Inter-Domain Routing
Internet-Draft
Updates: 4271 (if approved)
Intended status: Standards Track
Expires: 3 September 2026

Z. Li, Ed.
G. Song, Ed.
China Mobile

2 March 2026

BGP Capability for IPv6 BGP Identifier
draft-li-idr-ipv6-bgp-identifier-00

Abstract

This document defines a new BGP Capability that enables an IPv6 BGP Speaker to use its global unicast IPv6 address as its BGP Identifier. This mechanism simplifies configuration in IPv6-only networks by leveraging the inherent uniqueness of IPv6 addresses, while maintaining full backward compatibility with existing BGP implementations.

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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

A router that runs the Border Gateway Protocol (BGP) [RFC4271] is referred to as a BGP Speaker, and each BGP Speaker is uniquely identified by a BGP Identifier (BGP ID). The BGP ID is a critical parameter in the BGP protocol, used for establishing peering sessions, resolving connection collisions, and participating in best-path selection.

[RFC4271] specifies that the BGP ID is a 4-byte unsigned integer and should be configured as a valid IPv4 address assigned to one of the BGP Speaker's interfaces. However, in IPv6-only network environments, devices are typically not configured with any IPv4 addresses, making it impossible to fulfill this requirement and thereby preventing BGP from operating correctly.

[RFC6286] addresses this limitation by allowing the BGP ID to be any 4-byte unsigned integer, independent of interface addresses. Nevertheless, in IPv6-only deployments, operators must still manually assign a unique 4-byte BGP ID to each BGP Speaker and ensure that all BGP IDs within the same Autonomous System (AS) are distinct. This imposes additional operational complexity, particularly in large-scale or automated network scenarios.

[RFC5492] defines an Optional Parameter called Capabilities, which facilitates the introduction of new capabilities into the Border Gateway Protocol (BGP) by providing a graceful capability advertisement mechanism—eliminating the need to terminate BGP peering sessions when new capabilities are introduced.

This document proposes an operationally friendly solution for IPv6-only networks: allowing a BGP Speaker to use one of its own global unicast IPv6 addresses as its BGP Identifier, referred to as the IPv6 BGP ID. To this end, a new BGP Capability is defined.

The solution proposed in this document fully preserves compatibility with existing BGP implementations. The IPv6 BGP ID is used only between BGP Speakers that establish a BGP session over IPv6 and mutually support the new capability. Peers that do not support this capability will ignore the new option and continue to operate using the traditional 4-byte BGP Identifier as specified in [RFC4271] and [RFC6286].

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. IPv6 BGP Identifier

This document defines a new BGP capability, the IPv6 BGP Identifier (IPv6 BGP ID). An IPv6 BGP Speaker advertises its support for the IPv6 BGP ID to its peer by including this capability in the Optional Parameters of the BGP OPEN message.

[RFC4271] specifies the format of the OPEN message as follows:

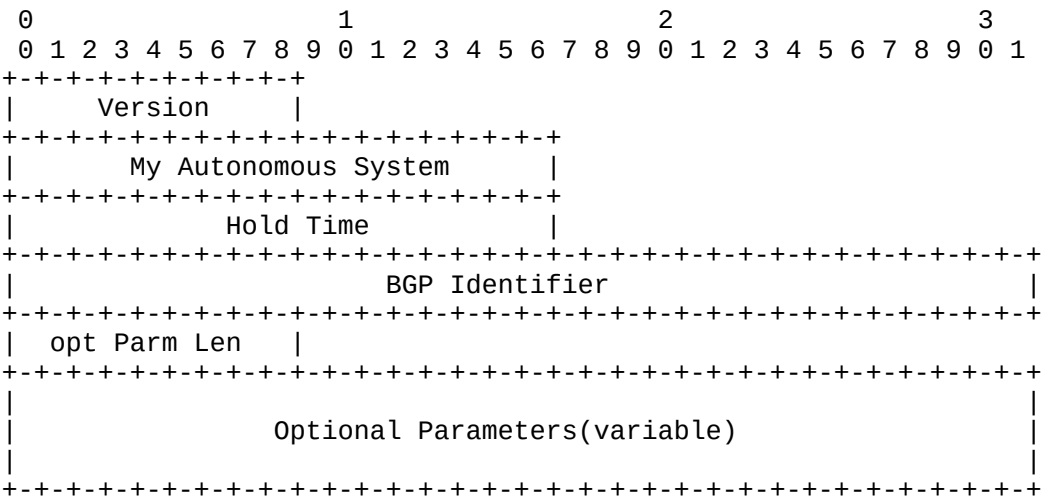

Figure 1: OPEN message

The Optional Parameters field, as shown below, contains a list of optional parameters.

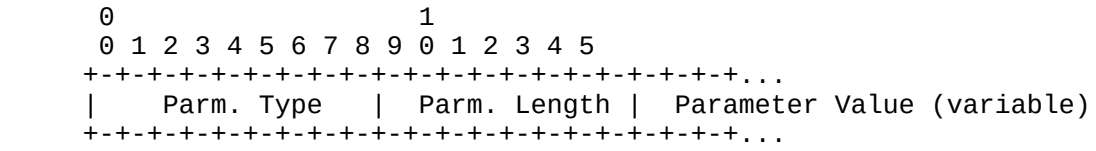

Figure 2: Optional Parameters

[RFC5492] defines the Capabilities Optional Parameter with Parameter Type 2. This parameter contains one or more triples <Capability Code, Capability Length, Capability Value>, where each triple is encoded as shown below:

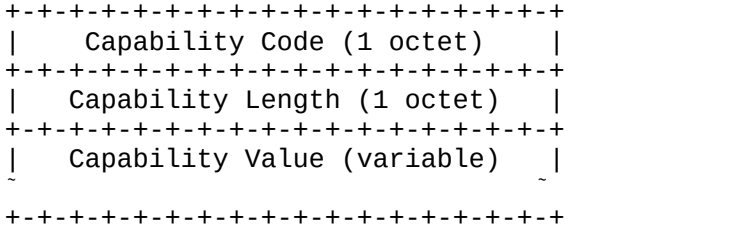

Figure 3: Capabilities Optional Parameter

The IPv6 BGP Identifier defined in this document is encapsulated in one triple of the Capabilities Optional Parameter, as shown below.

Capability Code：

1 octet. The specific value will be assigned by IANA and is used to indicate that this capability option represents the IPv6 BGP Identifier capability.

Capability Length:

1 octet. It has a value of 16, indicating that the Capability Value is 16 bytes (the IPv6 BGP Identifier).

Capability Value:

16 octets. This field contains the global unicast IPv6 address of the BGP Speaker that is used as its BGP Identifier.

In an OPEN message carrying the IPv6 BGP Identifier, the BGP Identifier field MUST be set to all zeros to indicate that the actual BGP Identifier is carried within the Capabilities Optional Parameter.

3. Open Message Processing

3.1. Constructing the OPEN Message

A BGP Speaker that supports the IPv6 BGP Identifier MUST set the BGP Identifier field in the OPEN message to zero and include the IPv6 BGP Identifier defined in this document as a capability option, where the Capability Value is a global unicast IPv6 address of the BGP Speaker.

One and only one IPv6 BGP Identifier SHOULD be carried in the OPEN message.

3.2. Receiving the OPEN Message

A BGP Speaker that supports the IPv6 BGP Identifier capability MUST examine the BGP Identifier field in the received OPEN message.

If this field is not set to zero, the speaker MUST process the OPEN message as if the peer does not support the IPv6 BGP Identifier capability. In this case, any instance of the IPv6 BGP Identifier capability carried in the Capabilities Optional Parameter MUST be ignored.

If the BGP Identifier field is zero, the speaker MUST inspect the Capabilities Optional Parameter for the presence of the IPv6 BGP Identifier capability defined in this document. If the capability is absent, the speaker MUST send a NOTIFICATION message with Error Code 2 (OPEN Message Error) and Error Subcode 3 (Bad BGP Identifier).

If the capability is present but the Capability Value does not represent a valid global unicast IPv6 address, the speaker MUST also send a NOTIFICATION message with Error Code 2 (OPEN Message Error) and Error Subcode 3 (Bad BGP Identifier).

If the IPv6 BGP Identifier capability is present in the OPEN message and its Capability Value is a valid global unicast IPv6 address, the BGP speaker proceeds to evaluate potential connection collision in accordance with Section 6.8 of [RFC4271], with the following modification:

For the purpose of collision resolution, the IPv6 BGP Identifier carried in the capability (not the 4-byte BGP Identifier field in the OPEN message, which is zero) is used as the BGP Identifier of the peer. The local system MUST compare its own IPv6 BGP Identifier with that of the remote peer. Each IPv6 BGP Identifier SHALL be interpreted as a 128-bit unsigned integer in host byte order. The connection initiated by the BGP speaker with the numerically larger IPv6 BGP Identifier MUST be retained.

If the OPEN message contains more than one IPv6 BGP Identifier, it MUST be treated as malformed. The speaker MUST send a NOTIFICATION message with Error Code 2 (OPEN Message Error) and Error Subcode 3 (Bad BGP Identifier) to its peer.

The format of the NOTIFICATION message follows the definition in Section 4.5 of RFC [RFC4271].

4. AGGREGATOR Attribute Processing

Since the BGP Identifier is also used in the AGGREGATOR path attribute of the BGP protocol, this document extends that attribute accordingly.

A BGP Speaker that supports the IPv6 BGP Identifier SHALL include its AS number and IP address in the attribute, and the included IP address SHOULD be identical to the speaker’s IPv6 BGP Identifier.

5. Route Decision Process

For a BGP speaker that supports the IPv6 BGP Identifier, the same route decision process defined in [RFC4271] applies, with the following extension to step f of the Phase 2 tie-breaking procedure specified in Section 9.1.2.2 of [RFC4271].

f) Remove from consideration all routes other than the route that was advertised by the BGP speaker with the lowest BGP Identifier value.

If routes are advertised by both IPv4 BGP Speakers and IPv6 BGP Speakers, the routes from IPv6 BGP Speakers are preferred.

If routes are advertised by multiple IPv6 BGP Speakers, the routes from the Speaker with the numerically smallest IPv6 BGP Identifier are preferred.

6. IANA Considerations

IANA is requested to assign new code points from the "BGP Capability Codes" registry for the following capability defined in this document:

Code Point	Description	Reference
TBD	IPv6 BGP ID	This document

Table 1: New BGP Capability for IPv6 BGP ID

7. Security Considerations

This extension to BGP does not introduce new security considerations. BGP security considerations are discussed in [RFC4271].

8. 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>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

[RFC6286] Chen, E. and J. Yuan, "Autonomous-System-Wide Unique BGP Identifier for BGP-4", RFC 6286, DOI 10.17487/RFC6286, June 2011, <https://www.rfc-editor.org/info/rfc6286>.

[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>.

Acknowledgements

The authors would like to acknowledge the supports from Cheng Chang, Bo Liu.

Authors' Addresses

Zhenqiang Li (editor)
China Mobile
China
Email: lizhenqiang@chinamobile.com

Guangchen Song (editor)
China Mobile
China
Email: songguangchenjc@chinamobile.com