimmed, or switched on/off. Several rooms may be covered by the same wireless subnetwork. To reduce network load, it is advisable that messages to the lights in a room are not distributed further in the mesh than necessary on the basis of intended receivers.

2.2.1. Human user responsiveness

While air conditioning and other environmental-control applications may accept certain response delays, alarm and light control applications may be regarded as soft real-time systems. A slight delay is acceptable, but the perceived quality of service degrades significantly if response times exceed 250 msec. If the light does not turn on at short notice, a user will activate the controls again, causing a sequence of commands such as Light{on,off,on,off,..} or Volume{up,up,up,up,up,...}.

The reactive discovery features of RPL-P2P ensures that commands are normally delivered within the 250msec time window and when connectivity needs to be restored, it is typically completed within seconds. In most cases an alternative route will work. Thus, route rediscovery is not even necessary.

2.2.2. Source-sink (SS) communication paradigm

Source-sink (SS) traffic is a common traffic type in home and building networks. The traffic is generated by environmental sensors which push periodic readings to a central server. The readings may be used for pure logging, or more often, to adjust light, heating and ventilation. Alarm sensors also generate SS style traffic.

With regards to message latency, most SS transmissions can tolerate worst-case delays measured in tens of seconds. Alarm sensors, however, represent an exception.

2.2.3. Peer-to-peer (P2P) communication paradigm

Peer-to-peer (P2P) traffic is a common traffic type in home networks. Some building networks also rely on P2P traffic while others send all control traffic to a local controller box for advanced scene and group control; thus generating more SS and P2MP traffic.

P2P traffic is typically generated by remote controls and wall controllers which push control messages directly to light or heat sources. P2P traffic has a strong requirement for low latency since P2P traffic often carries application messages that are invoked by humans. As mentioned in Section 2.2.1 application messages should be delivered within less than a second - even when a route repair is needed before the message can be delivered. .

2.2.4. Peer-to-multipeer (P2MP) communication paradigm

Peer-to-multipeer (P2MP) traffic is common in home and building networks. Often, a wall switch in a living room responds to user activation by sending commands to a number of light sources simultaneously.

Individual wall switches are typically inexpensive devices with extremely low memory capacities. Multi-purpose remote controls for use in a home environment typically have more memory but such devices are asleep when there is no user activity. RPL-P2P reactive discovery allows a node to wake up and find new routes within a few seconds while memory constrained nodes only have to keep routes to relevant targets.

2.2.5. RPL applicability per communication paradigm

TODO: align with new template

Describe here when we use RPL, RPL-P2P and MPL based on sections on SS P2P, PMP, and N-cast.

2.3. Link layer applicability

This document applies to [IEEE802.15.4] and [G.9959] which are adapted to IPv6 by the adaption layers [RFC4944] and [I-D.lowpanz].

Due to the limited memory of a majority of devices (such as individual light dimmers) RPL-P2P MUST be used with source routing in non-storing mode. The abovementioned adaptation layers leverage on the compression capabilities of [RFC6554] and [RFC6282]. Header compression allows small IP packets to fit into a single layer 2 frame even when source routing is used. A network diameter limited to 5 hops helps achieving this.

Packet drops are often experienced in the targeted environments. ICMP, UDP and even TCP flows may benefit from link layer unicast acknowledgments and retransmissions. Link layer unicast acknowledgments MUST be enabled when [IEEE802.15.4] or [G.9959] is used with RPL-P2P.

3. Using RPL-P2P to meet requirements

RPL-P2P SHOULD be used in home and building networks, as point-to-point style traffic is substantial and route repair needs to be completed within seconds. RPL- P2P provides a reactive mechanism for quick, efficient and root- independent route discovery/repair. The use of RPL-P2P furthermore allows data traffic to avoid having to go through a central region around the root of the tree, and drastically reduces path length [SOFT11] [INTEROP12]. These characteristics are desirable in home and building automation networks because they substantially decrease unnecessary network congestion around the tree’s root.

4. RPL Profile for RPL-P2P

RPL-P2P MUST be used in home and building networks. Non-storing mode allows for constrained memory in repeaters when source routing is used. Reactive discovery allows for low application response times even when on-the-fly route repair is needed.

4.1. RPL Features

TODO: New subsection for prefix and address assignment

In one constrained deployment, the link layer master node handing out the logical network identifier and unique node identifiers may be a remote control which returns to sleep once new nodes have been added. There may be no global routable prefixes at all. Likewise, there may be no authoritative always-on root node since there is no border router to host this function.

In another constrained deployment, there may be battery powered sensors and wall controllers configured to contact other nodes in response to events and then return to sleep. Such nodes may never detect the announcement of new prefixes via multicast.

In each of the abovementioned constrained deployments, the link layer master node SHOULD assume the role as authoritative root node, transmitting singlecast RAs with a ULA prefix information option to nodes during the inclusion process to prepare the nodes for a later operational phase, where a border router is added.

A border router SHOULD be designed to be aware of sleeping nodes in order to support the distribution of updated global prefixes to such sleeping nodes.

One COULD implement gateway-centric tree-based routing and global prefix distribution as defined by [RFC6550]. This would however only work for always-on nodes.

4.1.1. RPL Instances

When operating P2P-RPL on a stand-alone basis, there is no authoritative root node maintaining a permanent RPL DODAG. A node MUST be able to join one RPL instance as an instance is created during each P2P-RPL route discovery operation. A node MAY be designed to join multiple RPL instances.

4.1.2. Non-Storing Mode

Non-storing mode MUST be used to cope with the extremely constrained memory of a majority of nodes in the network (such as individual light switches).

4.1.3. DAO Policy

TBD.

4.1.4. Path Metrics

TBD.

4.1.5. Objective Function

OF0 MUST be supported and is the RECOMMENDED OF to use. Other Objective Functions MAY be used as well.

4.1.6. DODAG Repair

Since RPL-P2P only creates DODAGs on a temporary basis during route repair, there is no need to repair DODAGs.

4.1.7. Multicast

Commercial light deployments may have a need for multicast beyond the link-local scope. RPL and P2P-RPL do not provide any means for this transmission mode natively.

Several mechanisms exist for achieving such functionality; [MPL] is RECOMMENDED for home and building deployments.

[TODO/TBD: text on MPL repeater density]

4.1.8. Security

In order to support low-cost devices and devices running on battery, the following RPL security parameter values SHOULD be used:

- T = ’0’: Do not use timestamp in the Counter Field.
- Algorithm = ’0’: Use CCM with AES-128
- KIM = ’10’: Use group key, Key Source present, Key Index present
- LVL = 0: Use MAC-32

4.1.9. P2P communications

RPL-P2P [RPL-P2P] MUST be used to accommodate P2P traffic, which is typically substantial in home and building automation networks.

4.2. Layer 2 features

For deployments based on

[IEEE802.15.4] and [G.9959], security MUST be applied at layer 2 using the mechanisms provided by the relevant standards. Residential light control can accept a lower security level than other contexts

(e.g. a nuclear research lab). Safety critical devices like electronic door locks SHOULD employ additional higher-layer security while light and heating devices may be sufficiently protected by a single network key. The border router MAY enforce access policies to limit access to the trusted LLN domain from the LAN.

4.2.1. Security functions provided by layer-2

TBD.

4.2.2. 6LowPAN options assumed

TBD.

4.2.3. MLE and other things

TBD.

4.3. Recommended Configuration Defaults and Ranges

TODO

5. Manageability Considerations

TODO

6. Security Considerations

TODO

6.1. Security Considerations during initial deployment

TODO: (This section explains how nodes get their initial trust anchors, initial network keys. It explains if this happens at the factory, in a deployment truck, if it is done in the field, perhaps like http://www.lix.polytechnique.fr/hipercom/SmartObjectSecurity/papers/CullenJennings.pdf)

6.2. Security Considerations during incremental deployment

Replacing a failed node means re-assigning the short address of the failed node to the new node added to the network. This again allows a new node replacing a failed node to obtain the same IPv6 addresses as per the lines of [IPHC].

As it is recommended to base security on a shared group key, it is possible to replace failed nodes. For specific details on how to replace failed nodes; refer to the actual link layer documentation.

TODO / TBD: Special concerns for adding a new node?

7. Other related protocols

Application transport protocols may be CoAP over UDP or equivalents. Typically, UDP is used for IP transport to keep down the application response time and bandwidth overhead.

Several features required by [RFC5826], [RFC5867] challenge the P2P paths provided by RPL. Appendix A reviews these challenges. In some cases, a node may need to spontaneously initiate the discovery of a path towards a desired destination that is neither the root of a DAG, nor a destination originating DAO signaling. Furthermore, P2P paths provided by RPL are not satisfactory in all cases because they involve too many intermediate nodes before reaching the destination.

RPL-P2P [RPL-P2P] provides the features requested by [RFC5826] and [RFC5867]. RPL-P2P uses a subset of the frame formats and features defined for RPL [RFC6550] but may be combined with RPL frame flows in advanced deployments.

8. IANA Considerations

9. Acknowledgements

This document reflects discussions and remarks from several individuals including (in alphabetical order): Michael Richardson, Mukul Goyal, Jerry Martocci, Charles Perkins, and Zach Shelby

10. References

11. References

11.1. Normative References

[RFC5826] , "Home Automation Routing Requirements in Low-Power and Lossy Networks", .

[RFC5867] , "Building Automation Routing Requirements in Low-Power and Lossy Networks", .

[RFC5673] , "Industrial Routing Requirements in Low-Power and Lossy Networks", .

[RFC5548] , "Routing Requirements for Urban Low-Power and Lossy Networks", .

[IEEE802.15.4]

, "IEEE 802.15.4 - Standard for Local and metropolitan area networks -- Part 15.4: Low-Rate Wireless Personal Area Networks", , <IEEE Standard 802.15.4>.

[RFC4944] , "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", .

[G.9959] , "ITU-T G.9959 Short range narrow-band digital radiocommunication transceivers - PHY and MAC layer specifications", , <ITU-T G.9959>.

[I-D.lowpanz] Brandt, A., "Transmission of IPv6 Packets over ITU-T G.9959 Networks", , <draft-brandt-6man-lowpanz>.

[RFC6282] Hui, J., Thubert, P., , , , "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC6282 , September 2011.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., Manral, V., , "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC6554 , March 2012.

[RFC6550] , "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", .

[RPL-P2P] Goyal, M., Baccelli, E., Phillip, M., Brandt, A., and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low Power and Lossy Networks", draft-ietf-roll-p2p-rpl , May 2012.

11.2. Informative References

[SOFT11] Baccelli, E., Phillip, M., and M. Goyal, "The P2P-RPL Routing Protocol for IPv6 Sensor Networks: Testbed Experiments", Proceedings of the Conference on Software Telecommunications and Computer Networks, Split, Croatia, September 2011., September 2011.

[INTEROP12] Baccelli, E., Phillip, M., Brandt, A., Valev , H., and J. Buron , "Report on P2P-RPL Interoperability Testing", RR-7864 INRIA Research Report RR-7864, Janurary 2012.

Appendix A. RPL shortcomings in home and building deployments

This document reflects discussions and remarks from several individuals including (in alphabetical order): Charles Perkins, Jerry Martocci, Michael Richardson, Mukul Goyal and Zach Shelby.

A.1. Risk of undesired long P2P routes

The DAG, being a tree structure is formed from a root. If nodes residing in different branches have a need for communicating internally, DAG mechanisms provided in RPL [RFC6550] will propagate traffic towards the root, potentially all the way to the root, and down along another branch. In a typical example two nodes could reach each other via just two router nodes but in unfortunate cases, RPL may send traffic three hops up and three hops down again. This leads to several undesired phenomena described in the following sections

A.1.1. Traffic concentration at the root

If many P2P data flows have to move up towards the root to get down again in another branch there is an increased risk of congestion the nearer to the root of the DAG the data flows. Due to the broadcast nature of RF systems any child node of the root is not just directing RF power downwards its sub-tree but just as much upwards towards the root; potentially jamming other MP2P traffic leaving the tree or preventing the root of the DAG from sending P2MP traffic into the DAG because the listen-before-talk link-layer protection kicks in.

A.1.2. Excessive battery consumption in source nodes

Battery-powered nodes originating P2P traffic depend on the route length. Long routes cause source nodes to stay awake for longer periods before returning to sleep. Thus, a longer route translates proportionally (more or less) into higher battery consumption.

A.2. Risk of delayed route repair

The RPL DAG mechanism uses DIO and DAO messages to monitor the health of the DAG. In rare occasions, changed radio conditions may render routes unusable just after a destination node has returned a DAO indicating that the destination is reachable. Given enough time, the next Trickle timer-controlled DIODAO update will eventually repair the broken routes. In a worst-case event this is however too late. In an apparently stable DAG, Trickle-timer dynamics may reduce the update rate to a few times every hour. If a user issues an actuator command, e.g. light on in the time interval between the last DAO message was issued the destination module and the time one of the parents sends the next DIO, the destination cannot be reached. Nothing in RPL kicks in to restore connectivity in a reactive

fashion. The consequence is a broken service in home and building applications.

A.2.1. Broken service

Experience from the telecom industry shows that if the voice delay exceeds 250ms users start getting confused, frustrated and/or annoyed. In the same way, if the light does not turn on within the same period of time, a home control user will activate the controls again, causing a sequence of commands such as Light{on,off,off,on,off,..} or Volume{up,up,up,up,up,...} Whether the outcome is nothing or some unintended response this is unacceptable. A controlling system must be able to restore connectivity to recover from the error situation. Waiting for an unknown period of time is not an option. While this issue was identified during the P2P analysis it applies just as well to application scenarios where an IP application outside the LLN controls actuators, lights, etc.

Authors' Addresses

Anders Brandt
Sigma Designs

Email: abr@sdesigns.dk

Emmanuel Baccelli
INRIA

Email: Emmanuel.Baccelli@inria.fr

Robert Cragie
Gridmerge

Email: robert.cragie@gridmerge.com

Peter van der Stok
Consultant

Email: consultancy@vanderstok.org