

6man Working Group
Internet-Draft
Intended status: Informational
Expires: 29 November 2026

J. Lee, Ed.
J. Jeong, Ed.
B.A. Mugabarigira
Sungkyunkwan University
T. Yoshihiro
Wakayama University
28 May 2026

IPv6 Wireless Access in Satellite Networks (IPWASN): Problem Statement
and Use Cases

draft-lee-6man-ipv6-satellite-networks-00

Abstract

This document describes use cases and a problem statement for IPv6 Wireless Access in Satellite Networks (IPWASN). IPWASN aims at the IPv6-based wireless access in Non-Terrestrial Networks (NTNs), that is, satellite networks. It considers NTN characteristics such as dynamic topology, multi-hop communication over inter-satellite links, High-Altitude Platform Station (HAPS)-assisted relay paths, frequent handovers, variable link quality, and intermittent connectivity. Based on these characteristics, this document identifies key challenges in applying existing IPv6 protocols to NTN environments. It also analyzes the applicability of current IPv6 mechanisms and outlines requirements to support efficient data forwarding, Quality of Service (QoS), Segment Routing (SR)-based traffic engineering, and connectivity in satellite-based networks.

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 29 November 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Terminology	5
3. IPWASN Reference Scenario	6
4. Problem Statement	8
5. Use Cases	11
6. Requirements	14
7. Security Considerations	20
7.1. Neighbor Discovery and First-hop Security	20
7.2. Mobility Management and Control-plane Security	21
7.3. Trajectory, Contact, and Privacy Considerations	21
7.4. Other Threats	22
8. References	22
8.1. Normative References	22
8.2. Informative References	23
Acknowledgments	25
Contributors	25
Authors' Addresses	27

1. Introduction

Non-Terrestrial Networks (NTNs), which integrate satellites, High-Altitude Platform Stations (HAPS), and terrestrial networks, have emerged as a key technology for next-generation wireless communication systems that aim to provide seamless global connectivity. In particular, Low Earth Orbit (LEO) satellite networks enable wide-area coverage and continuous service availability in regions where terrestrial infrastructure is limited or unavailable, such as maritime, aeronautical, and remote environments. With the rapid deployment of large-scale satellite constellations, NTNs are increasingly considered an essential component for extending communication services beyond the limitations of ground-based infrastructures.

To support NTN environments, standardization bodies have defined technologies that incorporate satellite communications into existing mobile network architectures. In 3GPP Release 17 [TS-23.501-Rel17], the fundamental architecture and procedures for NTN support are specified, including adaptations for satellite-specific characteristics such as propagation delay and Doppler effects. Furthermore, 3GPP Release 18 [TS-23.501-Rel18] extends these capabilities by addressing enhanced features such as multi-link operation, handover optimization, and the utilization of Inter-Satellite Links (ISLs). These efforts aim to enable seamless integration between satellite networks and terrestrial networks while ensuring consistent service delivery across heterogeneous environments.

In addition, routing and packet delivery mechanisms for satellite networks have been investigated by the IETF. A routing architecture for satellite networks has been defined, taking into account ISLs and dynamic link environments [RFC9717]. Segment Routing (SR) architecture [RFC8402] and the data plane of Multi-Protocol Label Switching (MPLS) [RFC8660] provide source-routing mechanisms that may be useful for traffic engineering in satellite networks, while SRv6 mechanisms based on the IPv6 Segment Routing Header [RFC8754] provide an IPv6-native approach for steering packets through selected network paths. This work highlights the need for network-layer mechanisms that can adapt to rapidly changing connectivity conditions and provide reliable data delivery across multi-hop satellite paths.

Meanwhile, the IETF has standardized a wide range of IPv6-based mechanisms to support communications in highly dynamic and mobile environments. Based on the IPv6 specification [RFC8200], mobility management protocols such as Mobile IPv6 [RFC6275], Proxy Mobile IPv6 [RFC5213], Network Mobility (NEMO) Basic Support [RFC3963], and Distributed Mobility Management (DMM) [RFC7429] have been defined to support IP-based communication across heterogeneous access networks. Furthermore, IPv6 Wireless Access in Vehicular Environments (IPWAVE) has identified key challenges related to high mobility and dynamic topology [RFC9365]. These characteristics are also present in NTN environments, making such prior work directly relevant for extending IPv6-based communication to satellite networks.

HAPS has become an important component in NTN architectures. The ITU describes HAPS systems as platforms that can support broadband connectivity and transmission links between mobile networks and core networks [ITU-HAPS]. HAPS may provide relay, aggregation, and coverage-extension functions between terrestrial users, LEO satellites, and ground stations. Academic studies on HAPS architectures have identified backhaul, public-safety, Internet of Things (IoT), and wide-area wireless service scenarios as important

deployment targets [HAPS-ARCH]. For IPWASN, HAPS introduces additional forwarding choices and additional operational constraints. This is because traffic may traverse satellite-only, HAPS-assisted, or hybrid satellite-HAPS-ground paths, depending on service requirements and link availability.

This document considers IPv6 Wireless Access in Satellite Networks (IPWASN). This IPWASN aims at the IPv6-based wireless access in NTN. It presents use cases and a problem statement of IPWASN to reflect the characteristics of satellite networks. The scope of this document includes LEO satellite-based NTN environments, multi-hop communication using ISLs, HAPS-assisted relay paths, dynamic topology, handover, intermittent connectivity, the support of Quality of Service (QoS), and IPv6-based routing, forwarding, traffic engineering, and mobility management. This document does not define a new protocol. Instead, it identifies the gaps, requirements by analyzing the existing IPv6 protocols, MPLS, SR-MPLS, SRv6, and mobility-related mechanisms. They may need to be profiled, combined, or extended for NTN environments.

In particular, data forwarding issues, including multi-hop packet delivery, path selection, service continuity, and connectivity maintenance under dynamic network conditions, remain important considerations. This document also discusses QoS considerations for latency-sensitive and bandwidth-intensive services such as text messaging, emergency data, voice, video streaming, video conferencing, and live media delivery over HTTP/3 [RFC9114] and QUIC [RFC9000]. Therefore, the further analysis of IPv6-based mechanisms is required to support efficient and reliable communications in IPv6 satellite networks.

Studies on trajectory-based data forwarding in vehicular networks show that predictable movement information can be used to improve multihop forwarding decisions. Travel Prediction-based Data Forwarding (TPD) uses shared trajectories to predict encounter opportunities and construct forwarding sequences for delay-and-delivery-ratio-aware packet delivery [TPD-COMNET-2015]. Trajectory-based Statistical Forwarding (TSF) uses a destination trajectory and packet-delay distributions to select rendezvous target points for infrastructure-to-mobile delivery [TSF-TMC-2012]. Although satellite networks differ from vehicular networks, IPWASN can use similar design insights such as predictable trajectories of satellite and HAPS, and scheduled contact opportunities can be exploited for path computation, forwarding preparation, and disruption-tolerant packet delivery.

2. Terminology

This section provides definitions of the key terms and concepts used throughout this document. The terminology is intended to establish a common understanding of the components and operational characteristics of IPv6-based wireless access in satellite networks.

- * **Non-Terrestrial Networks (NTNs):** NTN refers to a network architecture that integrates satellite systems, High-Altitude Platform Stations (HAPS), and terrestrial networks to provide wide-area communication services. In this document, NTN primarily focuses on satellite-based communication systems that extend network coverage beyond the limitations of ground-based infrastructures.
- * **Low Earth Orbit (LEO):** LEO refers to satellites operating in low Earth orbit, typically characterized by relatively low altitude and high mobility. Due to their orbital movement, LEO satellites introduce dynamic network topology and frequent link changes, which significantly impact routing and data forwarding in NTN environments.
- * **Inter-Satellite Link (ISL):** ISL refers to communication links established directly between satellites. These links enable multi-hop data forwarding across satellite networks without relying solely on ground stations, and play a key role in extending connectivity and improving network resilience in NTN environments.
- * **User Equipment (UE):** UE denotes end-user devices that access network services through NTN infrastructure. In this document, UE may include mobile terminals, IoT devices, or other communication endpoints that connect to satellite networks via service links.
- * **Ground Station (GS):** GS refers to terrestrial infrastructure that connects satellite networks to ground-based networks or the Internet. Ground stations serve as gateways for data exchange between NTN and terrestrial networks, supporting feeder links and network interconnection.
- * **High-Altitude Platform Station (HAPS):** HAPS refers to an aerial platform operating in the stratosphere and used to provide communication services or relay connectivity. In IPWASN, a HAPS may act as an intermediate node between UE, LEO satellites, ground stations, and terrestrial networks. An HAPS can assist service continuity, improve coverage in remote or disaster areas, and provide an additional path for traffic engineering when direct satellite-to-ground connectivity is limited.

- * QoS Class: A QoS class refers to a group of application flows with similar requirements for latency, jitter, packet loss, bandwidth, reliability, and priority. IPWASN considers QoS classes such as text and emergency data, voice, real-time video, bulk data, and delay-tolerant IoT traffic.
- * Segment Routing (SR): SR refers to source routing based on an ordered list of instructions called segments [RFC8402]. SR can be instantiated over the MPLS data plane as SR-MPLS [RFC8660] or over IPv6 as SRv6 using the Segment Routing Header and SRv6 network programming mechanisms [RFC8754] [RFC8986].

3. IPWASN Reference Scenario

This section describes a reference scenario for IPv6 Wireless Access in Satellite Networks (IPWASN) considered in this document. This scenario illustrates an NTN environment where a User Equipment (UE) accesses IPv6 services through a network composed of LEO satellites, Inter-Satellite Links (ISLs), HAPS nodes, ground stations, and terrestrial networks. The purpose of this scenario is to provide a common understanding of the network structure and communication paths used in the subsequent problem statement and use cases.

In this scenario, UEs may connect directly to nearby LEO satellites through service links or may connect through an HAPS relay when the HAPS provides a better access path, a more stable relay, or additional coverage. The satellites are interconnected via ISLs, forming a multi-hop network in space. HAPS nodes may provide intermediate relay, aggregation, and backhaul functions between a UE, satellites, ground stations, and terrestrial networks. Ground stations serve as gateways between the satellite/HAPS network and terrestrial networks, enabling access to the IPv6 Internet. Depending on the availability of feeder links, HAPS links, ISLs, and the relative positions of satellites and ground stations, data packets may be delivered directly to a ground station, forwarded across multiple satellites, forwarded through an HAPS, or delivered through a hybrid satellite-HAPS-ground path before reaching a gateway.

Due to the orbital movement of LEO satellites, the network topology changes continuously over time. As satellites move along their trajectories, service links between UEs and satellites are frequently re-established, and ISLs among satellites may also be dynamically created or reconfigured. HAPS nodes are more stable than LEO satellites from the viewpoint of ground users, but they still introduce additional link-state, capacity, and coverage constraints. As a result, an End-to-End (E2E) communication path between a UE and the terrestrial network may vary over time even for ongoing sessions.

In addition, connectivity between satellites and ground stations may not always be available due to geographic constraints or satellite visibility. In such cases, packets may need to be forwarded across multiple satellite hops, through an HAPS, or through another available relay until a suitable ground station becomes reachable. This introduces challenges in path selection, data forwarding, QoS preservation, and connectivity maintenance in dynamic network conditions.

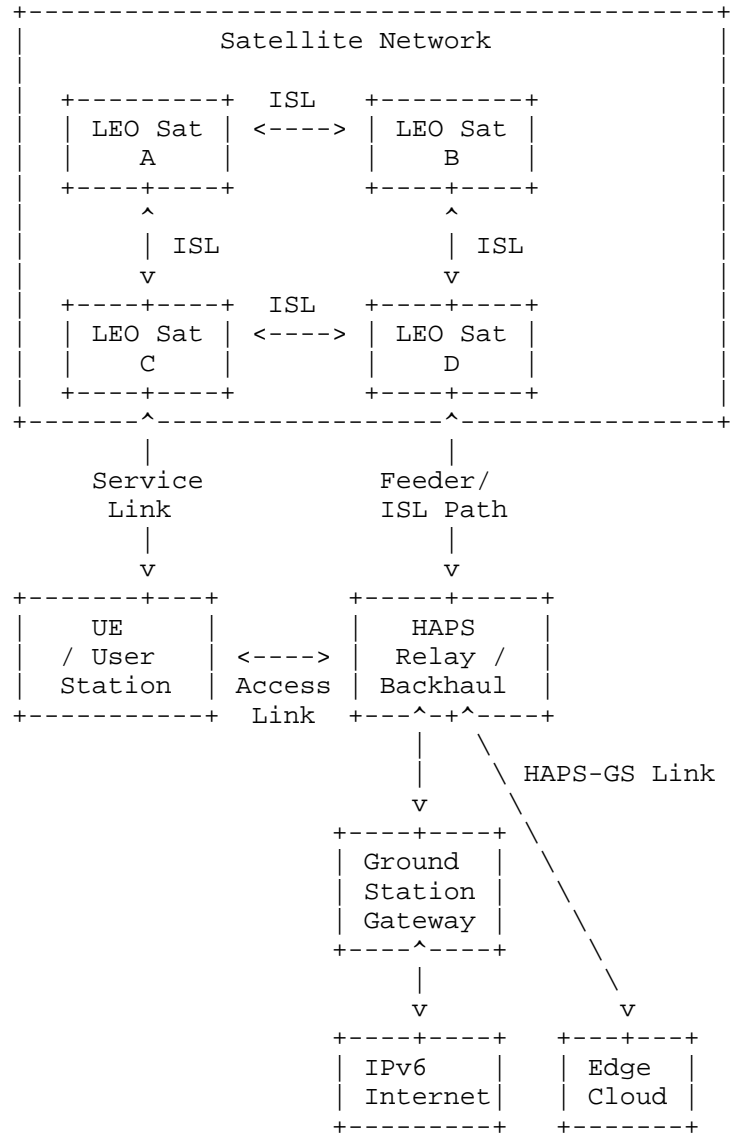


Figure 1: Reference Scenario for HAPS-assisted IPv6 Wireless Access in Satellite Networks

Figure 1 shows the reference scenario considered in this document. The scenario includes service links between a UE and satellites, HAPS access and backhaul links, ISLs among satellites, feeder links between satellites and ground stations, and IPv6 connectivity toward terrestrial networks. This follows the high-level view of user stations, satellites, gateways, and the Internet described in [RFC9717], while expanding the satellite network to show multiple LEO satellites connected by ISLs and HAPS-assisted relay paths. This reference scenario serves as a baseline for discussing the challenges of IPv6-based communication in NTN environments, including dynamic topology, multi-hop data forwarding across multiple satellites, HAPS-assisted forwarding, QoS support, traffic engineering, handover, and intermittent connectivity.

4. Problem Statement

Non-Terrestrial Networks (NTNs) introduce network characteristics that are fundamentally different from those of conventional terrestrial networks due to high satellite mobility, heterogeneous aerial and space links, and large-scale distributed network structures. These characteristics create several challenges for IPv6-based communication in satellite and HAPS-assisted NTN environments.

- * ***Dynamic Topology and Route Instability:*** In LEO satellite environments, a network topology changes continuously over time due to the orbital movement of satellites. Service links between a UE and satellites, ISLs, satellite-to-HAPS links, and HAPS-to-ground links may be dynamically established, reconfigured, or disconnected according to satellite movement, platform availability, weather, spectrum conditions, and network policy. These frequent topology changes may affect routing table convergence and make stable path maintenance difficult. As a result, existing IPv6 routing mechanisms, which are primarily designed for more stable terrestrial environments, may experience limitations in NTN environments.
- * ***Complexity of Multi-hop Packet Delivery:*** Satellite networks commonly rely on multi-hop communication through ISLs in order to provide wide-area connectivity. Depending on satellite visibility, HAPS availability, and gateway reachability, packets may traverse multiple satellites, an HAPS relay, or a hybrid satellite-HAPS-ground path before reaching terrestrial networks. However, in dynamic topology environments, forwarding paths may continuously change, potentially causing packet loss, jitter,

reordering, route instability, and forwarding inefficiency. Path selection and network state awareness therefore remain important considerations in IPv6-based NTN communication.

- * ***HAPS-assisted Relay and Hybrid Path Management:*** HAPS can improve coverage and provide relay or backhaul capacity, especially in remote, maritime, aeronautical, and disaster-recovery environments. However, the introduction of HAPS also creates hybrid paths with different delay, bandwidth, link-layer, and operational characteristics. A path through an HAPS may be preferable for some flows because of coverage or gateway visibility, while a direct satellite path may be preferable for other flows because of capacity, policy, or topology. IPv6 forwarding mechanisms need to account for these heterogeneous path properties without creating excessive control-plane churn.
- * ***Frequent Handover and Session Continuity:*** Due to the rapid movement of LEO satellites, a UE may frequently switch serving satellites within short periods of time. In HAPS-assisted environments, the UE may also switch between satellite access, HAPS access, and terrestrial access depending on coverage and service policy. Such frequent handovers may affect IP session continuity and increase signaling overhead for mobility management procedures. Existing mobility management mechanisms, such as Mobile IPv6 and Proxy Mobile IPv6, were primarily developed for terrestrial wireless environments and may encounter challenges in NTN environments characterized by long propagation delays and dynamic connectivity conditions.
- * ***Long Delay, Jitter, and Link Variability:*** Satellite communication environments typically experience relatively long RTT and varying link quality due to altitude, propagation distance, Doppler effects, atmospheric conditions, antenna tracking, gateway visibility, and congestion. HAPS-assisted paths may reduce some propagation delay compared with satellite-only paths, but may introduce different capacity and interference constraints. These characteristics may affect transport protocols, congestion control, path selection, and resource utilization in IPv6-based satellite communication.
- * ***QoS Support for Heterogeneous Application Classes:*** IPWASN needs to support application classes with very different service expectations. Text messaging and emergency data may tolerate delay but require high reliability and priority treatment. Voice requires bounded delay and jitter. Video streaming requires adequate throughput and controlled packet loss to avoid rebuffering. Video conferencing and live media require low conversational latency, low jitter, and sufficient uplink and

downlink capacity. IoT traffic may be delay-tolerant and energy constrained. DiffServ provides a framework for packet classification and per-hop behaviors in IP networks [RFC2474], and RFC 4594 provides configuration guidance for service classes [RFC4594]. However, NTN environments require further analysis of how such QoS classes can be preserved across satellite handover, HAPS relay changes, ISL reconfiguration, and gateway changes.

- * ***Traffic Engineering and Programmable Forwarding:** Multi-hop satellite paths may need to be selected according to service requirements such as latency, jitter, bandwidth, reliability, priority, policy, and gateway availability. SR-MPLS [RFC8660] can steer traffic through MPLS label stacks, while SRv6 mechanisms [RFC8754] [RFC8986] can steer packets using IPv6-based segment identifiers and network programming behaviors. SR Policy [RFC9256] provides a framework for steering traffic into source-routed policies with candidate paths and optimization objectives. However, NTN environments require further analysis of segment-list size, Maximum SID Depth constraints, SRH overhead, MPLS label-stack depth, control-plane scalability, policy recomputation frequency, and fast recovery during satellite mobility and link changes.
- * ***Direct-to-Device Satellite Access:** Direct smartphone access to satellite networks is emerging for messaging, emergency data, and limited data services. Such access may be extended in the future toward richer voice or video services, but bandwidth, latency, antenna, power, and duplexing constraints remain significant. IPWASN needs to consider how direct-to-device satellite access fits into the broader IPv6 architecture, including how service classes are mapped, how emergency traffic is prioritized, and how traffic is routed when full-duplex or high-throughput service requires dedicated ground stations, HAPS relays, or optical/laser links.

Another important characteristic of satellite networks is that satellite movement and orbital trajectories are generally predictable. Unlike many terrestrial mobile environments, future satellite positions and link availability can often be estimated in advance. Such predictability may provide opportunities for improving routing decisions, SR Policy computation, forwarding efficiency, handover preparation, and connectivity management in NTN environments. TPD and TSF demonstrate that trajectory information can reduce forwarding uncertainty by predicting encounters, selecting suitable forwarders or rendezvous points, and bounding delivery probability or delay [TPD-COMNET-2015] [TSF-TMC-2012]. In IPWASN, analogous information may include satellite ephemeris data, HAPS flight plans, scheduled ISL availability, gateway visibility windows, and predicted UE-to-satellite contact intervals.

In addition, NTN environments may experience intermittent connectivity due to satellite movement, temporary link disruptions, limited gateway visibility, HAPS availability, weather, or disaster conditions. In some situations, E2E paths between a UE and terrestrial networks may not always be immediately available. Therefore, additional considerations for handling intermittent connectivity and maintaining communication reliability are required in IPv6-based NTN environments.

Consequently, IPv6 communication in NTN environments requires further analysis regarding how existing IPv6 protocols and mechanisms can support dynamic topology adaptation, HAPS-assisted forwarding, QoS classification, SR-MPLS/SRv6-based traffic engineering, multi-hop data forwarding, mobility management, and intermittent connectivity. Additional requirements reflecting the characteristics of satellite networks also need to be identified.

5. Use Cases

This section describes representative use cases in which IPWASN can be utilized in NTN environments. These use cases illustrate communication scenarios that involve satellite mobility, HAPS-assisted relay paths, multi-hop data forwarding, intermittent connectivity, QoS variability, and heterogeneous network integration. The purpose of these scenarios is to identify key considerations and requirements for IPv6-based communication in satellite networks.

- * ***Remote Area Connectivity:** In remote environments such as maritime regions, deserts, mountainous areas, and rural regions where terrestrial communication infrastructure is limited or unavailable, a UE may rely on satellite networks to access IPv6 services and Internet connectivity. HAPS may be deployed as a regional relay or backhaul node to extend coverage and reduce the

dependency on immediate satellite-to-ground visibility. In such environments, direct communication between end users and terrestrial networks may not always be possible, requiring packets to be forwarded through multiple satellites, through HAPS, or through a hybrid path. Maintaining IPv6 connectivity, supporting multi-hop packet delivery, and selecting paths according to link availability and QoS class become important considerations.

- * ***Maritime and Aeronautical Communications:*** Moving platforms such as ships and aircraft require continuous network connectivity while traveling across wide geographic regions. Communication may depend not only on direct satellite access but also on packet forwarding through multiple satellites or HAPS nodes before reaching a ground station connected to terrestrial networks. As aircraft or vessels move across satellite and HAPS coverage areas, frequent handovers may occur. Such handovers may affect session continuity and introduce signaling overhead. Long-distance communication over satellite links may also experience long propagation delays and varying link quality, affecting E2E data delivery performance.
- * ***UAV and Aerial Network Integration:*** Unmanned Aerial Vehicles (UAVs), HAPS, and other aerial platforms may utilize NTN connectivity for data collection, surveillance, environmental monitoring, or communication relay services. In particular, UAVs and HAPS can operate as intermediate communication nodes in areas where terrestrial infrastructure is unavailable or partially disconnected. Communication paths may involve multiple network layers consisting of satellites, HAPS, UAVs, and terrestrial nodes. Since these platforms have different mobility and coverage characteristics, IPv6-based communication mechanisms need to consider dynamic path selection, multi-hop forwarding, and connectivity maintenance in heterogeneous aerial networking environments.
- * ***Disaster Recovery Communications:*** During disaster situations, terrestrial communication infrastructure may become damaged, overloaded, or temporarily unavailable. Satellite networks and HAPS can provide emergency communication services for first responders, public safety systems, and affected users. An HAPS may provide local coverage, aggregation, or backhaul when terrestrial towers are unavailable, while LEO satellites may provide wide-area reachability. Disaster environments may involve unstable topology conditions, unpredictable traffic patterns, and intermittent network connectivity. Emergency traffic may require priority forwarding and resilient path selection across satellite and HAPS relays.

- * ***Direct Smartphone Access to Satellite Networks:*** Smartphones or small mobile terminals may access satellite services directly for text messaging, emergency notification, location reporting, or low-rate data exchange. Such services may be delay-tolerant but often require high reliability and priority handling. Future voice, video, or full-duplex services may require additional network support, including HAPS relays, dedicated ground stations, higher-capacity feeder links, or optical inter-satellite or satellite-ground links. IPWASN should consider how IPv6 addressing, QoS marking, mobility, and traffic steering apply to direct-to-device access.
- * ***Video Streaming and Interactive Media over NTN:*** End users in remote, maritime, aeronautical, or disaster-recovery environments may use NTN access for video streaming, live broadcasting, video conferencing, online education, and cloud-based collaboration. These services include downlink-heavy cases such as video streaming and uplink-heavy or bidirectional cases such as live video upload and conferencing. HTTP/3 over QUIC can reduce head-of-line blocking at the transport layer and supports encrypted, multiplexed application traffic over UDP, but satellite mobility, long RTT, handover, changing ISL paths, and HAPS relay changes can still affect bitrate adaptation, startup delay, rebuffering, and conversational latency. Therefore, IPWASN needs to consider how QoS-aware forwarding, traffic engineering, and mobility support can preserve media quality across dynamic NTN paths.
- * ***IoT and Intermittent Connectivity Services:*** Satellite-based IoT environments may include sensors, monitoring systems, and low-power communication devices deployed in remote or infrastructure-limited regions. Such devices may periodically connect to satellite or HAPS networks to transmit sensing information or operational data. Continuous E2E connectivity may not always be available due to satellite movement, limited visibility, HAPS availability, or power constraints of IoT devices. As a result, data delivery may rely on intermittent communication opportunities, temporary packet buffering, or delayed forwarding mechanisms. IPv6-based communication in NTN environments needs to consider intermittent connectivity and efficient data delivery mechanisms for satellite-based IoT services.

6. Requirements

This section describes key requirements for supporting IPWASN based on the problem statements and use cases discussed in previous sections. These requirements are intended to identify important considerations for applying IPv6-based communication mechanisms in NTN environments characterized by dynamic topology, satellite mobility, HAPS-assisted relay paths, multi-hop communication, QoS variability, traffic engineering, and intermittent connectivity.

- * ***HAPS-assisted NTN Architecture Support:*** IPWASN should support architectures in which HAPS nodes are used as relay, access, aggregation, or backhaul nodes between a UE, LEO satellites, ground stations, and terrestrial networks. IPv6 mechanisms should be able to represent HAPS-assisted paths as first-class forwarding alternatives rather than as an external non-IP transport detail. The architecture should allow satellite-only, HAPS-assisted, terrestrial, and hybrid paths to be selected according to reachability, QoS class, policy, and gateway availability.
- * ***Adaptation to Dynamic Topology:*** Due to the orbital movement of satellites, NTN environments experience continuous network topology change. IPv6 routing and forwarding mechanisms need to adapt to frequent topology changes while minimizing routing instability, convergence delay, and signaling overhead. Predictable satellite movement patterns and HAPS coverage characteristics may provide opportunities for improving routing, pre-computing candidate paths, preparing handovers, and reducing service disruption.
- * ***Support for Multi-hop and Hybrid Data Forwarding:*** Satellite networks commonly rely on multi-hop communication through ISLs to provide wide-area connectivity. HAPS-assisted deployments add additional hybrid forwarding choices through satellite-HAPS-ground and UE-HAPS-ground paths. IPv6-based communication mechanisms should support efficient packet forwarding across multiple satellite and HAPS hops while considering varying network conditions, dynamic path changes, QoS requirements, and gateway availability. Path selection and forwarding efficiency remain important considerations for reliable E2E communication in NTN environments.
- * ***Trajectory- and Contact-aware Forwarding:*** IPWASN should consider forwarding mechanisms that can use predictable satellite, HAPS, and gateway contact information. Inspired by TPD and TSF, forwarding decisions may use predicted encounters, contact windows, target rendezvous points, delivery probability, expected delivery delay, and source-routed forwarding sequences

[TPD-COMNET-2015] [TSF-TMC-2012]. Such mechanisms should account for stale or inaccurate prediction information, packet header overhead for carrying forwarding sequences, scalability of contact-graph computation, and consistency with IPv6, SR-MPLS, SRv6, and DTN-related mechanisms.

- * ***Mobility Management and Session Continuity:*** A UE may frequently change serving satellites due to the rapid movement of LEO satellites. The UE may also switch between direct satellite access, HAPS access, and terrestrial access. IPv6 mobility management mechanisms need to support session continuity while reducing signaling overhead and service disruption during handover procedures. Existing mobility management approaches designed for terrestrial wireless environments may require additional considerations in NTN environments characterized by long propagation delay, heterogeneous access links, and dynamic connectivity conditions.
- * ***Handling of Intermittent Connectivity:*** NTN environments may experience intermittent connectivity due to satellite movement, temporary link disruption, limited gateway visibility, HAPS unavailability, weather conditions, or disaster conditions. IPv6-based communication mechanisms should consider communication continuity even when E2E paths are not immediately available. Approaches related to Delay/Disruption Tolerant Networking (DTN) architecture [RFC4838], Bundle Protocol Version 7 [RFC9171], buffering, scheduled contacts, and opportunistic forwarding may be relevant for supporting packet delivery in intermittently connected satellite environments.
- * ***QoS Class Identification and Treatment:*** IPWASN should analyze how traffic can be classified into QoS classes and how those classes can be preserved across satellite, HAPS, and ground network segments. DiffServ marking in IPv6 packets [RFC2474] and DiffServ service-class guidance [RFC4594] provide useful starting points, but NTN-specific treatment needs to consider long RTT, jitter, asymmetric capacity, handover, packet loss, and intermittent connectivity. At a minimum, IPWASN should consider separate treatment for emergency text/data, conversational voice, interactive video, streaming video, bulk data, control-plane signaling, and delay-tolerant IoT traffic.
- * ***QoS Parameter Mapping:*** Each QoS class should be mapped to relevant parameters such as one-way delay, RTT, jitter, packet loss, bandwidth, reliability, priority, and tolerance to disruption. For example, emergency text may require high reliability and priority while tolerating higher delay; voice and conferencing require bounded delay and jitter; streaming video

requires sustained throughput and controlled loss; and IoT traffic may require energy efficiency and delay-tolerant delivery. These mappings should guide path selection, queue management, admission control, and traffic engineering decisions. Table 1 summarizes representative QoS classes for IPWASN.

- * ***SR-MPLS and SRv6-based Traffic Engineering:*** Segment Routing may provide useful traffic-engineering tools for IPWASN. SR-MPLS can reuse the MPLS forwarding plane to steer traffic through selected paths, while SRv6 can provide IPv6-native source routing and service function chaining by using IPv6 segment identifiers and SRv6 endpoint behaviors [RFC8986]. SR Policy [RFC9256] provides a framework for steering traffic according to candidate paths, optimization objectives, constraints, and policy colors. IPWASN should analyze how SR-MPLS and SRv6 can support QoS-aware forwarding, HAPS-assisted path selection, gateway selection, fast reroute, and path optimization in NTN networks.
- * ***Fast Reroute and Handover Preparation:*** IPWASN should analyze fast reroute mechanisms for link changes, satellite handovers, HAPS relay changes, and gateway outages. SR Policy protection and local protection mechanisms can provide candidate techniques, and BFD [RFC5880] may be useful for detecting failures. However, NTN environments require careful evaluation of detection timers, false positives under variable delay, pre-computation of backup paths, and interaction with scheduled satellite mobility.
- * ***Gap Analysis for Existing MPLS and SR Technologies:*** Existing MPLS, SR-MPLS, SRv6, and SR Policy mechanisms were not designed specifically for rapidly moving satellite constellations and HAPS-assisted paths. IPWASN should therefore identify gaps related to label-stack depth, SRH overhead, Maximum SID Depth, MTU impact, segment-list compression, control-plane update rate, path-computation scalability, state distribution, OAM, failure detection, and policy consistency during frequent topology changes. This gap analysis should compare existing technologies with NTN requirements before any new protocol extension is proposed. Table 2 summarizes initial analysis items.
- * ***Scalability for Large-scale Satellite Networks:*** Large-scale satellite constellations may involve a significant number of satellites, HAPS nodes, gateways, and user devices operating simultaneously. IPv6-based communication mechanisms should consider scalability in terms of addressing, routing information management, segment information, forwarding efficiency, QoS state, telemetry, and overall network operation in large distributed NTN environments.

- * ***Operational Observability and Management:*** IPWASN should consider how operators can observe and manage dynamic satellite and HAPS paths. Useful information may include current and predicted link availability, QoS class performance, handover events, SR Policy state, packet loss, jitter, delay, and gateway utilization. Such information is needed for troubleshooting, policy computation, SLA reporting, and automated traffic engineering.

Traffic Class	Representative Services	Primary QoS Requirements	Forwarding Considerations
Emergency text/data	Emergency message, location report, public-safety alert	High reliability, high priority, loss avoidance; delay tolerant within service policy	Priority forwarding, resilient path selection, store-and-forward support during disruption
Conversational voice	Voice call, push-to-talk, public-safety voice	Bounded one-way delay, low jitter, moderate bandwidth, controlled packet loss	Low-latency path selection, jitter-aware queueing, fast reroute during handover
Interactive video	Video conferencing, live media, remote assistance	Low latency, low jitter, sufficient uplink and downlink bandwidth, low packet loss	QoS-aware SR policy, bandwidth-aware admission control, rapid recovery from path changes
Streaming video	Video streaming, online education, downlink media delivery	Sustained throughput, controlled loss, rebuffering avoidance; less strict	Throughput-aware path steering, cache or edge selection, adaptation to link-rate changes

		latency than conferencing	
IoT sensing	Telemetry, environmental sensing, asset monitoring	Low bandwidth, high energy efficiency, delay tolerance, reliability according to application	Opportunistic forwarding, aggregation, scheduled contact use, minimal signaling overhead
Control and routing signaling	Routing updates, mobility signaling, path- computation state, OAM	High reliability, bounded delivery time, protection from congestion and spoofing	Separate treatment from best-effort traffic, authentication, rate control, and policy consistency

Table 1: Representative QoS Classes for IPWASN

NTN Requirement	Existing MPLS/SR Capability	Gap in IPWASN Environments	Analysis Direction
QoS-aware path steering	SR Policy can steer traffic by candidate path, preference, constraints, and color.	Satellite, HAPS, and gateway conditions change rapidly, so policy validity can expire before or during use.	Analyze how latency, bandwidth, reliability, and gateway availability are measured and bound to SR policies.
Fast reroute during handover	MPLS and SR deployments can use local protection, backup paths, and failure detection	LEO handover and HAPS relay changes may be scheduled mobility events rather than ordinary	Evaluate pre- computed backup segment lists and timer settings that avoid false failure

	mechanisms.	failures.	detection under variable RTT.
Dynamic segment-list management	SR-MPLS label stacks and SRv6 segment lists encode explicit forwarding instructions.	Long multi-hop ISL or satellite-HAPS-ground paths may exceed practical label stack depth or Maximum SID Depth.	Study segment compression, hierarchical segments, binding SIDs, and path abstraction for large constellations.
Header and MTU efficiency	SR-MPLS uses label stacks; SRv6 uses the Segment Routing Header for explicit segment lists.	SRH overhead or deep MPLS label stacks can reduce effective payload capacity on constrained NTN links.	Quantify overhead for representative path lengths and identify limits for low-rate direct-to-device links.
HAPS-assisted hybrid path selection	SR can steer packets through selected nodes and service functions in terrestrial or provider networks.	HAPS introduces aerial relay availability, access/backhaul capacity, and coverage constraints that are not common in fixed networks.	Define metrics and policy inputs for choosing satellite-only, HAPS-assisted, terrestrial, or hybrid paths.
Control-plane scalability	Existing routing and controller-based SR deployments distribute topology, segment, and policy state.	Large satellite constellations produce frequent topology events and large numbers of time-dependent candidate paths.	Analyze aggregation, prediction-based computation, policy lifetime, and consistency across satellite, HAPS, and ground domains.
OAM and telemetry	MPLS, SR-MPLS, and SRv6 have OAM	Intermittent links, long RTT, and moving	Evaluate lightweight OAM, scheduled

	and telemetry mechanisms for path validation and failure localization.	relays may make continuous probing expensive or misleading.	measurement, and correlation with ephemeris, HAPS position, and gateway visibility.
--	--	---	---

Table 2: Initial SR Gap Analysis for IPWASN

7. Security Considerations

This document does not define new protocols packet formats, or on-the-wire behaviors. However, IPWASN combines IPv6 forwarding, mobility management, QoS treatment, traffic engineering, and intermittent-connectivity support in satellite and HAPS-assisted NTN environments. Therefore, deployments need to consider security and privacy risks that arise when existing IPv6 mechanisms are applied to highly dynamic and geographically wide-area wireless networks. The security considerations in RFC 9365 for IPv6 wireless access in vehicular environments are relevant because both environments involve mobile nodes, changing attachment points, neighbor discovery, mobility management, and privacy-sensitive location information [RFC9365].

7.1. Neighbor Discovery and First-hop Security

In IPWASN, IPv6 Neighbor Discovery (ND) and first-hop functions may operate over satellite service links, HAPS-assisted access links, and gateway-facing links. As discussed in RFC 9365, ND-related procedures can be abused for flooding, address spoofing, impersonation, and denial-of-service attacks [RFC9365]. In NTN environments, the impact of such attacks may be amplified by long RTT, constrained radio resources, intermittent connectivity, and frequent handover. Implementations and deployments should therefore filter suspicious ND traffic, rate-limit control messages where appropriate, authenticate routers or access nodes when feasible, and consider secure ND-related mechanisms such as SEND [RFC3971] or other deployment-specific authentication mechanisms.

Address ownership and source-address validation are also important for satellite access because spoofed IPv6 addresses may consume scarce satellite or HAPS capacity, pollute neighbor caches, or interfere with mobility bindings and traffic engineering policies. Operational guidance for IPv6 security [RFC9099] and known operational ND problems [RFC6583] should be considered when profiling ND behavior for IPWASN.

7.2. Mobility Management and Control-plane Security

IPWASN mobility management may involve frequent UE handovers among satellites, HAPS nodes, gateways, and terrestrial access networks. Similar to the mobility-management threats described in RFC 9365, a malicious node may attempt to register bogus identities, create false mobility bindings, exhaust resources in gateways or mobility anchors, or interfere with handover signaling [RFC9365]. Mobility-related control messages and tunnel endpoints should be mutually authenticated and protected for integrity and confidentiality. Secure channels such as IPsec [RFC4301] or TLS [RFC8446] may be used according to the deployment architecture.

Traffic-engineering and source-routing state also require protection. SR-MPLS and SRv6 policies, segment lists, contact schedules, and path-computation inputs can affect where packets are forwarded. Unauthorized modification of such information may cause traffic interception, blackholing, loop formation, policy bypass, or service degradation. Operators should protect control-plane distribution channels, authenticate path-computation entities, and validate forwarding policy updates before applying them in satellites, HAPS nodes, gateways, and ground networks.

7.3. Trajectory, Contact, and Privacy Considerations

TPD and TSF show that trajectory information can improve forwarding by predicting encounters and rendezvous points [TPD-COMNET-2015] [TSF-TMC-2012]. In IPWASN, similar inputs may include satellite ephemeris data, HAPS trajectories, gateway visibility, link schedules, and UE location or attachment information. These inputs can be operationally valuable, but they are also security- and privacy-sensitive. False trajectory or contact information may cause incorrect path computation, delayed delivery, excessive packet replication, or routing around intended policy constraints. Such information should therefore be authenticated, integrity protected, and checked against operator policy and telemetry when used for forwarding or handover decisions.

Location, attachment, and contact-history data can reveal user movement, service usage, emergency activity, or sensitive operational patterns. RFC 9365 notes that logging and address information can create privacy risks in mobile wireless environments [RFC9365]. IPWASN deployments should minimize collected location and contact data, protect stored and transmitted logs, restrict access to trajectory and telemetry databases, and consider IPv6 address-generation privacy guidance [RFC7721] where applicable.

7.4. Other Threats

IPWASN may rely on multi-hop paths through satellites, HAPS nodes, relay nodes, gateways, and terrestrial networks. Authentication or key-establishment messages may experience delay or loss over such paths, and compromised intermediate nodes may attempt to observe, delay, replay, or drop traffic. E2E security for user traffic and strong operational security for management interfaces are therefore important. Operators should also consider zero-trust assumptions for cross-domain NTN deployments, where satellite operators, HAPS operators, mobile network operators, and terrestrial Internet providers may be separate administrative entities.

8. References

8.1. Normative References

- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <<https://www.rfc-editor.org/info/rfc2474>>.
- [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/info/rfc3971>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <<https://www.rfc-editor.org/info/rfc6583>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.

- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8660] Bashandy, A., Ed., Filsfils, C., Ed., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with the MPLS Data Plane", RFC 8660, DOI 10.17487/RFC8660, December 2019, <<https://www.rfc-editor.org/info/rfc8660>>.
- [RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <<https://www.rfc-editor.org/info/rfc8754>>.
- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <<https://www.rfc-editor.org/info/rfc8986>>.
- [RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <<https://www.rfc-editor.org/info/rfc9000>>.
- [RFC9099] Vyncke, ., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <<https://www.rfc-editor.org/info/rfc9099>>.
- [RFC9114] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114, June 2022, <<https://www.rfc-editor.org/info/rfc9114>>.

8.2. Informative References

- [TS-23.501-Rel17]
"System Architecture for the 5G System (5GS); Stage 2 (Release 17)",
Available: <https://www.3gpp.org/DynaReport/23501.htm>, June 2023.
- [TS-23.501-Rel18]
"System Architecture for the 5G System (5GS); Stage 2 (Release 18)",
Available: <https://www.3gpp.org/DynaReport/23501.htm>, March 2024.

- [ITU-HAPS] "High-altitude platform systems", 2026.
- [HAPS-ARCH]
Alsharif, M.S., Kim, J., and J.H. Kim, "High Altitude Platform Stations (HAPS): Architecture and System Performance", arXiv 2103.03431, Available: <https://arxiv.org/abs/2103.03431>, March 2021.
- [TPD-COMNET-2015]
Jeong, J.P., Kim, J., Hwang, T., Xu, F., Guo, S., Gu, Y.J., Cao, Q., Liu, M., and T. He, "TPD: Travel Prediction-based Data Forwarding for Light-Traffic Vehicular Networks", Computer Networks Volume 93, pp. 166-182, DOI 10.1016/j.comnet.2015.10.016, December 2015, <<https://doi.org/10.1016/j.comnet.2015.10.016>>.
- [TSF-TMC-2012]
Jeong, J., Guo, S., Gu, Y., He, T., and D.H.C. Du, "Trajectory-Based Statistical Forwarding for Multihop Infrastructure-to-Vehicle Data Delivery", IEEE Transactions on Mobile Computing Volume 11, Number 10, pp. 1523-1537, DOI 10.1109/TMC.2011.189, October 2012, <<https://doi.org/10.1109/TMC.2011.189>>.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <<https://www.rfc-editor.org/info/rfc3963>>.
- [RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, DOI 10.17487/RFC4594, August 2006, <<https://www.rfc-editor.org/info/rfc4594>>.
- [RFC4838] Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture", RFC 4838, DOI 10.17487/RFC4838, April 2007, <<https://www.rfc-editor.org/info/rfc4838>>.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<https://www.rfc-editor.org/info/rfc5213>>.
- [RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <<https://www.rfc-editor.org/info/rfc5880>>.

- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<https://www.rfc-editor.org/info/rfc6275>>.
- [RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <<https://www.rfc-editor.org/info/rfc7429>>.
- [RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <<https://www.rfc-editor.org/info/rfc8402>>.
- [RFC9171] Burleigh, S., Fall, K., and E. Birrane, III, "Bundle Protocol Version 7", RFC 9171, DOI 10.17487/RFC9171, January 2022, <<https://www.rfc-editor.org/info/rfc9171>>.
- [RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <<https://www.rfc-editor.org/info/rfc9256>>.
- [RFC9365] Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", RFC 9365, DOI 10.17487/RFC9365, March 2023, <<https://www.rfc-editor.org/info/rfc9365>>.
- [RFC9717] Li, T., "A Routing Architecture for Satellite Networks", RFC 9717, DOI 10.17487/RFC9717, January 2025, <<https://www.rfc-editor.org/info/rfc9717>>.

Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. RS-2024-00398199, Standard Development of SDV Software Framework for Intelligent Convergence Services).

Contributors

This document is made by the group effort of 6man Working Group. The authors sincerely appreciate the contributions of 6man Working Group.

The following are the coauthors of this document:

Tae (Tom) Oh
School of Information
Rochester Institute of Technology
335 John Street
Rochester, NY 14623
United States of America
Phone: +1 585 475 7642
Email: thoics@rit.edu

Byoungman (Robert) An
Intelligent Information R and D Division Mobility Platform Research Center
Global R and D Center 6th floor
#22, Daewangpangyo-ro 712beon-gil
Seongnam
Gyeonggi-Do
13488
Republic of Korea
Phone: +82 31 739 7463
Email: bman@keti.re.kr
URI: <https://www.keti.re.kr/eng/main/main.php>

Yiwen Shen
Department of Software
Ajou University
206 Worldcup-Ro, Yeongtong-Gu
Suwon
Gyeonggi-Do
16499
Republic of Korea
Email: chrishen@ajou.ac.kr
URI: <https://chrishen.github.io>

Xiaohong (Dawn) Yu
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: rna0415@skku.edu
URI: <https://iotlab.skku.edu/people-dawnyu.php>

Xudong Wang
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: wangwudong28@skku.edu
URI: <https://iotlab.skku.edu/people-Xudong-Wang.php>

Eunjin Hwang
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: eunijhwang@skku.edu
URI: <https://iotlab.skku.edu/people-Eunjin-Hwang.php>

Shota Okazaki
Graduate School of Systems Engineering
Wakayama University
930 Sakaedani, Wakayama
640-8510
Japan
Email: okazaki.shota@g.wakayama-u.ac.jp

Authors' Addresses

Jimin Lee (editor)
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: jm.lee98@skku.edu
URI: <https://iotlab.skku.edu/people-Jimin-Lee.php>

Jaehoon Paul Jeong (editor)
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

Bien Aime Mugabarigira
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: bienaime@skku.edu
URI: <https://iotlab.skku.edu/people-Bien-Aime.php>

Takuya Yoshihiro
Faculty of Systems Engineering
Wakayama University
930 Sakaedani, Wakayama
640-8510
Japan
Email: tac@wakayama-u.ac.jp