SPRING
Internet-Draft
Intended status: Standards Track
Expires: 17 July 2026

W. Cheng
China Mobile
P. Ma
China Telecom
F. Ren
China Unicom
C. Lin
New H3C Technologies
L. Gong
China Mobile
S. Zadok
Broadcom
M. Wu
CentecNetworks
X. Wang
Ruijie Networks Co., Ltd.
13 January 2026

Encoding Network Slice Identification for SRv6
draft-cheng-spring-srv6-encoding-network-sliceid-12

Abstract

A Network Resource Partition (NRP) is a subset of the network resources and associated policies on each of a connected set of links in the underlay network. An NRP could be used as the underlay to support one or a group of enhanced VPN services. For packet forwarding in a specific NRP, some fields in the data packet are used to identify the NRP the packet belongs to, so that NRP-specific processing can be performed on each node along a path in the NRP.

This document describes a novel method to encode NRP-ID in the outer IPv6 header of an SRv6 domain, which could be used to identify the NRP-specific processing to be performed on the packets by each network node along a network path in the NRP.

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/.

Copyright Notice

Table of Contents

1. Introduction 2
  1.1. Requirements Language 3
  1.2. Terminology 3
2. Slice Identifier 3
3. SLID Assignment 4
4. Per-Slice Forwarding 5
5. Example 6
6. Backward Compatibility 7
7. Security Considerations 7
8. IANA Considerations 8
9. References 8
  9.1. Normative References 8
  9.2. Informative References 8
Authors' Addresses 9

1. Introduction

SRv6 Network Programming [RFC8986] enables the creation of overlays with underlay optimization to be deployed in an SR domain [RFC8402].

As defined in [RFC8754], all inter-domain packets are encapsulated for the part of the packet journey that is within the SR domain. The outer IPv6 header [RFC8200] is originated by a node of the SR domain and is destined to a node of the SR domain.

Network slicing provides the ability to partition a physical network into multiple isolated logical networks of varying sizes, structures, and functions so that each slice can be dedicated to specific services or customers. [RFC9543] defines the term "IETF Network Slice" and establishes the general principles of network slicing in the IETF context.

In a network that provides slicing services, the NRP-ID can be carried in the packet. In the process of packet forwarding, the routers on the forwarding path can extract NRP-ID from the packet, determine the NRP to which the packet belongs, and then forward the packet using the resources associated with the NRP.

This document describes a novel method to encode NRP-ID in the outer IPv6 header of an SRv6 domain, which could be used to identify the NRP-specific processing to be performed on the packets by each network node along a network path in the NRP.

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 [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997) and [RFC8174] (Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017).

1.2. Terminology

The key terms used in this document are defined below.

Network Resource Partition (NRP): a subset of the network resources and associated policies on each of a connected set of links in the underlay network. This term is defined in [RFC9543].

IETF Network Slice: The realization of the service in the provider’s network achieved by partitioning network resources and by applying certain tools and techniques within the network . This term is defined in [RFC9543].

2. Slice Identifier

The Slice identifier (SLID) is a network slicing identifier encoded within the IPv6 packet that allows transit routers to apply the proper forwarding treatment with associated network resources.

[RFC9543] defines the network resource mapped to the network slice as NRP (Network Resource Partition). A NRP may be associated with a unique IETF network slice or a group of slices. In this document, SLID also refers to NRP-ID, which is used to identify the network resource used in the forwarding process.

3. SLID Assignment

When an SR domain enables network slicing, a local policy MUST be defined and uniformly applied within the domain to govern the encoding of the Slice Presence Indicator (SPI) and the Slice Identifier (SLID). This policy includes the method to encode the SPI and the number of bits reserved for the SLID. When a packet enters the SR domain, the ingress PE encapsulates the packet with an outer IPv6 header and optional Segment Routing Header (SRH) as defined in [RFC8754]. The ingress PE MAY classify the packet into a slice and set the slice identifier as follows:

o Allocate a source IPv6 address for the outer header from a configured address block designated for network slicing.

o Encode the SLID in the least significant bits of this source address.

o Set the Slice Presence Indicator (SPI) in the outer IPv6 header to inform transit nodes that a valid SLID is present.

The SPI is a local designation within the SR domain. There are two proposed options for encoding the SPI, chosen by domain-wide policy:

o SPI Option A - Using a Bit in the Traffic Class Field: A specific, agreed-upon bit within the Traffic Class field of the IPv6 header is used as the SPI. If this option is used, all nodes within the SR domain participating in slice-aware forwarding MUST be upgraded to interpret this bit correctly. Packets with the SPI bit set may not be forwarded correctly by legacy nodes that are unaware of this new semantic for the Traffic Class field.

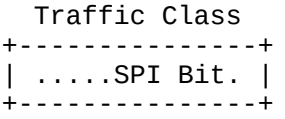

Figure 1: SPI Option A

o SPI Option B - Using a Designated Address Prefix in the Source Address: A specific IPv6 address prefix is configured and uniformly recognized within the SR domain as the "SPI Prefix". This prefix is

allocated from the operator's existing address space and is used exclusively as the network prefix for source addresses carrying SLIDs. The SPI is effectively indicated by the source address falling within this pre-defined prefix. The SLID is encoded in the least significant bits of the interface identifier portion of the address. This method does not alter the structure of the IPv6 address field itself; it simply designates a subset of the operator's address space for slice-enabled traffic. This option can provide better backward compatibility (see Section 6).

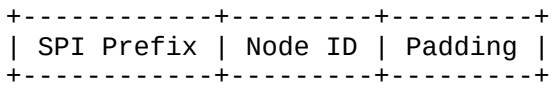

Figure 2: SPI Option B

The format for the SLID and SPI options in the IPv6 header is shown in Figure 3.

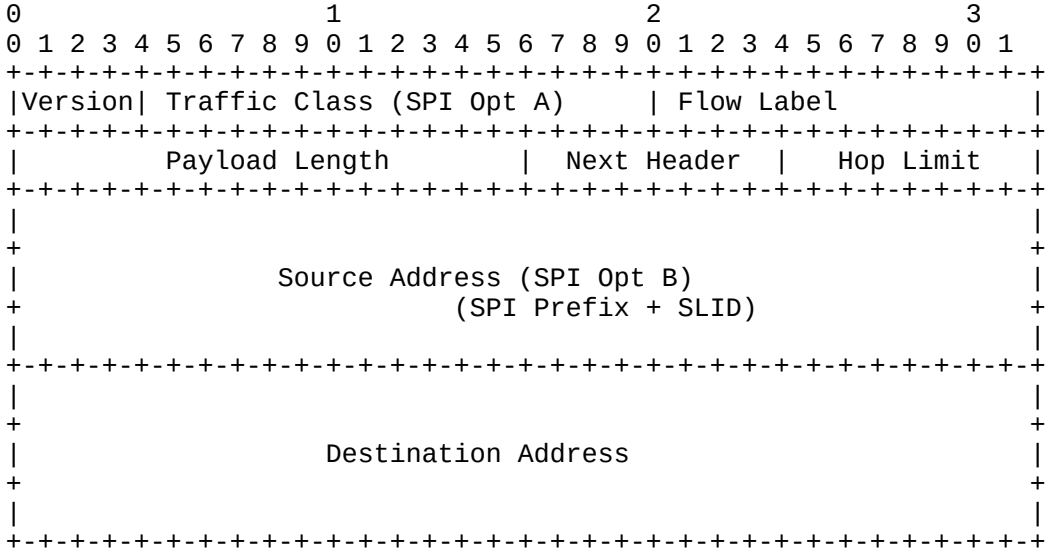

Figure 3: Encoding of SLID and SPI Option

4. Per-Slice Forwarding

Any router within the SR domain that forwards a packet with SPI set uses the SLID to select a slice and apply per-slice policies.

The most significant bit of SLID may be used to carry an S-flag, which is used to indicate whether the packet MUST be forwarded strictly using the network resource associated with the SLID. When the network resource associated with the SLID does not exist or is not available, if the S-flag is set to 1, the packet MUST be discarded, otherwise the packet SHOULD be forwarded using the default network resource or ignoring the SLID.

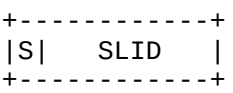

Figure 4: The SLID with S bit

5. Example

Figure 5 shows an example of network slice packet forwarding using the proposed encoding method. Assume the SPI is encoded using option B as the SPI prefix in Source Address.

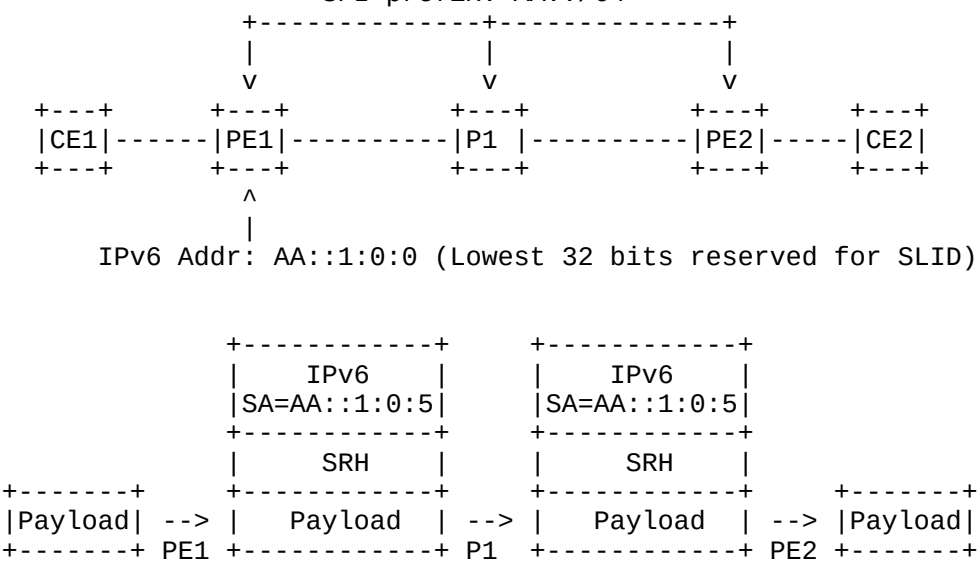

Figure 5: Packet Forwarding for Network Slice

The PE and P routers are configured to use the prefix AA::/64 as SPI. The IPv6 address AA::1:0:0 is assigned to PE1 as the source address used for network slicing. And the lowest 32 bits of the address is reserved for SLID.

PE1 encapsulates the network slice packet with an outer IPv6 header along with an SRH. The Source Address in the outer header is AA::1:0:5, in which the lowest 32 bits carries the SLID 5. P1 checks the Source Address and finds it matching the SPI prefix AA::/64. So, P1 parses SLID 5 from the Source Address, and uses the network resources associated with SLID 5 to forward the packet. PE2 decapsulates the outer IPv6 header and SRH.

6. Backward Compatibility

Backward compatibility differs based on the chosen SPI encoding method:

o For SPI Option A (Traffic Class bit): This method is not backward compatible. Legacy routers that do not recognize the new semantic of the designated Traffic Class bit will forward packets based on the standard interpretation of the header fields. They will not perform slice-specific processing. Successful end-to-end slice forwarding requires all routers along the path to be upgraded and configured to interpret the SPI bit correctly.

o For SPI Option B (Source Address Prefix): This method offers better backward compatibility. Legacy routers forward packets based on the destination address and standard routing rules. They treat the source address as a regular IPv6 address and ignore any slice semantics. Therefore, packets can traverse legacy nodes without issue, provided the path is otherwise valid. Only nodes that are explicitly configured to recognize the designated SPI prefix will inspect the source address, extract the SLID from its lower bits, and apply slice-specific forwarding policies. This allows for incremental deployment within an SR domain.

In both cases, ingress PEs that are not slice-aware will not set the SPI or encode a SLID. Slice-aware transit routers will not attempt to classify such packets into a slice and will forward them using default resources.

7. Security Considerations

The encoding mechanism defined in this document does not introduce new vulnerabilities or attack vectors to the SRv6 architecture. The security considerations discussed herein are inherent to the operation of network slicing and the use of source routing within a trusted domain, and they map to existing security paradigms for IPv6 and Segment Routing.

o Interaction with Legacy Nodes (SPI Option A): If SPI Option A (Traffic Class bit) is deployed, the risk of misforwarding by legacy nodes stems from reusing an existing field in a new way. This is a well-understood interoperability and incremental deployment consideration. Networks requiring end-to-end slice consistency must ensure path continuity, which may involve upgrading legacy nodes or selecting paths that exclude them.

o Address Space Management (SPI Option B): The need to carefully manage the address block used as the SPI Prefix to avoid overlap is a standard network planning requirement for any IPv6 deployment. It does not represent a new security flaw but emphasizes operational best practices.

8. IANA Considerations

TBD

9. References

9.1. 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/rfc/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/rfc/rfc8174>.

[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/rfc/rfc8200>.

[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/rfc/rfc8402>.

9.2. Informative References

[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/rfc/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/rfc/rfc8986>.

[RFC9543] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L., and J. Tantsura, "A Framework for Network Slices in Networks Built from IETF Technologies", RFC 9543, DOI 10.17487/RFC9543, March 2024, <https://www.rfc-editor.org/rfc/rfc9543>.

Authors' Addresses

Weiqiang Cheng
China Mobile
Beijing
China
Email: chengweiqiang@chinamobile.com

Peiyong Ma
China Telecom
Guangzhou
China
Email: mapeiy@chinatelecom.cn

Fenghua Ren
China Unicom
Beijing
China
Email: renfh3@chinaunicom.cn

Changwang Lin
New H3C Technologies
Beijing
China
Email: linchangwang.04414@h3c.com

Liyan Gong
China Mobile
Beijing
China
Email: gongliyan@chinamobile.com

Shay Zadok
Broadcom
Israel
Email: shay.zadok@broadcom.com

Mingyu Wu
CentecNetworks
China
Email: wumy@centec.com

Xuewei Wang
Ruijie Networks Co., Ltd.
Beijing
China
Email: wangxuewei1@ruijie.com.cn