Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 November 2025

Y. Liu
China Mobile
D. Voyer
Bell Canada
T. Graf
Swisscom
Z. Miklos
MTN
L. Contreras
Telefonica
N. Leymann
Deutsche Telekom
L. Song
Alibaba, Inc
S. Matsushima
SoftBank
C. Xie
China Telecom
X. Yi
China Unicom
6 May 2025

SRv6 Deployment and Operation Problem Summary
draft-liu-srv6ops-problem-summary-05

Abstract

This document aims to provide a concise overview of the common problems encountered during SRv6 deployment and operation, which provides foundations for further work, including for example of potential solutions and best practices to navigate deployment.

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 7 November 2025.

Table of Contents

1. Introduction

Segment Routing over IPv6 (SRv6) is a new technology that builds upon the existing IPv6 infrastructure to offer programmable data plane capabilities. This allows for more granular control over traffic forwarding, enabling flexible and scalable network designs. While SRv6 presents numerous potential benefits, such as improved traffic engineering, optimized resource utilization, its deployment and operation come with certain challenges.

This document aims to provide a concise overview of the common problems encountered during SRv6 deployment and operation, which provides foundations for further work, including for example potential solutions and best practices to navigate deployment . By understanding these challenges and exploring mitigation strategies, network administrators can make informed decisions when implementing and managing SRv6 networks.

This document identifies a number of Deployment and Operation Problems (DOPs) that require additional work within IETF.

1.1. Requirements Language

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

2. SRv6 Upgrade and Evolution

In the evolution from non-SRV6 networks to SRv6 networks, the upgrade from MPLS to SRv6 represents the most typical and common scenario, which requires consideration of two cases:

For SRv6 and MPLS coexistence, a smooth transition from an MPLS network to an SRv6 network is required, avoiding service interruptions. For instance, deploy dual-stack tunnels for VPN over MPLS and VPN over SRv6, with MPLS and SRv6 sharing VPN instances. When the next hop of the route is an IPv4 address, iterate through the MPLS tunnel; when the next hop is an IPv6 address, iterate through the SRv6 tunnel. Prefer VPN routes based on SRv6. Once the transition is complete, remove the MPLS tunnel.

For SRv6 and MPLS integration, the legacy MPLS network and the newly established SRv6 network coexist, ensuring intercommunication between the two networks. For instance, configure route regeneration and route re-advertisement functions between two address families (EVPN, VPN) on edge nodes.

In some cases, SRv6 needs to traverse third-party networks that may not natively support SRv6 even IPv6. One of the possible methods is to establish tunnels between nodes that support SRv6, and create SRv6 BE (Bandwidth Engineering) or SRv6 TE (Traffic Engineering) Policy across the tunnels as overlay network.

While traditional inter-domain implementations in service provider networks often rely on MPLS and leverage Option A. Option A approach has scalability limitations and presents relatively higher complexity in both deployment and maintenance. The ASBR needs to manage the routing of all VPNs and create VPN instances for each VPN. At the same time, it requests associating separate interfaces and corresponding VLANs for each inter-domain VPN. SRv6 presents an alternative approach with E2E inter-domain solution, potentially leading to simplification and improved scalability. SRv6 naturally support end-to-end inter-domain by utilizing IPv6 route reachability and IPv6 route aggregation reduces the number of SRv6 locators distribution for inter-domain deployment.

DOP-1 Upgrading (migration) from existing MPLS networks to SRv6, how to ensure interoperability, simplify deployment complexity, minimize network disruption, and maintain existing services with minimal impact.

3. SRv6 Network Visualization

The existing IETF data collection frameworks can be applied to SRv6 for both data plane and control plane monitoring, but currently lack critical capabilities for measuring SRv6-specific path performance metrics and granular traffic statistics. This significant visibility gap fundamentally limits the ability to conduct meaningful SRv6 network analysis, either making it completely impossible or severely compromising the effectiveness of such analysis, particularly for service chain validation, predictive traffic engineering, and microsecond-level performance troubleshooting in SRv6 deployments and operations.

DOP-2 The collection of SRv6 network data is incomplete and inefficient, making it challenging to visualize the information effectively.

Network data is collected through multiple channels such as BMP, IPFIX, and YANG push, but the lack of correlation among these datasets hinders effective network performance analysis and optimization. While various techniques can be applied to utilize the collected data for SRv6 network analysis and performance optimization (particularly for traffic engineering) once it’s gathered in defined formats, current limitations result in delayed fault detection and recovery, as well as inconsistencies between traffic patterns and routing behaviors. Furthermore, the diversity of applicable data models for SRv6 creates integration challenges, compounded by the absence of effective methods to interpret and present data using existing models.

DOP-3 Multi-source network data (BMP/IPFIX/YANG etc.) lacks correlation and model integration, hindering SRv6 performance analysis and causing delayed fault detection and recovery etc. challenges.

4. SRv6 Address Planning

Existing IPv6 address planning approach ensures efficient address utilization and simplifies network management for IPv6 netowrk, which can’t satisfy the SRv6 SID planning for service provider, especially considering the complexities introduced by advanced features like SRv6 compression. The allocation of SRv6 SID blocks should be strategically planned by holistically considering administrative division management and route aggregation requirements, while the distribution of NodeID and function segments needs to balance administrative convenience with optimal address space utilization based on the SRv6 SID structure. Some initial work could refer to [I-D.liu-srv6ops-sid-address-assignment]. In summary:

DOP-4 Traditional IPv6 address planning proves inadequate for SRv6 due to its SID structure, which introduces additional complexity in IPv6 architecture and complicates network planning.

DOP-5 In inter-domain scenarios, SRv6 address allocation may cause address space wastage, prevent route aggregation, and fail to ensure compression efficiency.

5. Traffic steering to SRv6

The general purpose of traffic steering is to optimize the allocation and transmission of network resources, ensure a balanced distribution of network traffic, improve network performance, reduce congestion, and increase available bandwidth to provide users with a better network experience. There are various SRv6 traffic steering methods, each with its own unique advantages and challenges. It is essential to choose the appropriate traffic steering method to SRv6 based on specific application scenarios to ensure efficient operation. Some initial work could refer to [I-D.geng-srv6ops-traffic-steering-to-srv6]. In summary:

DOP-6 There are various methods for SRv6 traffic steering, making it difficult to select the appropriate method for different scenarios, leading to deployment complexity.

6. Deployment Practice for SRv6 Protection

Implementing reliability practices can significantly enhance the stability and performance of networks based on SRv6. Network failures are inevitable in the real world. Reliability practices can help network engineers quickly identify, isolate, and fix faults, thus minimizing impact on services.

In summary, the necessity of SRv6 reliability practices is evident in several aspects, including improving network stability and performance, enhancing fault handling capabilities, ensuring security, improving compatibility and interoperability, optimizing management and monitoring, and enhancing deployment experience.

SRv6 offers multiple protection mechanisms, with different applications requiring different protection needs. It is challenging to select the most suitable protection mechanism, or a combination of mechanisms. When multiple protection mechanisms coexist, achieving the desired protection outcome becomes difficult, and there is a lack of effective coordination methods. Some initial work could refer to [I-D.liu-srv6ops-sr-protection].

DOP-7 SRv6 provides diverse protection mechanisms, but selecting optimal solutions for specific applications remains challenging, especially when coordinating multiple coexisting mechanisms effectively.

7. Challenges of Different Network Types

SRv6 deployment faces various challenges across different network environments, including not only carrier networks but also data centers and campus networks. Specifically, clos (Spine-Leaf) architecture of data center requires SRv6 path control (e.g., explicit paths) compatible with ECMP to ensure traffic balance, while addressing performance impacts from SRv6 overhead and enabling automated large-scale deployment. Campus networks require SRv6 integration with legacy protocols (e.g., OSPF/VLAN), IPv4-IPv6 transition support, enhanced security for source routing risks, and automated deployment to reduce operational complexity.

For instance, in the power grid, SRv6 is supposed to provide Quality of Service (QoS) guarantees, performance optimization, and other specialized features to meet specific demands based on the power application scenario.

DOP-8 It is difficult to apply a single deployment guideline to meet the diverse SRv6 requirements of different network types.

8. Security Considerations

TBD.

9. IANA Considerations

TBD

10. References

10.1. 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>.

[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>.

10.2. Informative References

[I-D.geng-srv6ops-traffic-steering-to-srv6] Geng, G., Liu, Y., Xie, C., and C. Lin, "Best practices for traffic steering to SRv6", Work in Progress, Internet-Draft, draft-geng-srv6ops-traffic-steering-to-srv6-00, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-geng-srv6ops-traffic-steering-to-srv6-00>.

[I-D.liu-srv6ops-sid-address-assignment] Liu, Y. and Y. Zhu, "IPv6 Address Assignment for SRv6", Work in Progress, Internet-Draft, draft-liu-srv6ops-sid-address-assignment-01, 25 February 2025, <https://datatracker.ietf.org/doc/html/draft-liu-srv6ops-sid-address-assignment-01>.

[I-D.liu-srv6ops-sr-protection] Liu, Y., Wenying, J., Lin, C., Geng, X., and Y. Liu, "Operational Guidance for Protection mechanisms in SRv6 Networks", Work in Progress, Internet-Draft, draft-liu-srv6ops-sr-protection-03, 20 March 2025, <https://datatracker.ietf.org/doc/html/draft-liu-srv6ops-sr-protection-03>.

Authors' Addresses

Yisong Liu
China Mobile
Email: liuyisong@chinamobile.com

Daniel Voyer
Bell Canada
Email: Danvoyer@gmail.com

Thomas Graf
Swisscom
Email: Thomas.Graf@swisscom.com

Zoltan Miklos
MTN
Email: Zoltan.Miklos@mtn.com

Luis Contreras
Telefonica
Email: luismiguel.contrerasmurillo@telefonica.com

Nicolai Leymann
Deutsche Telekom
Email: N.Leymann@telekom.de

Linjian Song
Alibaba, Inc
Email: linjian.slj@alibaba-inc.com

Satoru Matsushima
SoftBank
Email: satoru.matsushima@g.softbank.co.jp

Chongfeng Xie
China Telecom
Email: xiechf@chinatelecom.cn

Xinxin Yi
China Unicom
Email: yixx3@chinaunicom.cn