

V6ops Working Group
Internet-Draft
Intended status: Informational
Expires: 2 October 2026

C. Xie
China Telecom
X. Li
CERNET Center/Tsinghua University
31 March 2026

Classification of IPv6-Only Networks by Levels
draft-xie-v6ops-ipv6only-classification-00

Abstract

IPv6-only networking is recognized as the ultimate goal of network evolution. However, in practice, the understanding and implementation of IPv6-only varies significantly. To address ambiguity and improve communication, this document proposes a classification for IPv6-only networks. It defines three distinct levels, from a pure state with no IPv4 support to scenarios where IPv6-only and dual-stack coexistence exists. This approach of classification is applicable to all network scenarios and aids operators and protocol designers in precisely specifying the nature of their IPv6-only deployments.

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 2 October 2026.

Copyright Notice

Copyright (c) 2026 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	2
1.1. Requirements Language	3
2. Terminology	3
3. Classification of IPv6-Only Levels	3
4. Security Considerations	5
5. Operational Considerations	5
6. IANA Considerations	5
7. Acknowledgment	5
8. References	5
8.1. Normative References	5
8.2. Informative References	6
Authors' Addresses	8

1. Introduction

The deployment of IPv6-only networks represents a fundamental transition in internet architecture, where the network is built exclusively around the IPv6 protocol for addressing, routing, and interconnection. This model is widely recognized as the ultimate stage of IPv6 evolution. IPv6 only can be applied to various scenarios, such as backbone networks, metropolitan area networks (MANs), access networks, IDCs, enterprise networks, the Internet of Things (IoT), inter-network peering, and agent networks, among others. However, in practice, the path to a pure IPv6-only environment is shaped by the necessity to maintain backward compatibility with existing services, particularly those that do not support IPv6. To address this, various IPv4-as-a-Service (IPv4aaS) mechanisms, such as DS-Lite [RFC6333], Lightweight 4over6 [RFC7595], and IVI [RFC7915], have been developed and deployed.

For an operator, when all services have been migrated to IPv6, a fully realized IPv6-only network would require no support for IPv4 traffic whatsoever, representing a clean-state architecture. In contrast, many operational networks exhibit a mix of IPv6-only and dual-stack (IPv4/IPv6) components, with varying degrees of IPv6-only penetration. This heterogeneity leads to inconsistent interpretations of what constitutes an IPv6-only network, creating confusion in technical discussions, network planning and operation, and standardization efforts.

To address this ambiguity, this document proposes a graded classification approach for IPv6-only networks. The goal is to provide a standardized set of definitions that allow network operators to precisely characterize the extent to which their networks support IPv6-only operations, thereby facilitating clearer and more efficient communication and more consistent deployment practices. In addition, it enables the industry to develop different technical solutions and standards for different IPv6-only levels. When building an IPv6-only network, operators can also choose solutions that correspond to their respective levels. In the long run, it will benefit the overall IPv6-only deployment worldwide. This document does not intend to define new protocols or technological approaches.

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. Terminology

The following terms are defined and used in this document,

AS: Autonomous System.

CE: Customer Edge.

DC: Data Center.

NP: Network Provider.

NSP: Network-Specific Prefix.

P: Provider Router.

PE: Provider Edge (Section 5.2 of [RFC4026]).

3. Classification of IPv6-Only Levels

The following three levels are defined to describe the degree of IPv6-only adoption within a network. Each level reflects a distinct architectural state, ranging from full pure IPv6-only to partial coexistence with IPv4 capabilities.

IPv6-only Levels	Description	Degree of IPv6-only Support
Level-0	The network forwarding plane is entirely IPv6-only, and no IPv4 service support is provided. This represents the purest form of IPv6-only operation, where all traffic ---including any residual IPv4 dependencies ---is either absent or handled without network-level IPv4 mechanisms.	High
Level-1	The network core is IPv6-only, but IPv4 service capabilities are available at the edge through IPv4-as-a-Service (IPv4aaS) techniques such as DS-Lite, 4over6, or IVI. In this model, IPv4 traffic is encapsulated or translated, but the underlying transport infrastructure remains IPv6-only.	Medium
Level-2	The network is a mixed environment where IPv6-only and dual-stack (IPv4/IPv6) components coexist. A typical example is is an "IPv6-mostly" network, where most nodes operate in IPv6-only mode but certain segments or devices still maintain full dual-stack functionality. This level represents a transitional phase with lower overall IPv6-only consistency.	Low

Table 1: Representation Examples of IPv4-Embedded IPv6 Address

As mentioned before, these levels are intended to serve as a practical reference for network operators to assess and communicate the current state of their IPv6-only transition. By applying this classification, operators can more clearly define their architectural posture, identify transition milestones, and align with industry best practices. When an operator claims to have deployed an IPv6-only network, it is recommended to also specify the corresponding level defined in this document. Similarly, protocol designers developing solutions intended for IPv6-only environments are encouraged to clarify which level(s) their design targets, as the technical requirements may differ significantly between Level-0, Level-1, and Level-2 scenarios.

It should be noted that this classification is applicable to all types of network environments, including access networks, backbone networks, data center networks, and interconnection points between networks.

4. Security Considerations

This document presents a classification framework for IPv6-only networks and does not introduce new protocols or operational procedures. As such, no direct security implications are identified at this stage. However, it is worth noting that the security properties of a network may vary significantly across the defined levels. For instance, Level-0 networks, lacking any IPv4 support, inherently reduce the attack surface associated with legacy IPv4 stacks and transition mechanisms. Conversely, Level-1 and Level-2 networks may introduce additional considerations related to encapsulation, translation, and dual-stack coexistence, which should be addressed through appropriate security architectures.

5. Operational Considerations

This classification is designed to assist network operators in characterizing their IPv6-only deployment status. While no specific operational requirements are mandated, the grading approach can support use cases such as:

- 1) Benchmarking IPv6-only progress across different networks or time periods.
- 2) Clarifying assumptions in operational documentation, service-level agreements, and interconnection agreements.
- 3) Facilitating clearer communication between operational teams, vendors, and standardization bodies.

6. IANA Considerations

There are no other special IANA considerations.

7. Acknowledgment

8. References

8.1. 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>>.
- [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>>.
- [RFC5565] Wu, J., Cui, Y., Metz, C., and E. Rosen, "Softwire Mesh Framework", RFC 5565, DOI 10.17487/RFC5565, June 2009, <<https://www.rfc-editor.org/info/rfc5565>>.
- [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>>.
- [RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <<https://www.rfc-editor.org/info/rfc6877>>.
- [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>>.
- [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>>.

8.2. Informative References

- [I-D.ietf-v6ops-6mops] Buraglio, N., Caletka, O., and J. Linkova, "IPv6-mostly Networks: Deployment and Operations Considerations", Work in Progress, Internet-Draft, draft-ietf-v6ops-6mops-07, 2 March 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-6mops-07>>.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, DOI 10.17487/RFC4213, October 2005, <<https://www.rfc-editor.org/info/rfc4213>>.

- [RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <<https://www.rfc-editor.org/info/rfc4760>>.
- [RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, DOI 10.17487/RFC6144, April 2011, <<https://www.rfc-editor.org/info/rfc6144>>.
- [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <<https://www.rfc-editor.org/info/rfc6333>>.
- [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <<https://www.rfc-editor.org/info/rfc6480>>.
- [RFC6992] Cheng, D., Boucadair, M., and A. Retana, "Routing for IPv4-Embedded IPv6 Packets", RFC 6992, DOI 10.17487/RFC6992, July 2013, <<https://www.rfc-editor.org/info/rfc6992>>.
- [RFC7595] Thaler, D., Ed., Hansen, T., and T. Hardie, "Guidelines and Registration Procedures for URI Schemes", BCP 35, RFC 7595, DOI 10.17487/RFC7595, June 2015, <<https://www.rfc-editor.org/info/rfc7595>>.
- [RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <<https://www.rfc-editor.org/info/rfc7597>>.
- [RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", RFC 7599, DOI 10.17487/RFC7599, July 2015, <<https://www.rfc-editor.org/info/rfc7599>>.
- [RFC8585] Palet Martinez, J., Liu, H. M.-H., and M. Kawashima, "Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service", RFC 8585, DOI 10.17487/RFC8585, May 2019, <<https://www.rfc-editor.org/info/rfc8585>>.

- [RFC8950] Litkowski, S., Agrawal, S., Ananthamurthy, K., and K. Patel, "Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop", RFC 8950, DOI 10.17487/RFC8950, November 2020, <<https://www.rfc-editor.org/info/rfc8950>>.
- [RFC9313] Lencse, G., Palet Martinez, J., Howard, L., Patterson, R., and I. Farrer, "Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS)", RFC 9313, DOI 10.17487/RFC9313, October 2022, <<https://www.rfc-editor.org/info/rfc9313>>.

Authors' Addresses

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

Xing Li
CERNET Center/Tsinghua University
Shuangqing Road No.30, Haidian District
Beijing
100084
China
Email: xing@cernet.edu.cn