

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 1, 2011

L. Toutain  
N. Montavont  
Institut TELECOM ; TELECOM  
Bretagne  
D. Barthel  
France Telecom R&D  
June 30, 2010

Neighbor Discovery Suppression  
draft-toutain-6lowpan-ra-suppression-01.txt

## Abstract

We propose to strongly reduce the usage of Neighbor Discovery in WSN by ignoring the global IPv6 prefix inside the WSN. The IPv6 prefix will be added (resp. removed) by the Border Router during the header decompression (resp. compression). This proposal has three main advantages: (i) reduce the number of exchanges inside the WSN, (ii) reduce the time needed by a sensor node to join the WSN (this is important when sensors are moving inside the WSN) and finally (iii) simplify multi-homing management. This document also studies the impact of this proposal on different architectures (star, mesh, route over) with LOWPAN\_IPHC Encoding Format.

## 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 January 1, 2011.

## Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal

Internet-Draft

RA Suppression

June 2010

## Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Existing protocols for LoWPAN . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	Neighbor Discovery in LoWPAN . . . . .	<a href="#">3</a>
<a href="#">2.2.</a>	Header compression . . . . .	<a href="#">5</a>
<a href="#">3.</a>	Suppression of solicited RA . . . . .	<a href="#">5</a>
<a href="#">3.1.</a>	Star Topology Packet Format . . . . .	<a href="#">6</a>
<a href="#">3.2.</a>	Mesh Topology Packet Format . . . . .	<a href="#">7</a>
<a href="#">3.3.</a>	Routed Topology Packet Format . . . . .	<a href="#">9</a>
<a href="#">4.</a>	ULP checksum adaptation . . . . .	<a href="#">9</a>
<a href="#">5.</a>	Conclusion . . . . .	<a href="#">10</a>
<a href="#">6.</a>	Acknowledgement . . . . .	<a href="#">10</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">8.</a>	Normative References . . . . .	<a href="#">10</a>
	Authors' Addresses . . . . .	<a href="#">11</a>

## 1. Introduction

6LoWPAN WG aims to adapt IPv6 and associated protocols to sensor network environment. This leads to two categories of standards: those to transport IPv6 packets on LoWPAN links and those used to adapt associated protocols such as Neighbor Discovery Protocol (NDP) to 6LoWPAN environment. In this document, we propose a new approach to the address management, compatible with the ones already defined and that can be used to avoid running NDP on LoWPAN. We discuss the validity of this proposal in different topologies cases (star, mesh under and route over) and the implication of its use on the 6LoWPAN header compression mechanisms.

## 2. Existing protocols for LoWPAN

### 2.1. Neighbor Discovery in LoWPAN

While some solutions have been proposed to optimize the encapsulation of NDP messages, the load imposed by this protocol is still almost equivalent in WSN and in Ethernet-based networks.

[[I-D.ietf-6lowpan-nd](#)] lists the differences between NDP defines in [[RFC4861](#)] and the adaptation for LoWPAN.

In the past, some proposals have suggested limiting the use of broadcast because of energy constraint, by maintaining stateful information in the LoWPAN Border Router (LBR).

[[I-D.chakrabarti-6lowpan-ipv6-nd](#)] proposes some optimizations to minimize the number of messages generated by NDP and to limit the use of broadcasts in the network. NDP functionalities are concentrated in the LBR instead of being distributed in the network. Duplicate Address Detection (DAD) and Neighbor Solicitation (NS) are performed with point-to-point requests from the sensors to the LBR rather than with multicast packets spanning the whole WSN. Furthermore, nodes intercept initial multicast Router Solicitation (RS) messages and forward them directly to the PC instead of broadcasting them to the

whole network.

[I-D.thubert-6lowpan-backbone-router] extends the above proposal by allowing multiple routers in a WSN to share the same prefix. LBR only have a partial view of the addresses allocated on the WSN. They use a transit link to proxy NS for DAD and address resolution procedures. In addition, backbone routers have an L2 anycast address allowing sensors to easily contact the closest router.

These solutions have evolved to a consensus among 6LoWPAN WG, described in [I-D.ietf-6lowpan-nd] which releases some constraints imposed by [RFC4861]. DAD is no more mandatory for IID built on

well-known unique values (such as EUI-64 or DHCP allocated addresses). If DAD is needed, the query is sent to the LBR which will check the uniqueness of the address. Periodic Router Advertisements are disabled and nodes have to explicitly request RA through RS. Some options are added in RA to maintain a mapping between well known prefixes and a context value.

One major question is what is the need for source prefixes inside the WSN. In fact, prefix allocation requires a protocol which is difficult to deploy in a WSN environment and, once allocated, prefixes may require a more complex management of the network. For instance, none of these proposals touches on multi-homing or interaction with routing protocol such as RPL. Figure 1 shows a very simple network with two LBR announcing different prefixes in the LoWPAN.

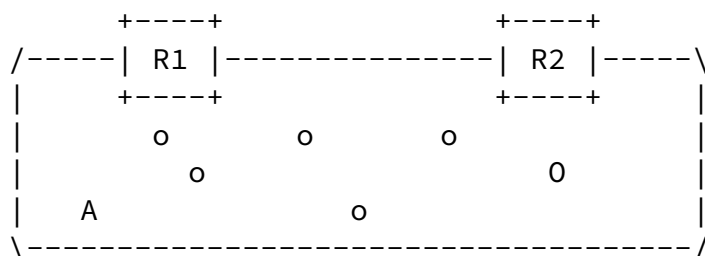


Figure 1: Address compression with [RFC 4944](#)

This is a very classical multi-homing problem in IPv6. Node A selects a prefix announced by router R2, but packets are routed

through R1. R1's ISP may reject the packet since the prefix of the source address ? was not allocated by this ISP.

Our motivation is to avoid announcing the IPv6 prefix to sensors that do not need to know their global IPv6 address, while still guaranteeing end-to-end communication between any equipment in the Internet and these sensors. Indeed, some categories of sensors do not require the knowledge of the prefix used in the network, i.e., their source address, as long as gateways are able to add and remove this information. For instance:

- o a mobile sensor unidirectionally reporting periodic values to a central database located outside the WSN does not need to know its IPv6 address;
- o a fixed sensor may have its address stored in the DNS database and can therefore be contacted from outside the WSN without having to know its own global address.

Our proposal does not require any change to the 6LoWPAN header compression scheme [[I-D.ietf-6lowpan-hc](#)] that suppresses the source

network prefix in compressed IPv6 headers.

## [2.2.](#) Header compression

6LoWPAN defines in [[I-D.ietf-6lowpan-hc](#)] a header compression scheme that divides the IPv6 address into the two distinct parts, the prefix and the interface identifier. The source address is compressed using the following algorithm. A first bit (SAC) in the compressed header tells if the source address is link-local or global, then two bits (SAM) indicate the length of the elided part:

- o 00: the address is sent in extenso,
- o 01: only the 64 bits of the IID are sent,
- o 10: 16 last bits of the IID are sent inline,
- o 11: the whole source address is elided and the IID will be reconstructed using the Layer 2 source address.

Except when SAM value is 00, the source prefix is not sent nor received by the Sensor Node. When a context is specified (CID=1), up to 16 prefix can be compressed. The relationship between the context value and the prefix can be carried in modified RA messages as described in [[I-D.ietf-6lowpan-nd](#)]. We propose to reserve value 15 for prefix not announced through RA. The compression method for the destination address is almost the same based on the DAC and DAM bits.

### [3.](#) Suppression of solicited RA

We propose not to distribute the IPv6 prefix inside the LoWPAN, which totally avoids the need for sending RS / RA exchange. Suppressing the initial RS/RA exchange requires the following changes in sensor nodes' behavior:

- o Sensor nodes do not learn the source prefix(es). With 6LoWPAN header compression, using the source address prefix can be avoided on the link, since a context value may be carried in the compressed header.
- o sensor nodes do not know their default router's address. In Route-Over, the IPv6 address of the default LBR can be learned from the routing protocol. For other topologies (star and mesh-under), we propose to use a predefined Layer 2 anycast address to identify default routers. (see sections [Section 3.1](#) and [Section 3.2](#))

We reserve a context value (e.g., 0xF) to indicate that the prefix is not carried in LoWPAN. The value 0xF may be chosen in order to be compatible with current implementations. In the following we discuss the three different topologies star, mesh-under and route-over. We finish the section by given sensor nodes and LBR behavior.

#### [3.1.](#) Star Topology Packet Format

In a Star topology (i.e. all the Sensor nodes are directly connected to the LBR), the source address of a packet generated by a sensor node can be totally elided (SAM=11) and the LBR may use the L2 information in the frame to reconstruct the IID. The destination address field should be the default router L2 address, which is usually learned from RA messages. If no RA is sent, the sensor node does not know the L2 address of the default router. To solve this issue, sensors may be configured with a predefined L2 anycast address that will be used when no L2 unicast address is known. The context value of the compression header must be 0xF for the source address prefix (i.e. the LBR must add the prefix and recompute L4 checksum). On the reverse path (from the LBR to the sensor node), 0xF indicates that the gateway has removed the prefix and has adapted the L4

checksum (see section [Section 4](#)).

From Sensor Node to LBR:

```

+-----L2-----+-----6LP-----+
|DA=L2Anycast SA=SN | CID=1 SAC=1 SAM=11 | ... 0xFx ...| ULP
+-----+-----+

```

Form LBR to Sensor Node:

```

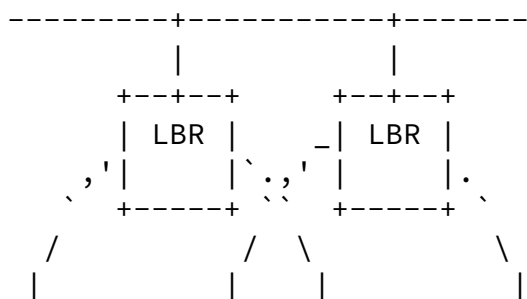
+-----L2-----+-----6LP-----+
|DA=SN SA=LBR      | CID=1 DAC=1 DAM=11 | ... 0xFF ... | ULP
+-----+-----+

```

Figure 2: Packet Header in Star Topology

Consider Figure Figure 3 where a star topology with a sensor node located in an area reachable by two LBRs is represented. The use of an anycast address could make the two LBR to both forward packets from the sensor node (to an outside network, e.g., the Internet) with several (two in the case of Figure Figure 3) different source addresses, composed of the (different) prefixes associated with each LBR and the same interface ID.

To avoid this, the anycast address should only be used with the first frames when the LBR address is unknown; when a Sensor Node receives a reply from a LBR, it uses this address as unicast instead of the L2 anycast address.



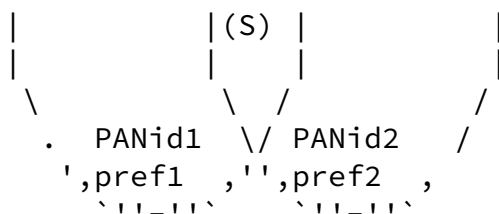


Figure 3: Star Topology

### 3.2. Mesh Topology Packet Format

In a Mesh topology, "routing" is done at layer 2. [RFC4944] provides a mesh header to carry the source and destination addresses. The Layer 2 header carries hop-by-hop source and destination addresses.

From Sensor Node to LBR:

```
+-----L2-----+-----mesh-----+-----HC-----+-----+
|DA=hop SA=hop | SN Anycast | CID=1 SAC=1 SAM=11 | ... 0xFx ...| ULP
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Form LBR to Sensor Node:

```
+-----L2-----+-----mesh-----+-----HC-----+-----+
|DA=hop SA=hop | LBR SN      | CID=1 SAC=1 SAM=11 | ... 0xFx ...| ULP
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Figure 4: Packet Header in Star Topology

Figure 5 represents a mesh topology; a routing protocol at layer 2 allows establishing the routes in the sensors network, especially from the sensor nodes to the LBR(s). Just as in the star topology, L2 anycast address can be used by the sensor nodes to reach a LBR (the L2 anycast address can be viewed as an identifier of a virtual equipment). LBR must inject routes to this L2 anycast address, so every nodes can forward packets to the closest LBR. A layer-2 anycast address is used in the mesh header only when a sensor node

sends a packet and can only be used as the destination address. The



next hop is obtained from the mesh routing table. In Figure 5 S sends a packet toward the gateway. The route goes through R which is in reach of two gateways. Since R has to select a Next Hop only one LBR will receive the packet even if several LBRs share the same PANid.

Anycast addresses should not be used as source addresses. Therefore, when a gateway forwards a packet to a sensor node, it sets the latter's physical address in the mesh header.

One drawback of this approach appears when messages sent by the sensor have to be fragmented: if the routes are unstable within the sensor network, some fragments may reach one default router and other fragments another router, making reassembly impossible. However, such situation is expected to be very uncommon and the sensors may use the LBR address received in the mesh header to increase stability. A trade-off is required between the sensors' mobility and the stability of the default router location.

The use of anycast addresses is also a solution for the issue of dead router detection. When a LBR fails, the routing protocol automatically forwards the frame to another active LBR.

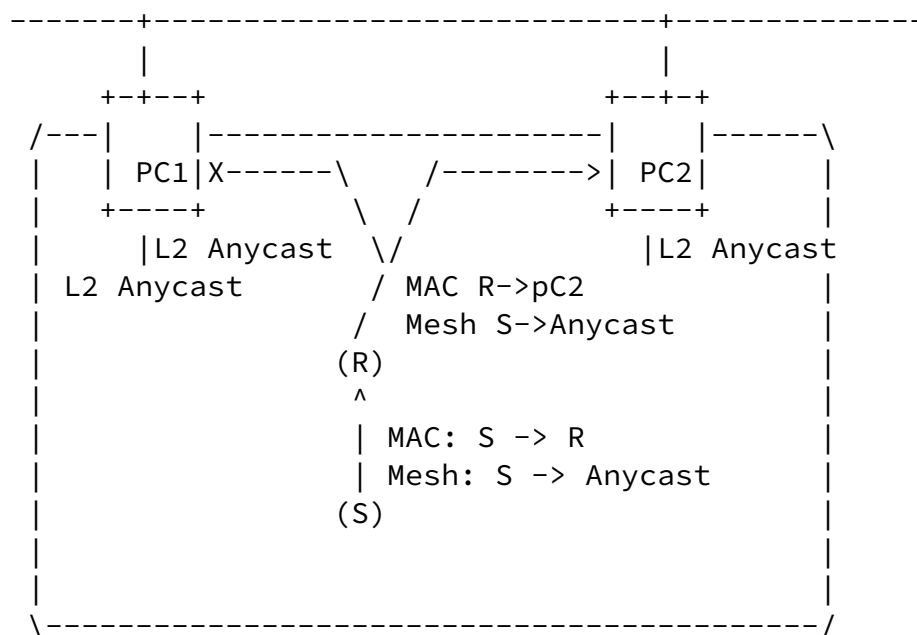


Figure 5: Mesh Topology

### 3.3. Routed Topology Packet Format

In a route-over network, packets are routed at layer 3. Since the Layer 2 addresses contained in the frame are generally that of intermediate nodes, IPHC compression of source or destination address cannot be as good as in mesh-under. We find similar information in the routing header to that contained in a mesh header, except it is stored after the HC field. Figure 5 represents a case where IID is fully sent after the HC field, but other SAM values such as 00 (with SAC/DAC equal to 0) and 01 can also be used.

From Sensor Node to LBR:

```

+-L2-+-----HC-----+---
|    | CID=1 SAC=1 SAM=10 | ... 0xFx IID ...| ULP
+----+-----+-----+

```

Form LBR to Sensor Node:

```

+-L2-+-----HC-----+---
|    | CID=1 DAC=1 DAM=10 | ... 0xFF IID ...| ULP
+----+-----+-----+

```

Figure 6: Packet Header in Route-Over Topology

The routing toward the LBR is done by the default route installed in the FIB of Sensor Nodes acting as routers in the WSN. A L2 anycast address is not necessary to identify the gateway.

## 4. ULP checksum adaptation

Sensor nodes may use their own layer-4 protocol (ULP: Upper Layer Protocol) however, regarding 6LoWPAN layer-4 compression values, UDP, TCP or ICMP are expected. IPv6 mandates the use of an L4 checksum for these protocols. The L4 checksum covers the data field and also a pseudo- header including IPv6 source and destination addresses.

The checksum algorithm is based on a sum of all the 16 bits words of the message. In our scheme, when a sensor node sends a packet to the outside world, it does not know its own global IPv6 address and cannot fill the source address field. Therefore, it has to compute an incomplete L4 checksum, setting the prefix part of the source address to zero. When receiving such a packet, the LBR can verify the validity of the checksum and fix its value by adding the prefix

checksum computed using the same algorithm. When receiving a packet from the outside world, the LBR can also adapt the L4 checksum by

subtracting the corresponding value. When a LBR receives an IPv6 packet from the Internet, it may be the case that it does not know if the Sensor Node supports RA suppression. In this situation, it must send the packet with the destination address uncompressed. The LBR may maintain a cache of addresses of Sensor Nodes that have previously sent packets using context 15. If the destination is in the cache, the LBR may adapt the checksum and use prefix compression.

## [5.](#) Conclusion

Although this proposal suppresses the first Neighbor Discovery exchanges to allow very resource-constrained equipments to communicate with any IPv6 hosts, the current IPv6 model is not broken. These optimizations may be applied to some classes of the sensors which do not require the knowledge of their own global IPv6 address. These optimizations enhance the performance of the network by limiting the number of packets sent, especially broadcast, and by reducing the time required for a node to enter the network. These optimizations are not mandatory and are fully compatible with the current behavior of the 6LoWPAN network.

## [6.](#) Acknowledgement

This work is supported by the French Ministry of Foreign Affairs within the Tiny6 project, by NIA (National Information Society Agency) of Korea with the MoMo project and the by the French National Research Agency via the ARESA2 project. A special thank to Dominique Barthel, Ratnajit Bhattacharjee, Claude Chaudet, Guillaume Chelius, Younghee Lee, Neelesh Srivastava, Bruno Stevant Sarah Tarrapey and Deepanshu Vasal.

## [7.](#) Security Considerations

## [8.](#) Normative References

[I-D.chakrabarti-6lowpan-ipv6-nd]  
Chakrabarti, S. and E. Nordmark, "LowPan Neighbor  
Discovery Extensions",  
[draft-chakrabarti-6lowpan-ipv6-nd-05](#) (work in progress),  
July 2008.

[I-D.ietf-6lowpan-hc]  
Hui, J. and P. Thubert, "Compression Format for IPv6  
Datagrams in 6LoWPAN Networks", [draft-ietf-6lowpan-hc-07](#)

Toutain, et al.

Expires January 1, 2011

[Page 10]

---

Internet-Draft

RA Suppression

June 2010

(work in progress), April 2010.

[I-D.ietf-6lowpan-nd]  
Shelby, Z., Chakrabarti, S., and E. Nordmark, "Neighbor  
Discovery Optimization for Low-power and Lossy Networks",  
[draft-ietf-6lowpan-nd-09](#) (work in progress), April 2010.

[I-D.thubert-6lowpan-backbone-router]  
Thubert, P., "6LoWPAN Backbone Router",  
[draft-thubert-6lowpan-backbone-router-01](#) (work in  
progress), July 2008.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,  
"Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#),  
September 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler,  
"Transmission of IPv6 Packets over IEEE 802.15.4  
Networks", [RFC 4944](#), September 2007.

#### Authors' Addresses

Laurent Toutain  
Institut TELECOM ; TELECOM Bretagne  
2 rue de la Chataigneraie  
CS 17607  
35576 Cesson-Sevigne Cedex  
France

Email: [Laurent.Toutain@telecom-bretagne.eu](mailto:Laurent.Toutain@telecom-bretagne.eu)

Nicolas Montavont  
Institut TELECOM ; TELECOM Bretagne  
2 rue de la Chataigneraie  
CS 17607  
35576 Cesson-Sevigne Cedex  
France

Email: [Nicolas.Montavont@telecom-bretagne.eu](mailto:Nicolas.Montavont@telecom-bretagne.eu)

Toutain, et al.

Expires January 1, 2011

[Page 11]

---

Internet-Draft

RA Suppression

June 2010

Dominique Barthel  
France Telecom R&D  
28 Chemin du Vieux Chene  
38243 Meylan Cedex  
France

Email: [dominique.barthel@orange-ftgroup.com](mailto:dominique.barthel@orange-ftgroup.com)

