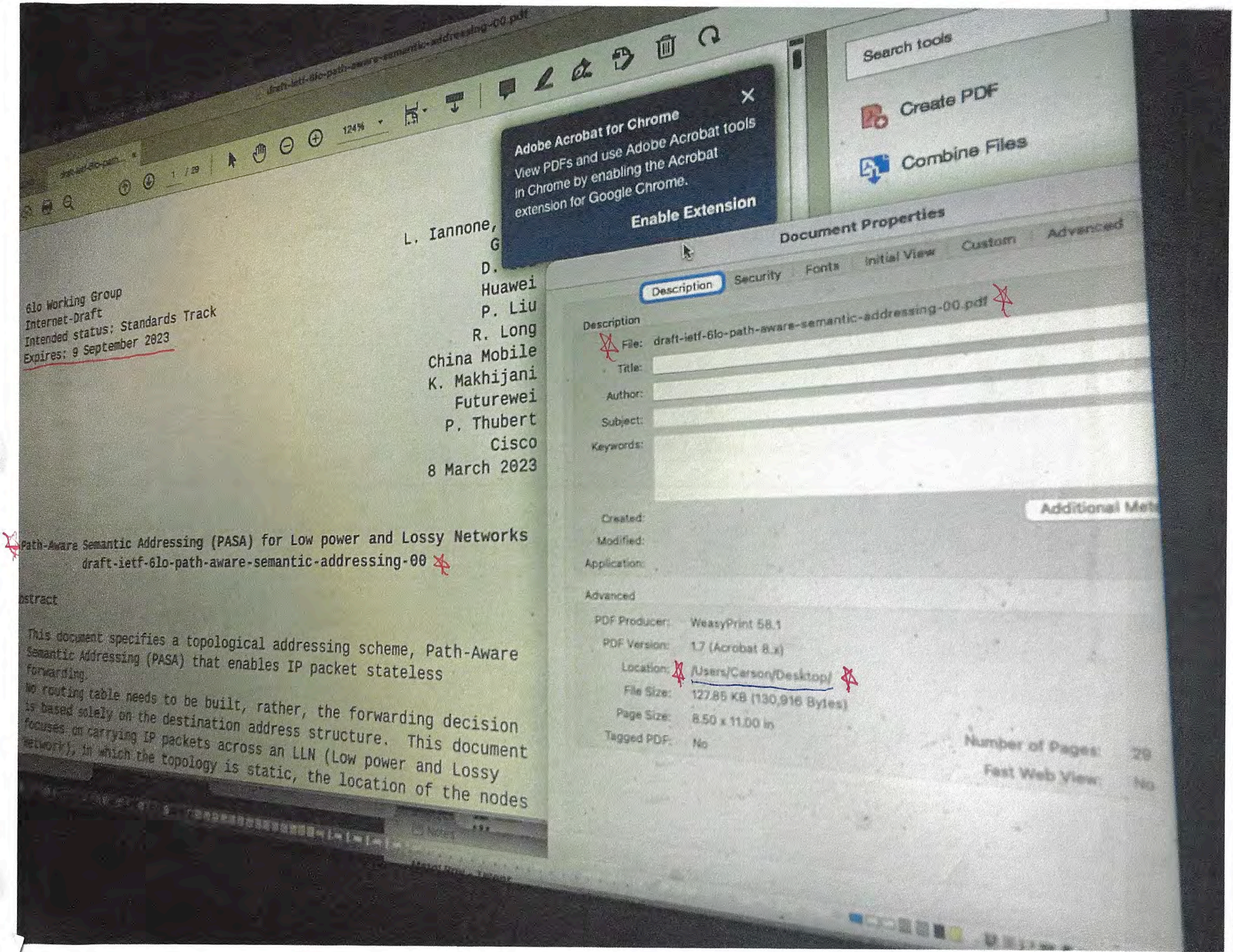


**Adobe Acrobat for Chrome**

View PDFs and use Adobe Acrobat tools in Chrome by enabling the Acrobat extension for Google Chrome.

**Enable Extension**

6lo Working Group
Internet-Draft
Intended status: Standards Track
Expires: 9 September 2023

L. Iannone,
G
D.
Huawei
P. Liu
R. Long
China Mobile
K. Makhijani
Futurewei
P. Thubert
Cisco
8 March 2023

Path-Aware Semantic Addressing (PASA) for Low power and Lossy Networks
draft-ietf-6lo-path-aware-semantic-addressing-00

bstract

This document specifies a topological addressing scheme, Path-Aware Semantic Addressing (PASA) that enables IP packet stateless forwarding.
No routing table needs to be built, rather, 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 etwork), in which the topology is static, the location of the nodes

Description

File: draft-ietf-6lo-path-aware-semantic-addressing-00.pdf
Title:
Author:
Subject:
Keywords:

Created:
Modified:
Application:

Advanced

PDF Producer: WeasyPrint 58.1
PDF Version: 1.7 (Acrobat 8.x)
Location: /Users/Carson/Desktop/
File Size: 127.85 KB (130,916 Bytes)
Page Size: 8.50 x 11.00 in
Tagged PDF: No
Number of Pages: 29
Fast Web View: No

6Lo Working Group
Internet-Draft
Intended status: Experimental
Expires: 19 June 2023

G. Li
D. Lou
L. Iannone
Huawei
P. Liu
R. Long
China Mobile
K. Makhijani
Futurewei
P. Thubert
Cisco

16 December 2022

Semantics = Relations b/w Vocabulary/
+ the knowledge Vocab represents

Semantics can be computed + inferred based on
the relations b/w attributes + feature set

# Path-Aware Semantic Addressing (PASA) for Low power and Lossy Networks
## draft-li-6lo-path-aware-semantic-addressing-01

## Abstract

This document specifies a topological addressing scheme, Path-Aware Semantic Addressing (PASA) that enables IP packet stateless forwarding.
No routing table needs to be built, rather, 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 static, the location of the nodes is fixed, and the connection between the nodes is also rather stable. This specifications describes the PASA architecture, along with PASA address allocation, forwarding mechanism, header format design, including length-variable fields, and IPv6 interconnection support.

## Status of This Memo

This Internet-Draft will expire on 19 June 2023.

Copyright Notice

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 3
2. Requirements Notation . . . . . . . . . . . . . . . . . . . . 4
3. Comprehensive Use Cases . . . . . . . . . . . . . . . . . . . 4
  3.1. Smart Grid . . . . . . . . . . . . . . . . . . . . . . . . 4
  3.2. Smart Home . . . . . . . . . . . . . . . . . . . . . . . . 5
  3.3. Data Center Monitoring . . . . . . . . . . . . . . . . . . 6
  3.4. Industrial Operational Technology Networks . . . . . . . . 8
4. Architectural Overview . . . . . . . . . . . . . . . . . . . . 9
5. PASA Allocation . . . . . . . . . . . . . . . . . . . . . . . 12
  5.1. PASA Addresses and IPv6 Addresses . . . . . . . . . . . . 15
  5.2. Limitation of Number of Child Nodes . . . . . . . . . . . 16
6. The PASA-6LoRH Header . . . . . . . . . . . . . . . . . . . . 16
  6.1. PASA-6LoRH Sequence . . . . . . . . . . . . . . . . . . . 16
  6.2. PASA-6LoRH Format . . . . . . . . . . . . . . . . . . . . 17
  6.3. PASA-6LoRH and LOWPAN_IPHC co-existence . . . . . . . . . 17
7. Forwarding in a PASA Network . . . . . . . . . . . . . . . . . 19
  7.1. Forwarding toward a local PASA endpoint . . . . . . . . . 19
  7.2. Forwarding toward an external IPv6 address . . . . . . . 21
8. PASA Address Configuration . . . . . . . . . . . . . . . . . . 22
9. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 23
  9.1. Critical 6LoWPAN Routing Header Type for PASA-6LoRH . . . 23
  9.2. Allocation Function Registry . . . . . . . . . . . . . . 24
  9.3. Address Registration Option Flags . . . . . . . . . . . . 24
10. Reliability Considerations . . . . . . . . . . . . . . . . . 25
11. Security Considerations . . . . . . . . . . . . . . . . . . . 25
Acknowledgements . . . . . . . . . . . . . . . . . . . . . . . . 25
References . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
  Normative References . . . . . . . . . . . . . . . . . . . . . 26
  Informative References . . . . . . . . . . . . . . . . . . . . 27
Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 28

## 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.

Particularly driven by the requirements stemming from Industry 4.0, Smart Grid and Smart City deployments, more and more devices/things are 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] 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 leverage on the presence of a routing protocol, are suitable in generic IoT scenarios and LLN networks. The above technologies leverage topology discovery or routing mechanisms, whereas there are several special-purpose networks, where routing protocols are not deployed and the networks are statically manageable [I-D.ietf-6lo-use-cases] (e.g. PLC [I-D.ietf-6lo-plc] or MS/TP [RFC8163], and Industrial IoT technologies like [RS485], etc.). In those 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 with that allows to avoid the use of routing protocol in favor of a topological stateless forwarding algorithm (see Section 3).

This specification document leverages on the 6Lo Routing Header (6LoRH) af 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 bandwidth. Compared to RPL-based routing [RFC6550], PASA avoids the extra overhead of address assignment by integrating address assignment and tree forming together. Furthermore, PASA provides much smaller forwarding table size than storing mode RPL.

## 2. Requirements Notation

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] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Comprehensive Use Cases

As mentioned in Section 1, the [I-D.ietf-6lo-use-cases] provides some 6lo use cases with wired connectivity, tree-based topology, and no mobility requirement (cf. Table 2 of [I-D.ietf-6lo-use-cases]). These use cases, where PASA can be used, include Smart Grid, Smart Building, etc. The PASA solution utilizes stable and static 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 extreme simple, few lines of code is sufficient to implement the stack. It enables the solution being ported onto extreme constrained nodes. In the following paragraphs, we will dive deeper into a few use cases to demo the applicability of the PASA solution.

### 3.1. 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 CBB. 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.

```
                            +---Voltage Transformer
                            |
                 +----------+-----------+
                 | PDC    +-+-+         |   SCB:Smart Circuit Breaker
                 |        |SCB|         |   PCS:Phase Change Switch
                 |        +-+-+         |   CBB:Cable Branch Box
                 |   +------+-------+   |   PDC:Power Distribution
                 | +-+-+  +-+-+   +-+-+ |       Cabinet
                 | |SCB|  |SCB|   |SCB| |
                 | +-+-+  +-+-+   +-+-+ |
                 +-+---------+-------+--+
                  /          |       +-------------------------+
                 /           +----------+                      |
                /                       |                      |
   +-----------+----------+ +-----------+----------+           |
   | CBB       |          | | CBB       |          |  Chargers |
   |   +-------+------+   | |   +-------+------+   |      ++   |
   | +-+-+   +-+-+  +-+-+ | | +-+-+   +-+-+  +-+-+ |      ||---+
   | |SCB|   |SCB|  |SCB| | | |SCB|   |SCB|  |SCB| |      ++   |
   | +-+-+   +-+-+  +-+-+ | | +-+-+   +-+-+  +-+-+ |      ++   |
   +---+-------+------+---+ +---+-------+------+---+      ||---+
       |       |      |         |       |      |          ++   |
       |       |      |       +-++    +-++ +--++
    +-+-+    +-+-+  +-+-+     +--+    +--+ +--+|
    |PCS|    |PCS|  |PCS|     Monitors for end |
    +---+    +---+  +---+                      |
                                   +CBB--------+----------+
                                   |  +--------+-------+  |
                                   |+-+-+   +-+-+    +-+-+|
                                   ||SCB|   |SCB|    |SCB||
                                   |+---+   +---+    +---+|
                                   +----------------------+
```

Figure 1: The topology of smart grid.

### 3.2. Smart Home

Smart home or home domotica is another example, as shown in figure 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.
- The smart home automation requires any to any communication.
- Lightweight communication stack with limited MCU and RAM consumption is desired.

```
                            /----------\
                           |  Internet  |
                            \-----+----/
                                  |
                           +------+------+
                           | Home Gateway|
                           +------+------+
                                  |
                   +--------------+----------------------+
+------------------|----++--------|-----------++---------|---------+
|                  |    ||        |           ||         |  Kitchen|
|  Living       +--+---+||    +---+--+ Bedroom||     +---+--+      |
|  Room         |PLC-R |||    |PLC-R |        ||     |PLC-R |      |
|               +---+--+||    +--+---+        ||     +---+--+      |
|                   |   ||       |            ||         |         |
|  +-----+-----+----+   ||  +----+--+------+  ||  +------+------+  |
|  |     |     |    |   ||  |       |      |  ||  |      |      |  |
|  |     |     |    |   ||  |       |      |  ||  |      |      |  |
| /+\   /+\   /+\  /+\  || /+\     /+\    /+\ || /+\    /+\    /+\ |
||   | |   | |   ||   | |||   |   |   |  |   ||||   |  |   |  |   ||
| \-/   \-/   \-/  \-/  || \-/     \-/    \-/ || \-/    \-/    \-/ |
|      Switches    Door ||Strip  Voice   Sound||Boiler Fridge  Dish|
|Light     door bell    ||Light  Command Boxes||             Washer|
+-----------------------+|       Device       |+-------------------+
                         +--------------------+
```

Figure 2: The topology of smart home.

### 3.3. Data Center Monitoring

Data centers is a significant infrastructure, which requires numerous safeguards in place to protect hardware assets against cyber-attacks. Besides, environmental issues such as extreme temperature, high humidity, water leakage and high dust concentration can cause device failures as well. 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 theFigure 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.

```
   NMS:Network Management System  /----\             //------\\
   SC :Supervisor Center         /      \          ||          ||
   FSU:Field Supervisor Unit    |   SC   +---------+|    NMS   ||
                                 \      /            \\------//
                                  \----/
                                 /      \
                               /         \
                           /----\         \
                          /      \          \
                         |   SC   |          \
                          \      /            \
                           \--X-/              \
                          /     \               \
                        /         \               \
                      /             \              \
                   /-/-\           /-\-\           /---\
                  | FSU |         | FSU |         | FSU |
                   \-X-/           \-X-/           \-X-/
                   /   \           /   \           /   \
                  /     \         /     \         /     \
               +---+   /--\    +---+   /--\    +---+   /--\
               |   |  |    |   |   |  |    |   |   |  |    |
               |   |  |    |   |   |  |    |   |   |  |    |
               +---+   \--/    +---+   \--/    +---+   \--/
               Smart   dumb    Smart   dumb    Smart   dumb
              Device  Device  Device  Device  Device  Device
```

Figure 3: The topology of 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 second. 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 relay 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 is 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.

### 3.4. 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 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.

- 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.

```
                  IPV6    +------+------------+
          +---------------| HMI/MES/FW/Gateway|----------+
          | PASA          +------+------------+          |
          |                                              |
     +----|------------------+                           | PASA
     | +--+---+              |                           |
     | |PLC   |--------------+-----------+               |
     | +---+--+              |           |      +--------+---------+
     |    | profinet         |  +--------+----+ |        |         |
     |    |                  |  |   +-----+   | |     +--+--+      |
     | +-----+-----+-----+   |  |   | PLC |   | |     | PLC |      |
     | |     |     |     |   |  |   +--+--+   | |     +--+--+      |
     | |     |     |     |   |  |      |      | |        |         |
     | /+\   /+\   /+\   /+\  |  | profi|bus   | |        |  modbus |
     | \-/   \-/   \-/   \-/  |  | +----+---+  | | +------+------+  |
     |  sensors/actuators    |  |  |       |  | | |      |      |  |
     | cell-site-A           |  |  |       |  | | |      |      |  |
     +-----------------------+  | /+\     /+\ | | /+\   /+\    /+\ |
                                | \-/     \-/ | | \-/   \-/    \-/ |
                                |             | | sensors/actuators|
                                | cell site B | | cell site C      |
                                +-------------+ +------------------+
```

Figure 4: Industrial Operational Technology Network topology.

## 4. 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 IPv6 prefix and the PASA itself (see Section 5.1). Inside the PASA domain, nodes communicate with each other by using only PASA addresses. It is a smaller addressing space compared to the huge IPv6 addressing space, but enabling stateless forwarding using the PASA-6LoRH header (see Section 6). 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.

```
                /|\             Internet (IPv6)
                 |             --------+--------
     IPv6 Domain |                     |
                 |                     |
                 |             +-------+-------+
   -------------------------   | Border Router |
                 |             |  (PASA Root)  |
                 |             +---------------+
                 |
                 |                       O
                 |
                 |               O        O  O
                 |                 O O
                 |            O                  O
     PASA Domain  |                         O
                 |         O      O O         O    O  O
                 |              O
                 |                    O   O
                 |                               O
                 |              O
                 |
                \|/         Low-Power and Lossy Network
```

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. There is typically only one root node in the PASA network.

- PASA Root: The root node is the router responsible for the management of the whole PASA network and routing/forwarding both internal and external traffic. It uses the address Allocation Function (AF) and performs the address assignment for its children. After successful address assignment, the root will keep the state of its direct children. The root node functions as gateway between the PASA domain and the Internet. As such it also operates the translation between LOWPAN_IPHC and IPv6 formats (cf. Section 7).

- PASA Router: A PASA Router is an internal node, different from the root, having least one child. It 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 right 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 an 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.

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]).

The address assignment described in this document relies on the address registration mechanism described in [RFC8505] (see Section 8). Each node acquiring a PASA address firstly needs to select a parent node by choosing among the nodes that replied with an Router Advertisement (RA) after an initial Router Solicitation (RS). A "first come first served" selection policy is sufficient. Then it registers its link-local address to the selected parent, asking at the same time for a PASA address. In its reply the parent will propose an address according to the node's role (indicated in the request). The proposed address is algorithmically calculated using an Allocation Function (AF). 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 neighbors.

The overall design objective is centered on reducing the size (or completely avoid the usage) of routing/forwarding table 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.

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

1. PASA Address allocation (see Section 5),
2. Stateless forwarding (see Section 7),

## 5. PASA Allocation

The basic rules of allocation include:

- Each node's address is prefixed by their parent's address.
- Routers (Root and routers) run an AF (Allocation Function) to generate its children's addresses.
- All nodes run the same AF in the same network instance.
- The maximum length of the PASA address MUST NOT exceed 64 bits.

Normally, the root role is assigned to the border router when the LLN bootstraps. An example of a possible result of a PASA deployment is shown in Figure 6.

```
                             root           +--------------------------+
                                  1         | append more bits to form |
                                  0 ----+   | brother's address        |
                               /  |  \   \  +--------------------------+
                              /   |   \    \
                             /    |    \     \
      +-------------+      /      |     \      \
      | PASA Router | 10 /       11   110\       \  111
      +-------------+  0 -        0       0        0
                     / |\ \               | \
                   /   | \  \             |  \
                 /     |  \    \          0   0
               /       |    \    \
           100/    1010|   101   1011   +--------------+
             0         0      0      0  |Prefix is '10'|
            /|        /|                +--------------+
           / |       / |
          0  0      0  0        +-----------+
       1001 10011 10101 101011  | PASA Host |
                                +-----------+
```

Figure 6: An example of PASA addresses allocation.

Every router node stores and maintain 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. The '+' symbol indicates a concatenation operation. The b() operation indicates the binary string of '1' with length equal to its argument, for instance b(3) returns '111'. The allocation function AF(role,i) used in this document is defined as:

```
AF(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 indexes of respectively the routers and the hosts at this layer (starting at 0). Taking the example of the topology in Figure 6, the proposed AF works as follows.

At the top level, there are 4 children of root, 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 AF as follows:

* For the first child, which is a router:

  - A('router', 0, 0) = '1'(root address) + b(0) + '0' = '1' + '' + '0' = 10

  - Index 'r' is increased by one and is now equal 1 (r=1)

* For the second child, which is a host:

  - A('host', 1, 0) = '1'(root address) + b(0) + '1' = '1' + '' + '1' = 11

  - Index 'h' is increased by one and is now equal 1 (h=1)

* For the third child, which is a router:

  - A('router', 1, 1) = '1'(root address) + b(1) + '0' = '1' + '1' + '0' = 110

  - Index 'r' is increased by one and is now equal 2 (r=2)

* For the fourth child, which is a host:

  - A('host', 2, 1) = '1'(root address) + b(1) + '1' = '1' + '1' + '1' = 111

  - Index 'h' is increased by one and is now equal 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 AF as follows:

* For the first child, which is a router:

  - A('router', 0, 0) = '10'(node address) + b(0) + '0' = '10' + '' + '0' = 100

  - Index 'r' is increased by one and is now equal 1 (r=1)

- For the second child, which is a host:

  - A('host', 1, 0) = '10'(node address) + b(0) + '1' = '10' + '' + '1' = 101

  - Index 'h' is increased by one and is now equal 1 (h=1)

- For the third child, which is a ruoter:

  - A('router', 1, 1) = '10'(node address) + b(1) + '0' = '10' + '1' + '0' = 1010

  - Index 'r' is increased by one and is now equal 2 (r=2)

- For the fourth child, which is a host:

  - A('host', 2, 1) = '10'(node address) + b(1) + '1' = '10' + '1' + '1' = 1011

  - Index 'h' is increased by one 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 AF algorithmically assigns addresses to the different nodes without the need to know the topology in advance. However, the largest address of the network will depend on the actual topology. Indeed, the maximum length of an address with the proposed AF 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 leaves, 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 l index which is the number of leaves minus one (because the first leaf has index 0), in this case since there are 4 leaves, 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 leaf address, and one for the final 1 the ends all leaves 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.

The Allocation Function can be different from the one defined in this specifications, where all nodes know which one to use by configuration (cf. Section 9). The use of one and only one AF is allowed in a PASA domain and MUST be the same for all nodes. It is RECOMMENDED that implementations support at least the AF proposed in this document.

Different allocation functions may, for example, leverage on a priori knowledge of the topology in order to optimize the maximum address size and make it smaller. For instance, because the order of address allocation has an impact on the size, the address of children with the largest subtree should be allocated in the first place so to reduce the average address length of the whole subtree. Also, knowing the traffic in advance, or being able to have an estimation, can help to minimize the size of addresses that have a lot of traffic. This kind of optimization can be an option, the specification of optimizations is out of the scope of this document and may be defined in new Allocation Functions to be added to the "Allocation Function Registry" (see Section 9).

## 5.1. PASA 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 bits. 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 6.3). The PASA is assigned by the root or router as previously described.

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

### 5.2. Limitation of Number of Child Nodes

The maximum number of child nodes is determined by the specific AF 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 AF used as example in this document does not need any specific setup network by network, though it is still limited by the maximum length of addresses. For the special case of the parent connecting to huge amount of children, a variant of the proposed AF can be designed to fulfill the requirement and optimize the address allocation (as previously described).

## 6. The PASA-6LoRH Header

The 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 mechanism 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.

### 6.1. PASA-6LoRH Sequence

The extension octets typical sequence for a compressed 6LowPAN packet with PASA Routing Header is shown in Figure 7, following the specification of [RFC8138].

```
+-----------+----...----+--------...------+----...----+
|  11110001 | PASA-6LoRH |   LOWPAN_IPHC   |  Payload  |
|  Page 1   |   Type 8   |                 |           |
+-----------+----...----+--------...------+----...----+
```

Figure 7: A lowPAN encapsulated IPv6 header compressed packet with PASA-6LoRH and LOWPAN_IPHC headers.

Where:

- PASA-6LoRH: is the PASA specific extension. See Section 6.2 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.

### 6.2. PASA-6LoRH Format

The format of the PASA-6LoRH header, is shown in Figure 8.

```
  0                                       1
  0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| 1 | 0 | 0 | Rsvd  |   Size    |          6LoRH Type           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|            Octet 1            |           Octet 2             |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
~                              ...                              ~
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|            Octet N-1          |          Octet N              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
            Where N = Size + 1, and 6LoRH Type = PASA
```

Figure 8: 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).

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

In a PASA domain every node has to use PASA and being able to compress/uncompress 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 6.2. 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 of the destination address is an address outside the PASA domain, there is not need to use the the PASA-6LoRH header, since the packet just need 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 111110, 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.

## 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. For external communications, the root is responsible to perform the translation between PASA addresses and IPv6 addresses. For instance, for a packet entering into the PASA domain, the root will extract the PASA of the destination from the suffix of the IPv6 address, reducing it to the smallest set of quad that can contain the address, by removing all leading octets that are just equal to 0x00. The the root will compress the original IPv6 and transport header 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 AF used. Here we will use the AF previously introduced (see Section 5) to illustrate the forwarding procedure.

### 7.1. Forwarding toward a local PASA endpoint

Inner-domain packets carry a PASA destination address in the PASA-6LoRH header. More specifically the destination address field is the address of another node in the same PASA domain. As such a PASA node performs the following sequence of actions (also see Figure 9):

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, exit. Otherwise, go to step 3.

3. If length of DA equals 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, exit.

5. Check whether CA is equal to the prefix of DA. If yes, go to step 6. Otherwise, send the packet to parent node, exit.

6. Calculate which child is the next hop address and forward packet to it. With the AF proposed in this document, such operation is reduced to reading the DA's bits starting from the position equals 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.

```
              /*\       DA:Destination Address
             |***|      CA:Current Node's Address
              \*/
               |
      +--------+--------+
      |Parse DA from pkt|
      +--------+--------+
               |
              \|/
       +-------+------+
      /                \  yes
     | Len(DA)<Len(CA)? |-------------------------------+
      \                /                                |
       +-------+------+                                 |
               | no                                     |
              \|/                                       |
       +-------+------+           +--------------+      |
      /                \  yes    /                \  no |
     | Len(DA)=Len(CA)? |------>|     CA == DA ?   |--->+
      \                /         \                /     |
       +-------+------+           +-------+------+      |
               | no                       | yes         |
              \|/                        /*\            |
       +-------+------+                 |***|           |
      /                \  no             \*/            |
     | CA==PrefixOf(DA)?|------------------------------>+
      \                /                                |
       +-------+------+                                 |
               | yes                                    |
              \|/                                      \|/
     +---------+---------+                    +---------+---------+
     | Calculate next-hop|                    | Forward to Parent |
     |         &         |                    +---------+---------+
     |      Forward      |                              |
     +---------+---------+                              |
               |<---------------------------------------+
              \|/
              /*\
             |***|
              \*/
```

Figure 9: 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 6.3. 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, so all PASA nodes (except 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 are based on RFC 8138, the source node encapsulates the 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 10.

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|0|1| Length  | 6LoRH Type 6  |  Hop Limit    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 10: 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 11.

```
+-----------+----...----+--------...------+----...----+
|  11110001 |  IP-in-IP  |   LOWPAN_IPHC    |  Payload  |
|  Page 1   |   6LoRH    |                  |           |
+-----------+----...----+--------...------+----...----+
```

Figure 11: A lowPAN encapsulated IPv6 header compressed packet with IP-in-IP and LOWPAN_IPHC headers.

## 8. PASA Address Configuration

[RFC8505] Registration Extensions for IPv6 over 6LowPAN Neighbor Discovery can be further extended to accommodate PASA address configuration. In order for a PASA node to request an address, the Extended Address Registration Option (EARO) message is uses, exploiting two of the reserved bits. The format of the EARO message is shown in Figure 12.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Length    |    Status     |    Opaque     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |Rsd|P|H| I |R|T|     TID       |     Registration Lifetime     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
   ...            Registration Ownership Verifier (ROVR)          ...
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 12: EARO Format.

All the fields in EARO message are defined in [RFC8505], except for bits P and H that are allocated by this document (see Section 9) and are defined as follows:

- PASA bit (P): If set, this flag indicates that the registration message is requesting or delivering a PASA address as part of the link-local address registration procedure.
- Host bit (H): If set, this flag indicates that the node is acting as a PASA Host, otherwise, it means that the node is acting as a PASA Router (cf. Section 4).

When a PASA node bootstraps, it typically does multicast a Routing Solicitation(RS) and receives one or more unicast Routing Advertisements (RA) messages from potential parents. it can choose a parent on a "first come first served" basis and send a Neighbor Solicitation (NS) with a EARO message to register its link-local address to the selected parent. In this EARO message it will set the P bit, to indicate that it is also requesting a PASA address. It will set the H accordingly to its intended role. The parent, acting as routing registrar will process the received EARO message and act according to [RFC8505], and the corresponding EARO message for the NA packet is generated. The NA message will carry the EARO message with the bits P and H set exactly as in the corresponding EARO message of the NS packet. If the returning status is 0, meaning "success" according to [RFC6775], the returning EARO message will carry as well the PASA address that the parent assigns to its child using the procedures described in Section 5. The PASA address is appended to the EARO message (whose length is now set to 3), so the returning format becomes the one depicted in Figure 13.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |  Length = 3   |  Status = 0   |    Opaque     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Rsd|P|H| I |R|T|     TID       |     Registration Lifetime     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Link-Local Address                       |
   |                          of the child                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Proposed  PASA Address                    |
   |                          of the child                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 13: NA EARO message example.

At this point, the child MUST register the PASA address to the same parent, but not using the P and L bits. This is in order to be in line with Section 5.6 of [RFC8505], requesting global unique addresses to be registered. Furthermore, the registration procedure has the nice property to confirm that the child accepted and will use the proposed address.

If the node that made the request is a router, it can start acting as a routing registrar so to allow other nodes to select it as a parent.

## 9. IANA Considerations

### 9.1. 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. [Note to RFC Editor: If IANA assign different values the authors will update the document accordingly]

| Value | Description | Reference |
|---|---|---|
| 8 (suggested) | PASA-6LoRH | [This Document] |

Table 1: Critical 6LoWPAN Routing Header Type for PASA

### 9.2. Allocation Function Registry

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].

IANA is asked to create a registry named "Path-Aware Semantic Addressing (PASA) Parameters".

Such registry should be populated with a one octet sub registry named "Allocation Function" and used to identify the AF used in a PASA deployment. The sub registry is populated as shown in Table 2:

| Value | AF Name | Reference |
|---|---|---|
| 0x00 | PASA Allocation Function | [This Document] |
| 0x01-0xFF | Un-assigned | |

Table 2: Allocation Function sub-registry

Values can be assigned by IANA on a "First Come, First Served" basis according to [RFC8126].

### 9.3. Address Registration Option Flags

IANA is requested to add the content show in Table 3 to the existing sub-registry "Address Registration Option Flags" under "Internet Control Message Protocol version 6".

| Bit | Description | Reference |
|---|---|---|
| 2 | P Flag | [This Document] |
| 3 | H Flag | [This Document] |

Table 3: New Address Registration Option Flags

## 10. Reliability Considerations

Because PASA uses algorithmically generated addresses based on the network topology, nodes do not generate and store forwarding table entries in the normal case. One of the potential issues is the risk of renumbering of addresses in case of topology changes. 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. Another case is temporary link failures, where the underlying technology 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.

More complex reliability scenarios and alternative solutions are beyond the scope of this document, which is focused only on the address allocation framework and stateless forwarding. Furthermore, specific reliability solutions can depend as well on the specific Allocation Function used (different from the one presented in this document). Reliability is discussed in more details in [I-D.li-6lo-pasa-reliability].

## 11. Security Considerations

An extended security analysis will be provided in future revision of this document. As of this point we consider that the security considerations of [RFC4944], [RFC6282], [RFC8138], and [RFC8505] apply.

## Acknowledgements

This document received many discussion and help from community people. 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.

## References

### Normative References

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

[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/info/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/info/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/info/rfc6550>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[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/info/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/info/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/info/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/info/rfc8505>.

## Informative References

[I-D.ietf-6lo-plc]
Hou, J., Liu, B. R., Hong, Y., Tang, X., and C. E. Perkins, "Transmission of IPv6 Packets over PLC Networks", Work in Progress, Internet-Draft, draft-ietf-6lo-plc-11, 18 May 2022, <https://www.ietf.org/archive/id/draft-ietf-6lo-plc-11.txt>.

[I-D.ietf-6lo-use-cases]
Hong, Y., Gomez, C., Choi, Y., Sangi, A. R., and S. Chakrabarti, "IPv6 over Constrained Node Networks (6lo) Applicability & Use cases", Work in Progress, Internet-Draft, draft-ietf-6lo-use-cases-14, 24 October 2022, <https://www.ietf.org/archive/id/draft-ietf-6lo-use-cases-14.txt>.

[I-D.li-6lo-pasa-reliability]
Li, G., Lou, Z., and L. Iannone, "Reliability Considerations of Path-Aware Semantic Addressing", Work in Progress, Internet-Draft, draft-li-6lo-pasa-reliability-00, 24 October 2022, <https://www.ietf.org/archive/id/draft-li-6lo-pasa-reliability-00.txt>.

[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", DOI 10.1109/jsac.2010.100902, IEEE Journal on Selected Areas in Communications vol. 28, no. 7, pp. 973-983, September 2010, <https://doi.org/10.1109/jsac.2010.100902>.

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

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

[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/info/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/info/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/info/rfc8799>.

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

[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/>.

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

## Authors' Addresses

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

Luigi Iannone
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour

92100 Boulogne-Billancourt
France

Email: luigi.iannone@huawei.com

Peng Liu
China Mobile
No. 53, Xibianmen Inner Street, Xicheng District
Beijing
100053
China

Email: liupengyjy@chinamobile.com

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

Pascal Thubert
Cisco Systems, Inc.
France

Email: pthubert@cisco.com

FUTUREWEI
Technologies

# New IP based semantic addressing and routing for LEO satellite networks

Lin Han, Alvaro Retana, Cedric Westphal, Richard Li
Futurewei Technologies, Inc.
U.S.A
{lhan,alvaro.retana,cedric.westphal,rli}@futurewei.com

Tianji Jiang, Meiling Chen
China Mobile
P.R.China
{tianjijiang,chenmeiling}@chinamobile.com

**Lin Han**
Distinguished Engineer
Network Technology Lab
Futurewei Technologies Inc.

FUTUREWEI INTERNAL

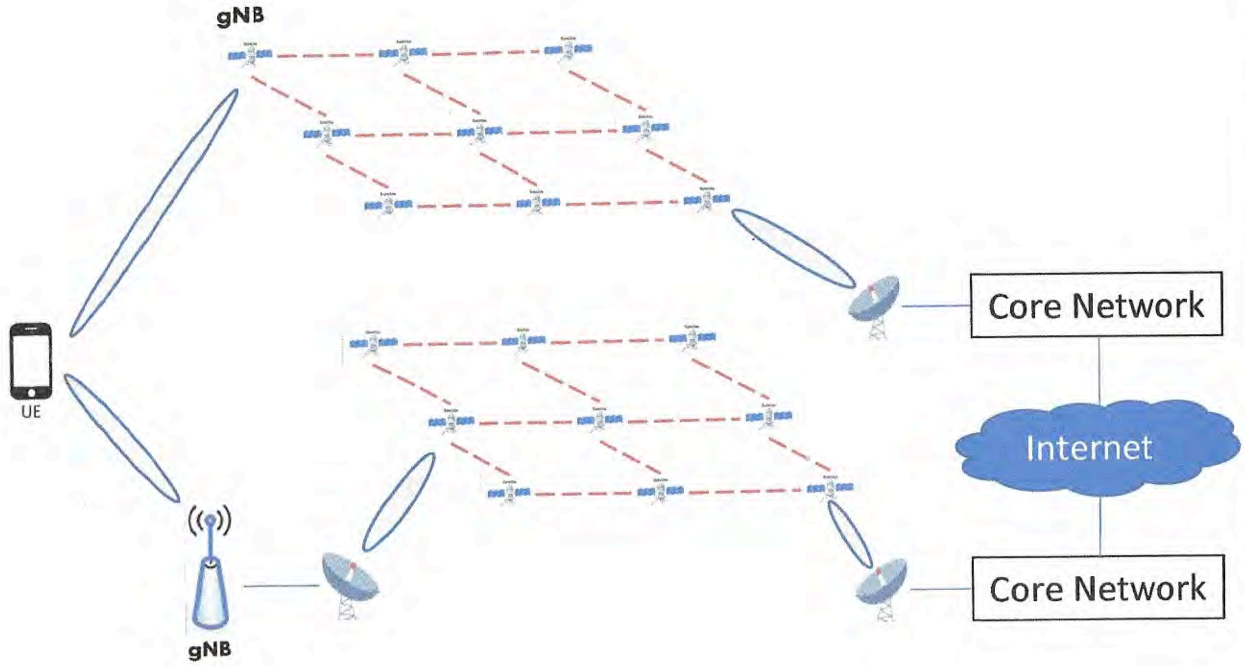
# Agenda

- LEO Satellite Network Status in Industry and SDOs
- IP networking for LEO in the future
- Challenging to the current IP networking technologies
- New IP based solution:
  - New IP review
  - Addressing
    - Semantic address for LEO Satellite
  - Routing
    - New solution summary
    - Control Plane: New IP based OSPF
    - Data Plane: Instructive routing
- Experiments
- Summary: IPv6 Solution vs New IP Solution

# LEO satellite network status – Industry

- StarLink
  - As of September 2022, over 2,300 functioning satellites, over 500,000 active subscribers
  - has started the ISL experiment from 2022. and provide service for polar area soon.
- Apple has started to provide emergency service for iphone14 by Globalstar LEO
  - Short msg with very low rate (<10k bps), sending only
  - Globalstar LEO is very small and early stage: (8 orbit planes) x (6 satellites/per orbit plane) at 1414 km altitudes, inclination 52°.
- Huawei has started to provide short msg service for new phone Mate50 by China GPS Beidou system
  - Limited size of msg with very low rate, sending only
  - Using GEO/MEO (3600km/21500km) from Beidou satellites (GPS satellites)
  - Is working to provide dual-directional messaging
- T-mobile and StarLink will collaborate to provide service from 2023

# LEO satellite network status –3GPP
# LEO satellite network for NTN integration, Key for 5G+ and 6G



LEO satellite network as 5G Access Network
- gNB on satellite
- DU and CU can be separated on satellite and ground respectively
- CN can be completely or partially (i.e, UPF) on satellite
- Radio: Based on 5G NR for Ku, Ka band
- Architecture: SBA with enhancements
- Satellite network:
  - IP network to support 5G functions and interworking with other network in Internet

LEO satellite network as 5G Back haul
- gNB on ground
- CN can be completely or partially (i.e, UPF) on satellite
- Radio: 5G NR or other technologies
- Satellite network:
  - If want to support 5G functions and interworking with other networks in Internet, must be IP network

# LEO satellite network status – IETF
# Slow but Start work for LEO satellites

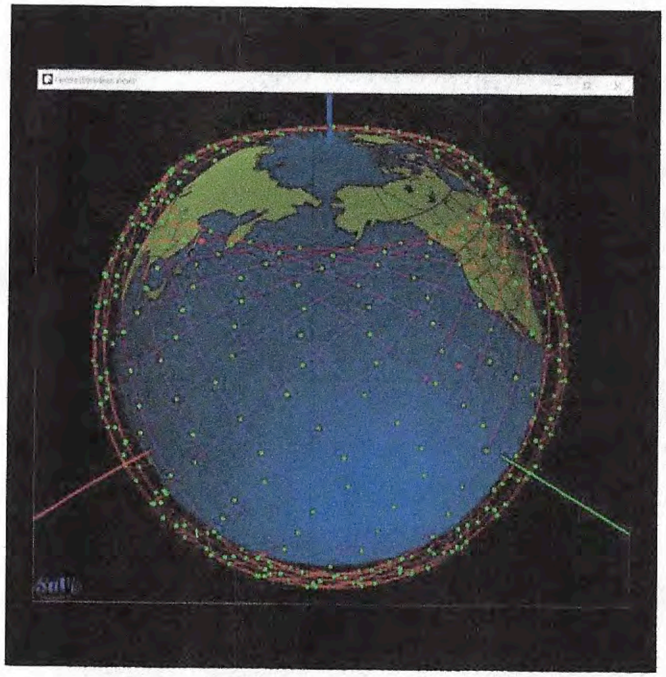
- IP over Satellite Links (ipsat) WG: IP over GEO, closed for unknown reason, and no output.
- Delay/Disruption Tolerant Networking (DTN WG): for GEO and inter-planetary communication, not fitting for LEO (due to short delay, less tolerance for disruption)
- L4 work
  - TCP Over Satellite (TCPSAT WG)
  - RFC2488, RFC2760,
- Network Coding for Satellite System: RFC8975
- SATCOM side meeting on IETF111
- Current drafts related to satellite network not belonging to any existing WG:
  - draft-li-istn-addressing-requirement
  - draft-jliu-istn-savi-requirement
  - draft-lai-bmwg-istn-methodology
  - draft-lhan-problems-requirements-satellite-net
  - draft-retana-lsr-ospf-monitor-node
  - draft-lhan-satellite-semantic-addressing
  - draft-lhan-satellite-instructive-routing
  - draft-kw-rtgwg-satellite-rtg-add-challanges-00

FUTUREWEI Technologies

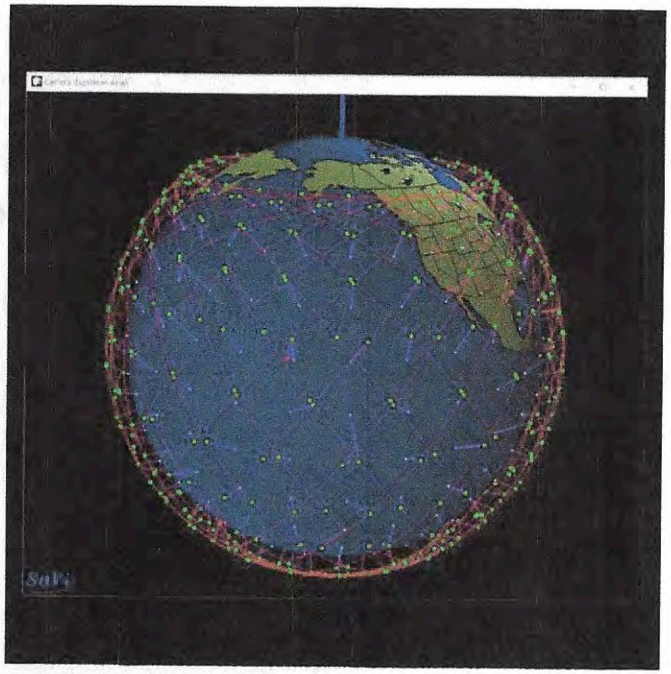
# IP networking for LEO in the future

- Why IP networking is needed
  - Large scale network with over 10k nodes connected by ISL and million sat-ground-station links
  - Interworking with other networks in Internet for NTN integration
  - 3GPP expected satellite network as part of wireless access or back haul, must support IP and 5G functions (i.e, UPF distribution in satellites)
- Problems for current IP networking technologies for LEO
  - Addressing, Routing, Traffic Engineering, Multi-path, Mobility
  - All current protocols will experience the issues when used for LEO (OSPF, IS-IS, BGP, MPLS, TE, MIPv6, DTN, etc.)
  - ☆ ISL link bandwidth is very precious (< tens of Gbps dependent on the distance), needs to save it as much as we can.
  - ☆ The most fundamental problem is routing. Without solving this, all other protocols, both from IETF and 3GPP, cannot work properly.
    - The usability of IGP will be dramatically reduced (<20%) due to the frequent LSA update caused by link flipping.
    - The BGP is hard to converge due to the frequent BGP update caused by link flipping.
    - The un-converged network can lead to IP routing table un-stable and un-usable. Thus, the IP packet forwarding is not reliable (packet loop or drop).

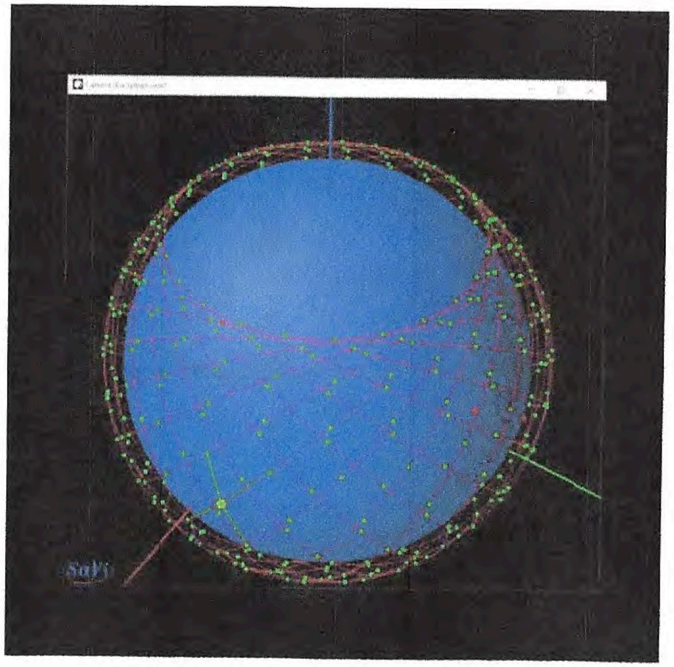
# LEO satellite constellation-
# Challenging to the current IP networking technologies



- LEO satellites move at ~7.x km/s with ~100min period
- 50% satellites move on different direction with another 50% satellites and form a dynamic interleaved network
- Earth is self-rotating at ~463m/s



- links between satellites and ground station (GS) will flip every ~5min for LEO satellites (~550 km altitude), distance keeps changing
- One satellite has multiple GS connected
- One GS has multiple satellites connected
- Huge number of Sat-GS links (> million)

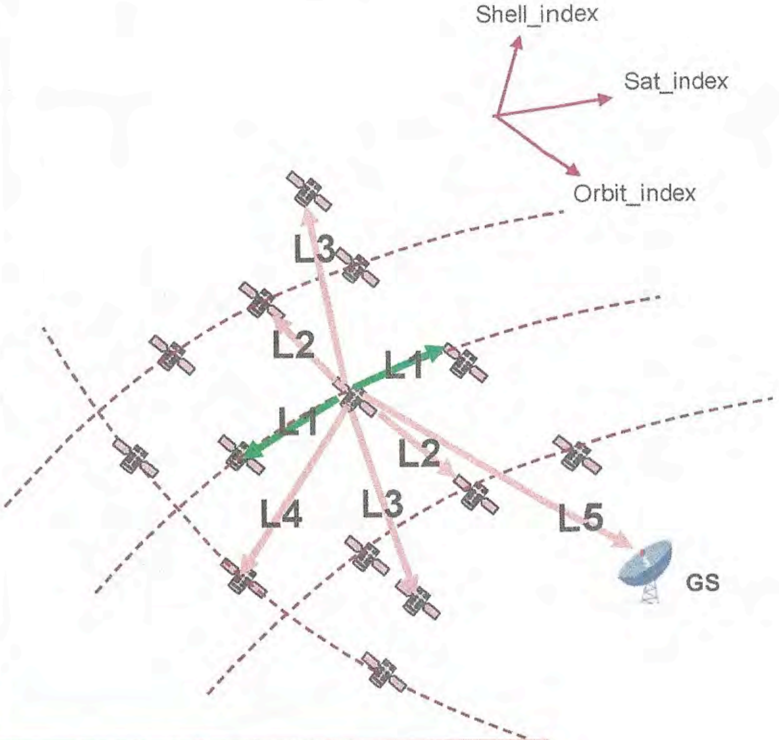


- ISL distance for satellites on adjacent orbits keep changing
- ISL direction swaps on polar areas

Simulation is by savi: https://savi.sourceforge.io/

# Routing: How to handle Links Life and Link Metrics?

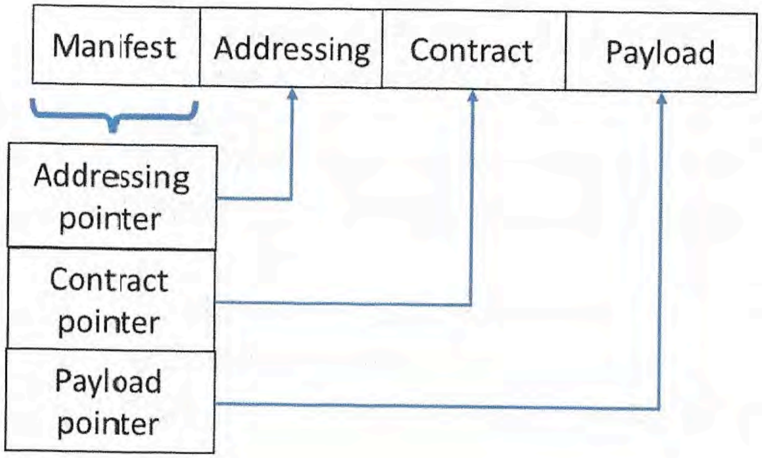
| Link type | Description | Link Life | Link Metrics |
|---|---|---|---|
| L1 | Between adjacent satellites on the same orbit plane | Steady | Steady |
| L2 | Between two satellites on the adjacent orbit | Unsteady, lasts tens of mins | Keep changing |
| L3 | Between two satellites on the adjacent orbit shell | Unsteady, lasts tens of mins | Keep changing |
| L4 | Between two satellites on the un-adjacent orbit | Unsteady, lasts couple of mins | Keep changing |
| L5 | Between satellite and ground station | Unsteady, lasts couple of mins | Keep changing |



Traditional routing protocol: detect the link state and measure the link metrics, populate LSA update
New IP routing protocol: only detect the link state and populate the LSA update, link metrices are calculate periodically when necessary.

FUTUREWEI Technologies

# New IP review
# a new protocol for LEO satellite routing solution



**Addressing** (for Omni-Convergence)
- Free Choice Addressing
    IPv4, IPv6, Lisp, Flexible Addressing System, Others
- Mix and Match

**Contract**
- KPI guarantee
    - In-time guarantee
    - On-time guarantee
    - Lossless networking
- User Programmable networking

**Payload**
- Native stream of Bits and Bytes
- Qualitative Payload
- Semantic Payload

- Routing protocol packet hdr use Non-IP satellite address
- 32-bit length
- LEO specific semantics

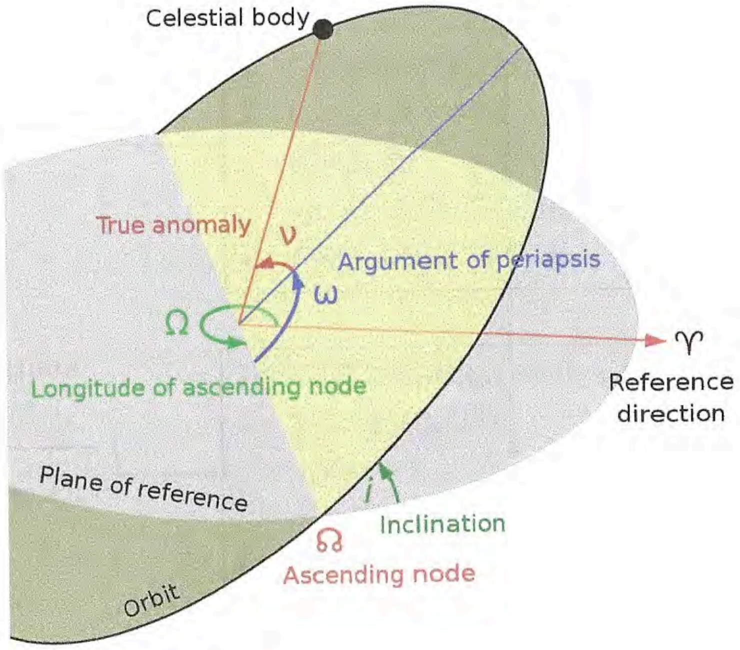
- User packet use Programmability for routing
- Instructive semantics
- Agnostic to address of user src/dest

FUTUREWEI Technologies

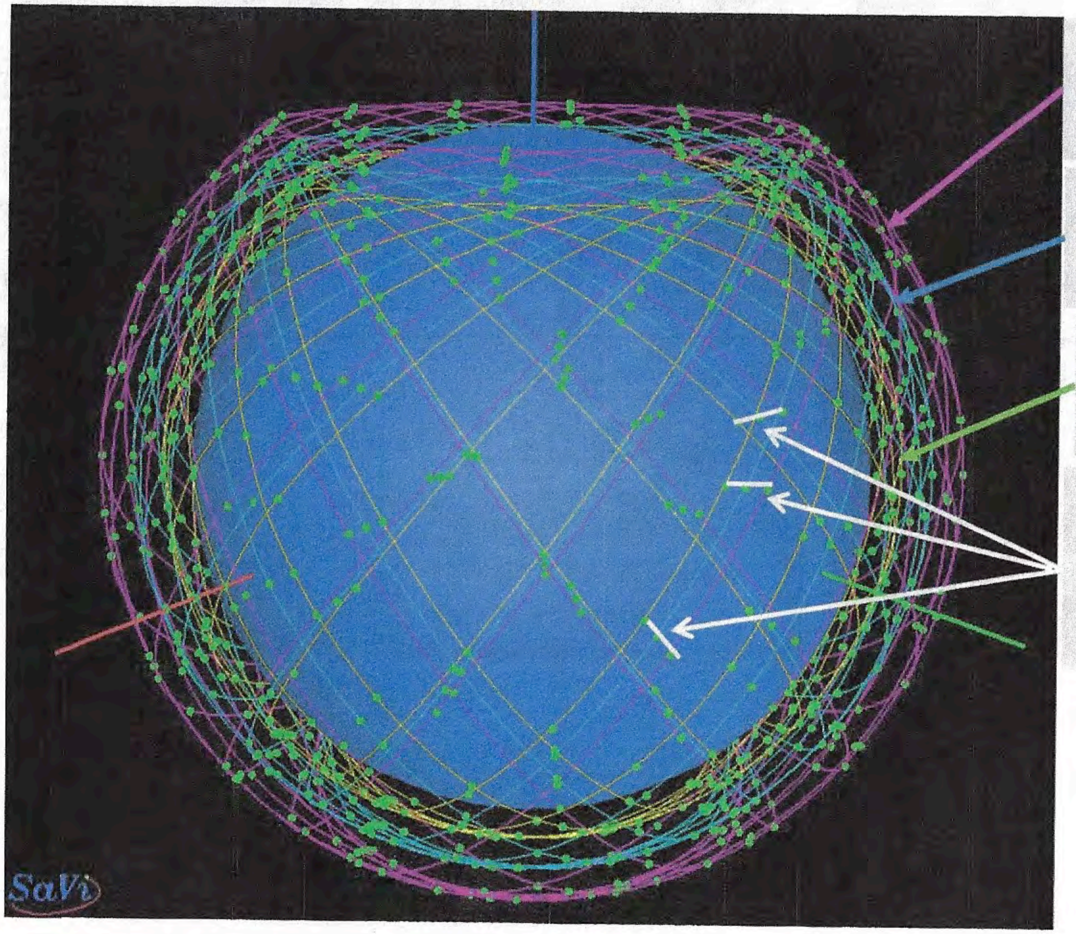
# Semantic Address for LEO satellites

- All satellites in LEO constellation are organized by
  - Altitude, Inclination
  - Longitude of Ascending Node
  - True Anomaly
- A scheme to uniquely identify a LEO satellite
  - 3 indexes to indicate the relative sequence value of orbit parameters
  - Indexes values assigned never changes even satellite is moving
  - Shell_Index: related to the {Altitude, Inclination}
  - Orbit_Index: related to the Longitude of the ascending node ($\Omega$)
  - Sate_Index: related to the True anomaly ($\nu$)
- Not IPv4/IPv6 address or prefix

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Owner Code  |  Shell_Index  |  Orbit_Index  |   Sat_Index   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



# Shell_index and associated segment



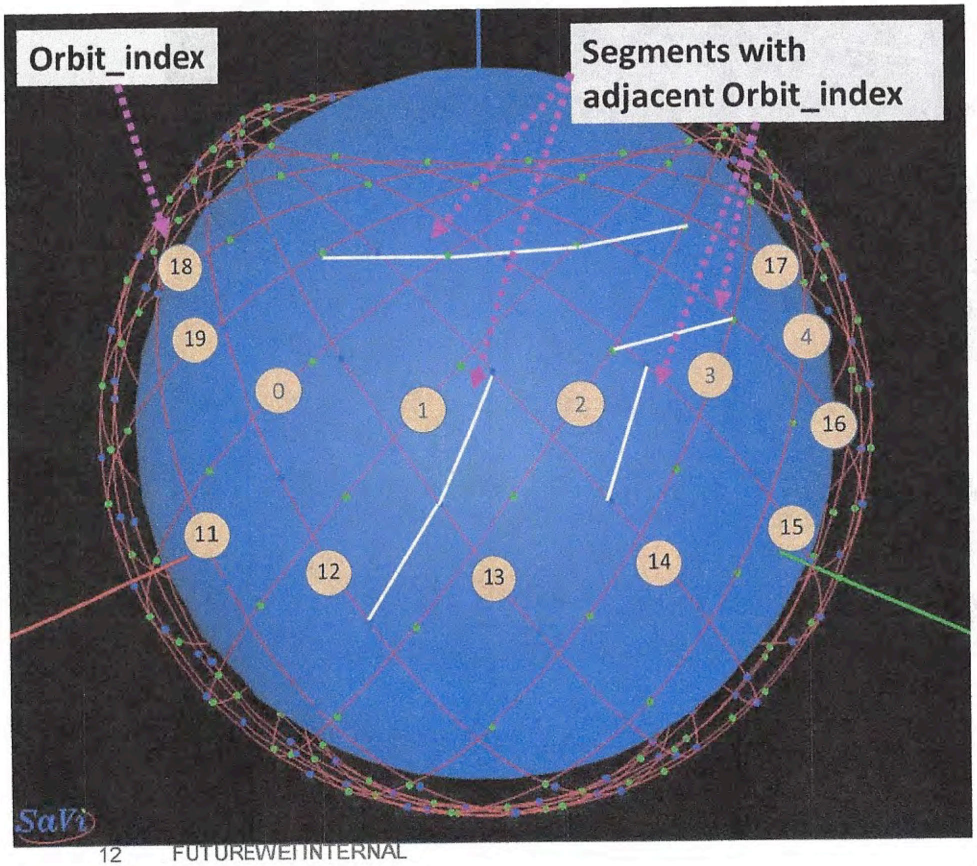
**Shell_index=2**
**(altitude = 1500km)**

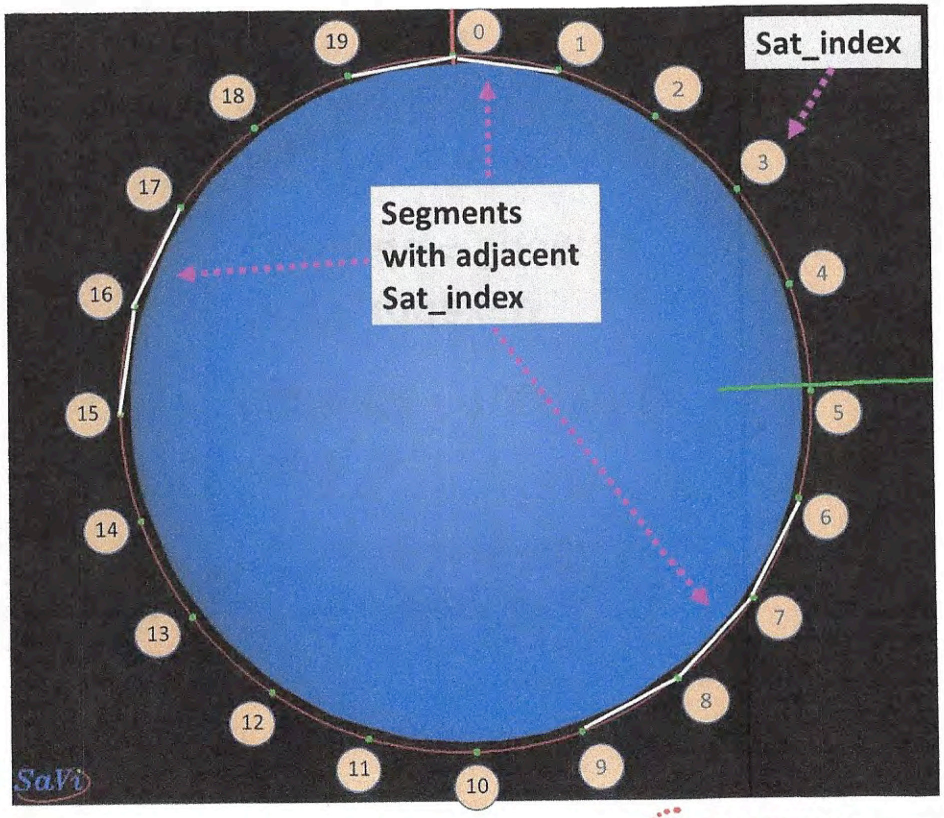
**Shell_index=1**
**(altitude = 1000km)**

**Shell_index=0**
**(altitude = 500km)**

**Segments with adjacent Shell_index**

# Orbit_index, Sat_Index and associated segment



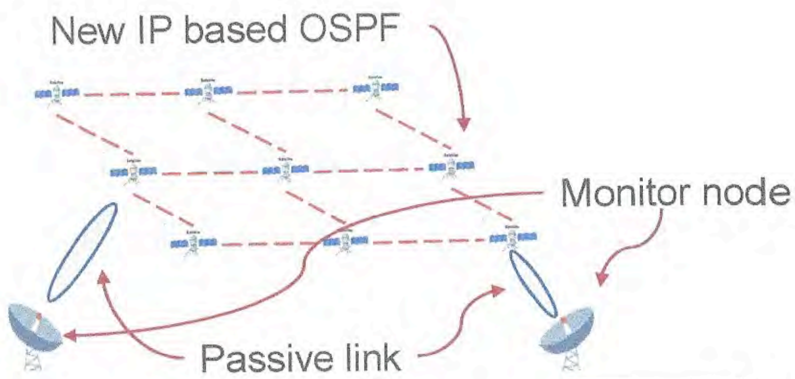


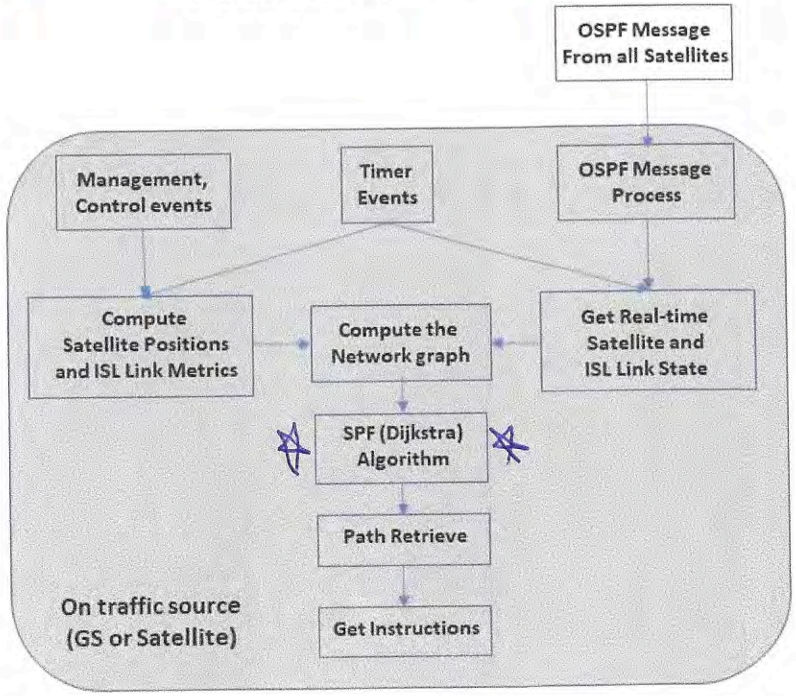
# Routing – New solution summary

- Control Plane: New IP based OSPF
  - New IP address family (address is TLV defined)
  - Router ID = Satellite Semantic Address
  - Satellites and ground-stations run OSPF
  - All nodes only populate Router LSA and attached network LSA
  - Sat-Ground links are passive, its flipping does not trigger the LSA
  - Ground stations receive LSA, but not advertise
  - Only traffic source, i.e, GS, calculate SPF tree, satellites does the SPF calculation unless it will send packets to others.
  - Path info (IP hop list) is retrieved from SPF tree.
- Data Plane: Instructive-semantics based routing
  - Periodically trigger OSPF at traffic source to calculation link metrics and SPF tree. retrieve the path info.
  - From path info -> segments-> instructions
  - Instructions embedded into user packet

# Control Plane:
# New IP based OSPF

- New IP address family (address is TLV defined)
- Router ID = Satellite Semantic Address
- Satellites and ground-stations run OSPF
- All nodes only populate Router LSA and attached network LSA
- Sat-Ground links are passive, its flipping does not trigger the LSA
- Ground stations receive LSA, but not advertise
- Only traffic source, i.e, GS, calculate SPF tree, satellites doe not unless send packets to others
- Periodically trigger OSPF at traffic source to calculation all link metrics and SPF tree
- Retrieve the path info from SPF tree
- Path info -> segments-> instructions




**OSPF Message From all Satellites**

**Management, Control events**

**Timer Events**

**OSPF Message Process**

**Compute Satellite Positions and ISL Link Metrics**

**Compute the Network graph**

**Get Real-time Satellite and ISL Link State**

**SPF (Dijkstra) Algorithm**

**Path Retrieve**

**Get Instructions**

On traffic source (GS or Satellite)

# Data Plane:
# Instructive Routing

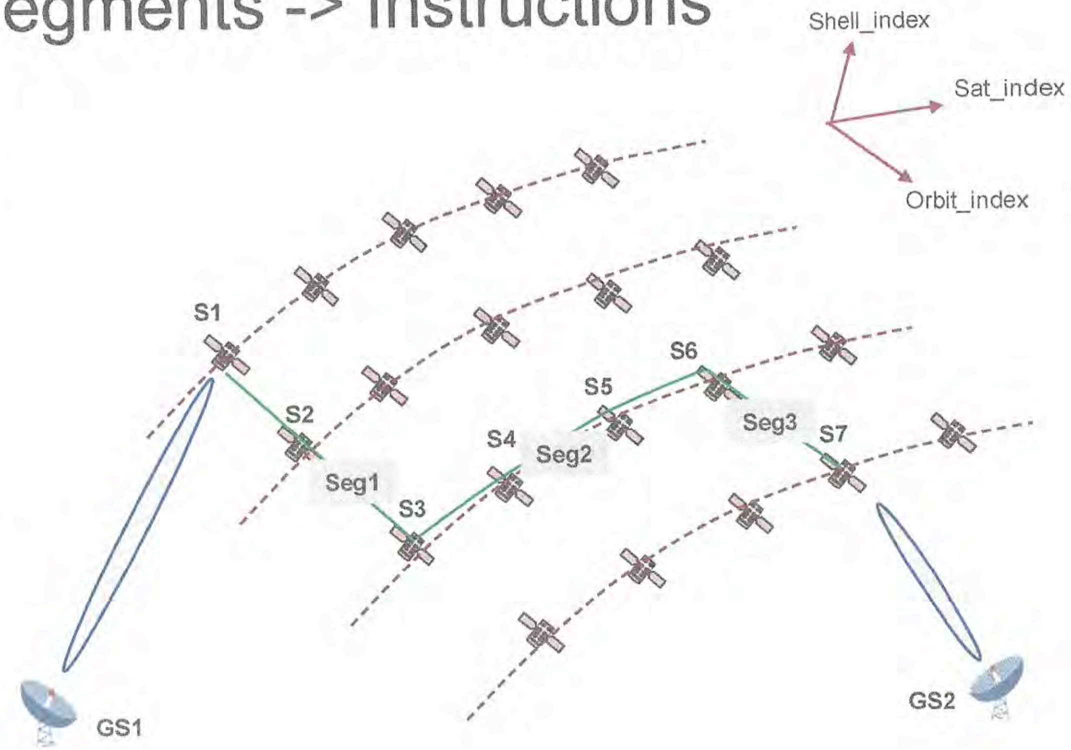
- Instructions embedded into user packet as Contract part
- Subtype Routing Programmability
- List of instructions
- Instruction = Function + Argument
- Instruction tells hardware to forward packet to specified direction and where to stop.
- Routing is no longer done by distributed routing calculation and TCAM lookup!

```
<Contract> := <Contract Clause>
          | <Contract Clause> AND <Contract>

<Contract Clause> := <Contract ECA> OR <Contract NP>

<Contract NP> := <Sat_Routing Contract>
          | <Sat_Routing Contract> AND <Contract NP>

<Sat_Routing Contract> := <Instruction>
          | <Instruction> AND <Sat_Routing Contract>

<Instruction> := <Func. Code> AND <Arguments>
          | <Func. Code> AND <Arguments> AND
            <Instruction>
```

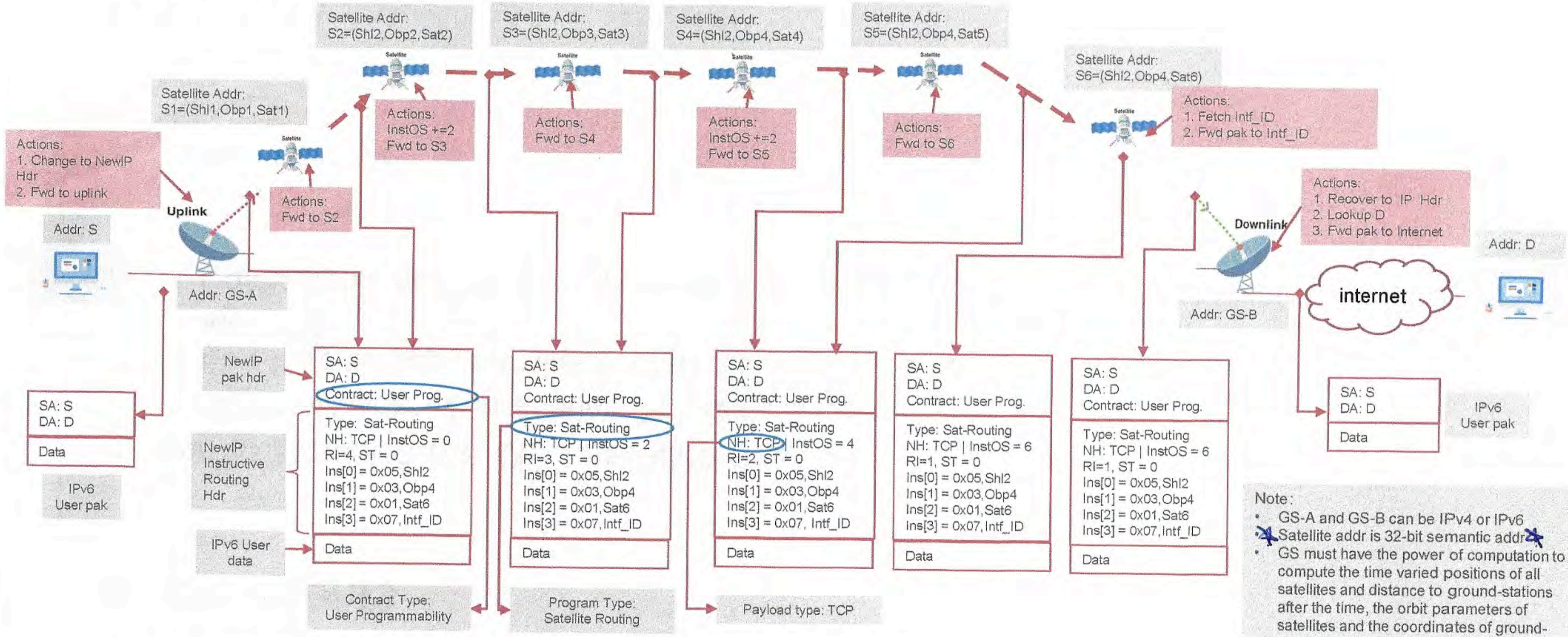
| Function Name/Hex Value | Arguments/Size (Octet) |
|---|---|
| **Fwd.Inc.Sat_Index**/0x01 | Sat_Index/1 |
| **Fwd.Dec.Sat_Index**/0x02 | Sat_Index/1 |
| **Fwd.Inc.Orbit_Index**/0x03 | Orbit_Index/1 |
| **Fwd.Dec.Orbit_Index**/0x04 | Orbit_Index/1 |
| **Fwd.Inc.Shell_Index**/0x05 | Shell_Index/1 |
| **Fwd.Dec.Shell_Index**/0x06 | Shell_Index/1 |
| **End.Intf_ID**/0x07 | Intf_ID/1 |
| **End.Punt**/0x08 | 0x0/1 |
| **End.Lookup**/0x09 | 0x0/1 |
| **End.Lookup.IPv4**/0x0A | IPv4_Addr/4 |
| **End.Lookup.IPv6**/0x0B | IPv6_Addr/4 |
| **Fwd.Sat_Addr**/0x0C | Sat_Addr/4 |
| **Fwd.Sat_MacAddr**/0x0D | Sat_MacAddr/6 |

# SPF tree -> path info -> Segments -> Instructions

- GS1 run OSPF to get SPF tree from GS1 to all destinations
- GS1 obtain the path to GS2 from SPF tree,
- GS1 to GS2 path info:
  - S1->S2->S3->S4->S5->S6->S7
- Route to segments:
  - Seg1(S1,S3) -> Seg2(S2, S6) -> Seg3(S5,S7)
  - Seg1, Seg3: Segment with adjacent Orbit_index
  - Seg2: Segment with adjacent Sat_Index
- Segments to instructions
  - Inst1: Fwd pak to the direction of Orbit_index increment until reach S3
  - Inst2: Fwd pak to the direction of Sat_index increment until reach S6
  - Inst3: Fwd pak to the direction of Orbit_index increment until reach S7
  - Inst4: Fwd pak to GS2



# New IP Instructive Routing for Satellite – Tunnel-less Mode Packet Format and Actions



Satellite Addr:
S1=(Shl1,Obp1,Sat1)

Satellite Addr:
S2=(Shl2,Obp2,Sat2)

Satellite Addr:
S3=(Shl2,Obp3,Sat3)

Satellite Addr:
S4=(Shl2,Obp4,Sat4)

Satellite Addr:
S5=(Shl2,Obp4,Sat5)

Satellite Addr:
S6=(Shl2,Obp4,Sat6)

Actions:
1. Change to NewIP Hdr
2. Fwd to uplink

Actions:
Fwd to S2

Actions:
InstOS +=2
Fwd to S3

Actions:
Fwd to S4

Actions:
InstOS +=2
Fwd to S5

Actions:
Fwd to S6

Actions:
1. Fetch Intf_ID
2. Fwd pak to Intf_ID

Actions:
1. Recover to IP Hdr
2. Lookup D
3. Fwd pak to Internet

Addr: S

Addr: GS-A

Addr: GS-B

Addr: D

SA: S
DA: D
Data

IPv6
User pak

NewIP
pak hdr

NewIP
Instructive
Routing
Hdr

IPv6 User
data

SA: S
DA: D
Contract: User Prog.
Type: Sat-Routing
NH: TCP | InstOS = 0
RI=4, ST = 0
Ins[0] = 0x05,Shl2
Ins[1] = 0x03,Obp4
Ins[2] = 0x01,Sat6
Ins[3] = 0x07,Intf_ID
Data

SA: S
DA: D
Contract: User Prog.
Type: Sat-Routing
NH: TCP | InstOS = 2
RI=3, ST = 0
Ins[0] = 0x05,Shl2
Ins[1] = 0x03,Obp4
Ins[2] = 0x01,Sat6
Ins[3] = 0x07,Intf_ID
Data

SA: S
DA: D
Contract: User Prog.
Type: Sat-Routing
NH: TCP | InstOS = 4
RI=2, ST = 0
Ins[0] = 0x05,Shl2
Ins[1] = 0x03,Obp4
Ins[2] = 0x01,Sat6
Ins[3] = 0x07, Intf_ID
Data

SA: S
DA: D
Contract: User Prog.
Type: Sat-Routing
NH: TCP | InstOS = 6
RI=1, ST = 0
Ins[0] = 0x05,Shl2
Ins[1] = 0x03,Obp4
Ins[2] = 0x01,Sat6
Ins[3] = 0x07,Intf_ID
Data

SA: S
DA: D
Contract: User Prog.
Type: Sat-Routing
NH: TCP | InstOS = 6
RI=1, ST = 0
Ins[0] = 0x05,Shl2
Ins[1] = 0x03,Obp4
Ins[2] = 0x01,Sat6
Ins[3] = 0x07,Intf_ID
Data

SA: S
DA: D
Data

IPv6
User pak

Contract Type:
User Programmability

Program Type:
Satellite Routing

Payload type: TCP

Note:
- GS-A and GS-B can be IPv4 or IPv6
- Satellite addr is 32-bit semantic addr
- GS must have the power of computation to compute the time varied positions of all satellites and distance to ground-stations after the time, the orbit parameters of satellites and the coordinates of ground-station are given

# Experiments

- Savi to simulate the LEO satellite network
  - 550km altitude; 53° inclination; 30 orbit x 30 satellites/orbit
  - Five ISLs for each satellite (four for adjacent satellites and one for non-adjacent satellite)
  - Configurable number of UL/DL: one, two, as many as possible (GS is in the coverage)

# GS-to-GS Delay estimation

$$Delay = D_P + D_{ISL}^{S} + D_{R}^{S} + D_{pak}^{p} \tag{1}$$

$$D_P = Dist/S_l \tag{2}$$

$$D_{ISL}^{S} = N_{ISL} * \frac{P_S}{S_{ISL}} = (N_{Sat} - 1) * \frac{P_S}{S_{ISL}} \tag{3}$$

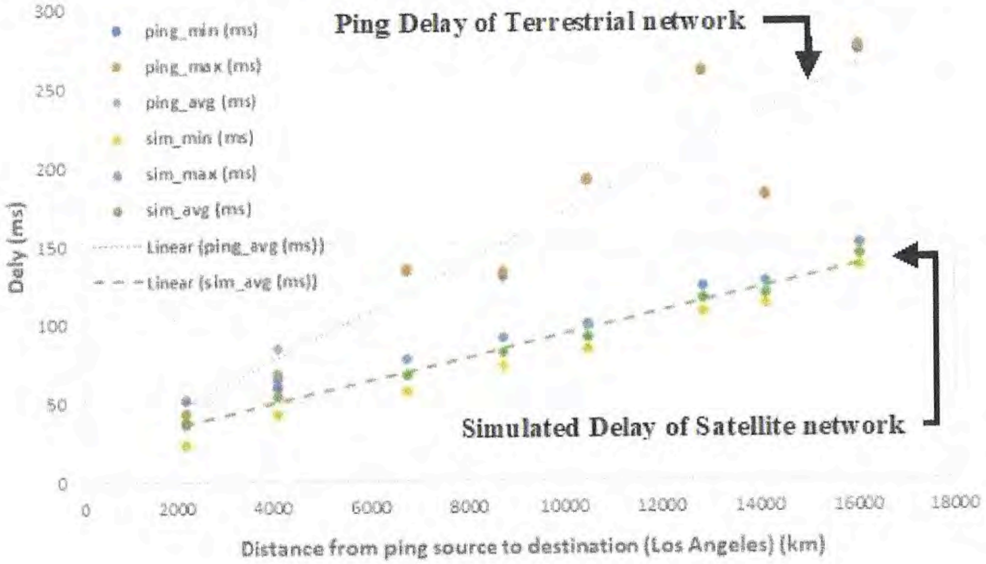
$$D_{R}^{S} = N_R * \frac{P_S}{S_R} \tag{4}$$

$$D_{pak}^{p} = (N_{Sat} + 2) d_{pak}^{p} \tag{5}$$

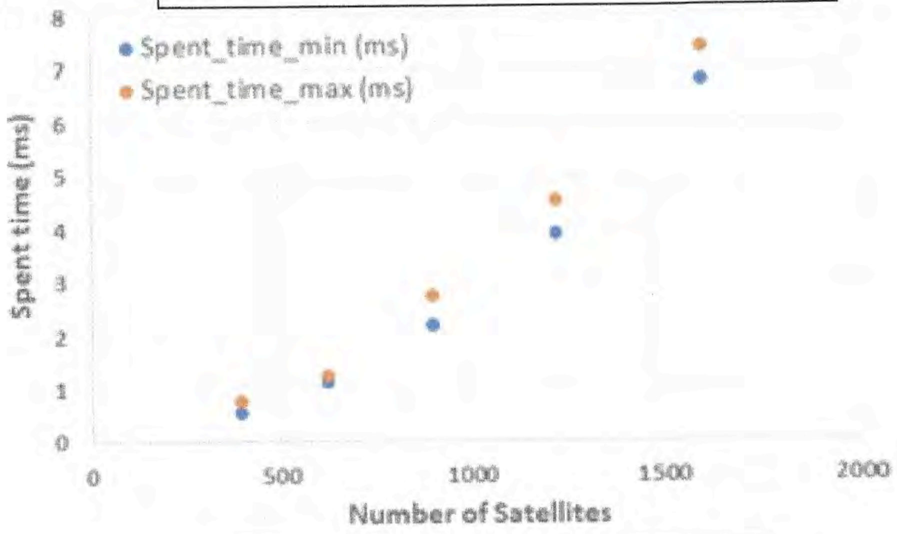
| | |
|---|---|
| $Delay$ | Total delay from src-GS to dst-GS |
| $D_P$ | Laser propagation delay in free space |
| $D_{ISL}^{S}$ | Packet transmission delay at all ISL links |
| $D_{R}^{S}$ | Packet transmission delay at all radio links |
| $D_{pak}^{p}$ | Total Packet processing delay at all satellites and GS |
| $Dist$ | Distance of the path from Src-GS to Dst-GS, obtained from simulation |
| $S_l$ | Speed of light in free space, $S_l = 300{,}000 km/s$ |
| $N_{Sat}$ | Number of satellites on the path, obtained from simulation |
| $N_{ISL}$ | Number of ISL links on the path, obtained from simulation |
| $P_S$ | Packet Size, assume $P_S = 1500 bytes$ in simulation |
| $S_{ISL}$ | ISL speed, assume $S_{ISL} = 10G\ bps$ in simulation |
| $N_R$ | Number of Radio Links, $N_R = 2$ in simulation |
| $S_R$ | Radio Link Speed, $S_R = 100\ Mbps$ in simulation |
| $d_{pak}^{p}$ | Packet processing delay at each hop, assume $d_{pak}^{p} = 100us$ in simulation |

# Delay, Performance, Salability

Simulated delay vs. Real ping delay of Internet



Time to compute SPF tree and routes



Num. of distinct path in 24 Hrs

| Src City | Distance to LA (km) | Number of path |
|---|---|---|
| Houston | 2207 | 1425 |
| Honolulu | 4117 | 1411 |
| Lima | 6727 | 1251 |
| London | 8758 | 1440 |
| Auckland | 10500 | 1307 |
| New Delhi | 12866 | 1394 |
| Singapore | 14129 | 1334 |
| Cape Town | 16056 | 1322 |

# Number of hops, and packet overhead

| Src City | Distance to LA(KM) | Hops No. (min/max) | Segment No. (min/max) |
|---|---|---|---|
| Houston | 2207 | 3/7 | 2/3 |
| Honolulu | 4117 | 5/9 | 2/4 |
| Lima | 6727 | 6/9 | 1/4 |
| London | 8758 | 10/13 | 2/7 |
| Auckland | 10500 | 8/12 | 1/4 |
| New Delhi | 12866 | 12/16 | 2/6 |
| Singapore | 14129 | 12/15 | 1/4 |
| Cape Town | 16056 | 12/18 | 2/4 |

NUMBER OF HOPS & SEGMENTS FROM THE DIFFERENT SOURCE CITY TO LA ( FOR 24 HOUR SIMULATION)

| Src City | Our method | SRv6 |
|---|---|---|
| Houston | 6/8 | 32/48 |
| Honolulu | 6/10 | 32/64 |
| Lima | 4/10 | 16/64 |
| London | 6/16 | 32/112 |
| Auckland | 4/10 | 16/64 |
| New Delhi | 6/14 | 32/96 |
| Singapore | 4/10 | 16/64 |
| Cape Town | 6/10 | 32/64 |

Packet header overhead (min/max, in octets) for different path (for 24 hour simulation)

# Summary: IPv6 Solution vs New IP Solution

| **Items** | **IPv6** | **New IP** | **New IP Benefit** |
|---|---|---|---|
| Control Plane: Network state and topology detection | • Use Modified OSPF for IPv6 (RFC5340) | • Use the OSPF that is designed for New IP address family;<br>• Similar modification should be done like Modified OSPF for IPv6; | • New IP OSPF messages have shorter size; saving link bandwidth |
| Control Plane: Source routing instruction | • Use New Routing subtype in IPv6 Extension Header | • Use New IP Programmability subtype in Contract Field | |
| Data Plane: User address type | • IPv6 | • IPv4<br>• IPv6<br>• Other address type | • New IP supports more type of user addresses |

# Thank You.

FUTUREWEI
Technologies