Network Working Group
Internet-Draft
Updates: 4271 (if approved)
Intended status: Standards Track
Expires: November 22, 2018

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

May 21, 2018

Extended Message support for BGP
draft-ietf-idr-bgp-extended-messages-25

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 November 22, 2018.

Copyright Notice

Copyright (c) 2018 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. BGP Extended Message 2
3. Extended message Capability for BGP 3
4. Operation 3
5. Error Handling 4
6. Changes to RFC4271 4
7. IANA Considerations 4
8. Security Considerations 4
9. Acknowledgments 5
10. References 5
10.1. Normative References 5
10.2. Informative References 5
Authors' Addresses 6

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., [I-D.ietf-sidr-bgpsec-protocol]), 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 octetsfor 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.

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

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

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 received the Extended Message Capability from that peer.

The Extended Message Capability only applies to all messages except for the OPEN message. This exception is reduce compexity 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.

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 putting an attribute which can not be decomposed to 4096 octets or less in an Extended Message is a likely path to routing failure.

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 accomodate 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 MAY implement a more liberal policy and accept Extended Messages, even from a peer to which it has not advertised the capability, in the interest of preserving the BGP session if at all possible.

A BGP speaker that does not advertise the BGP Extended Messages capability might also genuinely not support Extended Messages. Such a speaker would be expected to 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 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 allowed a receiver to accept an Extended Message even though they had not advertised the capability. This slippery slope will surely 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 (over [RFC4272]) memory requirements for buffering, there may be increased exposure to resource exhaustion, intentional or unintentional.

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>.

[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>.

10.2. Informative References

[I-D.ietf-sidr-bgpsec-protocol] Lepinski, M., "BGPSEC Protocol Specification", draft-ietf-sidr-bgpsec-protocol-07 (work in progress), February 2013.

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