v6ops Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

C. Li
C. Xie
China Telecom

7 July 2025

Basic Requirements for IPv6-only Provider Edge Routers
draft-li-v6ops-ipv6only-pe-requirements-00

Abstract

This document specifies the basic requirements for multi-domain IPv6-only Provider Edge (PE) routers. The requirements cover several key aspects: support for fundamental IPv6 protocols, such as, MP-BGP and ICMPv6, implementation of 4map6 based MP-BGP extensions, stateless encapsulation and translation functions using IPv6 mapping prefixes as well as support for SRv6 and NAT64 functionalities. By defining these requirements, this document aims to facilitate the development, deployment and interoperability of such PE routers, thereby promoting the smooth establishment and operation of multi-domain IPv6-only Networks.

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 8 January 2026.

Copyright Notice

Table of Contents

1. Introduction

1.1. IPv6-only Evolution Trend

[I-D.ietf-v6ops-framework-md-ipv6only-underlay] describes a framework for deploying IPv6-only underlay in multi-domain networks, IPv4 packets are statelessly translated or encapsulated into IPv6 packets for transmission. This framework requires IPv4/IPv6 address mapping rule to support stateless packet conversion at Provider Edge (PE) routers. In recent years, the deployment of IPv6 has been accelerating globally. Many regions and service providers have started to promote the use of IPv6 in their networks. As IPv6 traffic gradually increases in some networks, showing a trend of exceeding IPv4 traffic, there is a growing need to consider systematically the transition from IPv4/IPv6 dual-stack networks to IPv6-only networks.

The evolution towards IPv6-only networks aims to simplify the network architecture, eliminate the complexity caused by the co-existence of IPv4 and IPv6 protocols, and fully leverage the advantages of IPv6. By removing the redundant functions related to IPv4, network operators can optimize resource utilization, reduce operational costs, and improve the overall efficiency and performance of the network.

The framework of multi-domain IPv6-only underlay network is defined in [I-D.ietf-v6ops-framework-md-ipv6only-underlay]. A multi-domain IPv6-only Network refers to a network environment where multiple autonomous systems (ASs) or administrative domains operate with IPv6 as the sole network protocol. In such a network, all internal network devices, e.g. core routers, are configured to support only IPv6 for addressing, routing, and packet forwarding. This type of network is designed to provide seamless end-to-end IPv6 connectivity across different domains, enabling more efficient use of IPv6 resources and better support for emerging IPv6-based applications.

In a multi-domain IPv6-only Network, the cooperation and interoperability between different domains are crucial. To achieve this, standardized protocols and mechanisms are required to ensure the correct exchange of routing information, the seamless transfer of packets across domain boundaries, and the proper handling of various network services.

Provider Edge (PE) devices are the edge routers located at the boundary between a service provider’s network and its customer networks or other service provider networks in a multi-domain IPv6-only network. These devices play a vital role in connecting different networks and facilitating the exchange of traffic. In an IPv6-only environment, PE devices are responsible for performing a series of functions, such as routing IPv6 packets between different

domains, providing connectivity for customer networks, and handling the translation and encapsulation of packets when necessary to support legacy IPv4 services.

PE devices need to support a wide range of IPv6-related features and protocols to ensure smooth operation in the multi-domain IPv6-only network. They must be able to interact with other network devices, both within the same domain and across different domains, in a compliant and efficient manner.

1.2. Scope of this Document

This document focuses on defining the basic requirements for PE Routers located at the edge of multi-domain IPv6-only networks. It outlines the necessary functions and capabilities that PE devices should possess to operate effectively in a multi-domain IPv6-only Network environment. The requirements include the support for fundamental IPv6 protocols, the implementation of extensions related to MP-BGP for 4map6, the ability to perform encapsulation and translation based on IPv6 mapping prefix, as well as the support for SRv6 and NAT64 functions.

It should be noted that this document does not cover all the requirements for PE devices, it only introduces the parts directly related to IPv6-only. By specifying these requirements, this document aims to provide a common recommendation for equipment vendors and network operators, facilitating the development, deployment, and interoperability of multi-domain IPv6-only PE Routers. This will ultimately contribute to the successful establishment and operation of multi-domain IPv6-only network.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] .

3. Terminology

The following terms are defined in this draft:

* multi-domain IPv6-only underlay network: IPv6-only underlay network which consists of multiple ASes operated by single or multiple operators.

* AS: Autonomous System

* ICMPv6:Internet Control Message Protocol for the Version 6 Internet Protocol

* MP-BGP: Multiprotocol Border Gateway Protocol

* SRv6: Segment Routing over IPv6

* PE: Provider Edge, defined in [RFC4026]

4. IPv6 Base Protocols Requirements

4.1. IPv6 Addressing

PE devices must support [RFC8200] and correctly handle different IPv6 address formats, including unicast, multicast, and anycast addresses. They should be able to identify and process these address types in routing and packet forwarding operations. The representation of IPv6 addresses should follow the standard notation defined in [RFC5952].

For instance, when a PE router receives a packet destined for a multicast IPv6 address, it should be able to forward the packet to the appropriate multicast group members based on its multicast routing table, which is built using protocols like Multicast Listener Discovery for IPv6.

4.2. IPv6 Routing Protocols

4.2.1. Interior Gateway Protocols

PE devices must support at least one IGP protocols such as IS-IS [RFC5308], OSPFv3[RFC5340],, etc., though the specific protocol employed is at the operator’s discretion. This document provides no specific recommendations in this regard.

4.2.2. Exterior Gateway Protocol

PE devices shall support Multi-Protocol Border Gateway Protocol (MP-BGP), MP-BGP is essential for inter - domain routing in a multi-domain IPv6-only Network. PE routers shall use MP-BGP to exchange routing information with other autonomous systems. They should be able to establish MP-BGP sessions with peer routers in other domains, advertise and receive IPv6 routes, and apply appropriate routing policies. For example, when a service provider’s network needs to connect to another service provider’s multi-domain IPv6-only network, the PE routers at the inter-domain boundaries use MP-BGP to exchange routing information, enabling the transfer of traffic between the two networks.

4.3. Internet Control Message Protocol version 6 (ICMPv6)

PE devices must fully support ICMPv6 as defined in [RFC4443]. ICMPv6 is used for various control and diagnostic functions in IPv6 networks. PE routers should be able to generate, process, and forward ICMPv6 messages such as echo requests and replies, router solicitations and advertisements, and neighbor solicitations and advertisements.

For example, when receiving a Neighbor Solicitation (NS) message sent by a host in the user-side network, the PE router can respond with a Neighbor Advertisement (NA) message. The PE router can advertise the routing information of the user network to the service provider, enabling routing intercommunication between the enterprise network and the external network, so that devices within the enterprise can communicate with the external network.

Additionally, ICMPv6 error messages, such as destination unreachable messages, are crucial for network troubleshooting.PE routers must be able to correctly handle and forward these error messages to the appropriate sources.

5. MP-BGP Extension for IPv4/IPv6 Mapping Advertisement

5.1. Overview of IPv4/IPv6 Mapping Advertisement

IPv4/IPv6 mapping advertisement mechanism can be used to support the translation and encapsulation of IPv4 packets in an IPv6-only network environment(i.e. IPv4-as-a-Service). It allows for the co-existence of IPv4 services within a multi-domain IPv6-only Network. In this case, IPv4 addresses are mapped to IPv6 addresses, enabling the transfer of IPv4-based traffic over an IPv6 infrastructure.

5.2. MP-BGP Extension Requirements

5.2.1. Route Type

PE routers must support the new route types defined for the MP-BGP extension related to 4map6 as specified in [I-D.ietf-idr-mpbgp-extension-4map6]. These route types are used to carry information about the mapping between IPv4 addresses and IPv6 addresses. For example, the PE router should be able to advertise and receive routes that contain information about which IPv4 address ranges are associated with which IPv6 mapping prefixes. This information is crucial for other routers in the network to correctly route IPv4-mapped traffic.

5.2.2. Attribute Support

MP-BGP Attributes for IPv4/IPv6 mapping advertisement: PE devices need to support the specific MP-BGP attributes defined for 4map6. These attributes carry additional information related to the 4map6 translation and encapsulation process. The PE router must be able to correctly attach and interpret these attributes when advertising and receiving routes.

5.2.3. Route Advertisement and Withdrawal

PE routers should be capable of accurately advertising 4map6-related routes to other routers in the network. When a new IPv4-to-IPv6 mapping is established, the PE router must advertise the relevant route information to its peers in a timely manner. Similarly, when a mapping is removed or changed, the PE router should withdraw the old route and advertise the updated information. This ensures that the network's routing tables are always up-to-date and that traffic is routed correctly.

For example, if a new enterprise customer with IPv4-only applications is added to the multi-domain IPv6-only Network, the PE router serving that customer needs to advertise the appropriate 4map6 routes to other routers in the service provider's network, enabling the delivery of the customer's IPv4 traffic.

6. Encapsulation and Translation Based on IPv6 Mapping Prefix

6.1. Stateless IPv4-in-IPv6 Encapsulation

PE devices must support the encapsulation of IPv4 packets within IPv6 packets. When an IPv4 packet needs to be transported over an IPv6-only network, the PE router should be able to encapsulate the IPv4 packet inside an IPv6 header. The IPv6 header will contain the source and destination IPv6 addresses, which are used for routing the encapsulated packet through the IPv6 network.

For example, consider a scenario where a customer in a multi-domain IPv6-only Network has an application that still uses IPv4. When the customer's device sends an IPv4 packet, the PE router at the edge of the customer's network encapsulates this IPv4 packet within an IPv6 packet. The IPv6 packet is then routed through the service provider's IPv6-only network until it reaches the appropriate egress PE router, which will decapsulate the IPv4 packet and forward it to the final IPv4-based destination.

6.2. Translation Function

6.2.1. Stateless IPv4/IPv6 Translation

PE devices must support the stateless translation mechanism as defined in [RFC7915]. Stateless translation allows for the translation of IPv4 packets to IPv6 packets and vice versa without maintaining state information about the translation. When an IPv4 packet arrives at a PE router in an IPv6-only network, the router should be able to translate the IPv4 packet into an IPv6 packet. This involves translating the IPv4 header fields, such as source and destination addresses, into their equivalent IPv6 formats.

For example, if an IPv4-only server is accessed from a client in an IPv6-only network, the PE router at the network edge can use Stateless IPv4/IPv6 Translation to translate the IPv4 packets sent by the server into IPv6 packets that can be routed through the IPv6 network to reach the client. Similarly, when the client sends a response, the PE router can translate the IPv6 packet back into an IPv4 packet for the server to understand.

6.2.2. Stateful NAT64

PE routers shall support Stateful NAT64 [RFC6145] to connect with the customer network and enable IPv6-only users to access IPv4 services over IPv6-only network. Stateful NAT64 is a technology used to enable communication between IPv6-only hosts and IPv4-only hosts as defined in RFC 6146. It allows IPv6-only devices to access IPv4-based services by translating IPv6 addresses to IPv4 addresses. In a multi-domain IPv6-only Network, NAT64 is important for providing backward compatibility and enabling the continued use of legacy IPv4 applications.

PE routers must support the translation of IPv6 addresses to IPv4 addresses. When an IPv6-only host in a customer network connected to a PE router attempts to access an IPv4-only server, the PE router should be able to translate the IPv6 source and destination addresses in the packet to their equivalent IPv4 addresses. This translation process involves mapping the IPv6 addresses to an available pool of IPv4 addresses maintained by the PE router.

For example, if an IPv6-only mobile device in a customer’s network tries to access an IPv4 - based website, the PE router serving that customer will perform the IPv6-to-IPv4 translation. It will select an available IPv4 address from its pool, and create a stateful NAT64 IP address translation state.

7. SRv6 Support

7.1. Segment Routing over IPv6 (SRv6) Basics

SRv6 [RFC8402] is a form of segment routing that uses IPv6 as the underlying technology. It allows for the encoding of a sequence of network segments (represented as IPv6 addresses) in the packet header, enabling more flexible and programmable routing. In a multi-domain IPv6-only Network, SRv6 can be used to provide efficient traffic engineering, simplify network operations, and support new services.

7.2. SRv6 Functionality Requirements in PE Routers

7.2.1. SRv6 Endpoint Function

PE routers shall support the SRv6 endpoint function. This means that when a packet arrives at a PE router with an SRv6 segment list in its header, the router should be able to process the segment list and perform the appropriate actions. The PE router may need to pop the top - most segment from the list, forward the packet to the next hop based on the remaining segment list, or perform other operations as defined by the SRv6 architecture.

For example, in a service provider network using SRv6 for traffic engineering, a PE router may receive a packet with an SRv6 segment list that directs the packet to traverse a specific path through the network. The PE router, acting as an SRv6 endpoint, will process the segment list and forward the packet accordingly, ensuring that the packet follows the intended path.

7.2.2. SRv6 Policy Support

PE devices should support SRv6 policies. These policies can be used to define how traffic should be routed based on various criteria such as source and destination addresses, application type, or QoS requirements. The PE router must be able to enforce these policies by correctly handling SRv6-enabled packets. For instance, a service provider may define an SRv6 policy that routes high-priority video traffic along a different path than regular data traffic. The PE router, upon receiving packets marked as high-priority video traffic, will apply the SRv6 policy and route the packets along the pre-defined path.

7.2.3. SRv6-related Routing Information Exchange

PE routers need to participate in the exchange of SRv6-related routing information. This may involve advertising SRv6 capabilities, segment lists, and other relevant information to other routers in the network. The exchange of this information can be achieved through existing routing protocols such as MP-BGP, where additional attributes or extensions can be used to carry SRv6-specific information. For example, a PE router may advertise its SRv6 capabilities and the available segment lists to its MP-BGP peers, enabling them to make informed routing decisions when handling SRv6-enabled traffic.

8. Configuration and Management Considerations

As a forwarding node in IPv6-only networks, PE router shall accept centralized policy scheduling from the network controller and implementing automated configuration through the NETCONF protocol/ YANG model. Meanwhile, the PE supports syslog and SNMP Trap alarm mechanisms, enabling rapid fault location and security incident tracing through standardized logs.

9. Security Considerations

TBD

10. Acknowledgements

TBD

11. References

11.1. 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/info/rfc2119>.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, DOI 10.17487/RFC2473, December 1998, <https://www.rfc-editor.org/info/rfc2473>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, DOI 10.17487/RFC4026, March 2005, <https://www.rfc-editor.org/info/rfc4026>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, DOI 10.17487/RFC5308, October 2008, <https://www.rfc-editor.org/info/rfc5308>.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <https://www.rfc-editor.org/info/rfc5340>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, DOI 10.17487/RFC6145, April 2011, <https://www.rfc-editor.org/info/rfc6145>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC7915] Bao, C., Li, X., Baker, F., Anderson, T., and F. Gont, "IP/ICMP Translation Algorithm", RFC 7915, DOI 10.17487/RFC7915, June 2016, <https://www.rfc-editor.org/info/rfc7915>.

[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>.

[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/info/rfc8402>.

[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>.

[RFC9514] Dawra, G., Filsfils, C., Talaulikar, K., Ed., Chen, M., Bernier, D., and B. Decraene, "Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing over IPv6 (SRv6)", RFC 9514, DOI 10.17487/RFC9514, December 2023, <https://www.rfc-editor.org/info/rfc9514>.

11.2. Iormative References

[I-D.ietf-idr-mpbgp-extension-4map6]
Xie, C., Dong, G., Li, X., Han, G., and Z. Guo, "MP-BGP Extension and the Procedures for IPv4/IPv6 Mapping Advertisement", Work in Progress, Internet-Draft, draft-ietf-idr-mpbgp-extension-4map6-04, 14 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-mpbgp-extension-4map6-04>.

[I-D.ietf-v6ops-framework-md-ipv6only-underlay]
Xie, C., Ma, C., Li, X., Mishra, G. S., and T. Graf, "Framework of Multi-domain IPv6-only Underlay Network and IPv4-as-a-Service", Work in Progress, Internet-Draft, draft-ietf-v6ops-framework-md-ipv6only-underlay-11, 30 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-framework-md-ipv6only-underlay-11>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <https://www.rfc-editor.org/info/rfc6052>.

Authors' Addresses

Cong Li
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China

Email: licong@chinatelecom.cn

Chongfeng Xie
China Telecom
Beiqijia Town, Changping District
Beijing
Beijing, 102209
China
Email: xiechf@chinatelecom.cn