spring
Internet-Draft
Intended status: Standards Track
Expires: 15 August 2025

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

11 February 2025

The Correspondence between Packets and SRv6 Tunnels
draft-zhao-spring-srh-extended-srv6-policy-key-02

Abstract

This paper introduces a new extension header, the SRv6 Policy Key, which addresses the issues of timeliness and accuracy in controller-aware path management within SRv6 networks. By adding a unique path identifier to the message header, this scheme enables network nodes to report path information to the controller. This ensures that the controller maintains a real-time and accurate view of the SR path status, even if the SID is lost during transmission or if the controller cannot monitor it in real time and accurately.

The approach aims to enhance network availability and operational efficiency, particularly in scenarios involving multi-path tunnel configurations and load balancing.

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 15 August 2025.

Copyright Notice

Copyright (c) 2025 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

In SRv6 networks, the software-defined network (SDN) controller serves as a core component, responsible for the centralized management and dynamic configuration of network resources. It is crucial for achieving network flexibility and intelligence. Currently, the controller's perception of SRv6 message paths relies on theoretical derivation, with limitations in timeliness and accuracy. State update latency and acquisition malfunctions pose challenges for real-time scenarios. Using the configuration of multipath tunnels as an example, ideally, it should dynamically adjust traffic routing based on the master-standby relationships and priority levels of the three preconfigured tunnels. This adjustment is crucial for ensuring the high availability and operational efficiency of the network. In practical applications, controller state-sensing latency causes failure to react promptly to network linkage changes, leading to inaccurate path determinations and affecting traffic-related operations.. Moreover, In tunnel load-balancing scenarios with multiple parallel sub-paths, hashing/random-based traffic distribution strategies boost bandwidth efficiency but

increase maintenance complexity as real-time packet route tracking is difficult. To address these issues, this paper defines a new SRH extension header called "SRv6 Policy Key," which is used to identify the tunnel.

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 Policy KEY

We define a new SRH extension header called "SRv6 Policy Key," which is used to identify the tunnel. This identifier is conveyed through the message header and communicated to the controller by the network node. This process empowers the controller to discern the SR path, thereby enhancing its state-aware capabilities within the Segment Routing domain. As a result, the controller can apprehend the network’s real-time status with greater speed and accuracy, significantly aiding in the facilitation of operational maintenance decision-making processes.

2.1. Format of an SRv6 Policy KEY

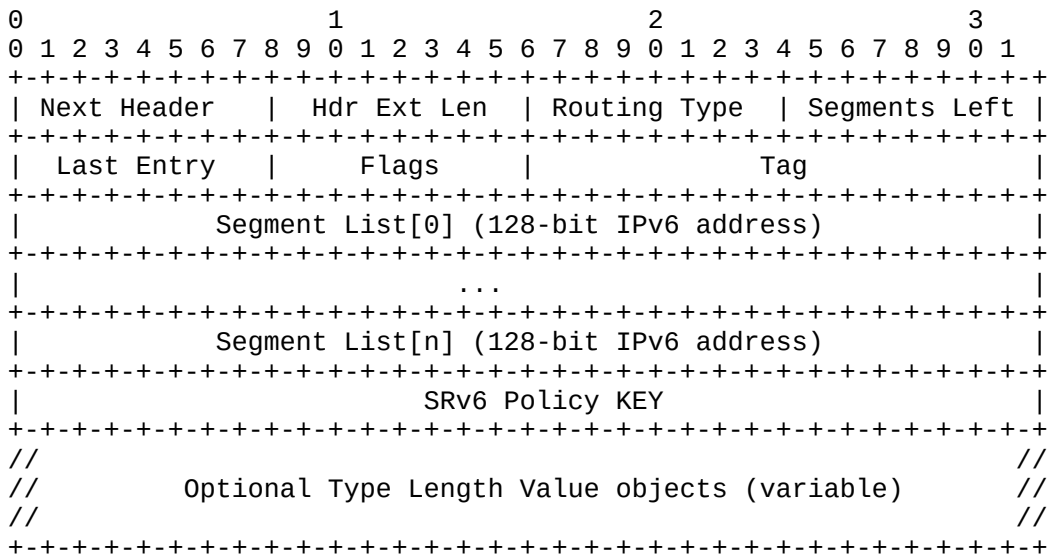


Figure 1: Format of an SRv6 Policy KEY

2.2. SRv6 Policy KEY TLV

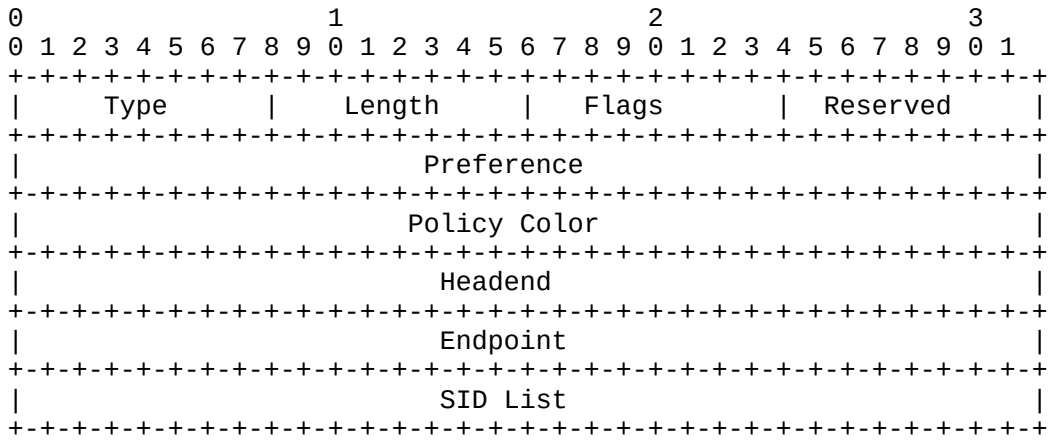


Figure 2: SRv6 Policy KEY TLV

* Type: An 8-bit code point.
* Length: The length of the variable-length data field in bytes 6.
* Flags: 8bit, marks list.
* Preference: 32bit, marks SRv6 Policy Candidate Path.
* Policy Color: 32bit, a Color of SRv6 Policy.
* Headend: 128bit, first node of SRv6 Policy.
* Endpoint: 128bit, destination address of SRv6 Policy.

3. Functional Description

3.1. Function1: Path Consistency Verification

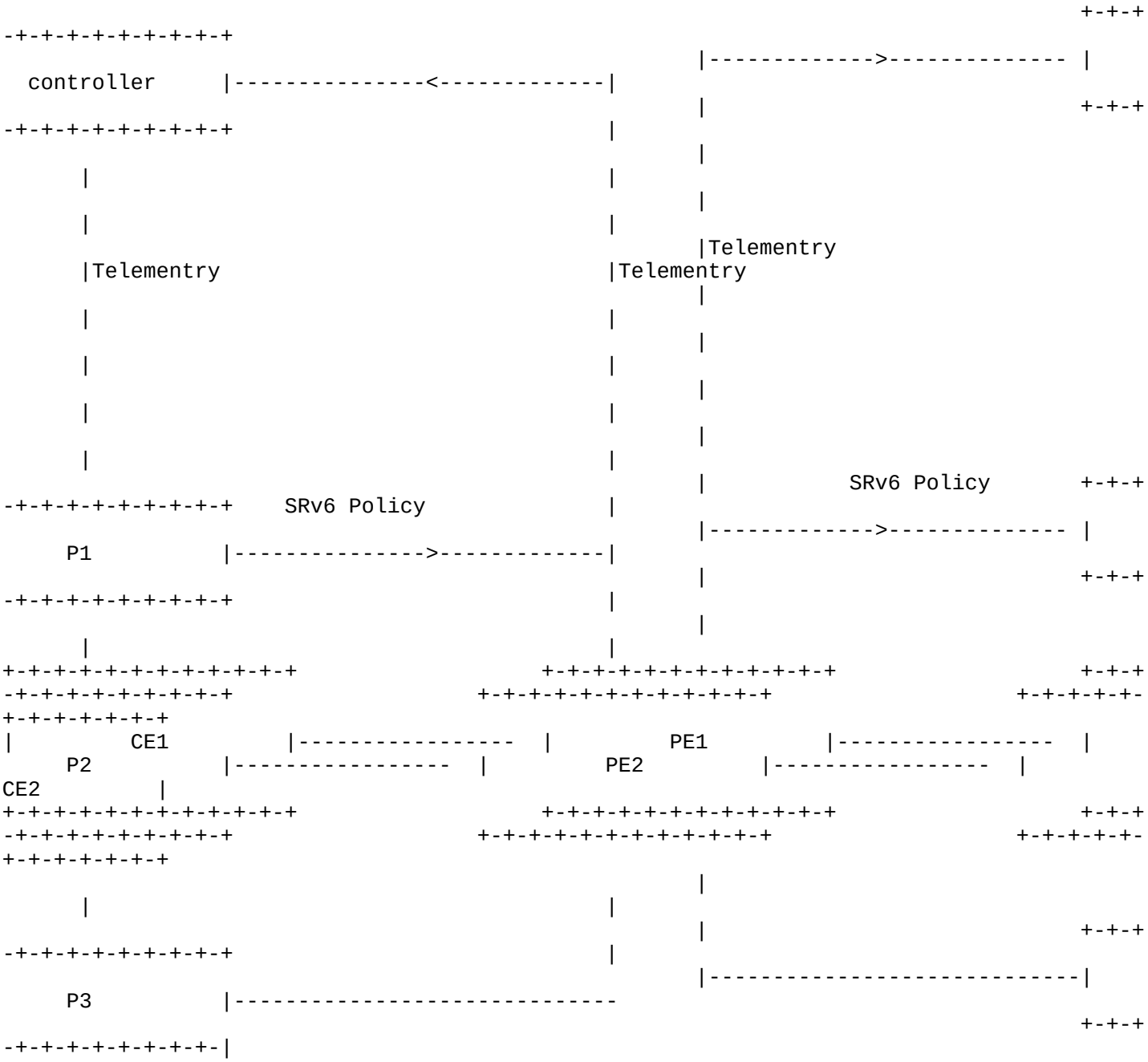
The awareness of actual paths ensures the controller can accurately evaluate the congruence between the factual routes of data transmission and the pre-established ideal paths. This procedure encompasses a systematic comparison of network packets'forwarding trajectories against the planned routes, aiming to detect and rectify potential deviations in path. Consequently, this boosts the network's reliability and operational efficiency.

3.2. Function2: Service flow analysis function

A network node can document the traversal of SRv6 Policies, Candidate Paths, and Lists, and accumulate statistics in accordance with the service logic at these three hierarchical levels. In instances of node upgrade or relocation, the impacted services can thus be identified. Network nodes are capable of gathering traffic statistics based on the SRv6 Policies, Candidate Paths, and Lists that traverse the node, correlating these statistics with the service logic at the three tiers.

3.3. Function3: Controller path visualization

The controller gathers the header information from packets processed at each network node and conducts statistical analyses, thereby enriching the visibility and manageability of network path data.



Enable SRv6 Policy Path Identifier Function. Enable this function at the head node (PE1) of the SRv6 Policy either through the controller or the device command-line interface. When a packet enters the head node of the SRv6 tunnel, the head node adds the SRv6 Policy Key to the packet.

Packet Identification and Path Awareness.

* Enable the detection function at the intermediate nodes (P1,P2,P3) or the destination node (PE2) either through the controller or the device command-line interface.

* Nodes will parse all SRv6 Policy packets passing through themselves and extract service information and the SRv6 Policy Key from these packets. Within a specific time period, statistics on the service information associated with each SRv6 Policy Key are collected and the statistical results are reported to the controller. The controller uses the SRv6 Policy Key to query the candidate path list under the corresponding SRv6 policy, so as to obtain the service details of each path passing through this node, thereby perceiving the real path of the packet.

4. Use Case

4.1. Case 1: Enhancing Real-Time Path Recognition

The controller can’t sense packet paths in real-time. The SRv6 Policy Key provides unique path identifiers, enhancing real-time path-identification ability. Latency in path-information sensing hampers the accuracy of deducing real paths. Link-state update delays and revalidation needs pose challenges. The SRv6 Policy Key strengthens the controller’s instant path-recognition capacity, addressing network device configuration update delays. By embedding unique path identifiers, the SRv6 Policy Key eases path-decision-making based on immediate info, ensuring network control accuracy and efficiency. This is evident in two scenarios: - In the architectural design featuring triple-redundant tunnels, achieving a seamless switch-over between the primary and backup tunnels necessitates precise awareness of the state of each path to uphold uninterrupted service delivery. - Under the single-tunnel multipath policy, traffic is dynamically distributed according to link conditions and priority levels, needing accurate path awareness for efficient handling and network performance optimization.

4.2. Case 2: Improving Path Visibility

The controller cannot sense the actual paths in real-time. In intricate network load-balancing scenarios, a single path is bifurcated into three concurrent sub-paths to collaboratively bear the traffic load, with allocation executed randomly by devices following designated hash rules. Through the SRv6 Policy Key, the controller can attain real-time visibility of paths, thereby overcoming the uncertainty and unpredictability of paths engendered by the original random allocation mechanism.

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. 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