spring
Internet-Draft
Intended status: Standards Track
Expires: 13 March 2026

J. Zhao, Ed.
W. Lv, Ed.
China Unicom

9 September 2025

The Correspondence between Packets and SRv6 Tunnels
draft-zhao-spring-srh-extended-srv6-policy-key-03

Abstract

This document defines a new extension header called the SRv6 Policy Key, which enhances path awareness in SRv6 networks. By embedding a unique path identifier within the packet header, network nodes can report path information to the controller. This enables the controller to maintain a real-time and accurate view of SR path status—even when Segment Identifiers (SIDs) are lost or real-time monitoring is infeasible. The mechanism significantly improves network availability and operational efficiency, especially in multi-path and load-balancing scenarios.

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 13 March 2026.

Copyright Notice

Table of Contents

1. Introduction

In SRv6 networks, the Software-Defined Networking (SDN) controller is responsible for centralized management and dynamic configuration of network resources, which is essential for achieving network flexibility and intelligence. However, the controller' s awareness of SRv6 packet paths currently relies on theoretical derivation, which lacks timeliness and accuracy. Delays in state updates and failures in acquiring real-time path information pose challenges in dynamic network environments.

For instance: * In multi-path tunnel configurations, the controller should adjust traffic routing based on the active/standby status and priority of pre-configured tunnels. Latency in state awareness can prevent prompt response to network changes, resulting in inaccurate path decisions. * In load-balancing scenarios with multiple parallel sub-paths, traffic distribution strategies (e.g., hashing or random selection) improve bandwidth utilization but complicate operations due to the difficulty of tracking packet routes in real time. To

address these issues, this document defines a new Segment Routing Header (SRH) extension: the SRv6 Policy Key, which serves as a unique tunnel identifier. ## 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 Policy KEY

This document defines a new SRH extension header, the SRv6 Policy Key, which is used to identify an SRv6 policy tunnel. This identifier is carried within the packet header and reported by network nodes to the controller. Using this identifier, the controller can accurately determine the actual path taken by packets within the Segment Routing domain. This significantly enhances the controller’ s state awareness, allowing it to obtain a more timely and accurate view of network status, thereby improving operational maintenance and decision-making processes.

2.1. Format of an SRv6 Policy KEY

The SRv6 Policy Key is appended to the end of the standard SRH (as defined in RFC9386) and has the following format:

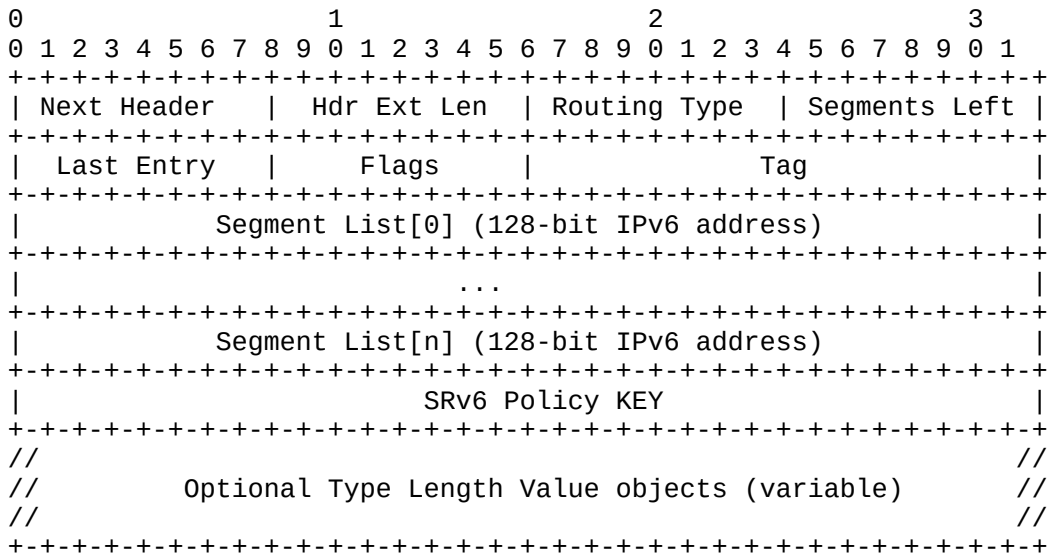


Figure 1: Format of an SRv6 Policy KEY

* SRv6 Policy KEY Field: Carries the core identifier information of the SRv6 tunnel, implemented in TLV format (see Section 3.2 for details).

* Other fields (Next Header, Hdr Ext Len, etc.): Comply with the standard SRH definition in RFC9386 to ensure compatibility with existing SRv6 devices.

2.2. SRv6 Policy KEY TLV

The SRv6 Policy Key is encapsulated in a TLV structure, which contains all parameters required to identify the SRv6 tunnel and its candidate paths. The TLV format is as follows:

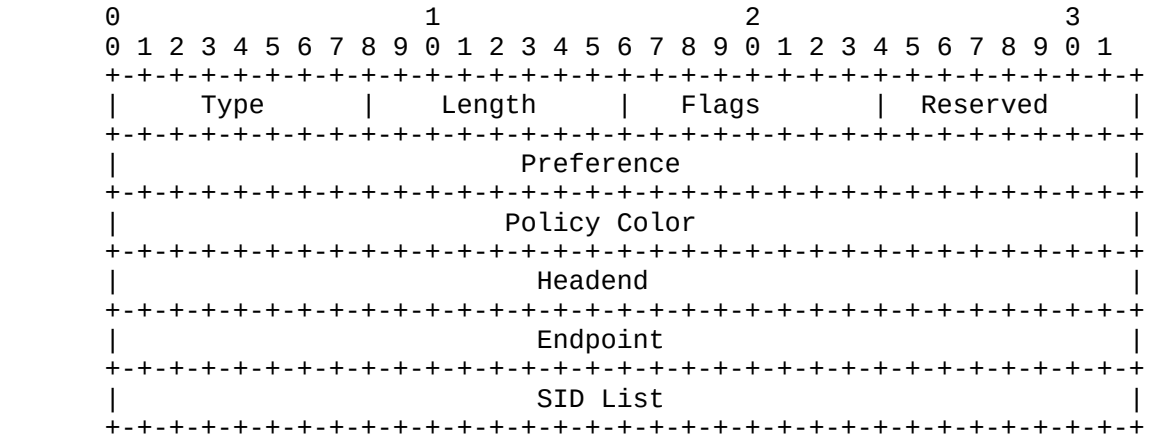


Figure 2: SRv6 Policy KEY TLV

* Type: 8-bit code point

* Length: Variable-length field size

* Flags: 8-bit flag field

* Preference: 32-bit priority value for candidate paths

* Policy Color: 32-bit color identifier

* Headend: 128-bit IPv6 address of the tunnel start point

* Endpoint: 128-bit IPv6 address of the tunnel endpoint

* SID List: Segment Identifier list for candidate paths under the policy.

3. Key Technologies and Implementation

3.1. Overall Interaction Architecture

The solution adopts a collaborative "controllernetwork node" architecture as its core: the controller assumes centralized analysis and decision-making responsibilities, while network nodes (including source nodes, destination nodes, and intermediate forwarding nodes) are responsible for packet processing and information reporting. Through the interaction mechanism of configuration distribution and information reporting, precise identification of service transmission tunnels is achieved.

3.2. Detailed Steps

3.2.1. Pre-configuration (Controller-Driven)

The controller configures the source node to embed a "SRv6 Policy Key" containing key tunnel information in the Segment Routing Header (SRH) of SRv6 packets when sending them. Simultaneously, it configures relevant network nodes, such as source nodes, destination nodes, or intermediate forwarding nodes, to detect SRv6 packets carrying specific service data, extract the service information and SRv6 Policy Key from them, and report these to the controller. If dynamic adjustment is not required, these configurations can also be pre-configured on the nodes.

3.2.2. Packet Processing (Executed by Network Nodes)

When generating SRv6 packets carrying specific service data, the source node attaches the SRv6 Policy Key in the SRH of the packets as per the pre-configuration and sends them. During the process of forwarding or receiving packets, network nodes such as source nodes, destination nodes, or intermediate forwarding nodes automatically extract the service information (e.g., service type, traffic characteristics) and SRv6 Policy Key from detected SRv6 packets carrying service data, preparing them for subsequent reporting.

3.2.3. Information Reporting and Tunnel Identification (Collaborative Completion)

Network nodes report the extracted service information and SRv6 Policy Key to the controller, supporting batch reporting of multiple sets of associated information over a specific time period. After receiving the information, the controller parses the corresponding SRv6 tunnel authentic specific service path using the SRv6 Policy Key, ultimately establishing a clear association that "a specific service is transmitted through a specific SRv6 tunnel."

4. Functional Description

4.1. Function1: Path Consistency Verification

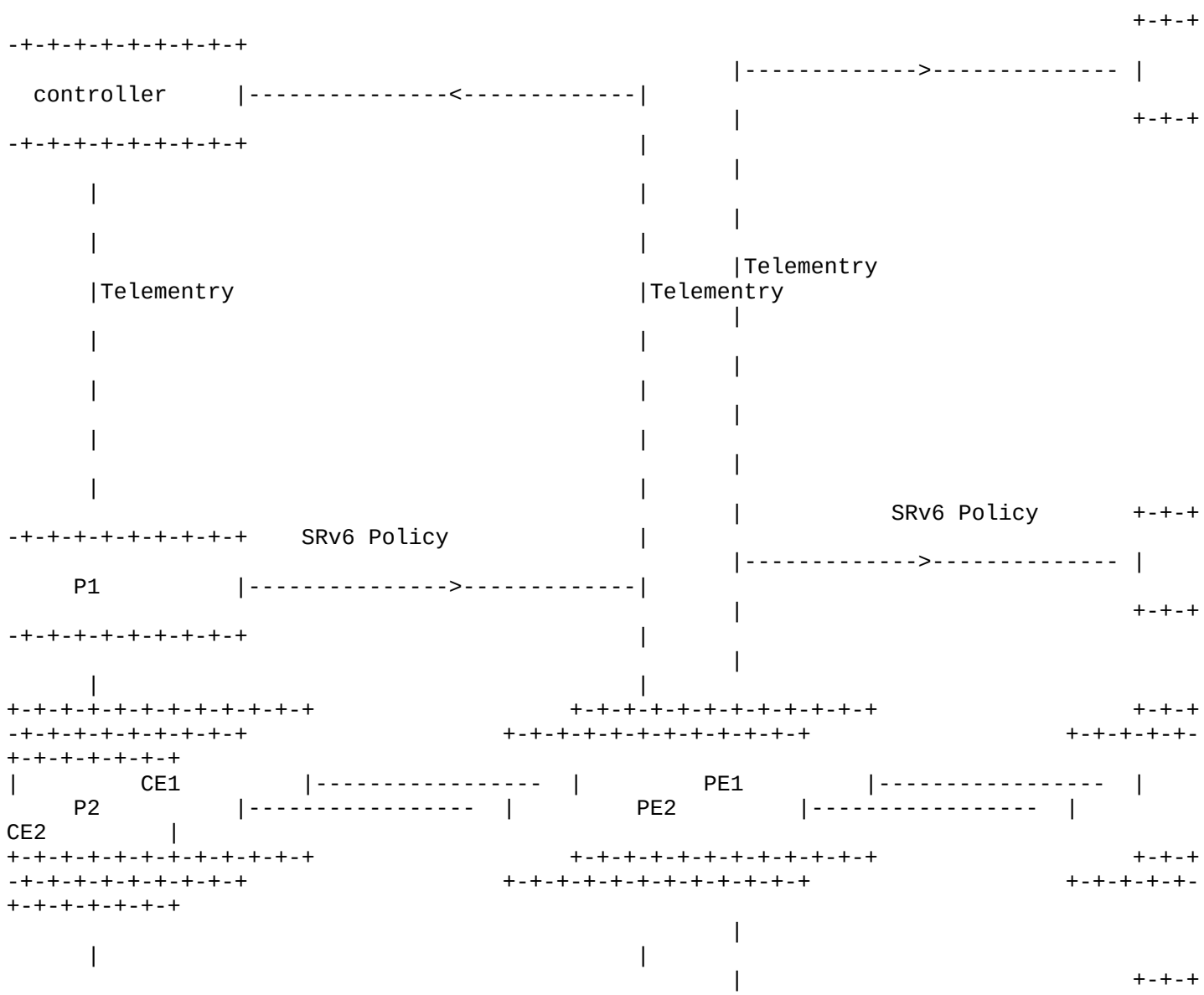
The controller uses the SRv6 Policy Key to compare actual packet paths against intended paths. This ensures congruence between data transmission routes and pre-configured paths, enhancing reliability and operational efficiency.

4.2. Function2: Service flow analysis function

Network nodes record and perform statistics on service flows based on the SRv6 Policy Key, candidate paths, and segment lists. This enables service impact analysis during node upgrades or relocations.

4.3. Function3: Controller path visualization

The controller collects and analyzes packet headers from network nodes, improving path visibility and manageability. The SRv6 Policy Key enables the controller to query candidate paths and reconstruct real-time service trajectories.



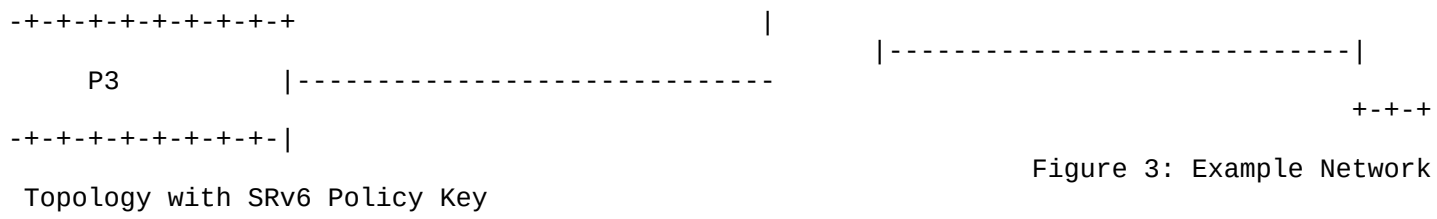


Figure 3: Example Network Topology with SRv6 Policy Key

5. Use Case

5.1. Enhancing Real-Time Path Recognition

In practical SRv6 deployments, the controller often lacks real-time awareness of actual packet paths due to state update latency and acquisition malfunctions. The SRv6 Policy Key provides a unique identifier that enhances real-time path recognition.

As shown in Figure 3, when a packet enters the headend node PE1, the SRv6 Policy Key is added to the packet header. This key carries essential tunnel identification information that enables precise path recognition throughout the transmission path.

This enhancement is particularly valuable in:

* Triple-Redundant Tunnels (P1, P2, P3): Achieving seamless switch-over between primary and backup tunnels requires precise awareness of each path’s state. The SRv6 Policy Key enables each node (P1, P2, P3) to accurately identify and report the path being used, allowing informed switching decisions.

* Single-Tunnel Multipath Policy: Traffic is dynamically distributed among multiple paths (P1, P2, P3) according to link conditions and priority levels. The SRv6 Policy Key provides accurate path awareness at each transit node, enabling efficient traffic handling and network optimization.

5.2. Improving Path Visibility

In the network topology shown in Figure 3, intricate load-balancing scenarios present significant challenges for path visibility. A single logical path from PE1 to PE2 may be distributed across three concurrent sub-paths (via P1, P2, P3) following hash rules.

Through the SRv6 Policy Key mechanism, each node along the path (P1, P2, P3, and PE2) can detect and report the actual path usage to the controller. This enables the controller to:

* Identify exactly which sub-path (P1, P2, or P3) is carrying specific traffic flows

* Monitor load distribution patterns in real-time across all available paths

* Correlate service performance metrics with specific paths through the network

* Make data-driven decisions for traffic engineering and optimization

This enhanced visibility is crucial for maintaining service level agreements and troubleshooting performance issues.

6. Security Considerations

TBD.

7. IANA Considerations

TBD.

8. Normative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <https://www.rfc-editor.org/info/rfc2460>.

[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>.

[RFC9386] Fioccola, G., Volpato, P., Palet Martinez, J., Mishra, G., and C. Xie, "IPv6 Deployment Status", RFC 9386, DOI 10.17487/RFC9386, April 2023, <https://www.rfc-editor.org/info/rfc9386>.

[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>.

Authors' Addresses

Jing Zhao (editor)
China Unicom
Beijing
China
Email: zhaoj501@chinaunicom.cn

Wenxiang Lv (editor)
China Unicom
Beijing
China
Email: lvwx28@chinaunicom.cn