

6LoWPAN Working Group  
Internet-Draft  
Expires: May 21, 2009

E. Kim  
ETRI  
D. Kaspar  
Simula Research Laboratory  
C. Gomez  
Tech. Univ. of Catalonia/i2CAT  
C. Bormann  
Universitaet Bremen TZI  
November 17, 2008

Problem Statement and Requirements for 6LoWPAN Routing  
draft-dokaspar-6lowpan-routreq-08

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on May 21, 2009.

Internet-Draft

6LoWPAN Routing Requirements

November 2008

## Abstract

This document provides the problem statement for 6LoWPAN routing. It also defines the requirements for 6LoWPAN routing considering IEEE 802.15.4 specificities and the low-power characteristics of the network and its devices.

## Table of Contents

<a href="#">1.</a>	Problem Statement . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Design Space . . . . .	<a href="#">6</a>
<a href="#">3.</a>	Scenario Considerations and Parameters for 6LoWPAN Routing . .	<a href="#">8</a>
<a href="#">4.</a>	6LoWPAN Routing Requirements . . . . .	<a href="#">13</a>
<a href="#">4.1.</a>	Support of 6LoWPAN Device Properties . . . . .	<a href="#">13</a>
<a href="#">4.2.</a>	Support of 6LoWPAN Link Properties . . . . .	<a href="#">15</a>
<a href="#">4.3.</a>	Support of 6LoWPAN Network Characteristics . . . . .	<a href="#">17</a>
<a href="#">4.4.</a>	Support of Security . . . . .	<a href="#">21</a>
<a href="#">4.5.</a>	Support of Mesh-under Forwarding . . . . .	<a href="#">22</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">23</a>
<a href="#">6.</a>	Acknowledgements . . . . .	<a href="#">24</a>
<a href="#">7.</a>	References . . . . .	<a href="#">25</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">25</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">25</a>
	Authors' Addresses . . . . .	<a href="#">27</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">28</a>

## 1. Problem Statement

In the context of this document, low-power wireless personal area networks (LoWPANs) are formed by devices that are compatible with the IEEE 802.15.4 standard [\[6\]](#). Most of the LoWPAN devices are distinguished by their low bandwidth, short range, scarce memory capacity, limited processing capability and other attributes of inexpensive hardware. In this document, the characteristics of nodes participating in LoWPANs are assumed to be those described in [RFC 4919](#) [\[3\]](#).

IEEE 802.15.4 networks support star and mesh topologies and consist of two different device types: reduced-function devices (RFDs) and full-function devices (FFDs). RFDs have the most limited capabilities and are intended to perform only simple and basic tasks, such as reporting sensed data. RFDs may only associate with a single FFD at a time, but FFDs may form arbitrary topologies and implement more advanced functions, such as multi-hop routing.

However, neither the IEEE 802.15.4 standard nor the 6LoWPAN format specification ("IPv6 over IEEE 802.15.4" [\[4\]](#)) define how mesh topologies could be obtained and maintained. Thus, the 6LoWPAN formation and multi-hop routing should be supported by higher layers, either the 6LoWPAN adaptation layer or the IP layer. A number of IP layer routing protocols have been developed in various IETF working groups. However, these existing routing protocols may not satisfy the requirements of mesh routing in LoWPANs, for the following reasons:

- o 6LoWPAN nodes have special types and roles, such as primary battery-operated RFDs, battery-operated and mains-powered FFDs, possibly various levels of RFDs and FFDs, mains-powered and high-performance gateways, data aggregators, etc. 6LoWPAN routing protocols should support multiple device types and roles.
- o The more stringent requirements that apply to 6LoWPANs, as opposed

to higher performance or non-battery-operated networks, may not suffice. 6LoWPAN nodes are characterized by small memory sizes, low processing power, and are running on very limited power supplied by primary non-rechargeable batteries (a few KBytes of RAM, a few dozens of KBytes of ROM/flash memory, and a few MHz of CPU is typical). A node's lifetime is usually defined by the lifetime of its battery.

- o Handling sleeping nodes is very critical in 6LoWPANs, more than in traditional ad-hoc networks. 6LoWPAN nodes might stay in sleep-mode for most of the time. Time synchronization is important for efficient forwarding of packets.

- o Routing in LoWPANs might possibly translate to a simpler problem than routing in higher-performance networks. 6LoWPANs might be either transit networks or stub networks. Under the assumption that 6LoWPANs are never transit networks (as implied by [4] and [8]), routing protocols may be drastically simplified. This document will primarily focus on stub networks. Based on the necessity, this document may be extended with 6LoWPAN network configurations that include transit networks.
- o Routing in 6LoWPANs might possibly translate to a harder problem than routing in higher-performance networks. Routing in 6LoWPANs requires power-optimization, stable operation in harsh environments, data-aware routing, etc. These requirements are not easily satisfiable all at once.

This creates new challenges on obtaining robust and reliable routing within LoWPANs.

The 6LoWPAN problem statement document ("6LoWPAN Problems and Goals" [3]) briefly mentions four requirements on routing protocols;

- (a) low overhead on data packets
- (b) low routing overhead
- (c) minimal memory and computation requirements
- (d) support for sleeping nodes considering battery saving

These four high-level requirements only describe the need for low overhead and power saving. But, based on the fundamental features of LoWPAN, more detailed routing requirements are presented in this document, which can lead to further analysis and protocol design.

Using the 6LoWPAN header format [4], there are two layers routing protocols can be defined at, commonly referred to as "mesh-under" and "route-over". The mesh-under approach supports routing under the IP link and is directly based on the link-layer IEEE 802.15.4 standard, therefore using (64-bit or 16-bit short) MAC addresses. On the other hand, the route-over approach relies on IP routing and therefore supports routing over possibly various types of interconnected links (see also Figure 1). Most statements in this document consider both the mesh-under and route-over cases.

[Note] The ROLL WG is now working on the protocol survey for Low power and Lossy Networks (LLNs), not specifically for 6LoWPAN. After that survey, it will be decided whether new solutions will be developed or not. This document is focused on 6LoWPAN specific requirements, in alignment with the ROLL WG.

Considering the problems above, detailed 6LoWPAN routing requirements must be defined. Application-specific features affect the design of 6LoWPAN routing requirements and the corresponding solutions. However, various applications can be profiled by similar technical characteristics, although the related detailed requirements might differ (e.g., a few dozens of nodes for home lighting system need appropriate scalability for the applications, while billions of nodes for a highway infrastructure system also needs appropriate scalability). This document states the routing requirements of 6LoWPAN applications in general, while trying to give examples for different cases of routing. This routing requirement document does not imply that a single routing solution may be the best one for all 6LoWPAN applications.

## 2. Design Space

Apart from a wide variety of routing algorithms possible for 6LoWPAN, the question remains as to whether routing should be performed mesh-under (in the adaptation layer defined by the 6lowpan format document [\[4\]](#)), or by the IP-layer using a route-over approach. The most significant consequence of mesh-under routing is that routing would be directly based on the IEEE 802.15.4 standard, therefore using (64-bit or 16-bit short) MAC addresses instead of IP addresses, and a LoWPAN would be seen as a single IP link. In case a route-over mechanism is to be applied to a LoWPAN it must also support 6LoWPAN's unique properties using global IPv6 addressing. One radio hop would be seen as a single IP link [\[8\]](#). In case a route-over mechanism is to be applied to a LoWPAN it must also support 6LoWPAN's unique properties of global IPv6 addressing.

Figure 1 shows the place of 6LoWPAN routing in the entire network stack.

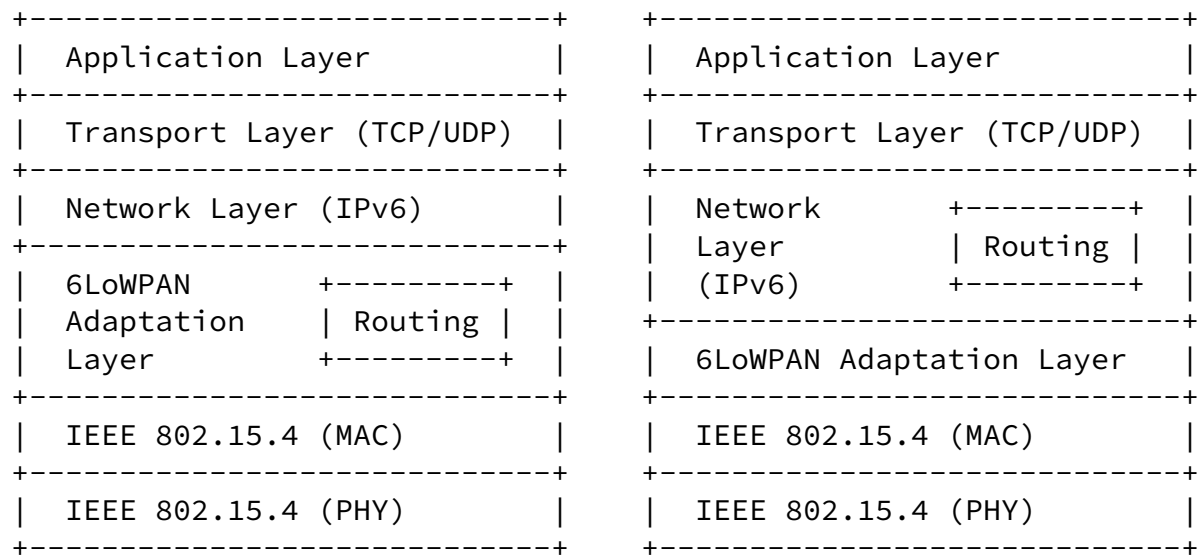


Figure 1: Mesh-under (left) and route-over routing (right)

In order to avoid packet fragmentation and the overhead for reassembly, routing packets should fit into a single IEEE 802.15.4 physical frame and application data should not be expanded to an extent that they no longer fit.

If a mesh-under routing protocol is built for operation in 6LoWPAN's adaptation layer, routing control packets are placed after the 6LoWPAN Dispatch, unless a new code type is assigned for mesh-under routing. Multiple routing protocols can be supported by the usage of different Dispatch bit sequences. In use cases where predefined layer two forwarding is appropriate, the mesh-header defined in RFC

4944 [4] is sufficient. When a route-over protocol is built in the IPv6 layer, the Dispatch value can be chosen as one of the Dispatch patterns for 6LoWPAN, compressed or uncompressed IPv6, followed by the IPv6 header.

As described in RFC 4944 [4], if a 6LoWPAN is formed, the Edge Router (ER) is the only IPv6 router in the LoWPAN (see Figure 2). A mesh-under routing mechanism MUST be provided to forward packets which

require multi-hop forwarding.

If route-over routing is used in the stub-network, not only the ER but also other intermediate nodes become LoWPAN router and set up IPv6 paths for multi-hop transmission.

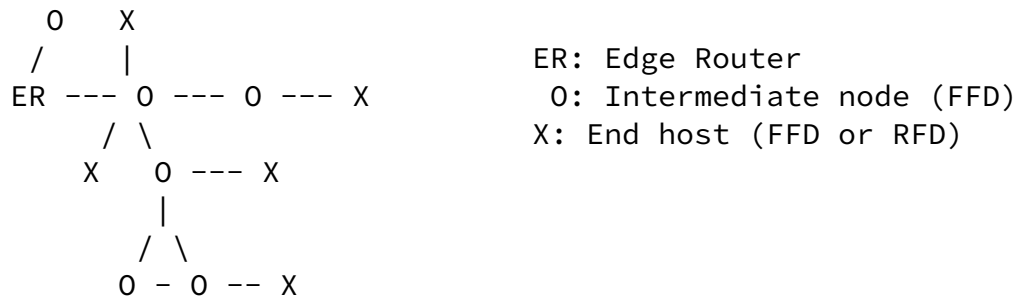


Figure 2: An example of a 6LoWPAN

If multiple 6LoPWANs are formed with globally unique IPv6 addresses in the 6LoWPANs, and node (a) of 6LoWPAN [A] wants to communicate with node (b) of 6LoWPAN [B], the normal IPv6 mechanisms can be employed. For mesh-under, one way is to configure the ER as the default router for the outgoing packets of the 6LoWPAN. This, of course, assumes the existence of a mesh-under routing protocol in order to reach the ER. For route-over, a default route to the ER could be inserted into the routing system.



IP-based low-power WPAN technology is still in its early stage of development, but the range of conceivable usage scenarios is tremendous. The numerous possible applications of sensor networks make it obvious that mesh topologies will be prevalent in LoWPAN environments and robust routing will be a necessity for expedient communication. Research efforts in the area of sensor networking have put forth a large variety of multi-hop routing algorithms [7]. Most related work focuses on optimizing routing for specific application scenarios, which can largely be categorized into several models of communication, including the following ones:

- o Flooding (in very small networks)
- o Data-aware routing (dissemination vs. gathering)
- o Event-driven vs. query-based routing
- o Geographic routing
- o Probabilistic routing
- o Hierarchical routing

Depending on the topology of a 6LoWPAN and the application(s) running over it, different types of routing may be used. However, this document abstracts from application-specific communication and describes general routing requirements valid for overall routing in 6LoWPANs.

The following parameters can be used to describe specific scenarios in which the candidate routing protocols could be evaluated.

a. Network Properties:

- \* Number of Devices, Density and Network Diameter:  
These parameters usually affect the routing state directly (e.g. the number of entries in a routing table or neighbor list). Especially in large and dense networks, policies must be applied for discarding "low-quality" and stale routing entries in order to prevent memory overflow.
- \* Connectivity:  
Due to external factors or programmed disconnections, a 6LoWPAN can be in several states of connectivity; anything in the range from "always connected" to "rarely connected". This poses great challenges to the dynamic discovery of routes

---

across a LoWPAN.

- \* **Dynamicity (including mobility):**  
Location changes can be induced by unpredictable external factors or by controlled motion, which may in turn cause route changes. Also, nodes may dynamically be introduced into a LoWPAN and removed from it later. The routing state and the volume of control messages may heavily dependent on the number of moving nodes in a LoWPAN and their speed.
- \* **Deployment:**  
In a LoWPAN, it is possible for nodes to be scattered randomly or to be deployed in an organized manner. The deployment can occur at once, or as an iterative process, which may also affect the routing state.
- \* **Spatial Distribution of Nodes and Gateways:**  
Network connectivity depends on the spatial distribution of the nodes, and on other factors like device number, density and transmission range. For instance, nodes can be placed on a grid, or can be randomly placed in an area (bidimensional Poisson distribution), etc. In addition, if the LoWPAN is connected to other networks through infrastructure nodes called gateways, the number and spatial distribution of gateways affects network congestion and available bandwidth, among others.
- \* **Traffic Patterns, Topology and Applications:**  
The design of a LoWPAN and the requirements on its application have a big impact on the network topology and the most efficient routing type to be used. For different traffic patterns (point-to-point, multipoint-to-point, point-to-multipoint) and network architectures, various routing mechanisms have been introduced, such as data-aware, event-driven, address-centric, and geographic routing.
- \* **Classes of Service:**  
For mission-critical applications, support of multiple classes of service may be required in resource-constrained LoWPANs and may require a certain degree of routing protocol overhead.
- \* **Security:**  
LoWPANs may carry sensitive information and require a high level of security support where the availability, integrity, and confidentiality of data are primordial. Secured messages cause overhead and affect the power consumption of LoWPAN

b. Node Parameters:

- \* Processing Speed and Memory Size:  
These basic parameters define the maximum size of the routing state. LoWPAN nodes may have different performance characteristics beyond the common RFD/FFD distinction.
- \* Power Consumption and Power Source:  
The number and topology of battery- and mains-powered nodes in a LoWPAN affect routing protocols in their selection of optimal paths for network lifetime maximization.
- \* Transmission Range:  
This parameter affects routing. For example, a high transmission range may cause a dense network, which in turn results in more direct neighbors of a node, higher connectivity and a larger routing state.
- \* Traffic Pattern: This parameter affects routing since high-loaded nodes (either because they are the source of packets to be transmitted or due to forwarding) may incur a greater contribution to delivery delays and may consume more energy than lightly loaded nodes. This applies to both data packets and routing control messages.

c. Link Parameters:

This section discusses link parameters that apply to IEEE 802.15.4 legacy mode (i.e. not making use of improved modulation schemes).

- \* Throughput:  
The maximum user data throughput of a bulk data transmission between a single sender and a single receiver through an unslotted IEEE 802.15.4 2.4 GHz channel in ideal conditions is as follows [[19](#)]:
  - + 16-bit MAC addresses, unreliable mode: 151.6 kbps
  - + 16-bit MAC addresses, reliable mode: 139.0 kbps

- + 64-bit MAC addresses, unreliable mode: 135.6 kbps
- + 64-bit MAC addresses, reliable mode: 124.4 kbps

In the case of 915 MHz band:

- + 16-bit MAC addresses, unreliable mode: 31.1 kbps

- + 16-bit MAC addresses, reliable mode: 28.6 kbps
- + 64-bit MAC addresses, unreliable mode: 27.8 kbps
- + 64-bit MAC addresses, reliable mode: 25.6 kbps

In the case of 868 MHz band:

- + 16-bit MAC addresses, unreliable mode: 15.5 kbps
- + 16-bit MAC addresses, reliable mode: 14.3 kbps
- + 64-bit MAC addresses, unreliable mode: 13.9 kbps
- + 64-bit MAC addresses, reliable mode: 12.8 kbps

\* Latency:

The range of latencies of a frame transmission between a single sender and a single receiver through an unslotted IEEE 802.15.4 2.4 GHz channel in ideal conditions are as shown next [\[19\]](#). For unreliable mode, the actual latency is provided. For reliable mode, the round-trip-time including transmission of a layer two acknowledgment is provided:

- + 16-bit MAC addresses, unreliable mode: [1.92 ms, 6.02 ms]
- + 16-bit MAC addresses, reliable mode: [2.46 ms, 6.56 ms]
- + 64-bit MAC addresses, unreliable mode: [2.75 ms, 6.02 ms]
- + 64-bit MAC addresses, reliable mode: [3.30 ms, 6.56 ms]

In the case of 915 MHz band:

- + 16-bit MAC addresses, unreliable mode: [5.85 ms, 29.35 ms]
- + 16-bit MAC addresses, reliable mode: [8.35 ms, 31.85 ms]
- + 64-bit MAC addresses, unreliable mode: [8.95 ms, 29.35 ms]
- + 64-bit MAC addresses, reliable mode: [11.45 ms, 31.85 ms]

In the case of 868 MHz band:

- + 16-bit MAC addresses, unreliable mode: [11.7 ms, 58.7 ms]
- + 16-bit MAC addresses, reliable mode: [16.7 ms, 63.7 ms]

- + 64-bit MAC addresses, unreliable mode: [17.9 ms, 58.7 ms]
- + 64-bit MAC addresses, reliable mode: [22.9 ms, 63.7 ms]

#### [4.](#) 6LoWPAN Routing Requirements

This section defines a list of requirements for 6LoWPAN routing. The most important design property unique to low-power networks is that 6LoWPANs have to support multiple device types and roles, for example:

- o primarily battery-operated host nodes (called "power-constrained nodes" in the following)
- o mains-powered host nodes (an example for what we call "power-affluent nodes")
- o power-affluent (but not necessarily mains-powered) high-performance gateway(s)
- o possibly various levels of nodes (data aggregators, relayers, etc.)

Due to these unique device types and roles 6LoWPANs need to consider the following two primary attributes:

- o Power conservation: some devices are mains-powered, but most are battery-operated and need to last several months to a few years with a single AA battery. Many devices are mains-powered most of the time, but still need to function for possibly extended periods from batteries (e.g. on a construction site before building power is switched on for the first time).
- o Low performance: tiny devices, small memory sizes, low-performance processors, low bandwidth, high loss rates, etc.

These fundamental attributes of LoWPANs affect the design of routing solutions, so that existing routing specifications should be simplified and modified to the smallest extent possible when there are appropriate solutions to adapt, otherwise, new solutions should be introduced in order to fit the low-power requirements of LoWPANs, meeting the requirements described in the following.

#### [4.1.](#) Support of 6LoWPAN Device Properties

The general objectives listed in this section should be followed by 6LoWPAN routing protocols. The importance of each requirement is dependent on what device type the protocol is running on and what the role of the device is. The following requirements are based on battery-powered LoWPAN devices.

[R01] 6LoWPAN routing protocols SHOULD allow to be implemented with

small code size and require low routing state to fit the typical 6LoWPAN node capacity (e.g., code size considering its typical flash memory size, and routing table less than 32 entries).

A LoWPAN routing protocol solution should consider the limited memory size typically starting at 4KB. RAM size of 6LoWPAN nodes often ranges between 2KB and 10KB, and program flash memory normally consists of 48KB to 128KB. (e.g., in the current market, MICAz has 128KB program flash, 4KB EEPROM, 512KB external flash ROM; TIP700CM has 48KB program flash, 10KB RAM, 1MB external flash ROM).

Due to these hardware restrictions, code length should be considered to fit within a small memory size; no more than 48KB to 128KB of flash memory including at least a few tens of KB of application code size. A routing protocol of low complexity helps to achieve the goal of reducing power consumption, improves robustness, requires lower routing state, is easier to analyze, and may be implicitly less prone to security attacks.

In addition, operation with low routing state (such as routing tables and neighbor lists) SHOULD be maintained since some typical memory sizes preclude to store state of a large number of nodes. For instance, industrial monitoring applications need to support at maximum 20 hops [15]. Small networks can be designed to support a smaller number of hops. It is highly dependent on the network architecture, but considering the 6LoWPAN device properties, there should be at least one mode of operation that can function with 32 forwarding entries or less.

[R02] 6LoWPAN routing protocols SHOULD cause minimal power consumption by the efficient use of control packets (e.g., minimize expensive multicast which cause broadcast to the entire LoWPAN) and by the efficient routing of data packets.

One way of battery lifetime optimization is by achieving a minimal control message overhead. Compared to functions such as in many devices, computational operations or taking sensor samples, radio communications is by far the dominant factor of power consumption [9]. Power consumption of transmission and/or reception depends linearly on the length of data units and on the frequency of transmission and reception of the data units [12].

The energy consumption of two example RF controllers for low-power nodes is shown in [10]. The TR1000 radio consumes 21mW when transmitting at 0.75mW, and 15mW on reception (with a receiver sensitivity of -85dBm). The CC1000 consumes 31.6mW when transmitting 0.75mW, and 20mW for receiving (with a receiver

sensitivity of -105dBm). The power continuation under the concept of an idealized power source is explained in [10]. Based on the energy of an idealized AA battery, the CC1000 can transmit for approximately 4 days straight or receive for 9 consecutive days.



Note that availability for reception consumes power as well.

One multicast packet causes reception of the entire nodes in the LoWPAN, while only the nodes in the path use the reception energy at unicast. Thus, 6LoWPAN routing protocol SHOULD minimize the control cost by the routing packets. Another document discusses control cost of routing protocols in low power and lossy networks [[18](#)].

#### [4.2](#). Support of 6LoWPAN Link Properties

6LoWPAN links have the characteristics of low bandwidth and possibly high loss rates. The routing requirements described in this section are derived from the link properties.

[R03] 6LoWPAN routing protocol control messages SHOULD not create fragmentation of physical layer (PHY) frames.

In order to save energy, routing overhead should be minimized to prevent fragmentation of frames on the physical layer (PHY). Therefore, 6LoWPAN routing should not cause packets to exceed the IEEE 802.15.4 frame size. This reduces the energy required for transmission, avoids unnecessary waste of bandwidth, and prevents the need for packet reassembly. As calculated in [RFC4944](#) [[4](#)], the maximum size of a 6LoWPAN frame, in order not to cause fragmentation on the PHY layer, is 81 octets. This may imply the use of semantic fragmentation and/or algorithms that can work on small increments of routing information.

[R04] The design of routing protocols for 6LoWPANs must consider the fact that packets are to be delivered with sufficient probability according to application requirements.

Requirements on successful end-to-end packet delivery ratio (where delivery may be bounded within certain latency) vary depending on applications. In industrial applications, some non-critical monitoring applications may tolerate successful delivery ratio of less than 90% with hours of latency; in some other cases, a delivery ratio of 99.9% is required [[15](#)]. In building automation applications, application layer errors must be below 0.01% [[17](#)].

Successful end-to-end delivery of packets in a IEEE 802.15.4 mesh depends on the quality of the path selected by the routing protocol and on the ability of the routing protocol to cope with

short-term and long-term quality variation. The metric of the routing protocol strongly influences performance of the routing protocol in terms of delivery ratio.

The quality of a given path depends on the individual qualities of the links (including the devices) that compose that path. IEEE 802.15.4 settings affect the quality perceived at upper layers. In particular, in IEEE 802.15.4 reliable mode, if an acknowledgment frame is not received after a given period, the originator retries frame transmission up to a maximum number of times. If an acknowledgment frame is still not received by the sender after performing the maximum number of transmission attempts, the MAC sub-layer assumes the transmission has failed and notifies the next higher layer of the failure. Note that excessive retransmission may be detrimental, see [RFC 3819](#) [5].

[R05] The design of routing protocols for 6LoWPANs must consider the end-to-end latency requirements of applications and IEEE 802.15.4 link latency characteristics.

Latency requirements may differ from a few hundreds milliseconds to minutes, depending on the type of application. Real-time building automation applications usually need response times below 500 ms between egress and ingress, while forced entry security alerts must be routed to one or more fixed or mobile user devices within 5 seconds [17]. Non-critical closed loop applications for industrial automation have latency requirements that can be as low as 100 ms but many control loops are tolerant of latencies above 1s [15]. In contrast to this, urban monitoring applications allow latencies smaller than the typical intervals used for reporting sensed information; for instance, in the order of seconds to minutes [16].

The range of latencies of a frame transmission between a single sender and a single receiver through an ideal unslotted IEEE 802.15.4 2.4 GHz channel is between 2.46ms and 6.02ms in 64 bit MAC address unreliable mode and 2.20 ms to 6.56ms in 64 bit address reliable mode. The range of latencies of 868 MHz band is from 11.7 ms to 63.7 ms, depending on the address type and reliable/unreliable mode used. Note that the latencies may be larger than that depending on channel load, MAC sublayer settings that regulate medium access procedure, reliable/unreliable mode choice and nodes sleeping.

Some routing protocols are aware of the hop count of a path. This parameter may be used as an input to select paths on an end-to-end latency basis if necessary.

Note that a tradeoff exists between [\[R05\]](#) and [\[R04\]](#).

[R06] 6LoWPAN routing protocols SHOULD be robust to dynamic loss caused by link failure or device unavailability either in short-term (e.g. due to RSSI variation, interference variation, noise and asynchrony) or in long-term (e.g. due to a depleted power source, hardware breakdown, operating system misbehavior, etc).

An important trait of 6LoWPAN devices is their unreliability due to limited system capabilities, and also because they might be closely coupled to the physical world with all its unpredictable variation. In harsh environments, LoWPANs easily suffer from link failure. Collision or link failure easily increases Send Queue/Receive Queue (SQ/RQ) and it can lead to queue overflow and packet losses.

For home applications, where users expect feedback after carrying out actions (such as handling a remote control while moving around), routing protocols must converge within 2 seconds if the destination node of the packet has moved and must converge within 0.5 seconds if only the sender has moved [\[14\]](#). The tolerance of the recovery time can vary depending on the application, however, the routing protocol must provide the detection of short-term unavailability and long-term disappearance. The routing protocol has to exploit network resources (e.g. path redundancy) to offer good network behavior despite of node failure.

[R07] 6LoWPAN routing protocols SHOULD be designed to correctly operate in the presence of link asymmetry.

Link asymmetry occurs when the probability of successful transmission between two nodes is significantly higher in one direction than in the other one. This phenomenon has been reported in a large number of experimental studies and it is expected that 6LoWPANs will exhibit link asymmetry.

#### [4.3.](#) Support of 6LoWPAN Network Characteristics

6LoWPANs can be deployed in different sizes and topologies, adhere to various models of mobility, tolerate various levels of interference,

etc. In any case, 6LoWPANs must maintain low energy consumption. The requirements described in the following subsection are derived from the network attributes of 6LoWPANs.

[R08] 6LoWPAN routing protocols SHOULD be reliable despite unresponsive nodes due to periodic hibernation.

Many nodes in 6LoWPAN environments might periodically hibernate (i.e. disable their transceiver activity) in order to save energy. Therefore, routing protocols must ensure robust packet delivery despite nodes frequently shutting off their radio transmission interface. Feedback from the lower IEEE 802.15.4 layer may be considered to enhance the power-awareness of 6LoWPAN routing protocols.

CC1000-based nodes must operate at a duty cycle of approximately 2% to survive for one year from idealized AA battery power source [10]. For home automation purposes, it is suggested that the devices have to maximize the sleep phase with a duty cycle lower than 1% [14], while in building automation applications, batteries must be operational for at least 5 years when the sensing devices are transmitting data (e.g. 64 bytes) once per minute [17].

Dependent on the application in use, packet rates differ from 1/sec to 1/day. Routing protocols need to know the cycle of the packet transmission and utilize the information to calculate routing paths.

[R09] The metric used by 6LoWPAN routing protocols MAY utilize a combination of the inputs provided by the MAC layer and other measures to obtain the optimal path considering energy balance and link quality.

In homes, buildings, or infrastructure, some nodes will be installed with mains power. Such power-installed nodes MUST be considered as a relay points for more roles in packet delivery. 6LoWPAN routing protocols MUST know the power constraints of the nodes.

Simple hop-count-only mechanisms may be inefficient in 6LoWPANs.

There is a Link Quality Indicator (LQI), Link Delivery Ratio (LDR), or/and RSSI from IEEE 802.15.4 that may be taken into account for better metrics. The metric to be used (and its goal) may depend on application and requirements.

The numbers in Figure 3 represent the Link Delivery Ratio (LDR) of each pair of nodes. There are studies that show a piecewise linear dependence between LQI and LDR [\[13\]](#).

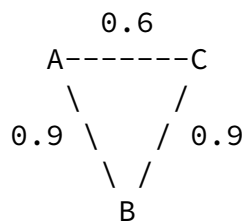


Figure 3: An example network

In this simple example, there are two options in routing from node A to node C, with the following features:

A. Path AC:

- +  $(1/0.6) = 1.67$  avg. transmissions needed for each packet
- + one-hop path
- + good in energy consumption and end-to-end latency of data packets, bad in delivery ratio (0.6)
- + bad in probability of route reconfigurations

B. Path ABC

- +  $2 \times (1/0.81) = 2.47$  avg. transmissions needed for each packet

- + two-hop path
- + bad in energy consumption and end-to-end latency of data packets, good in delivery ratio (0.81)

If energy consumption of the network must be minimized, path AC is the best (this path would be chosen based on a hop count metric). However, if the delivery ratio in that case is not sufficient, the best path is ABC (it would be chosen by an LQI based metric). Combinations of both metrics can be used.

The metric also affects the probability of route reconfiguration. Route reconfiguration, which may be triggered by packet losses, may require transmission of routing protocol messages. It is possible to use a metric aimed at selecting the path with low route reconfiguration rate by using LQI as an input to the metric. Such a path has good properties, including stability and low control message overhead.

[R10] 6LoWPAN routing protocols SHOULD be designed to achieve both scalability from a few nodes to millions of nodes and minimality in

terms of used system resources.

A 6LoWPAN may consist of just a couple of nodes (for instance in a body-area network), but may expand to much higher numbers of devices (e.g. monitoring of a city infrastructure or a highway). For home automation applications it is envisioned that the routing protocol must support 250 devices in the network [14], while routing protocols for metropolitan-scale sensor networks must be capable of clustering a large number of sensing nodes into regions containing on the order of  $10^2$  to  $10^4$  sensing nodes each [16]. It is therefore necessary that routing mechanisms are designed to be scalable for operation in various network sizes. However, due to a lack of memory size and computational power, 6LoWPAN routing might limit forwarding entries to a small number, such as at maximum 32 routing table entries.

[R11] The procedure of route repair and related control messages should not harm overall energy consumption from the routing protocols.

Local repair improves throughput and end-to-end latency, especially in large networks. Since routes are repaired quickly, fewer data packets are dropped, and a smaller number of routing protocol packet transmissions are needed since routes can be repaired without source initiated Route Discovery [11]. One important consideration here may be to avoid premature depletion, even in case that impairs other requirements.

[R12] 6LoWPAN routing protocols SHOULD allow for dynamically adaptive topologies and mobile nodes. When supporting dynamic topologies and mobile nodes, route maintenance should keep in mind the goal of a minimal routing state and routing protocol message overhead.

Building monitoring applications, for instance, require that the mobile devices SHOULD be capable of leaving (handing-off) from an old network joining onto a new network within 15 seconds [17]. More interactive applications such as used in home automation systems, where users are giving input and expect instant feedback, mobility requirements are also stricter and a convergence time below 0.5 seconds is commonly required [14]. In industrial environments, where mobile equipment such as cranes move around, the support of vehicular speeds of up to 35 km/ph are required to be supported by the routing protocol [15]. Currently, 6LoWPANs are not being used for such a fast mobility, but dynamic association and disassociation MUST be supported in 6LoWPAN.

There are several challenges that should be addressed by a 6LoWPAN routing protocol in order to create robust routing in dynamic

environments:

- \* Mobile nodes changing their location inside a 6LoWPAN:  
If the nodes' movement pattern is unknown, mobility cannot easily be detected or distinguished by the routing protocols. Mobile nodes can be treated as nodes that disappear and re-appear in another place. Movement pattern tracking increases complexity and can be avoided by handling moving nodes using reactive route updates.
- \* Movement of a 6LoWPAN with respect to other (inter)connected 6LoWPANs:

Within stub networks, more powerful gateway nodes need to be configured to handle moving 6LoWPANs.

- \* Nodes permanently joining or leaving the 6LoWPAN:  
In order to ease routing table updates and reduce error control messages, it would be helpful if nodes leaving the network inform their coordinator about their intention to disassociate.

[R13] 6LoWPAN routing protocol SHOULD support various traffic patterns; point-to-point, point-to-multipoint, and multipoint-to-point, while avoid excessive multicast traffic (broadcast in link layer) in 6LoWPAN.

6LoWPANs often have point-to-multipoint or multipoint-to-point traffic patterns. Many emerging applications include point-to-point communication as well. 6LoWPAN routing protocols should be designed with the consideration of forwarding packets from/to multiple sources/destinations. Current WG drafts in the ROLL working group explain that the workload or traffic pattern of use cases for 6LoWPANs tend to be highly structured, unlike the any-to-any data transfers that dominate typical client and server workloads. In many cases, exploiting such structure may simplify difficult problems arising from resource constraints or variation in connectivity.

#### [4.4.](#) Support of Security

The routing requirement described in this subsection allows secure transmission of routing messages. Solutions may take into account the specific features of IEEE 802.15.4 MAC layers.

[R14] 6LoWPAN protocols SHOULD support secure delivery of control messages. A minimal security level can be achieved by utilizing AES-based mechanism provided by IEEE 802.15.4.

Security threats within LoWPANs may be different from existing threat models in ad-hoc network environments. Neighbor Discovery in IEEE 802.15.4 links may be susceptible to threats as listed in [RFC3756](#) [2]. Bootstrapping may also impose additional threats. Security is also very important for designing robust routing



protocols, but it should not cause significant transmission overhead. While there are applications which require very high security, such as in traffic control, other applications are less easily harmed by wrong node behavior, such as a home entertainment system.

The IEEE 802.15.4 MAC provides an AES-based security mechanism. Routing protocols need to define how this mechanism can be used to obtain the intended security. Byte overhead of the mechanism, which depends on the security services selected, must be considered. In the worst case in terms of overhead, the mechanism consumes 21 bytes of MAC payload.

#### [4.5.](#) Support of Mesh-under Forwarding

Reception of an acknowledgement after a frame transmission may render unnecessary the transmission of explicit Hello messages, for example.

[R15] In case a routing protocol operates in 6LoWPAN's adaptation layer, then routing tables and neighbor lists MUST support 16-bit short and 64-bit extended addresses.

[R16] For neighbor discovery, 6LoWPAN devices SHOULD avoid sending "Hello" messages. Instead, link-layer mechanisms (such as acknowledgments) MAY be utilized to keep track of active neighbors.

Reception of an acknowledgement after a frame transmission may render unnecessary the transmission of explicit Hello messages, for example.

[R17] In case there are one or more nodes allocated to coordinator roles, the coordinators MAY take the role of keeping track of node association and de-association within the LoWPAN.

[R18] If the routing protocol functionality includes enabling IP multicast, then it may want to employ coordinator roles, if any, as relay points of group-targeting messages instead of using link-layer multicast (broadcast).

## 5. Security Considerations

Security issues are described in [Section 4.4](#). Security considerations of [RFC 4919](#) [3] and [RFC 4944](#) [4] apply as well. More security considerations will result from the 6LoWPAN security analysis work.

## [6.](#) Acknowledgements

The authors thank Myung-Ki Shin for giving the idea of writing this draft. The authors also thank to S. Chakrabarti who gave valuable comments for mesh-under requirements.

Internet-Draft

6LoWPAN Routing Requirements

November 2008

## [7.](#) References

### [7.1.](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [3] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", [RFC 4919](#), August 2007.
- [4] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", [RFC 4944](#), September 2007.
- [5] Karn, P., Bormann, C., Fairhurst, G., Grossman, D., Ludwig, R., Mahdavi, J., Montenegro, G., Touch, J., and L. Wood, "Advice for Internet Subnetwork Designers", [BCP 89](#), [RFC 3819](#), July 2004.
- [6] IEEE Computer Society, "IEEE Std. 802.15.4-2006 (as amended)", 2007.

### [7.2.](#) Informative References

- [7] Bulusu, N. and S. Jha, "Wireless Sensor Networks", July 2005.
- [8] Shelby, Z., Thubert, P., Hui, J., Chakrabarti, S., and E. Nordmark, "LoWPAN Neighbor Discovery Extensions, [draft-shelby-6lowpan-nd-00](#) (work in progress)", October 2008.

- [9] Pister, K. and B. Boser, "Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes".
- [10] Hill, J., "System Architecture for Wireless Sensor Networks".
- [11] Lee, S., Belding-Royer, E., and C. Perkins, "Scalability Study of the Ad Hoc On-Demand Distance-Vector Routing Protocol", March 2003.
- [12] Shih, E., "Physical Layer Driven Protocols and Algorithm Design for Energy-Efficient Wireless Sensor Networks", July 2001.
- [13] Chen, B., Muniswamy-Reddy, K., and M. Welsh, "Ad-Hoc Multicast

Routing on Resource-Limited Sensor Nodes", 2006.

- [14] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirement in Low Power and Lossy Networks, [draft-ietf-roll-home-routing-reqs-04](#) (work in progress)", October 2008.
- [15] Pister, K., Thubert, P., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low Power and Lossy Networks, [draft-ietf-roll-indus-routing-reqs-01](#) (work in progress)", July 2008.
- [16] Dohler, M., Watteyne, T., Winter, T., Barthel, D., and C. Jacquenet, "Urban WSNs Routing Requirements in Low Power and Lossy Networks, [draft-ietf-roll-urban-routing-reqs-02](#) (work in progress)", October 2008.
- [17] Martocci, J., De Mil, P., Vermeylen, W., and N. Riou, "Building Automation Routing Requirements in Low Power and Lossy Networks, [draft-ietf-roll-building-routing-reqs-01](#) (work in progress)".
- [18] Levis, P., Tavakoli, A., and S. Dawson-Haggerty, "Overview of Existing Routing Protocols for Low Power and Lossy Networks , [draft-ietf-roll-protocols-survey-02](#) (work in progress)".
- [19] Latre, M., De Mil, P., Moerman, I., Dhoedt, B., and P. Demeester, "Throughput and Delay Analysis of Unslotted IEEE

#### Authors' Addresses

Eunsook Eunah Kim  
ETRI  
161 Gajeong-dong  
Yuseong-gu  
Daejeon 305-700  
Korea

Phone: +82-42-860-6124  
Email: eunah.ietf@gmail.com

Dominik Kaspar  
Simula Research Laboratory  
Martin Linges v 17  
Snaroya 1367  
Norway

Phone: +47-6782-8223  
Email: dokaspar.ietf@gmail.com

Carles Gomez  
Tech. Univ. of Catalonia/i2CAT  
Escola Politecnica Superior de Castelldefels  
Avda. del Canal Olimpic, 15  
Castelldefels 08860  
Spain

Phone: +34-93-413-7206  
Email: carlesgo@entel.upc.edu

Carsten Bormann  
Universitaet Bremen TZI  
Postfach 330440  
Bremen D-28359  
Germany

Phone: +49-421-218-63921  
Fax: +49-421-218-7000  
Email: cabo@tzi.org

#### Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).