SPRING Working Group
Internet-Draft
Intended status: Standards Track
Expires: 14 November 2025

C. Huang
China Telecom
X. Song
ZTE Corp.

13 May 2025

SRv6 for PPPoE Transport
draft-song-spring-pppoe-srv6-00

Abstract

This document presents a method of utilizing IPv6 underlay tunnels to transfer the PPPoE session information in broadband networks. By taking advantage of the programmability of SRv6 SIDs, it not only enables trusted authentication and secure access for broadband users but also meets the needs of operators to provide differentiated services to broadband users and flexibly deploy services.

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 14 November 2025.

Copyright Notice

Table of Contents

1. Introduction

PPPoE, see [RFC2516] as a traditional protocol for broadband user authentication and access, was widely used in the DSL era. With the development of the Internet and the digital transformation of industries, operators are required to offer refined, differentiated, and deterministic broadband services to users. These services demand that the broadband network can allocate necessary network resources based on service requirements, and support refined operation capabilities such as service-based billing. This may involve functional requirements like network slicing and dynamic QoS, which are difficult to support with traditional PPPoE.

This document proposes a method of transmitting PPPoE session information through IPv6 underlay tunnel technology. By leveraging the PPPoE session management capabilities and the programmability of SRv6 [RFC8986], it not only provides broadband users with trusted authentication and secure access but also meets the operators' needs for ensuring differentiated services and flexibly deploying specific services.

2. Conventions

2.1. 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.

2.2. Terminology

Refer to [RFC2516], [RFC8986] for the key terms used in this document.

3. Use Case

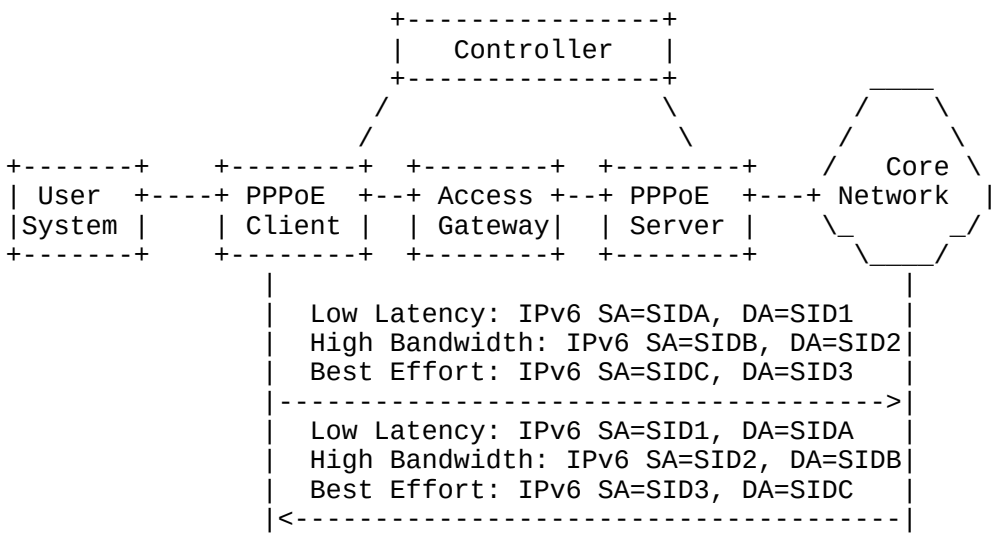

Figure 1: PPPoE over SRv6 in SD-WAN Network

The PPPoE client initiates dial-up connections to the PPPoE server using different IPv6 Source Addresses(SA) and Destination Addresses(DA) based on specific service requirements (e.g., low latency, high bandwidth, isolated VPN, etc.). These IPv6 SA and DA are 128-bit Segment Identifier(SID) addresses with programmabilty. Each SID represents distinct processing behaviors, such as directing traffic to a low-latency channel, high-bandwidth channel, or dedicated VPN channel. As shown in the figure, the management and control system configures and distributes IPv6 SA and DA to both the PPPoE client and server. For example:

The SID A assigned to the PPPoE client and SID 1 assigned to the PPPoE server indicate traffic routing through a low-latency channel,

While SID B at the PPPoE client and SID 2 at the PPPoE server indicate traffic routing through a high-bandwidth channel.

Here, the management and control system, for example, an SDN controller or orchestration systems can manage devices and distribute parameters to the PPPoE client and server via protocols such as NETCONF or BBF TR-069.

4. PPPoE over SRv6 Tunnel

After the PPPoE client and the PPPoE server obtain the SRv6 tunnel address, they construct a tunnel to achieve communication from the PPPoE client to the server. After a successful dial-up, the PPPoE client obtains the service address used for PPPoE communication through the allocation by the PPPoE server and enters the data transmission stage. Among them, the session management process of PPPoE over SRv6, including PPPoE negotiation, PPP negotiation and other processes, shall comply with the PPPoE communication specified in [RFC2516] and [RFC5072]. It’s noted that this specification does not change the PPP and PPPoE negotiation processes, and only realizes the carrying of PPPoE session information through the IPv6 header. The acquisition of Prefix Delegation (PD) addresses by both the PPPoE client and the PPPoE server can be statically configured or dynamically obtained, such as through the DHCPv6 method.

Static configuration: The suffix part of the IPv6 address is statically configured, and the 128-bit address generated by the PD prefix address plus the suffix address is used as the outer-layer IPv6 tunnel address.

Dynamic configuration: The PPPoE client establishes a connection with the management and control system. After passing the authentication, the management and control system issues the suffix information to the PPPoE client. The PPPoE client uses the 128-bit address generated by the PD prefix address plus the suffix address as the outer-layer IPv6 tunnel address.

The client assembles the complete outer-layer IPv6 address, which is used for the outer-layer encapsulation of establishing the SRv6 tunnel. The source address is the PPPoE client address, which has mapping of MAC address of PPPoE client to SRv6 SID , and the destination address is the PPPoE server address.

After receiving the dial-up request initiated by the PPPoE client, the PPPoE server can map the service addresses of the client with the server to the public network or the enterprise intranet through NAT or routing policies.

5. Encapsulation for PPPoE over SRv6

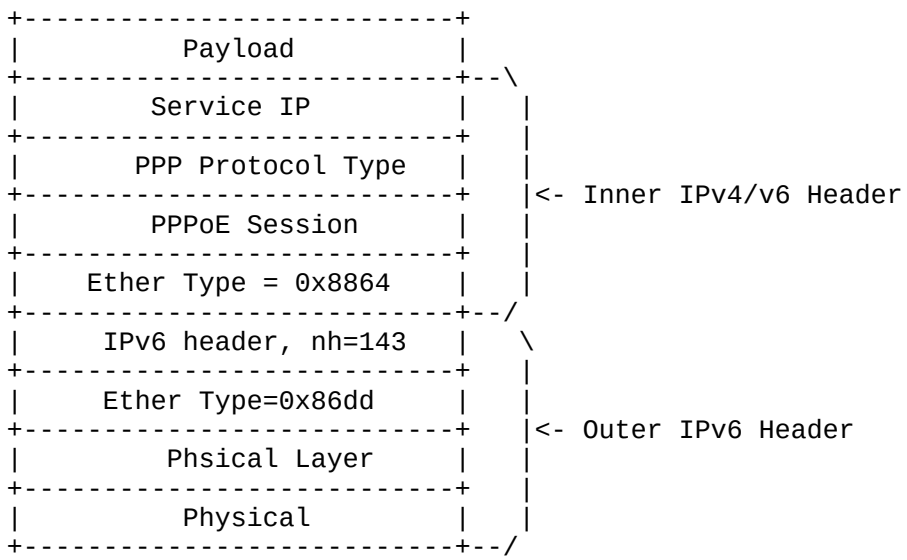

Figure 2: Encapsulation for PPPoE over SRv6

This document introduces a method for PPPoE information carried in IPv6 tunnel. The IPv6 header format is defined in [RFC8200]. The PPPoE information is carried in Ethernet format which is not changed in this document. So the next header for the IPv6 packet is set as 143. The PPPoE packet format follows [RFC2516]. Specifically, in the outer-layer IPv6 header, VLAN configuration on demand is supported, which is used for the service identification. If the VLAN is configured, the VLAN will terminate at the next SRv6 node. The VLAN allocation on demand is also supported for the inner-layer IPv6/ IPv4. If the VLAN is configured, the VLAN will terminate at the PPPoE server. The source address and destination address of the IPv6 packet are encapsulated as SRv6 SID format, which is introduced in the section 5.

6. SID Format

The SRv6 SID is consisted of LOC:FUNCT:ARG, where a locator (LOC) is encoded in the L most significant bits of the SID, followed by F bits of function (FUNCT) and A bits of arguments (ARG). The SID format is defined in [RFC8986].

The PPPoE client and PPPoE server deploy SRv6 tunnel across the broadband networks. The PPPoE client and server are required to enable for SRv6 and advertise SRv6 SIDs. The SRv6 SID is in the Destination Address field of an IPv6 header of a packet in this document. Specifically:

The locator is the Prefix Delegation assigned by the IPv6 access gateway.

The function defines the processing behavior executed at an SRv6 Segment Endpoint node.

The arguments are optional parameters, used for the identifier of service type, such as VLAN ID used in this document.

This document introduces new SRv6 Function types to support PPPoE operations, which require an extension based on [RFC8986]. Specifically, the PPPoE server should support the following Functions:

End.DXPPPoE SID (Decapsulation and IPv4 Cross - connect):

The behaviors associated with this SID is endpoint behavior with decapsulation and IPv4 cross-connect. The processing actions involve stripping the IPv6 tunnel header, the PPPoE header, and the PPP header, and then forwarding the decapsulated IPv4/IPv6 packet to a specific next-hop through the Layer 3 interface associated with this SID.

End.DX3PPPoE SID (Decapsulation and PPPoE L3VPN table lookup):

The behaviors associated with this SID is endpoint behavior with decapsulation and PPPoE L3VPN table lookup. The processing actions involve removing the IPv6 tunnel header, the PPPoE header, and the PPP header, and then performing a VPN lookup and forwarding based on the inner-layer PPPoE session information in the packet. This SID is mainly used in L3VPN scenarios.

End.DT46PPPoE SID (Decapsulation and Specific IP Table Lookup):

The behaviors associated with this SID is endpoint behavior with decapsulation and specific IP table lookup. The processing actions involve stripping the IPv6 tunnel header, the PPPoE header, and the PPP header, and then forwarding the decapsulated IPv4/IPv6 packet according to the routing table.

The PPPoE client SHOULD support the following Function:

End.DT46PPPoE SID (Decapsulation and Specific IP Table Lookup):

It supports the forwarding action of decapsulating the packet. The decapsulation actions involve removing the IPv6 tunnel header, the PPPoE header, and the PPP header, and then forwarding the decapsulated IPv4/IPv6 packet according to the routing table.

During the address encapsulation process, the PPPoE client will encapsulate the SID field with the corresponding function identifier as the destination IPv6 address based on application requirements. Once the PPPoE server receives this packet, it will conduct packet decapsulation. Then, it will parse the packet and perform forwarding operations in accordance with the defined decapsulation actions. When encapsulating packets, the PPPoE server will use the End.DPPPoET46 SID field as the destination IPv6 address. Upon receipt of the packet, the PPPoE client will decapsulate it and carry out corresponding forwarding and other operations.

7. IANA Considerations

IANA is requested to allocate values for the new SRv6 SID introduced in this document.

8. Security Considerations

The header information of SRv6, such as the Segment List and SID fields in the SRH, is transmitted in plain text, which may be eavesdropped on or tampered with. If the PPPoE payload content is not encrypted, user authentication information such as CHAP passwords and PPPoE Session IDs may be intercepted. It is necessary to authenticate SRv6 tunnel nodes and strongly bind them with PPPoE authentication to prevent unauthenticated SRv6 tunnel nodes from handling PPPoE traffic, which could lead to unauthorized access or man - in - the - middle attacks.

In terms of data protection, it is recommended to enable IPsec to encrypt SRv6 traffic and protect the SRH and payload content.

The security considerations of SRv6 [I-D.ietf-spring-srv6-security] and the security considerations of PPPoE introduced in [RFC2516] apply to this document.

9. Acknowledgements

The authors would like to acknowledge Zhenlin Tan for his helpful comments.

10. 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>.

[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>.

[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/info/rfc8986>.

11. Informative References

[I-D.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-03, 5 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-security-03>.

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, DOI 10.17487/RFC2516, February 1999, <https://www.rfc-editor.org/info/rfc2516>.

[RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007, <https://www.rfc-editor.org/info/rfc5072>.

Authors' Addresses

Cancan Huang
China Telecom
China
Email: huangcanc@chinatelecom.cn

Xueyan Song
ZTE Corp.
China
Email: song.xueyan2@zte.com.cn