Network Working Group
Internet-Draft
Updates: 4271 (if approved)
Intended status: Standards Track
Expires: September 11, 2019

R. Bush
Internet Initiative Japan
K. Patel
Arrcus, Inc.
D. Ward
Cisco Systems

March 10, 2019

# Extended Message support for BGP
# draft-ietf-idr-bgp-extended-messages-29

## Abstract

The BGP specification mandates a maximum BGP message size of 4096 octets. As BGP is extended to support newer AFI/SAFIs and other features, there is a need to extend the maximum message size beyond 4096 octets. This document updates the BGP specification RFC4271 by providing an extension to BGP to extend its current maximum message size from 4096 octets to 65535 octets for all except the OPEN message.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without normative meaning.

## 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 September 11, 2019.

Table of Contents



## 1. Introduction

The BGP specification [RFC4271] mandates a maximum BGP message size of 4096 octets. As BGP is extended to support newer AFI/SAFIs and newer capabilities (e.g., BGPsec, [RFC8205], BGP-LS, [RFC7752]), there is a need to extend the maximum message size beyond 4096 octets. This draft provides an extension to BGP to extend its current message size limit from 4096 octets to 65535 octets for all except the OPEN message.

## 2. BGP Extended Message

A BGP message over 4096 octets in length is a BGP Extended Message.

BGP Extended Messages have maximum message size of 65535 octets. The smallest message that may be sent consists of a BGP header without a data portion (19 octets).

## 3. Extended Message Capability for BGP

To advertise the BGP Extended Message Capability to a peer, a BGP speaker uses BGP Capabilities Advertisement [RFC5492]. By advertising the BGP Extended Message Capability to a peer, a BGP speaker conveys that it is able to send, receive, and properly handle BGP Extended Messages.

The BGP Extended Message Capability is a new BGP Capability [RFC5492] defined with Capability code 6 and Capability length 0.

A peer which does not advertise this capability MUST NOT send BGP Extended Messages, and BGP Extended Messages MUST NOT be sent to it.

## 4. Operation

A BGP speaker that is capable of sending and receiving BGP Extended Messages SHOULD advertise the BGP Extended Message Capability to the peer using BGP Capabilities Advertisement [RFC5492]. A BGP speaker MAY send Extended Messages to its peer only if it has fully exchanged the Extended Message Capability with that peer.

The Extended Message Capability applies to all messages except for the OPEN message. This exception is made to reduce complexity of providing backward compatibility

An implementation that advertises support for BGP Extended Messages MUST be capable of receiving a message with a length up to and including 65535 octets.

Applications generating information which might be encapsulated within BGP messages MUST limit the size of their payload to take the maximum message size into account.

If a BGP update with a payload longer than 4096 octets is received by a BGP listener who has neither advertised nor agreed to accept BGP Extended Messages, the listener MUST treat this as a malformed update message, and MUST raise an UPDATE Message Error (see [RFC4271] Sec 6.3).

A BGP announcement will, in the normal case, propagate throughout the BGP speaking Internet; and there will undoubtedly be BGP speakers which do not have the Extended Message capability. Therefore, having an attribute set which can not be decomposed to 4096 octets or less in an Extended Message will likely raise errors.

A BGP speaker with a mixture of peers some of which have negotiated BGP Extended Message capability and some which have not, MUST

- support [RFC7606], and
- "treat as withdraw' (see [RFC7606]) a BGP attribue/NLRI pair which is too large to be sent to a peer which does not support BGP Extended Messages.

The BGP speaker MAY remove some BGP attributes which are eligible to use the Attribute discard approach in [RFC7606].

In an iBGP mesh, all peers SHOULD support the BGP Extended Message Capability and [RFC7606]. Only then is it consistent to deploy with eBGP peers.

During the incremental deployment of BGP Extended Messages and [RFC7606] in an iBGP mesh, or with eBGP peers, the operator should monitor any routes dropped as "treat as withdraw".

It is RECOMMENDED that BGP protocol developers and implementers are conservative in their application and use of Extended Messages. Future protocol specifications will need to describe how to handle peers which can only accommodate 4096 octet messages.

## 5. Error Handling

A BGP speaker that has the ability to use Extended Messages but has not advertised the BGP Extended Messages capability, presumably due to configuration, SHOULD NOT accept an Extended Message. A speaker SHOULD NOT implement a more liberal policy accepting BGP Extended Messages.

A BGP speaker that does not advertise the BGP Extended Messages capability might also genuinely not support Extended Messages. Such a speaker will follow the error handling procedures of [RFC4271] if it receives an Extended Message. Similarly, any speaker that treats an improper Extended Message as a fatal error, MUST treat it similarly.

The inconsistency between the local and remote BGP speakers MUST be flagged to the network operator through standard operational interfaces. The information should include the NLRI and as much relevant information as reasonably possible.

## 6. Changes to RFC4271

[RFC4271] states "The value of the Length field MUST always be at least 19 and no greater than 4096." This document changes the latter number to 65535 for all except the OPEN message.

[RFC4271] Sec 6.1, specifies raising an error if the length of a message is over 4096 octets. For all messages except the OPEN message, if the receiver has advertised the capability to receive Extended Messages, this document raises that limit to 65535.

## 7. IANA Considerations

The IANA has made an early allocation for this new BGP Extended Message Capability referring to this document.

Registry: BGP Capability Code

| Value | Description | Document |
|---|---|---|
| 6 | BGP-Extended Message | [this draft] |

## 8. Security Considerations

This extension to BGP does not change BGP's underlying security issues; see [RFC4272].

Section 5 allows a receiver to accept an Extended Message even though it had not advertised the capability. This slippery slope could lead to sloppy implementations sending Extended Messages when the receiver is not prepared to deal with them, e.g. to peer groups. At best, this will result in errors; at worst, buffer overflows.

Due to increased memory requirements for buffering, there may be increased exposure to resource exhaustion, intentional or unintentional.

As this draft requires support for [RFC7606] update error handling, it inherits the security considerations of [RFC7606]. BGP peers may avoid such issues by using Authenticated Encryption with additional Data (AEAD) ciphers [RFC5116] and discard messages that do not verify.

If a remote attacker is able to craft a large BGP Extended Message to send on a path where one or more peers do not support BGP Extended Messages, peers which support BGP Extended Messages may incur resource load (processing, message resizing, etc.) reformatting the large messages. Worse, ([RFC7606] "treat as withdraw" may consistently withdraw announcements causing inconsistent routing.

BGP routes are filtered by policies set by the operators. Implementations may provide policies to filter routes that would cause the "treat as withdraw" from being pass by an extended message speaker.

## 9. Acknowledgments

The authors thank Alvaro Retana, Enke Chen, Susan Hares, John Scudder, John Levine, and Job Snijders for their input; and Oliver Borchert and Kyehwan Lee for their implementations and testing.

## 10. References

### 10.1. 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, <http://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, <http://www.rfc-editor.org/info/rfc4271>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <http://www.rfc-editor.org/info/rfc4272>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <http://www.rfc-editor.org/info/rfc5116>.

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

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <http://www.rfc-editor.org/info/rfc7606>.

### 10.2. Informative References

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <http://www.rfc-editor.org/info/rfc7752>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

## Authors' Addresses

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington  98110
United States of America

Email: randy@psg.com

Keyur Patel
Arrcus, Inc.

Email: keyur@arrcus.com

Dave Ward
Cisco Systems
170 W. Tasman Drive
San Jose, CA  95134
United States of America

Email: dward@cisco.com