6lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 March 2026

L. Iannone, Ed.
G. Li
D. Lou
Huawei
P. Liu
China Mobile
P. Thubert

16 September 2025

# Path-Aware Semantic Addressing (PASA) for Low power and Lossy Networks
draft-ietf-6lo-path-aware-semantic-addressing-13

## Abstract

This document specifies a topological addressing scheme, Path-Aware Semantic Addressing (PASA), that enables IP packet stateless forwarding. The forwarding decision is based solely on the destination address structure. This document focuses on carrying IP packets across an LLN (Low power and Lossy Network), in which the topology is quite static, the location of the nodes is fixed for long period of time, and the connection between the nodes is also rather stable. These specifications describe the PASA architecture, along with PASA address allocation, forwarding mechanism, routing header format, and IPv6 interconnection support.

## 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 https://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 20 March 2026.

## Copyright Notice

Table of Contents

## 1. Introduction

There is an ongoing massive expansion of the network edge, driven by the "Internet of Things" (IoT), especially over low-power links which often, in the past, did not support IP packet transmission. Driven by the requirements stemming initiatives like Industry 4.0, Smart Grid, and Smart City, among others, an increasing number of devices and "things" are being connected to the Internet. Sensors in plants/parking bays/mines/data-centers, temperature/humidity/flash sensors in buildings/museums, normally are located in a fixed position and are networked by low power and lossy links even in hardwired networks. Comparing with traditional scenarios, scalability of the (edge) network along with lower power consumption are key technical requirements. Moreover, large-scale Low power Lossy Networks (LLNs) are expected to be able to carry IPv6 packets over their links, together with an efficient access to native IPv6 domains.

The work in [SIXLOWPAN], [SIXLO], [LPWAN], and [SCHC] Working Groups addresses many fundamental issues for those type of deployments, which can be considered an instantiation of what [RFC8799] defines as "limited domains". For instance, the 6LoWPAN compression ([RFC4944], [RFC6282]) addresses the problem of IPv6 transmission over LLNs, making it possible to interconnect IPv6-based IoT networks and the Internet. [RFC8138] introduces a framework for implementing multi-hop routing on an LLN using a compressed routing header, which works also with RPL (Routing Protocol for LLNs [RFC6550]). This technique enables the ability to forward IPv6 packets within the domain without the need of decompression. In addition, SCHC (Generic Framework for Static Context Header Compression and Fragmentation [RFC8724]) enables even more compression by using a common stateful static context.

The aforementioned technologies, which when used in multi-hop network topologies leverage on the presence of a routing protocol, are suitable in generic IoT scenarios and LLN networks. These technologies leverage topology discovery and routing mechanisms, whereas there are several special-purpose networks, where routing protocols are not deployed and the networks are statically manageable [RFC9453] (e.g. PLC [RFC9354] or MS/TP [RFC8163], and Industrial IoT technologies like [RS485], etc.). In these kinds of deployments, topologies are planned in advance and well provisioned, with sensor nodes usually in fixed locations. This document introduces a topology-based addressing mechanism that allows, in the latter scenarios, to avoid the use of routing protocol in favor of a topological stateless forwarding algorithm (see Section 4). The syntax of the IPv6 addresses used in the present specification is unchanged, as for [RFC4291], however, the way addresses are assigned adds path awareness semantic to them, hence the name "Path-Aware Semantic Addressing".

This specification document leverages on the 6Lo Routing Header (6LoRH) as defined in [RFC8138] and LOWPAN_IPHC header compression [RFC6282]. The use of other compression techniques is out of the scope of this document, and may be the object of separate specifications. The proposed addressing is independent of Unique Local Addresses [RFC4193], which has a dependency on specific link-layer conventions [RFC6282]. It is also different from stateful address allocation that requires all nodes to obtain addresses from a centralized DHCP server, which leads to increased network startup time and consumption of extra resources, such as bandwidth and energy. Path-Aware Semantic Addressing (PASA), defined in this document, relies on the neighbor discovery Generic Address Assignment Option (GAAO) [I-D.ietf-6lo-nd-gaao] in order to recursively assign addresses.

## 2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Definition of Terms

PASA Root: The PASA Root is the router responsible for the

management of the whole PASA network and routing/forwarding both internal and external traffic. It uses an Address Assignment Function (AAF) and performs the address assignment for its children. The root node functions as gateway between the PASA Domain and the Internet, acting as what [RFC8505] names 6LBR (6LoWPAN Border Router).

PASA Host: A PASA Host is a node with no children (i.e., a leaf), it is what [RFC8505] names 6LN (6LoWPAN Node). This node does not perform the AAF. It merely requests an address from its selected parent.

PASA Router: A PASA Router is an internal node, different from the PASA Root, acting as a router, hence as what [RFC8505] names 6LR (6LoWPAN Router). Before acting as a router, it will act as a PASA Host by acquiring an address. Then, similar to the PASA Root, it uses the AAF and performs the address assignment for its children. According to [I-D.ietf-6lo-nd-gaao] and [RFC8505], PASA Routers are expected to store in non-volatile memory state about address registration and assignment.

PASA Domain: A network limited domain [RFC8799] in which PASA is deployed.

Address Assignment Function (AAF): As defined in [I-D.ietf-6lo-nd-gaao].

Tree Address Assignment Function (TAAF): As defined in Section 6. Used by PASA Root and PASA Routers to assign addresses to their children.

## 4. Comprehensive Use Cases

As mentioned in Section 1, [RFC9453] provides some 6lo use cases with wired connectivity, tree-based topology, and no mobility requirement (cf. Table 2 of [RFC9453]). These use cases, where PASA can be used, include Smart Grid, Smart Building, etc., were topologies remain unchanged for long period of time, and very often topology changes are known in advance. The PASA solution utilizes stable topology information to allocate addresses for nodes, which enables stateless forwarding. It saves overhead of messages triggered by routing protocols and reduces RAM footprint for routing table storage. Thus, it will reduce the overall energy consumption. The PASA forwarding logic is simple, enabling the solution being ported onto very constrained nodes. Yet, networks are unlikely to be immutable, changes, even at large time scale, happen (e.g., change of sensors, new smart-furniture, etc.). PASA can handle very easily changes at the edge (leaves) of the topology, but may require some

reconfiguration for more important topology changes (see Section 12 for details).

In the following, a few use cases are discussed in-depth to demo the applicability of the PASA solution.

### 4.1. Smart Grid

A typical smart grid network topology whose purpose is to distribute electricity to homes in a residential area consists of Smart Circuit Breaker (SCB), Phase Change Switch (PCS), Cable Branch Box (CBB) and Power Distribution Cabinet (PDC), as shown in Figure 1. The PDC, containing a few SCBs, phase compensation units, sensors and actuators, is responsible for the power distribution towards CBBs. The CBB containing SCBs and sensors further distributes the power to PCS and eventually to the home. The smart grid power distribution network forms a typical tree topology, where the PLC communication technology is used to collect data (meter numbers, phases, etc.) and perform control/management of the overall system.

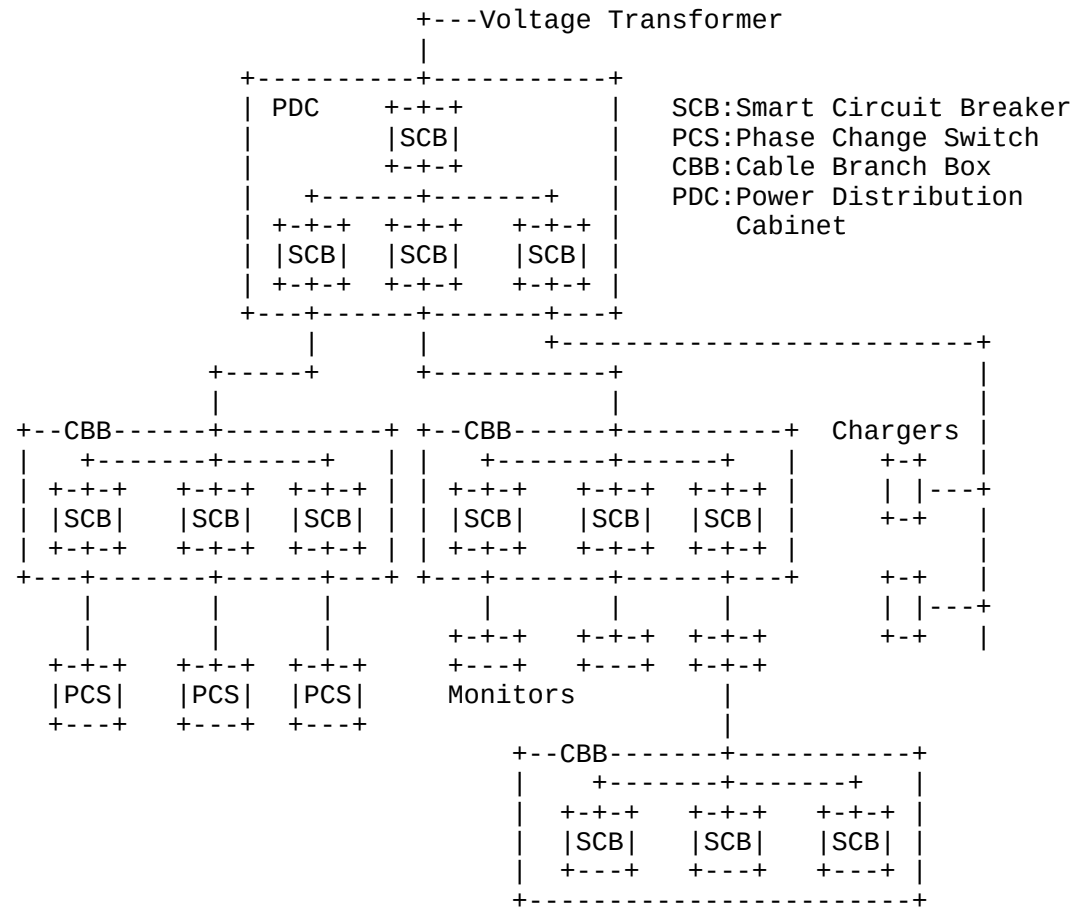


Figure 1: Example of topology of a smart grid.

## 4.2. Smart Home

Smart home or home domotics [DOMOTICS] is another example, as shown in Figure 2, where a PLC router (PLC-R) in each room is used to connect home appliances (boiler, dishwasher, fridge, etc.) and devices (lights, doorbell, sound boxes, etc.) to home network and sometimes to the Internet. The network can be further extended if a switch/router is connected. As it leverages the power line distribution, the network forms a typical tree topology as well. Some observations and considerations are:

* Usually a Home Gateway bridges the smart home to the Internet.

* The Home Gateway, the PLC routers, and most of the home appliance are fixed in different locations. They rarely move after setup, but the network can be extended with new smart objects.

* The smart home automation requires any to any communication.

* Lightweight communication stack with limited MCU and RAM consumption is desired.

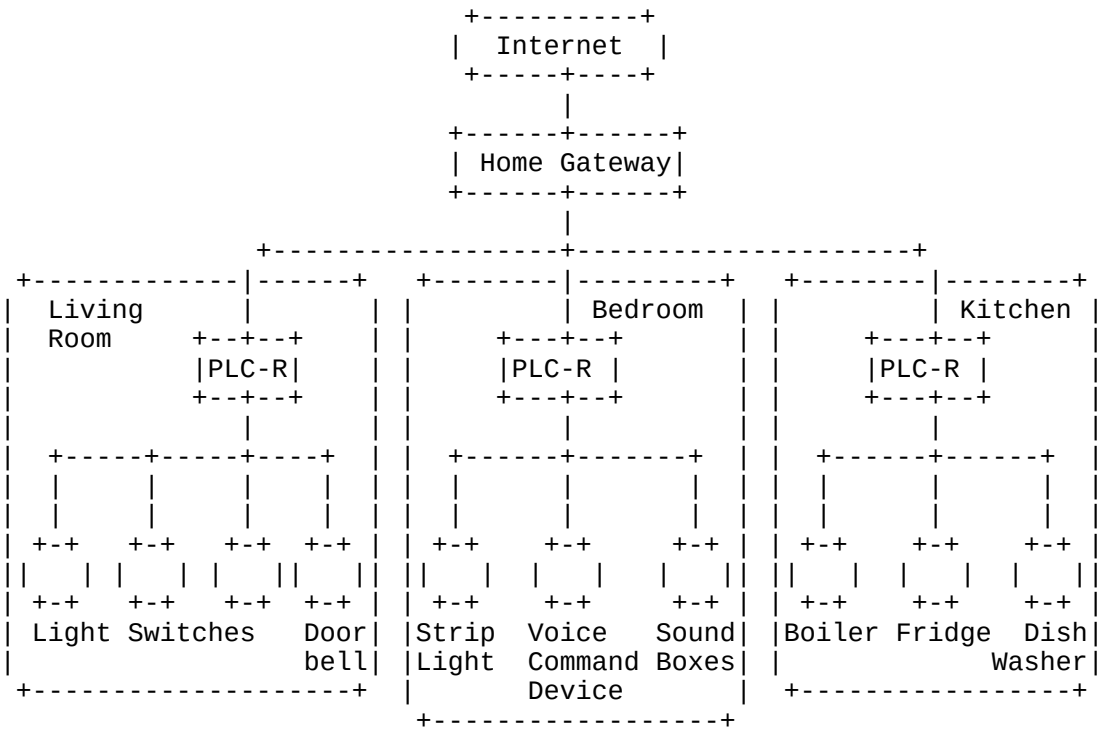


Figure 2: Example of topology of a smart home.

## 4.3. Data Center Monitoring

Data centers represent a significant infrastructure, requiring to be protected from environmental issues such as extreme temperature, high humidity, water leakage and high dust concentration, which can cause device failures. Therefore, it is critical to deploy sensors to monitor environmental factors to make sure data center is running efficiently.

The network topology of the data center supervision system is hierarchical, and mainly consists of Network Management System (NMS), Supervision Center (SC), Field Supervision Unit (FSU), dumb and smart devices, as shown in Figure 3. The smart devices refer to smart air conditioner, smart door lock and power equipment with embedded sensors to report their working status. The dumb devices refer to the many devices without embedded sensors, which require additional sensors to collect and update information of environment.

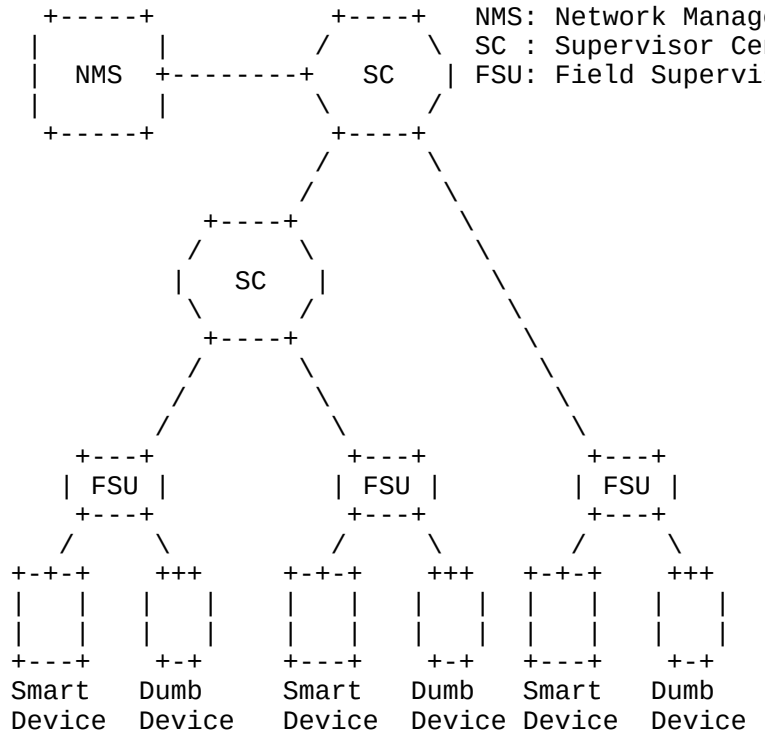


Figure 3: Example of topology of a Data Center Power & Environment Supervisor System.

Both dumb and smart devices are connected to the FSU, which monitors and connects all devices of the whole floor. The number of ports on FSU is limited, where one FSU usually contains 8 analog input ports, 16 digital input ports, 4 digital output ports, 8 RS485 ports and 4 IP ports. The terminal devices report working status and environmental information to FSUs every 3 seconds. If values that are abnormal or above a certain threshold are detected, the FSU reports it to the SC immediately and keeps on reporting it in real-time for next couple of hours, until the manager issues new commands. The SC can be constructed as required. The FSU reports to the local SC first, then relays the message to the central SC for data analyzing and management.

In this scenario, deployed devices (usually 600-1000 sensors per floor), due to the shortage of ports and limitation of voltage supply, use additional power supply or batteries. Since battery replacement and maintenance are costly, it is desired to have low energy consumption for longer service life. We should not only reduce the power consumption on the device level, but also on the data transmission level. The data transmission also causes huge power consumption, which can be reduced by leveraging low power transmission protocol. The FSU connects to sensors with wired technology, such as AI/DI/RS232/RS485/single pair Ethernet. Multiple FSUs will connect to hierarchical supervision centers and then make data communication with supervision platform by IPv6.

### 4.4. Industrial Operational Technology Networks

The Operational Technology (OT) networks are not pure IP networks. Shop floors deploy fieldbus protocols such as Modbus, Profinet/IP, BacNET, CAN, etc. for process control using field devices (sensors and actuators). To improve automation, Industry 4.0 is looking at means to integrate process control in OT domain with the applications residing in IPv6 domains (the enterprise networks). This leads to three primary requirements:

* Continuity in connectivity between the end devices and applications, both of which follow different address structures.

* The OT networks are traditionally designed as layer-2 and OT operators are not expected to deploy or maintain IT style routing infrastructure, hence auto-configuration mechanisms for device addresses and reachability are preferred.

* The OT networks are also delay-intolerant; therefore, compact and lean message structures are favored over encapsulations to minimize processing and translation overheads.

Using PASA, as described in details later in this document, the following applies:

* The OT network is represented as a PASA Domain, interfacing with native IPv6 applications, e.g., Human-Machine Interface (HMI), Manufacturing Execution System (MES). In general, on shop floors, devices are at fixed locations or cell-sites and the PASA tree hierarchy described in Figure 4 applies suitably.

* In an idealized PASA-based OT domain, a leaf-node could be a field device (sensor or actuator) that always connects to PLC serving as last node forwarding traffic to/from the leaves, i.e. sensors and actuators. Hence, the PLC will work as a PASA Router only for field devices supporting IPv6. For field devices not supporting IPv6, the PLC will assign PASA addresses for each of them, and then translate between IPv6 packets and the device protocol, making the devices appear as PASA Hosts within the enclosing PASA Domain.

* The border node may be at the root for any IT application requirement. Then the packet communication inside the PASA Domain will strictly follow PASA structure whereas communications with IPv6 domain networks will use the Border router for translations.

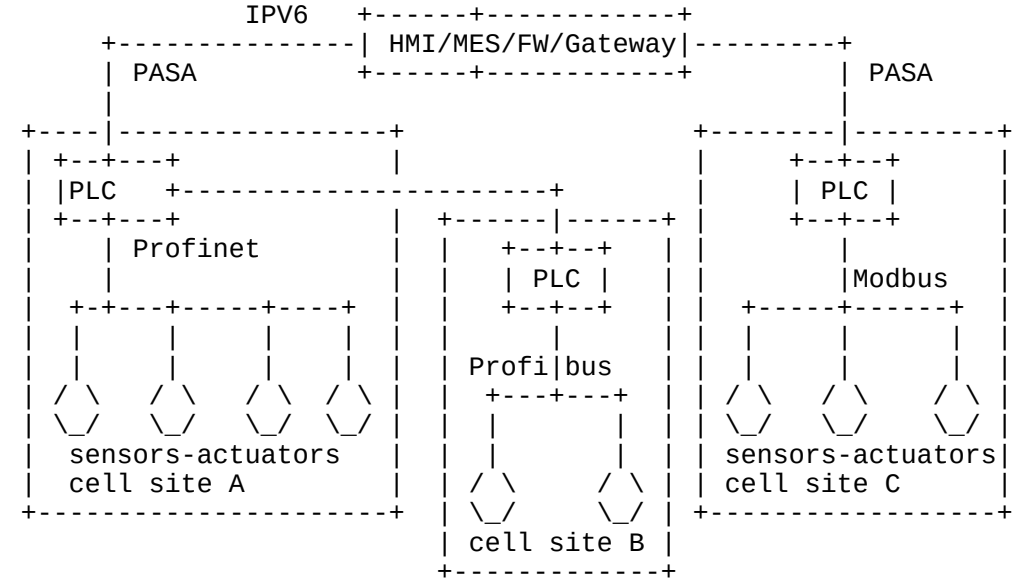


Figure 4: Example of an Industrial Operational Technology Network topology.

## 5. Architectural Overview

Path-Aware Semantic Addressing (PASA) is an efficient topology-based network layer address assignment and packet forwarding mechanism. Each PASA node is aware of its own IPv6 address, constructed by an IPv6 prefix and the PASA itself (see Section 6.3). Inside the PASA Domain, nodes communicate with each other by using PASA addresses. It is a smaller addressing space compared to the huge /64 IPv6 addressing space, but enabling stateless forwarding using the PASA-6LoRH header (see Section 8). When IPv6 communication occurs between nodes inside the PASA Domain and external IPv6 nodes, the border router, which plays as well the role of "root" in the addressing tree, performs packet decompression (as per Section 7.2 and [RFC6282]). Note that packets destined outside the PASA Domain do not need to use the PASA-6LoRH header, since they can be easily forwarded to the root following the default gateway (see Section 7.2). However, an IP-in-IP header, as for [RFC8138], is used to avoid compression/decompression at each hop. The architecture of PASA network is shown in Figure 5.

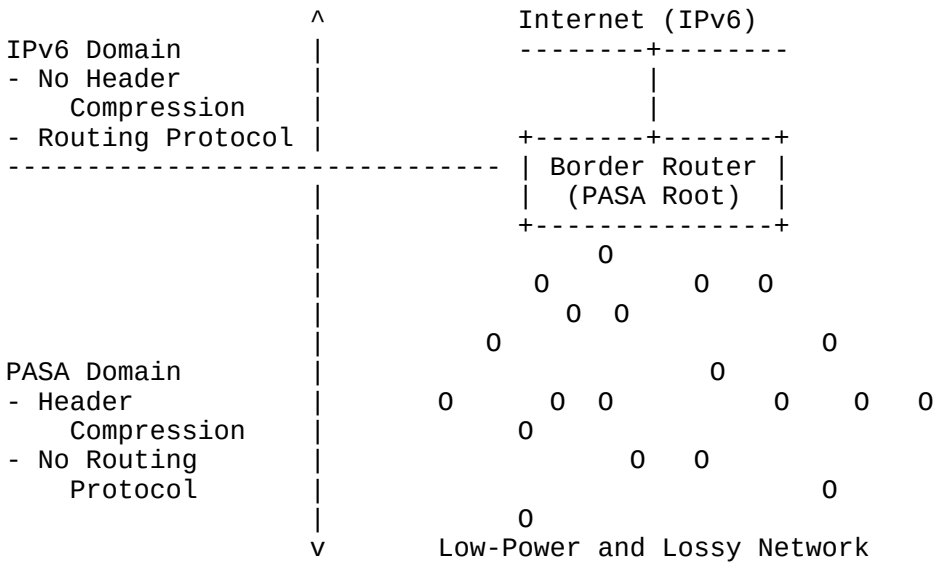


Figure 5: The architecture of general PASA networks.

In the PASA network, there are 3 types of nodes, the PASA Root, the PASA Router and the PASA Host (See Section 3).

PASA Root: Since the root node is responsible for the whole PASA

network and acts as gateway for external traffic, it also operates the translation between LOWPAN_IPHC and IPv6 formats (cf. Section 7). It assigns addresses to its children using the AAF. There is one root node in the PASA network.

PASA Router: A PASA Router is basically the root of a subtree and as such it is a router forwarding traffic between its parent and its children according to the addressing. When handling a packet, if the destination is in one of its subtrees, it forwards the packet to the corresponding child, otherwise it simply sends it to its parent.

PASA Host: A PASA Host is a node with no children, hence a leaf. It operates as a host, since it is either destination or source of every packet it handles. If it is the source of packets, it simply sends the packets to its parent.

The address assignment described in this document relies on the Generic Address Assignment mechanism described in [I-D.ietf-6lo-nd-gaao] (see Section 10). The use of multicast messages is limited as for [RFC8505]; no new multicast requirements are introduced. The PASA Root and PASA Routers have to act as IPv6 ND Registrars. Each node newly joining the network and acquiring a PASA address firstly needs to select a parent node by choosing among the nodes that replied with a Router Advertisement (RA) after an initial Router Solicitation (RS). In general, "first come first served" selection policy is sufficient; however, some deployments may have tighter constraints on the router selection, but enforcing such selection is beyond the scope of this document. Once the parent node is selected, the node asks for a PASA address. In its reply the parent will propose an address according to the node’s role, which is indicated in the D-bit of the GAAO message (see Section 10). The proposed address is algorithmically calculated using the PASA AAF. The address assigner is the parent of the node and becomes as well the default gateway from a routing perspective (used for destinations that are not in the local PASA Domain). The node will then ignore replies from other 6LR neighbors.

A node that, for any reason, reboots does not need to restart the whole procedure. According to [I-D.ietf-6lo-nd-gaao] and [RFC8505] address registration state has to be stored in non-volatile memory, hence, when the nodes is up again there is no need to go through parent selection and address request, it can just re-register the previously obtained address.

The overall design objective is centered on reducing the size of routing/forwarding tables by using a topological addressing scheme. PASA reduces the amount of information synchronization messages, so

it actually reduces computation complexity during packets parsing and forwarding. As such, PASA may save communication energy in an IoT LLN network [LI22]. Compared to RPL-based routing [RFC6550], PASA avoids the extra overhead of address assignment by integrating address assignment and tree forming together. Compared to RPL storing mode, PASA uses smaller forwarding tables, hence less memory, since there is no need to store topology information. Compared to RPL non-storing mode, PASA has lower overhead in terms of bandwidth since, instead of an explicit list of addresses, it encodes the path directly in the address itself. The overhead in both modes, while smaller compared to routing protocols not designed for 6LoWPAN environments, is still not negligible [CHING21]. PASA addressing has also lower overhead compared to BABEL, since there is no need to share a routing table among neighbors ([NEUMANN15], [RFC8966]).

There are two distinct PASA features that allow PASA to be efficient, namely:

1. PASA Tree Address Assignment Function (see Section 6),

2. Stateless Forwarding (see Section 7),

these features are separately discussed in the following.

# 6. PASA Address Assignment

The basic rules for the AAF include:

* Routers (Root and routers) run the AAF to generate their children’s addresses.

* All nodes run the same AAF in the same network instance.

* The maximum length of the PASA address MUST NOT exceed 64 bits.

In the following, a tree-based AAF is defined for PASA.

## 6.1. Tree Address Assignment Function (TAAF)

In the Tree Address Assignment Function the address of each node is prefixed by the address of their parent, starting from the root. Normally, the root role is assigned to the border router when the LLN bootstraps. PASA Root is MUST use the single bit address ’1’ (see Section 6.3). An example of a possible result of a PASA deployment is shown in Figure 6.

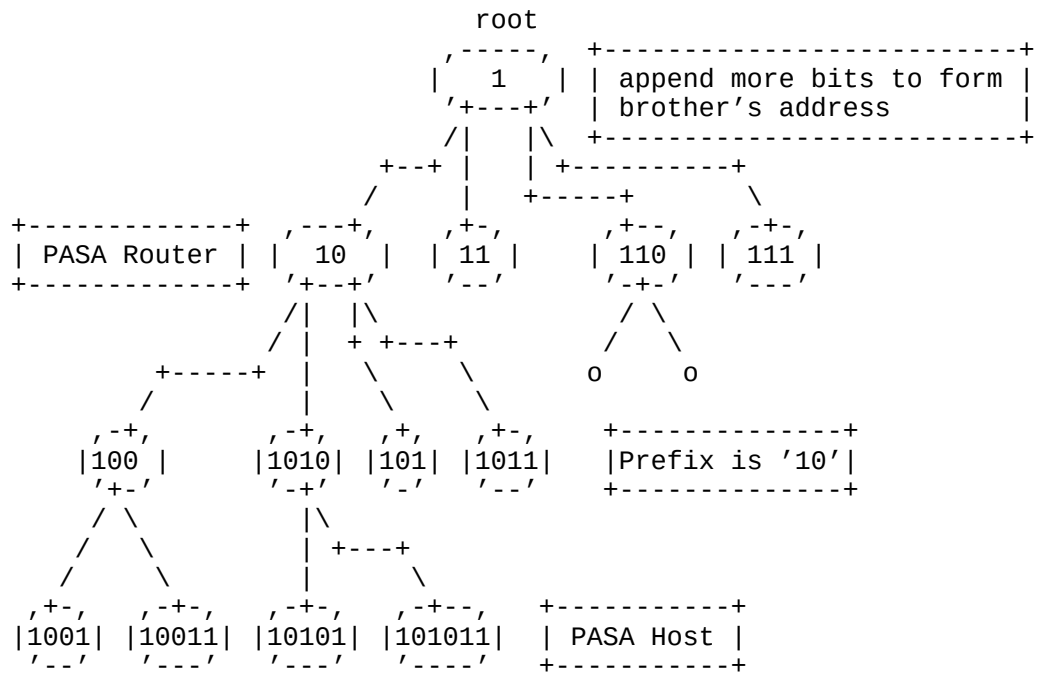


Figure 6: An example of PASA Tree Addresses Assignment Function.

Every router node maintains two indexes, one for the children that are also routers and one for the children that are hosts (starting at 0 for the first child in each role). The first index is named 'r', as of routers, and the second 'h' as for hosts. These two indexes MUST be stored in non-volatile memory along with address assignment state, so that in case of reboot a PASA-Router can continue its role without disrupting the addressing. PASA Routers' address MUST terminate with the bit '0', while PASA Hosts' address MUST terminate with the bit '1'.
The Tree Address Allocation Function TAAF(role,r,h) used in this document is defined as:

```
TAAF(role, r, h) = 'address of the node performing the function'
                   + (role == host? b(h++):b(r++))
                   + (role == host?'1':'0')
```

Where ’r’ and ’h’ are the two indexes defined above, respectively the routers and the hosts at this layer (starting at 0). The ’+’ symbol indicates a concatenation operation. The symbol ’++’ is the equivalent of the C language increment operator used as postfix, meaning that the value of the variable is increase after its use in the expression [UNIX]. The b() operation indicates the binary string of ’1’ with length equal to its argument, for instance b(3) returns ’111’ and b(0) returns an empty string.

Taking the example of the topology in Figure 6, the proposed TAAF works as follows. At the top level, the root has 4 children, two are routers and the other two are hosts. Starting from the left most node and moving to the right, the root node applies the TAAF as follows:

* For the first child, which is a router:

```
TAAF(’router’, 0, 0) = ’1’(root address) + b(0) + ’0’
                     = ’1’ + ’’ + ’0’
                     = ’10’
```

  Index ’r’ is increased by one after its value ’0’ has been used in the expression and is now equal to 1 (r = 1).

* For the second child, which is a host:

```
TAAF(’host’, 1, 0) = ’1’(root address) + b(0) + ’1’
                   = ’1’ + ’’ + ’1’
                   = ’11’
```

  Index ’h’ is increased by one after its value ’0’ has been used in the expression and is now equal to 1 (h = 1).

* For the third child, which is a router:

```
TAAF(’router’, 1, 1) = ’1’(root address) + b(1) + ’0’
                     = ’1’ + ’1’ + ’0’
                     = ’110’
```

  Index ’r’ is increased by one after its value ’1’ has been used in the expression and is now equal to 2 (r = 2).

* For the fourth child, which is a host:

```
TAAF(’host’, 2, 1) = ’1’(root address) + b(1) + ’1’
                   = ’1’ + ’1’ + ’1’
                   = ’111’
```

Index ’h’ is increased by one after its value ’1’ has been used in the expression and is now equal to 2 (h = 2).

The first level addresses have now been assigned. Let’s now have a look to how the node 10 (the first router child of the root) applies the same allocation function. Note that node 10 will use its own ’r’ and ’h’ indexes initialized to 0. Starting again from the left most node, node 10 applies the TAAF as follows:

* For the first child, which is a router:

```
TAAF(’router’, 0, 0) = ’10’(node address) + b(0) + ’0’
                     = ’10’ + ’’ + ’0’
                     = ’100’
```

Index ’r’ is increased by one after its value ’0’ has been used in the expression and is now equal 1 (r = 1).

* For the second child, which is a host:

```
TAAF(’host’, 1, 0) = ’10’(node address) + b(0) + ’1’
                   = ’10’ + ’’ + ’1’
                   = ’101’
```

Index ’h’ is increased by one after its value ’0’ has been used in the expression and is now equal 1 (h = 1).

* For the third child, which is a router:

```
TAAF(’router’, 1, 1) = ’10’(node address) + b(1) + ’0’
                     = ’10’ + ’1’ + ’0’
                     = ’1010’
```

Index ’r’ is increased by one after its value ’1’ has been used in the expression and is now equal 2 (r = 2).

* For the fourth child, which is a host:

```
TAAF(’host’, 2, 1) = ’10’(node address) + b(1) + ’1’
                   = ’10’ + ’1’ + ’1’
                   = ’1011’
```

Index ’h’ is increased by one after its value ’0’ has been used in the expression and is now equal 2 (h = 2).

Note how the children of the same parent all have the same prefix (10 in this example) and such parent will be their default gateway. The proposed TAAF algorithmically assigns addresses to the different

nodes without the need to know the topology in advance. However, once the addresses have been assigned, the proposed TAAF encodes the topology in the addresses themselves, which enables stateless forwarding, but if used beyond the PASA Domain it exposes the internal topology. See Section 14 for further details. TAAF creates unique addresses for each node, as such there is no need to perform Duplicate Address Detection (DAD) procedure.

### 6.2. Limitation on the Number of Child Nodes

The maximum number of children of a node is determined by the specific AAF used. IEEE 802.15.5 has explored the use of a per-branch setup, which, however, incurs scalability problems [LEE10]. PASA allocation design is more flexible and extensible than the one proposed in IEEE 802.15.5.

The TAAF defined in this document does not need any network-specific setup, though it is still limited by the maximum length of addresses. The largest address of the network will depend on the actual topology. Indeed, the maximum length of an address with the proposed TAAF grows linearly at each level of the tree with the number of siblings from the same parent. Let’s take again the example in Figure 6 and let’s assume that the children of node 10 are all hosts, for the largest address we need 2 bits to encode the parent node prefix (10 in this case) to which we need to add a number of ’1’ equal to the value of the h index which is the number of hosts minus one (because the first host has index 0), in this case since there are 4 hosts, the index value is 3 and we add the ’111’ string, hence the address length would be 6 (2 for the prefix, 3 to encode the 4th host address, and one for the final 1 the ends all hosts’ addresses). In a more formal way the maximum address length at each level can be calculated as:

```
Max_Length = length(Parent address) +
             length(b(max(r,h)))
             + 1
```

Where ’r’ and ’h’ are the indexes counting respectively the routers and the hosts at this level.

Note that Max_length can never be more than 64 bits, the IID part of an IPv6 address. This means that, with the proposed TAAF, each PASA Router with an address of length N bits, can have maximum "64 - N - 1" children of the same type. This is because the construction of the addresses. Each new child’s address starts with the address of the parent, which is N bits, and ends with one bit indicating the role (either PASA Router or PASA Host), and the whole length can be at maximum 64 bits, the IID of an IPv6 address.

For the special case of the parent connecting to a large number of children, a variant of the proposed TAAF (or a new different AAF) can be designed to fulfill the requirement and optimize the address allocation (as previously described).

### 6.3. PASA TAAF Addresses and IPv6 Addresses

Obtaining a full IPv6 address from a PASA address is pretty straightforward. First the PASA address is concatenated to the configured IPv6 prefix. Since the length of the PASA address is smaller than or equal to 64 bits (the interface ID length in IPv6), the node needs to pad it with zeros (’0’) used as most significant bit. The full IPv6 address will look like: IPv6 prefix + "000...000" + PASA (or in IPv6 notation <IPv6 Prefix>::<PASA>). This is equivalent of doing a coalescence operation as described in [RFC8138] (see as well Section 8.3). The PASA address is assigned by the root or router as previously described.

The converse operation, from full IPv6 format to PASA format is very simple. Firstly, the configured IPv6 prefix is cut out. Secondly, on the remaining 64 bits, all leading zeros can be trimmed. Indeed, because all TAAF addresses are derived from the PASA Root, and since the latter has address ’1’, all TAAF generated addresses always start with ’1’ (See Section 6.1). As such, trimming the leading zeros is a safe operation returning a PASA TAAF address.

PASA does not prevent the normal checksum calculation for the transport layer (e.g., TCP or UDP) or IPSec encapsulation. Indeed, any PASA node is aware of its full IP address, which can be used for the calculation.

## 7. Forwarding in a PASA Network

Internal and external communications in a PASA network work slightly differently. For internal communications, among PASA endpoints, packets carry PASA destination addresses in the PASA-6LoRH Header (defined in Section 8). For external communications, the root is responsible to perform the translation between the compressed PASA address format and normal IPv6 addresses. For instance, for a packet entering into the PASA Domain, the root will extract the PASA address of the destination from the suffix of the IPv6 address, reducing it to the smallest set of hexadecimal quadruplets (two octets) that can contain the address, by removing all leading octets that are just equal to 0x00. Then the root will compress the original IPv6 and transport headers according to [RFC6282] and prepend the PASA-6LoRH header according to [RFC8138].

The following details the forwarding operations for both internal and external communication. The intra-network forwarding decision depends on the specific AAF used. Here we will use the TAAF previously introduced (see Section 6) to illustrate the forwarding procedure.

### 7.1. Forwarding toward a local PASA endpoint

Intra-domain packets carry a PASA destination address in the PASA-6LoRH header, such address is the address of another node in the same PASA Domain.
In the proposed TAAF algorithm the length of the addresses increases with the distance from the root, whose address has length 1. The length operation, indicated by Len(X), of a PASA address X, returns the number of bits between the most significant bit of the IID that is set to 1 and the least significant bit. For instance, for and address encoded on two bytes, Len(0x00010010) = 5.
Such property can be used to quickly take forwarding decisions based on the length of the destination address. Indeed, when a PASA router receives a packet destined to local PASA Domain, one of the following three cases may arise:

* The length of the destination address is shorter than the address of the PASA Router. This means the destination is closer to the root and just forwarding to its parent is enough.

* The length of the destination address is equal to the address of the PASA Router. In this case the destination is either the PASA Router itself, or another node in a different branch of the tree. The PASA Router compares its address and the destination address. If they are equal, then the packet has reached its destination. Otherwise the packet has to be sent to the parent in order to reach the right branch.

* The length of the destination address is greater than the address of the PASA Router. In this case the destination is either in a sub-branch rooted in PASA router itself or in a totally different branch of the tree. In the former case the packet has to be forwarded toward the correct child, in the latter just sent to the parent. In order to decide which operation to do, the router compares its own address with the most significant bits of the destination address, in other words whether its own address is a prefix of the destination address. If there is a match, then a child is selected as next hop based on the remaining bits of the destination address, otherwise, the destination is in a totally different branch and the packet is sent to the parent.

More formally, when a PASA node receives a packet, it performs the following sequence of actions (also see Figure 7):

1. Get destination address from the PASA-6LoRH (abbreviated to DA) and the current node’s address (abbreviated to CA). Go to step 2.

2. If length of DA, is smaller than length of CA, send the packet to parent node and exit. Otherwise, go to step 3.

3. If length of DA is equal to length of CA, go to step 4. Otherwise, go to step 5.

4. If DA and CA are the same, the packet arrived at destination, exit. Otherwise, send the packet to parent node and exit.

5. Check whether CA is equal to the prefix of DA (indicated by PrefixOf() operation). If yes, go to step 6. Otherwise, send the packet to parent node and exit.

6. Calculate which child is the next hop address and forward packet to it. With the TAAF proposed in this document, such operation is reduced to reading the DA’s bits starting from the position equal to the length of CA, then skip all ’1’ until the first ’0’ or the last bit of DA. The sub-string obtained in such a way is the address of direct child of current node.

7. If any exception happens in the above steps, drop the packet and send an ICMPv6 "No Route to Host" notification back to the source address.

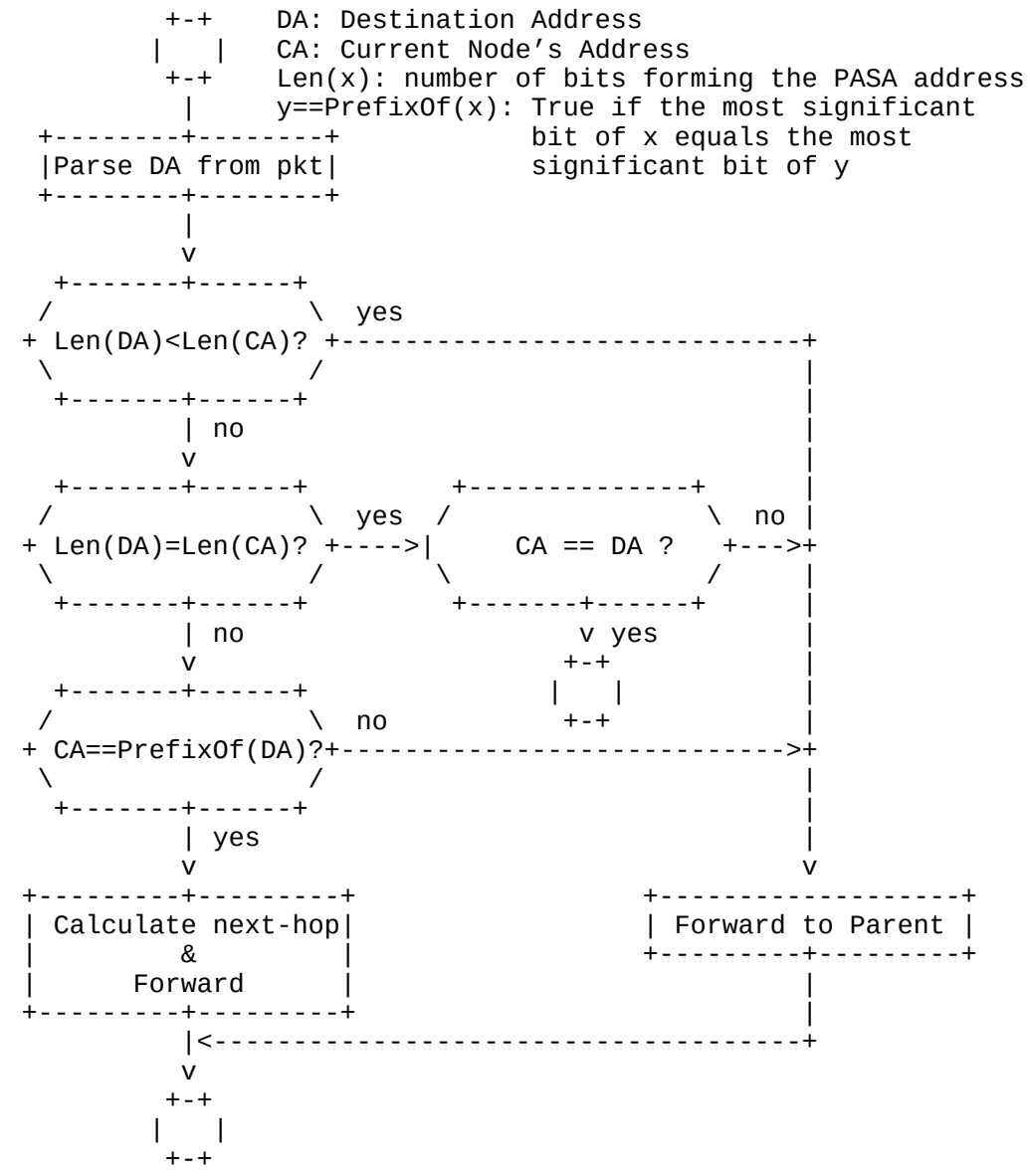


Figure 7: Flow Chart of Internal Forwarding Procedure

In the case of packets arriving from the Internet (external IPv6 domain toward the local PASA Domain) header adaptation operation is performed by the root node. It first compresses the IPv6 header according to [RFC6282] and also described in Section 8.3. The root builds the PASA address of the destination by removing the prefix and

the leading ’0’s octets of the suffix of the destination address. Then the root creates the inner-domain packet with the PASA-6LoRH header. It uses the PASA address as destination, so to route the packet as described above to the destination node.

## 7.2. Forwarding toward an external IPv6 address

When the packet is destined to an external IPv6 address, it is an outer-domain packet. In this case there is no need to use the PASA-6LoRH encapsulation. Indeed, since each node has a default gateway entry in the routing table, namely its parent, all PASA nodes (except the root) just send packets that are destined outside the local domain to their parent. Eventually all packets will reach the root node, which acts as border gateway.

When the network forwarding operation is based on [RFC8138], the source node encapsulates the LOWPAN_IPHC packet with the IP-in-IP 6LoRH Header defined in Section 7 of [RFC8138]. Where the encapsulator address is always the source address in the LOWPAN_IPHC header and the destination is always implicitly the root node. The latter will decapsulate and decompress the packet. Hence, according to [RFC8138] the IP-in-IP 6LoRH will have the form depicted in Figure 8.

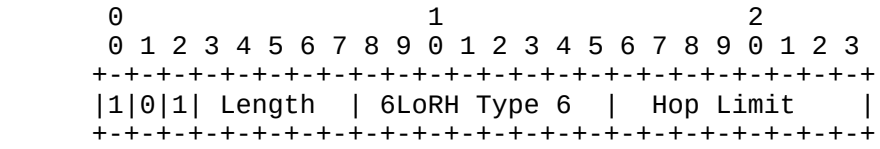


Figure 8: IP-in-IP 6LoRH in a PASA Domain.

Where the Length field is set to 1 to indicate that only the Hop Limit field is present. Such a header is positioned before LOWPAN_IPHC as shown in Figure 9.

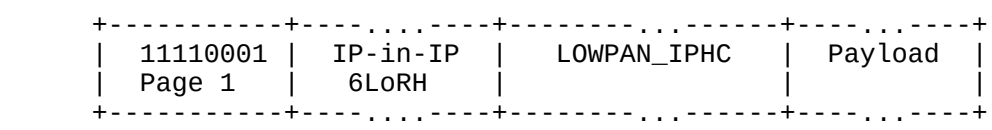


Figure 9: A LoWPAN encapsulated IPv6 header compressed packet with IP-in-IP and LOWPAN_IPHC headers.

# 8. PASA-6LoRH Header

PASA encodes path information into addresses to enable stateless forwarding. Such operation can be performed without touching the stateful forwarding procedure (based on the presence of a routing protocol like RPL), aka without modifying the 6LoWPAN architecture, rather leveraging on mechanisms already defined. In particular, by using the 6LoWPAN Routing Header in Page 1, defined in [RFC8138], it is possible to define a new Critical 6LoWPAN Routing Header Type, named PASA-6LoRH, that will be used by nodes to perform stateless PASA forwarding as described in Section 7.

## 8.1. PASA-6LoRH Sequence

The extension octets typical sequence for a compressed 6LoWPAN packet with PASA Routing Header is shown in Figure 10, following the specification of [RFC8138].

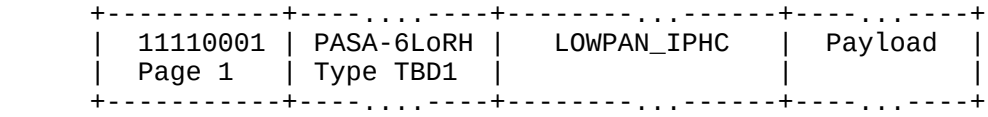


Figure 10: A LoWPAN encapsulated IPv6 header compressed packet with PASA-6LoRH and LOWPAN_IPHC headers.

Where:

* PASA-6LoRH: is the PASA specific extension. See Section 8.2 for details.

* LOWPAN_IPHC: IPv6 compressed header according to [RFC6282].

These two fields are followed by the packet payload.

All nodes of a PASA Domain MUST recognize the PASA critical 6LoWPAN Routing Header and be able to handle the packets according to these specifications. Otherwise, packets can be dropped, hence disrupting communications.

## 8.2. PASA-6LoRH Format

The format of the PASA-6LoRH header, is shown in Figure 11.

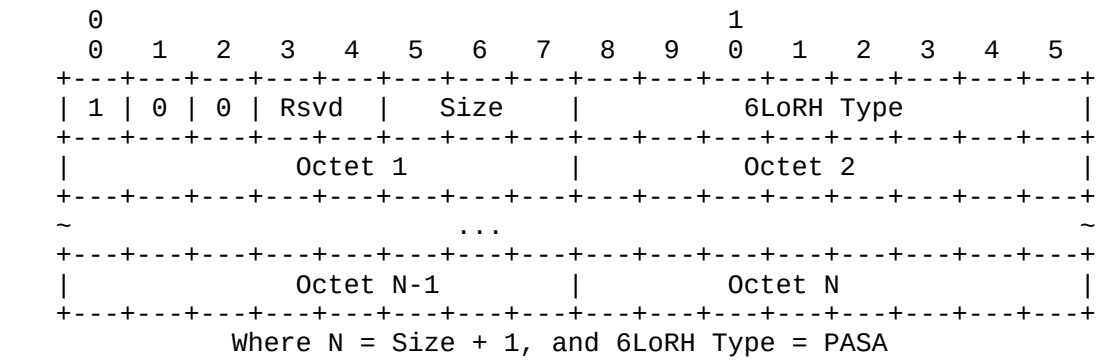


Figure 11: The PASA 6Lo Routing Header format.

Where:

* Reserved (Rsvd): Reserved for future use. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

* Size: indicates the length of the PASA address in octets. The length N equals Size plus 1, which indicates that the length of the PASA address in PASA-6LoRH is at least 1 octet and no more than 8 octets.

* Octet 1 .. Octet N: the PASA destination address used for forwarding purposes. See Section 7 for detailed forwarding operation. PASA addresses are aligned on the least significant bits. For instance, to encode the address b1011, which is the address of a host node since it terminates with '1', the corresponding octet would be b00001011 (or in hexadecimal: 0x0B).

### 8.3. PASA-6LoRH and LOWPAN_IPHC co-existence

In a PASA Domain every node has to use PASA and be able to compress/decompress PASA addresses according to this specification. The reference prefix of the PASA Domain represents a context that can be used to compress addresses in accordance to [RFC6282] and decompress using the context and the coalescence procedure in [RFC8138]. As such the simplest mode of co-existence of PASA-6LoRH with LOWPAN_IPHC is to use stateful address compression in the LOWPAN_IPHC header using the PASA context, then the PASA engine can just read the destination address from the LOWPAN_IPHC header, encoding it in the PASA_6LoRH header according to format previously described in Section 8.2. However, this mode of operation is sub-optimal because PASA-6LoRH already includes the destination address, hence, it can be completely elided from the LOWPAN_IPHC header.

For nodes sending packets, the first step is to create a compressed packet using [RFC6282], where the source PASA address is statefully compressed using the context and the destination PASA address statefully completely elided. The destination address is then encoded in the PASA-6LoRH in its shorter form.

In case where the destination address is an address outside the PASA Domain, there is no need to use the PASA-6LoRH header, since the packet just needs to follow the default route until it reaches the root node (more details in Section 7.2).

The root node, when relaying a packet coming from outside the PASA Domain, compresses the source address in the LOWPAN_IPHC header according to [RFC6282] specifications.

The opposite operations need to be performed on the receiving node. Since the destination address is completely elided in LOWPAN_IPHC the IID is obtained by its encapsulation, in this case the PASA-6LoRH. The full destination address, including the IID, can be obtained via a coalescence operation with the PASA prefix in the context as described in Section 4.3.1 of [RFC8138]. The source address is handled as defined in [RFC6282]. As an example, let’s assume that the PASA IPv6 prefix is 2001:db8::/64, as for [RFC8138] the reference address will be 2001:db8:0:0. Let the PASA address in the PASA-6LoRH header be b111110, which in hexadecimal is 0x3E, then the complete IPv6 address is:

```
2001:db8:0:0:0:0:0:0    Reference address
                    3E  Compressed address

2001:db8:0:0:0:0:0:3E   Coalesced address
```

In compact notation the address is: 2001:db8::3E.

## 9. Nodes role indication

PASA Routers and Hosts roles can be assigned similarly to IEEE 802.15.4, which distinguishes between Full-Function Devices (FFD) and Reduced Function Devices (RFD) (cf., [ZigBee]). Such a role is notified using the 6LoWPAN Capability Indication Option (6CIO) as defined in [RFC7400] and [RFC8505]. In particular, a PASA Root will set the B-bit to indicate that it is a border router, a PASA Router will set the L-bit to indicate it is a router. Nodes with neither the B nor L bit set are considered PASA Hosts.

Note that since PASA Routers MUST act as IPv6 ND Registrars the E-bit of the 6CIO MUST be set as well.

## 10. PASA Address Configuration Procedure

PASA address configuration leverages on the Generic Address Assignment Option [I-D.ietf-6lo-nd-gaao]. When a PASA node bootstraps, and it has address configuration state in its non-volatile memory, it will re-register the address to its parent using [RFC8505] procedures. Otherwise, if there is no configuration state in the non-volatile memory, it will multicast a Routing Solicitation (RS) and may receive one or more unicast Routing Advertisement (RA) messages from potential parents. The node can choose a parent on a "first come first served" basis and send a Neighbor Solicitation (NS) with a GAAO message to request an address to the selected parent (see Figure 12 for an example of such option).

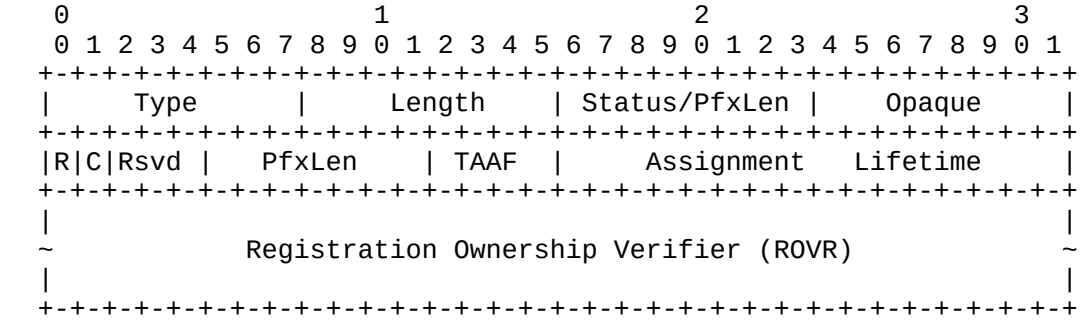


Figure 12: NS GAAO option example.

The requester MUST indicate its role as indicated in Section 9. If the node acts as a PASA Router it means that the address will be further delegated. Otherwise, if the node acts as a PASA Host, the address will not be further delegated. The parent, acting as IPv6 ND Registrar will process the received GAAO message and act according to [I-D.ietf-6lo-nd-gaao], and the corresponding GAAO message for the NA packet is generated. The NA message will carry the GAAO message with the AAF field set to the PASA TAAF value (see Section 11). Furthermore, the R-bit of the GAAO message in the NA message MUST be set in order to request confirmation of address usage through explicit registration. The returning GAAO message will carry as well the PASA address that the parent assigns to its child using the procedures described in Section 6. The PASA address is appended to the GAAO message (see Figure 13) and its prefix length is indicated in the PfxLen field.

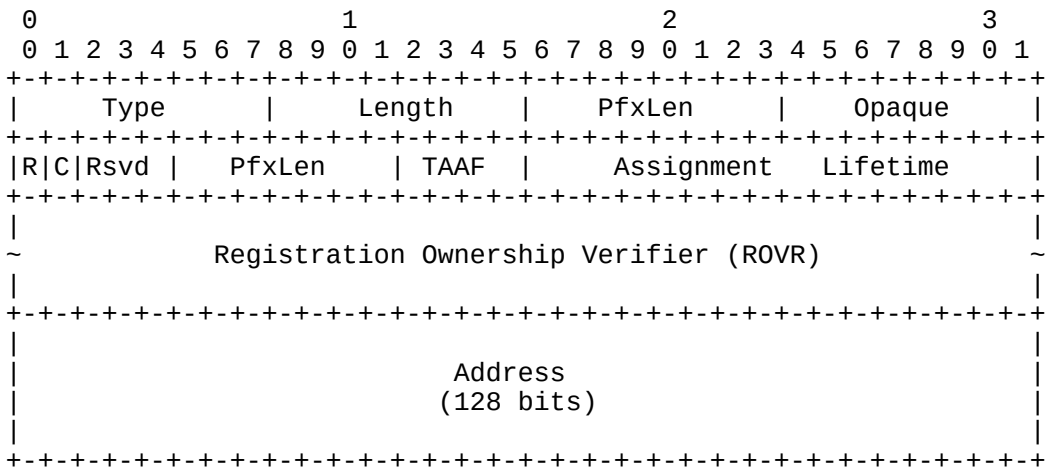


Figure 13: NA GAAO option example.

## 11. IANA Considerations

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of values related to the PASA specification, in accordance with BCP 26 [RFC8126].

### 11.1. Critical 6LoWPAN Routing Header Type for PASA-6LoRH

This document requires IANA to assign one value of the "Critical 6LoWPAN Routing Header Type" registry, to be used according to the specification in this document, as shown in Table 1.

| Value | Description | Reference |
|---|---|---|
| TBD1 | PASA-6LoRH | [This Document] |

Table 1: Critical 6LoWPAN Routing Header Type for PASA

### 11.2. PASA Address Assignment Function

This document requires IANA to assign one value from the "Address Assignment Function" registry in the "Generic Address Assignment Option" registry group, as shown in Table 2 and to be used according to the specification in this document.

| Value | AAF Name | Reference |
|---|---|---|
| TBD2 | PASA Tree Address Allocation Function | [This Document] |

Table 2: PASA TAAF.

[Temporary NOTE: This registry is not yet existing. It is defined in [I-D.ietf-6lo-nd-gaao] on which this document relies.]

## 12. Deployments Considerations

### 12.1. Topology Changes

Because PASA uses algorithmically generated addresses, based on the network topology, nodes do not generate and store forwarding table entries in the normal case. They are limited to have a default gateway and the ND table. One of the potential issues is the risk of renumbering of addresses in case of topology changes. Topology changes due to PASA Hosts joining and leaving have no real impact. It is just a matter to allocate new addresses, or re-use addresses previously assigned to PASA Host that left the network.

More structural changes, where PASA Routers are added or removed have more impact. However, because of the applicability domain of PASA, the common case of topology change is known in advance and can be planned, so to reduce disruption due to renumbering (see Section 4). Adding PASA Routers simply creates new branches in the logical tree and is not a disruptive operation. However, removing a PASA Router may require to partial renumbering the network, depending on the position of the PASA Router that is removed, and it may just involve a small branch of the tree.

### 12.2. Reliability

Another type of topology change is the case of temporary link failures or temporary node failures, where the network is still able to provide connectivity through alternative links, which is strictly related to the underlying technology, the network topology, the deployed redundancy, and the expected reliability. Failures may raise the issue of topology changes and re-numbering. Such issues can be avoided, or at least mitigated, following the procedure in Section 5.7 of [RFC8505] and keeping state in non-volatile memory.

Reliability of external connectivity, with more than one node functioning as gateway, can be achieved in several ways. One simple solution is to use a multi topology approach, where each gateway acts

as a root for a logically independent topology, identified via a different prefix. The multiple topologies can either be used at the same time or with a primary/backup policy. This solution is particularly suitable in case the PASA Domain is multihomed.

An alternative solution is to separate root and gateway roles, setting up the topology so that some of the children of the root will also function as gateways, offering external connectivity. In this way traffic destined outside the local PASA Domain will still forwarded using a simple default route toward the root, and then sent outside when they reach one of the root's children or the root itself. This second solution allows to accommodate load balancing external connectivity through the selection of the nodes that offer gateway service.

A third solution consists in creating a PASA Root backup with the same address using the Virtual Router Redundancy Protocol (VRRP [RFC9568]). However, in order to offer full resilience, the address allocation state in the primary PASA Root has to be duplicated in the secondary PASA Root.

One last resort, to ensure reliability, is to use a routing protocol, however, such a solution, would annihilate the advantages of the PASA addressing scheme, namely the stateless forwarding.

A more in-depth discussion about reliability, including the case of multiple roots, can be found in [I-D.li-6lo-pasa-reliability]. Furthermore, specific reliability solutions depend as well on the specific Address Assignment Function used (different from the one presented in this document).

## 13. Security Considerations

Communication in a PASA Domain is based on [RFC4944], [RFC6282], and [RFC8138], hence, the security considerations of those specifications apply here as well.

This document re-uses mechanisms defined in [RFC8505] and [I-D.ietf-6lo-nd-gaao], as such the security considerations of both documents apply to this specification. In particular, the link layer SHOULD provide protection to prevent potential attacks, for instance using [MACSec]. Recommendations listed in Section 7 of [RFC8505] SHOULD be applied as well to this specification.

As discussed in Section 6.2, depending on the AAF in use, the number of available addresses may encounter some limitation. A rogue node may leverage on this knowledge to carry out address exhaustion attacks by impersonating different nodes and performing multiple registrations to specific PASA Routers. Such kind of attacks can be mitigated using cryptographic signatures (e.g., [RFC3971]).

## 14. Privacy Considerations

Depending on the AAF, the algorithmically built addresses may reveal topology information outside the PASA Domain. In particular the Tree Assignment Function (TAAF) proposed in this specification reveals the path between the root and a node. For instance, let us take the example of the address 2001:db8::2B/64. Knowing that this address belongs to a PASA Domain using the AAF of this specification implies that the PASA address is 0x2B, which in binary form is b101011. The trailing bit 1 exposes the fact that this is a PASA Host, whose parent has the address 1010, meaning a PASA Router, whose parent is 10 (just looking at the preceding 0, cf. Section 6), a PASA Router directly connected to the root. So, this leads to the path: 1 -> 10 -> 1010 -> 101011. This example is build based on the topology in Figure 6. In scenarios where it is preferable to conceal the topology of the PASA Domain, it is advisable to deploy address privacy protection mechanisms (e.g., using opaque addresses for external communications [RFC7217]).

## Acknowledgements

This document received many comments and help from community people. Erik Kline, Tommaso Pecorella, Esko Dijk, Dominique Barthel, Adnan Rashid, Michael Richardson, Brian Carpenter, did provide technical comments for this document. The authors would like to thank all of them. Thanks also to Carles Gomez for his thorough shepherd review of the document.

## References

### Normative References

[I-D.ietf-6lo-nd-gaao]
Iannone, L., Lou, D., and A. Rashid, "Generic Address Assignment Option for 6LoWPAN Neighbor Discovery", Work in Progress, Internet-Draft, draft-ietf-6lo-nd-gaao-07, 2 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6lo-nd-gaao-07>.

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

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/rfc/rfc4291>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/rfc/rfc4944>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/rfc/rfc6282>.

[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, <https://www.rfc-editor.org/rfc/rfc6550>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/rfc/rfc7400>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", RFC 8138, DOI 10.17487/RFC8138, April 2017, <https://www.rfc-editor.org/rfc/rfc8138>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/rfc/rfc8505>.

Informative References

[CHING21] Ching, T., Aman, A., Azamuddin, W., Sallehuddin, H., and Z. Attarbashi, "Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery", 2021 3rd International Cyber Resilience Conference (CRC) pp. 1-6, DOI 10.1109/crc50527.2021.9392475, January 2021, <https://doi.org/10.1109/crc50527.2021.9392475>.

[DOMOTICS] "Home automation", n.d., <https://en.wikipedia.org/wiki/Home_automation>.

[I-D.li-6lo-pasa-reliability] Li, G., Lou, D., and L. Iannone, "Reliability Considerations of Path-Aware Semantic Addressing", Work in Progress, Internet-Draft, draft-li-6lo-pasa-reliability-04, 18 September 2024, <https://datatracker.ietf.org/doc/html/draft-li-6lo-pasa-reliability-04>.

[LEE10] Lee, M., Zhang, R., Zheng, J., Ahn, G., Zhu, C., Park, T., Cho, S., Shin, C., and J. Ryu, "IEEE 802.15.5 WPAN mesh standard-low rate part: Meshing the wireless sensor networks", IEEE Journal on Selected Areas in Communications vol. 28, no. 7, pp. 973-983, DOI 10.1109/jsac.2010.100902, September 2010, <https://doi.org/10.1109/jsac.2010.100902>.

[LI22] Li, G., Lou, D., and L. Iannone, "Topological addressing enabling energy efficient IoT communication", Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing pp. 12-17, DOI 10.1145/3527974.3545722, August 2022, <https://doi.org/10.1145/3527974.3545722>.

[LPWAN] "IPv6 over Low Power Wide-Area Networks (lpwan) WG", n.d., <https://datatracker.ietf.org/wg/lpwan/about/>.

[MACSec] "IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security", IEEE standard, DOI 10.1109/ieeestd.2006.245590, September 2008, <https://doi.org/10.1109/ieeestd.2006.245590>.

[NEUMANN15] Neumann, A., Lopez, E., and L. Navarro, "Evaluation of mesh routing protocols for wireless community networks", Computer Networks vol. 93, pp. 308-323, DOI 10.1016/j.comnet.2015.07.018, December 2015, <https://doi.org/10.1016/j.comnet.2015.07.018>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/rfc/rfc3971>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/rfc/rfc4193>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/rfc/rfc7217>.

[RFC8163] Lynn, K., Ed., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks", RFC 8163, DOI 10.17487/RFC8163, May 2017, <https://www.rfc-editor.org/rfc/rfc8163>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/rfc/rfc8724>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/rfc/rfc8799>.

[RFC8966] Chroboczek, J. and D. Schinazi, "The Babel Routing Protocol", RFC 8966, DOI 10.17487/RFC8966, January 2021, <https://www.rfc-editor.org/rfc/rfc8966>.

[RFC9354] Hou, J., Liu, B., Hong, Y., Tang, X., and C. Perkins, "Transmission of IPv6 Packets over Power Line Communication (PLC) Networks", RFC 9354, DOI 10.17487/RFC9354, January 2023, <https://www.rfc-editor.org/rfc/rfc9354>.

[RFC9453] Hong, Y., Gomez, C., Choi, Y., Sangi, A., and S. Chakrabarti, "Applicability and Use Cases for IPv6 over Networks of Resource-constrained Nodes (6lo)", RFC 9453, DOI 10.17487/RFC9453, September 2023, <https://www.rfc-editor.org/rfc/rfc9453>.

[RFC9568] Lindem, A. and A. Dogra, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 9568, DOI 10.17487/RFC9568, April 2024, <https://www.rfc-editor.org/rfc/rfc9568>.

[RS485] "TIA-485-A Revision of EIA-485", n.d..

[SCHC] "Static Context Header Compression (schc) WG", n.d., <https://datatracker.ietf.org/wg/schc/about/>.

[SIXLO] "IPv6 over Networks of Resource-constrained Nodes (6lo) WG", n.d., <https://datatracker.ietf.org/wg/6lo/about/>.

[SIXLOWPAN] "IPv6 over Low power WPAN (6LoWPAN) - Concluded WG", n.d., <https://datatracker.ietf.org/wg/6lowpan/about/>.

[UNIX] Ritchie, D., Johnson, S., Lesk, M., and B. Kernighan, "UNIX Time-Sharing System: The C Programming Language", Bell System Technical Journal vol. 57, no. 6, pp. 1991-2019, DOI 10.1002/j.1538-7305.1978.tb02140.x, July 1978, <https://doi.org/10.1002/j.1538-7305.1978.tb02140.x>.

[ZigBee] "ZigBee Wireless Networks and Transceivers", Elsevier edited-book, DOI 10.1016/b978-0-7506-8393-7.x0001-5, 2008, <https://doi.org/10.1016/b978-0-7506-8393-7.x0001-5>.

## Contributors

Rong Long
China Mobile
No. 53, Xibianmen Inner Street, Xicheng District
Beijing
100053
China
Email: longrong@chinamobile.com

Kiran Makhijani
Futurewei
United States of America

Email: kiranm@futurewei.com

## Authors' Addresses

Luigi Iannone (editor)
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour
92100 Boulogne-Billancourt
France
Email: luigi.iannone@huawei.com

Guangpeng Li
Huawei Technologies
Beiqing Road, Haidian District
Beijing
100095
China
Email: liguangpeng@huawei.com

David Lou
Huawei Technologies Duesseldorf GmbH
Riesstrasse 25
80992 Munich
Germany
Email: zhe.lou@huawei.com

Peng Liu
China Mobile
No. 53, Xibianmen Inner Street, Xicheng District
Beijing
100053
China
Email: liupengyjy@chinamobile.com

Pascal Thubert
06330 Roquefort-les-Pins
France
Email: pascal.thubert@gmail.com