Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 4, 2016

M. Richardson
SSW

May 3, 2016

# ROLL Applicability Statement Template
# draft-ietf-roll-applicability-template-09

## Abstract

This document is a template applicability statement for the Routing over Low-power and Lossy Networks (ROLL) WG. This document is not for publication, but rather is to be used as a template.

## 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 4, 2016.

## Copyright Notice

Table of Contents

## 1. Introduction

This document describes a series of questions which should be answered. This document is intended to remain as a Internet Draft.

The idea is that current and future Applicability statements will use the table of contents provided. The goal is that all applicability statements will have to cover the listed items as a minimum.

### 1.1. Relationship to other documents

EDITORIAL: The following should appear in all applicability statements:

ROLL has specified a set of routing protocols for Lossy and Low-resource Networks (LLN) [RFC6550]. This applicability text describes a subset of these protocols and the conditions which make the subset the correct choice. The text recommends and motivates the accompanying parameter value ranges. Multiple applicability domains are recognized including: Building and Home, and Advanced Metering Infrastructure. The applicability domains distinguish themselves in the way they are operated, their performance requirements, and the most probable network structures. Each applicability statement identifies the distinguishing properties according to a common set of subjects described in as many sections.

A common set of security threats are described in [RFC7416]. The applicability statements complement the security threats document by describing preferred security settings and solutions within the applicability statement conditions. This applicability statements may recommend more light weight security solutions and specify the conditions under which these solutions are appropriate.

### 1.2. Requirements Language

(RFC2119 reference)

### 1.3. Terminology

A reference to draft-ietf-roll-terminology is appropriate. A reference to layer-2 specific terminology and/or inclusion of any terms that are normatively referenced is appropriate here.

### 1.4. Required Reading

References/Overview of requirements documents, both IETF and industry group. (two pages maximum. This text should be (very) technical, should be aimed at IETF *participants*, not industry group participants, and should explain this industries' specific issues)

### 1.5. Out of scope requirements

This should list other documents (if any) which deal with situations where things are not in scope for this document.

(For instance, the AMI document tries to cover both line-powered urban metering networks, and energy-constrained metering networks, and also tries to deal with rural requirements. This should be three or four documents, so this section should list the limits of what this document covers)

## 2. Deployment Scenario

### 2.1. Network Topologies

describe a single scenario, with possibly multiple topologies that a single utility would employ.

### 2.2. Traffic Characteristics

Explain what kind of traffic is being transmitted, where it is initiated, and what kinds of protocols (CoAP, multicast, HTTPS, etc.) are being used. Explain what assumptions are being made about authentication and authorization in those protocols.

#### 2.2.1. General

#### 2.2.2. Source-sink (SS) communication paradigm

#### 2.2.3. Publish-subscribe (PS, or pub/sub) communication paradigm

Explain what layer-2 technologies this statement applies to, and if there are options, they should be listed generally here, and specifically in section 4.2.



This should explain in general terms how RPL is going to be used in this network topology. If trees that are multiple layers deep are expected, then this should be described so that the fan out is understood. Some sample topologies (from simulations) should be explained, perhaps with images references from other publications.

This section should tell an *implementer* in a lab, having a simulation tool or a building/city/etc. to use as a testbed, how to construct an LLN of sufficient complexity (but not too much) to validate an implementation.



This section should list the various features of RPL plus other layers of the LLN, and how they will be used.

4.1.6. DODAG Repair

4.1.7. Multicast

4.1.8. Security

4.1.9. P2P communications

4.1.10. IPv6 address configuration

4.2. Layer-2 features

4.2.1. Specifics about layer-2

this section should detail the specific layer-2 network technology that this document applies to. A class of technologies is generally not acceptable.

4.2.2. Services provided at layer-2

4.2.3. 6LowPAN options assumed.

4.2.4. MLE and other things

4.3. Recommended Configuration Defaults and Ranges

4.3.1. Trickle Parameters

This section is intended to document the specific value (or ranges) appropriate for this kind of deployment. This includes trickle specific parameters such as those of RFC6550, section 8.3.1: Imin (DIOInternvalMin), Imax (DIOIntrevalDoublings), and k (DIORedundancyConstant). While it is not necessary to hard code these parameters into RPL nodes, as they are announced as part of the DIO message, it is important for researchers who are trying to validate the convergence properties of the resulting deployment to understand what values have been selected.

4.3.2. Other Parameters

There are additional values which are present in the DODAG Configuration option. The purpose of this section is to: a) document what values are configured, b) if a default value is used, if it is appropriate for this deployment.

These values include: MaxRankIncrease, MinHopRankIncrease, the Objective Code Point to use, Default Lifetime, Lifetime Units...

In addition, the kinds of metrics which will be used (RFC6551) needs to be specified. If Objective Function 0 (RFC6552) is used, then it specifies a number of values, but also needs definitions of the stretch_of_rank, and rank_factor.

If MRHOF (RFC6719) is used, then section 5 of this document requires selection of: MAX_LINK_METRIC, MAX_PATH_COST, PARENT_SWITCH_THRESHOLD, PARENT_SET_SIZE, and ALLOW_FLOATING_ROOT.

## 5. MPL Profile

This section should list the various features of MPL. In considering the parameters, a number of questions come up:

1) What are the maximum and minimum 1-hop MPL router neighbours of all the MPL routers?

2) what is the arrival rate of new packets that need repetition in a MPL router

3) Is there a deadline associated with the packets

4) What is the shortest number of hops of the longest path between sources and destinations

5) What are the values of the MAC: back-off values, retries, buffer size.

6) What is the background load of other non MPL applications.

7) arrival probability of 1-hop packets

As the corresponding design space is incredibly large, probably only a limited subset of the design space is viable.

Here is an example scenario:

- 5 neighbours
- once every 100 ms (rate at sources is once every 300-500 ms)
- yes, 200 ms
- 5 hops, with mostly 1 hop
- no buffer, retry 1, back-off 2
- absent

- o 100-80%

leading to k=3-5, Imin =30-70 ms, repeat = 2, Imax n/a.

It is crital operational boundary conditions together with appropriate MPL parameter values are published in this applicability statements. All applicability statements together may give a good hint which MPL parameters and boundary conditions to choose.

## 5.1. Recommended Configuration Defaults and Ranges

### 5.1.1. Trickle Parameters

#### 5.1.1.1. Imin

#### 5.1.1.2. Imax

### 5.1.2. Other Parameters

#### 5.1.2.1. Hot Limit

# 6. Manageability Considerations

# 7. Security Considerations

## 7.1. Security Considerations during initial deployment

(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)

## 7.2. Security Considerations during incremental deployment

(This section explains how that replaces a failed node takes on the dead nodes' identity, or not. How are nodes retired. How are nodes removed if they are compromised)

## 7.3. Security Considerations for P2P uses

(When layer-3 RPL security is used, P2P DODAGs are ephemeral, and may have different security needs.)

## 8. Other Related Protocols

## 9. IANA Considerations

## 10. Acknowledgements

This document was created from a number source applicatbility templates, including draft-ietf-roll-applicability-ami-06.txt, draft-phinney-rpl-industrial-applicability-00.txt.

The document has benefitted from advance review by the IETF Security Directorate.

A number of edits were contributed from Peter van der Stok, including the MPL considerations/calculations

## 11. References

### 11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <http://www.rfc-editor.org/info/rfc7416>.

### 11.2. Informative References

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, DOI 10.17487/RFC6206, March 2011, <http://www.rfc-editor.org/info/rfc6206>.

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

Author's Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/