SPRING
Internet-Draft
Intended status: Standards Track
Expires: 19 June 2026

F. Yang
China Mobile
C. Lin
New H3C Technologies

16 December 2025

SID as source address in SRv6
draft-yang-spring-sid-as-source-address-07

Abstract

SRv6 is being rapidly deployed and is currently primarily used in trusted-domain backbone networks. However, we have also observed that SRv6 is beginning to extend toward end-user devices, e.g., in SD-WAN deployments. SD-WAN can be deployed in third-party clouds or at customer sites, causing the physical boundary of SRv6 to become blurred. This introduces certain security issues, such as middlebox filtering and unauthorized access to others' VPN in Section 8.1 and Section 6 in [I-D.draft-ietf-spring-srv6-security]. This proposal mitigates these risks by using SID as source address in SRv6 packets.

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 19 June 2026.

Copyright Notice

Table of Contents

1. Introduction

SRv6 is being rapidly deployed and is currently primarily used in trusted-domain backbone networks. However, we have also observed that SRv6 is beginning to extend toward end-user devices, e.g., in SD-WAN deployments. SD-WAN can be deployed in third-party clouds or at customer sites, causing the physical boundary of SRv6 to become blurred. This introduces certain security issues, such as middlebox filtering and unauthorized access to others' VPN in Section 8.1 and Section 6 in [I-D.draft-ietf-spring-srv6-security]. This proposal

mitigates these risks by using SID as source address in SRv6 packets.

On one hand, SRv6 packets carry SIDs that dictate packet forwarding behavior; if a VPN SID is tampered, it will compromise the isolation of the VPN. On the other hand, using loopback as source address in SRv6 packets will cause legitimate traffic be blocked by the firewall. The reason has been elaborated in Section 8.1 of [I-D.draft-ietf-spring-srv6-security]. By using SID as source address can solve both issues.

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. Using SRv6 SID as Source Address

There are still the following key gaps in current network technology:

Application-aware features. It is necessary to provide differentiated services based on the different services of the same user. For example, video conferencing needs to avoid stuttering or screen tearing due to congestion and packet loss to ensure a customer experience, while general web browsing services can strive for the best.

Data plane programming capabilities. Identify and classify user application data, and transfer it to the appropriate service-level tunnel based on the results.

Ability to perceive the user experience. Through real-time detection and perception of user-level service experience, it works with intelligent routing to ensure service assurance for high-priority services. Currently, there is a lack of traffic identification for rapid classification and statistical analysis of the user experience of this type of traffic.

Ability to prevent leakage of network services. The security of the access network is relatively poor, and there is a risk of leakage of information related to user applications.

2.1. User Traffic

There are several cases for using SRv6 SID as source address.

2.1.1. L2 VPN Virtual Private Wire Service(VPWS)

For L2 VPN VPWS case, the user traffic towards SRv6 provider backbone will be encapsulated in SRv6 tunnel. When constructing an SRv6 packet, the source address field of the SRv6 packet should be assigned with the local VPN SID value of the PE device. The local VPN SID value can be determined by L2 Cross-Connect.

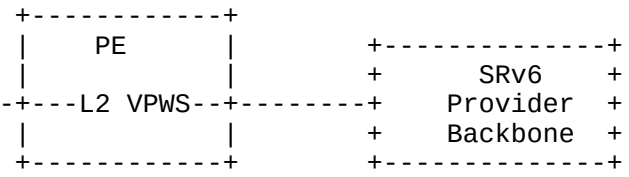

Figure 1: L2 VPWS

2.1.2. L2 VPN Virtual Private LAN Service(VPLS)

For L2 VPN VPLS, the user traffic towards SRv6 provider backbone will be encapsulated in SRv6 tunnel. When constructing an SRv6 packet, the source address field of the SRv6 packet should be assigned with the local VPN SID value of the PE device. The local VPN SID value can be determined by L2 VPN VPLS.

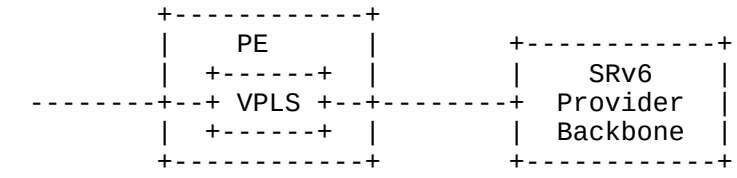

Figure 2: L2 VPLS

2.1.3. L3 IPv4/IPv6 VPN Service

For L3 IPv4/IPv6 VPN Service case, the user traffic towards SRv6 provider backbone will be encapsulated in SRv6 tunnel. When constructing an SRv6 packet, the source address field of the SRv6 packet should be assigned with the local VPN SID value of the PE device. The local VPN SID value can be determined by the L3 IPv4/ IPv6 VPN.

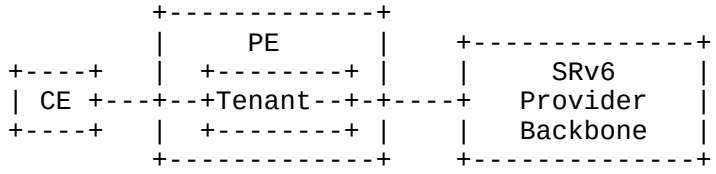

Figure 3: L3 VPN

2.2. Control Traffic

Control traffic will not be terminated by VPN, thus should not be impacted.

2.3. OAM Traffic

OAM traffic terminated by the SRv6 tunnel may use the SRv6 SID as source address, such as ping, trace. Refer to RFC 8986 4.1.1, Allowing the processing of specific Upper-Layer header types is useful for Operations, Administration, and Maintenance (OAM). As anexample, an operator might permit pinging of SIDs. To do this, they may enable local configuration to allow Upper-Layer header type 58(ICMPv6).

2.4. Management Traffic

Management traffic will not be terminated by VPN, thus should not be impacted.

3. Using Source Address for Validation in SRv6 Network

Refer to Figure 7, when the traffic is passing through the SRv6 bearer network, the received traffic can be verified at the following two locations.

* Ingress PE node of IPv6 backbone network

* C-PE node of destination tenant site or destination client network

3.1. Source Verification on the SRv6 Tunnel 2nd Hop Node

Main reason for doing this is to prevent SRv6 tunnel source address fraud.

On the C-PE node, it will receive one or more local SRv6 SIDs configuration from controller or generate SRv6 SID locally. On the nexthop node, i.e. PE node, it can learn those SRv6 SID either from controller or IGP protocol.

Suppose the C-PE will generate SRv6 packets with the SRv6 SID as source address, when the SRv6 end point node next to the C-PE, i.e. PE node, receives the packets, it can do forward table lookup with incoming interface and source address as key for forwarding table lookup. If the lookup failed, it is considered as illegal traffic and should not be forwarded. Otherwise, the source address is legal.

3.2. Source Verification on the SRv6 Tunnel Tail

Main reason for doing this is to prevent SRv6 tunnel tail SID fraud or misconfiguration. Only after the packet is forwarded to the SRv6 egress node (that is, the access point of the destination client network, such as C-PE) can we have the opportunity to continue to verify whether the packet is legal.

As mentioned before, the source C-PE will generate SRv6 packets with the SRv6 SID as source address. On the destination C-PE, it has source verification table with all of source VPN SIDs have been authorized for access.

After receiving SRv6 packet, based on the source address, it can check the SRv6 packet for authorized access.

If the SRv6 packet passes check, it will forward the SRv6 packet; otherwise, discard it.

3.2.1. Content of SRv6 Source Verification Entry

Every VPN will have a source verification table. And there are multiple source verification entries in the source verification table, and each table entry contains the following contents:

The source service address which is encapsulated as the outer source IPv6 address of the packet, used to identify the service of the source client network. For example, the source service SID of SRv6.

The source service address is the content that must be verified.

3.2.2. Management of SRv6 Source Verification Table

The SRv6 source verification entry can be created in the following ways:

* Manual static configuration on the SRv6 egress node. Configure the source address in local L3VPN/L2VPN source address Verification table.

* Dynamic creation after learning the service address of the source client network through BGP. When the L3VPN/L2VPN route with the remote L3VPN/L2VPN service id is inserted into the local VPN table, the relationship between the local L3VPN/L2VPN service sid of the destination VPN table and the remote L3VPN/L2VPN service id is recorded to form a dynamic source address Verification table in local VPN table.

4. Use Cases

4.1. SRv6 Network with SR-aware Stateful Firewall

4.1.1. Problem Statement

To provide VPN service in an SRv6 network [RFC9252], the ingress PE encapsulates the payload in an outer IPv6 header with the Segment Routing Header (SRH) [RFC8754] carrying the SR Policy segment list along with the VPN Service SID. If the VPN service is with best-effort connectivity, the destination address of the outer IPv6 header carries the VPN service SID and the SRH is omitted.

Along the forwarding path in the SRv6 network, firewalls may be deployed to filter the traffics. If a firewall is SR-aware, it will retrieve the final destination of an SRv6 packet from the last entry in the SRH rather than the destination address field of the IPv6 header [I-D.draft-ietf-spring-sr-service-programming].

A stateful firewall keeps a track of the state of the network connections traveling across it. Whenever a packet arrives to seek permission to pass through it, the firewall checks from its state table if there is an active connection between identified by 3 tuple or 5 tuple. Thus only legitimate packets are allowed to be transmitted across it.

Figure 4 and Figure 5 show the bidirectional VPN traffic packets passing through a firewall in an SRv6 network.

The source address of the outer IPv6 header is the IPv6 address of ingress PE. The final destination address of the outer IPv6 header is the VPN Service SID of egress PE. In the SR-Policy-based way, the final destination address is encapsulated in the last entry in the SRH, Segment[0]. In the best-effort way, the SRH is omitted.

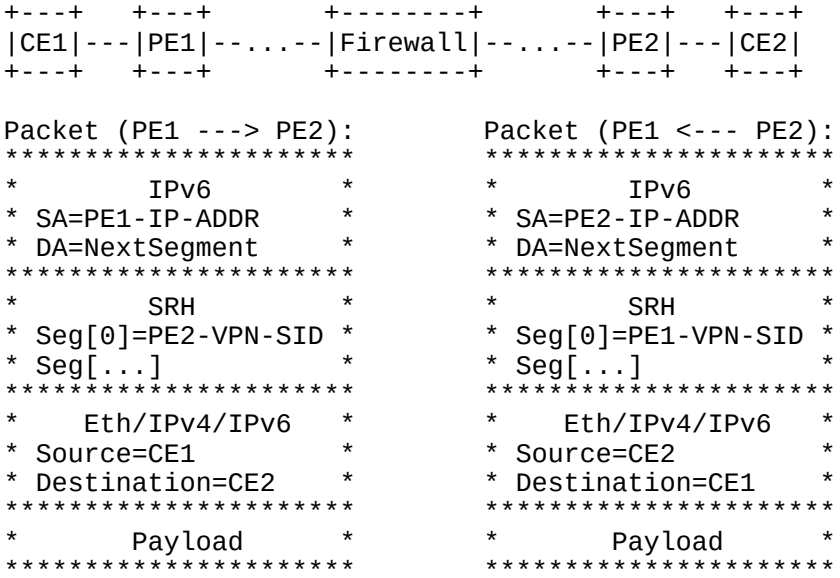

Figure 4: SR-Policy-based VPN Traffic across Firewall

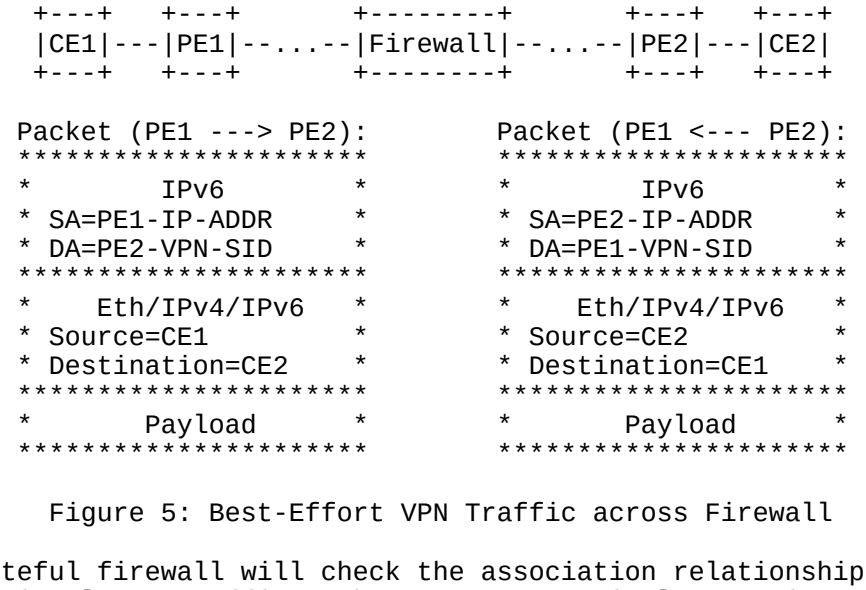

Figure 5: Best-Effort VPN Traffic across Firewall

The stateful firewall will check the association relationships of the bidirectional VPN traffic packets. A common implementation may record the key information of the packets on forward way(internal to external), such as source address and destination address. When receiving a packet on backward way(external to internal), it checks the state table if there is an existing forward packet flow. For

example, the firewall may require that the source address of packet on backward way matches the destination address of packet on forward way, and destination address will be checked in the similar way. If not matched, the packet on the backward path will be regarded as illegal and thus dropped.

An SR-aware firewall is able to retrieve the final destination of an SRv6 packet from the last entry in the SRH. The <source, destination> tuple of the packet from PE1 to PE2 is <PE1-IP-ADDR, PE2-VPN-SID>, and the other direction is <PE2-IP-ADDR, PE1-VPN-SID>. However, the source address of the outer IPv6 packet is usually a loopback interface of the ingress PE. Eventually, the source address and destination address of the forward and backward VPN traffic are regarded as different flow, and they may be blocked by the firewall.

4.1.2. Solution for SRv6 Traffic Pass Thru SR-aware Stateful Firewall

In the SRv6-based VPN service, the final destination of the outer IPv6 header is the VPN-SID of the egress PE, which is associated with that VPN service. But the source address of the outer IPv6 header is usually unrelated to the VPN service. So, it can be difficult for a stateful firewall to establish the association relationship between the bidirectional traffic flows.

The proposed solution is to unify the semantic of the source and destination address thus ensure the symmetry of the bidirectional flow.

When an ingress PE receives the client packet from CE, it checks which L3 VPN service it belongs to, and uses the VPN-SID associated with that L3 VPN service as the source address when encapsulating the outer IPv6 header with the optional SRH.

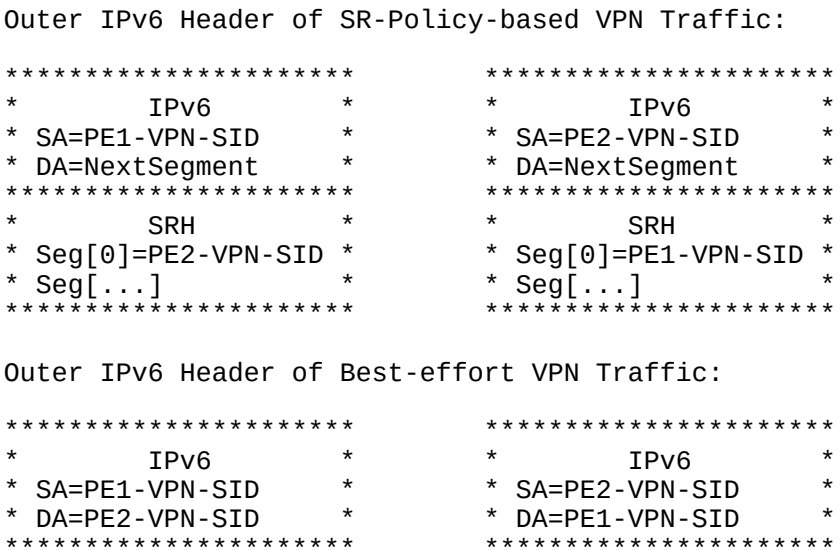

Figure 6: Outer IPv6 Header in the Proposed Solution

According to [RFC8402] and [RFC8986], an SRv6 VPN Service SID is an IPv6 address, and it is routable by its Locator prefix in the SRv6 network. In the proposed solution, when an SRv6 VPN Service SID is used as the source address of the outer IPv6 header in the SRv6 network, it is treated as a normal IPv6 address and does not perform any special behavior.

4.2. Enhanced Traffic Isolation between VPNs

4.2.1. Problem Statement

As analyzed in [RFC5920], there is no 100% safe network. There is a risk of traffic being hijacked or tampered anywhere in the network.

In SRv6 network when someone manipulate the SRH, he/she can reach any VPNs without authorized. In other words, VPN isolation needs be improved in the source routing scenario.

Taking the SRv6 SDWAN overlay network as an example, if C-PE is hijacked, misconfigured or misconnected, the services that should be isolated between CPE sites can be accessible to each other.

As shown in the figure below, C-PE is deployed in the tenant site, and the tenant of the site is responsible for operation and maintenance management. Normally users in client network 1 (CN1) of C-PE1 can only communicate with users in CN1 of other C-PEs through IPv6 backbone network. CN1 is isolated from other client networks, and traffic cannot be forwarded to each other.

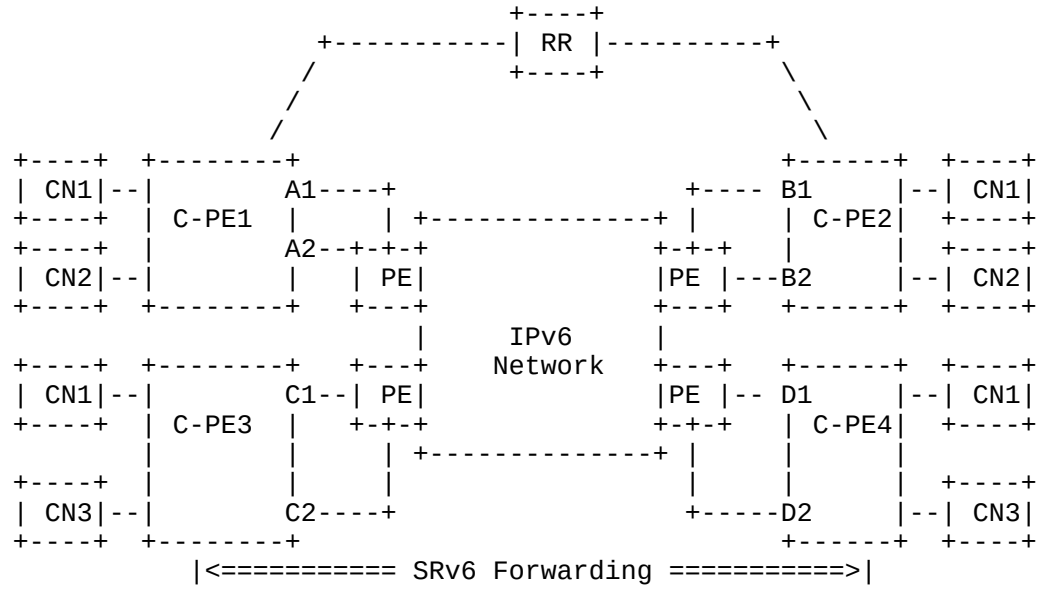

Figure 7

However, due to some misconfiguration or security issues, the destination address of VPN packets sent by C-PE to other destination client networks may be filled in as the service address of other client networks.

For example, the destination address of the traffic from CN1 of C-PE1 to CN1 of C-PE2 is misconfigured or tampered with as the service SID of CN3 of C-PE4. The traffic can be send to C-PE4. If the service SID happens to exist in CN3 of C-PE4, the traffic will be forwarded to CN3. This is a very serious security vulnerability for client networks that should be completely isolated.

In theory, the HMAC TLV in the SRH with integrity check on the way can address this problem. However, HMAC integrity check is hard to be supported by the routers hardware in line rate. Thus nobody actually do that on router.

By leveraging the routes' native search capability, we introduce a source address verification mechanism to address such problem.

4.2.2. Source Validation Solution for SRv6 SDWAN Network

In the SRv6 SDWAN overlay network, in order to completely isolate the VPN services of different tenant sites, the SRv6 source verification function can be enabled on the C-PE of the tenant site connecting to the IPv6 backbone network. At the same time, specify which user sites from which C-PE can communicate with it on each C-PE.

That is, destination C-PE verifies the source VPN SID, destination VPN SID.

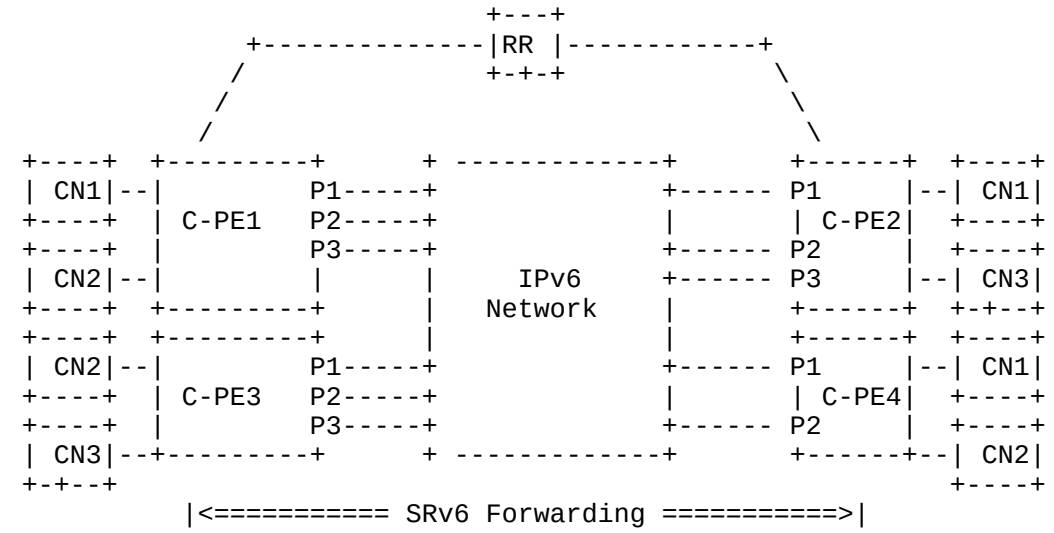

Figure 8: SDWAN

Taking the networking shown in Figure 8 as an example, C-PE1 connects two VPN tenants CN1 and CN2, and C-PE2 connects VPN tenants CN1 and CN3.

1) Configure VPN SID.

```
   VPN SID on C-PE1:
      CN1:
         vpn-instance 1 end-dt4 100::100
      CN2:
         vpn-instance 2 end-dt4 100::200
   VPN SID on C-PE2:
      CN1:
         vpn-instance 1 end-dt4 200::100
      CN3:
         vpn-instance 3 end-dt4 200::300
   VPN SID on C-PE3:
      CN2:
         vpn-instance 2 end-dt4 300::200
      CN3:
         vpn-instance 3 end-dt4 300::300
   VPN SID on C-PE4:
      CN1:
         vpn-instance 1 end-dt4 400::100
      CN2:
         vpn-instance 3 end-dt4 400::200
```

2) Configure source address verification entries.

```
   Source address verification table on C-PE1:
         vpn-instance 1:
             Trusted-source-address 200::100
             Trusted-source-address 400::100
         Vpn-instance 2:
             Trusted-source-address 300::200
             Trusted-source-address 400::200
   Source address verification table on C-PE2:
         Vpn-instance 1:
             Trusted-source-address 100::100
             Trusted-source-address 400::100
         Vpn-instance 3:
             Trusted-source-address 300::300
```

4.2.3. Source Validation Solution for SRv6 Core Network

Some operators are currently building, or plan to build an IPv6-only native infrastructure for their core network. These operators are also looking at the possibility to set up an explicit path based on the IPv6 source address for specific types of traffic in order to efficiently use their network infrastructure. In such an environment, the IPv6 source address could be used by the edge nodes of the network to steer traffic and forward it through a specific path other than the optimal path. Additionally, one of the fundamental requirements for SRv6 core network architecture is to

provide scalable, isolated tenant networks.

Due to some misconfiguration or security issues, when the traffic is pass through the SRv6 core network, the received traffic can be verified by source verification. The SRv6 source verification function can be enabled on the PE of the tenant network connecting to the PE-based SRv6 core network.

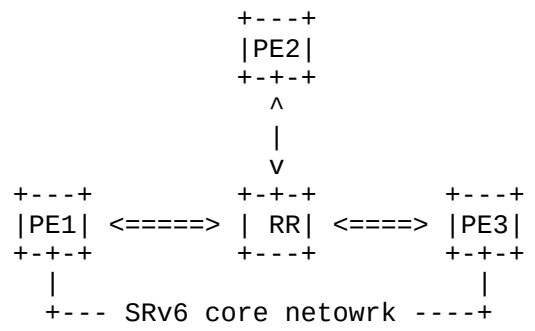

Figure 9: PE-based SRv6 core network

5. IANA Considerations

This document has no IANA actions.

6. Security Considerations

TBD.

7. References

7.1. 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/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>.

[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>.

[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/rfc/rfc4301>.

[RFC9252] Dawra, G., Ed., Talaulikar, K., Ed., Raszuk, R., Decraene, B., Zhuang, S., and J. Rabadan, "BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)", RFC 9252, DOI 10.17487/RFC9252, July 2022, <https://www.rfc-editor.org/rfc/rfc9252>.

[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>.

7.2. Informative References

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, DOI 10.17487/RFC5920, July 2010, <https://www.rfc-editor.org/rfc/rfc5920>.

[I-D.draft-ietf-spring-sr-service-programming] Abdelsalam, A., Xu, X., Filsfils, C., Bernier, D., Li, C., Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and S. Salsano, "Service Programming with Segment Routing", Work in Progress, Internet-Draft, draft-ietf-spring-sr-service-programming-12, 3 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-service-programming-12>.

[I-D.draft-ietf-spring-srv6-security] Buraglio, N., Mizrahi, T., tongtian124, Contreras, L. M., and F. Gont, "Segment Routing IPv6 Security Considerations", Work in Progress, Internet-Draft, draft-ietf-spring-srv6-security-09, 6 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-security-09>.

Authors' Addresses

Feng Yang
China Mobile
China
Email: Email [REPLACE/DELETE]

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