IDR Workgroup
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2020

M. Zheng
Individual Contributor
A. Lindem
Cisco Systems
J. Haas
Juniper Networks, Inc.
A. Fu
Bloomberg L.P.

November 4, 2019

BGP BFD Strict-Mode
draft-ietf-idr-bgp-bfd-strict-mode-02

Abstract

This document specifies extensions to RFC4271 BGP-4 that enable a BGP speaker to negotiate additional Bidirectional Forwarding Detection (BFD) extensions using a BGP capability. This BFD capability enables a BGP speaker to prevent a BGP session from being established until a BFD session is established. It is referred to as BGP BFD "strict-mode". BGP BFD strict-mode will be supported when both the local speaker and its remote peer are BFD strict-mode capable.

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 May 7, 2020.

Copyright Notice

Copyright (c) 2019 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

Bidirectional Forwarding Detection BFD [RFC5882] enables routers to monitor data plane connectivity and to detect faults in the bidirectional forwarding path between them. This capability is leveraged by routing protocols such as BGP [RFC4271] to rapidly react to topology changes in the face of path failures.

The BFD interaction with BGP is specified in Section 10.2 of [RFC5882]. When BFD is enabled for a BGP neighbor, faults in the bidirectional forwarding detected by BFD result in session termination. It is possible in some failure scenarios for the network to be in a state such that a BGP session may be established but a BFD session cannot be established. In some other scenarios, it may be possible to establish a BGP session, but a degraded or poor-quality link may result in the corresponding BFD session going up and down frequently.

To avoid situations which result in routing churn and to minimize the impact of network interruptions, it will be beneficial to disallow BGP to establish a session until BFD session is successfully established and has stabilized. We refer to this mode of operation as BGP BFD "strict-mode". However, always using "strict-mode" would preclude BGP operation in an environment where not all routers support BFD strict-mode or have BFD enabled. This document defines BGP "strict-mode" operation as preventing BGP session establishment until both the local and remove speakers have a stable BFD session.

The document also specifies the BGP protocol extensions for BGP capability [RFC5492] for announcing BFD parameters including a BGP speaker's support for "strict-mode", i.e., requiring a BFD session for BGP session establishment.

2. 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.

3. BFD Strict-Mode Capability

The BGP Strict-Mode Capability [RFC5492] will allow a BGP speaker's to advertise this capability. The capability is defined as follows:

Capability code: TBD

Capability length: 0 octets

4. Operation

A BGP speaker which supports capabilities advertisement and has BFD strict-mode enabled MUST include the BFD strict-mode capability.

A BGP speaker which supports the BFD Strict-Mode capability, examines the list of capabilities present in the capabilities that the speaker receives from its peer. If both the local and remote BGP speakers include the BFD strict-mode capability, the BGP finite state machine does not transition to the Established state from OpenSent or OpenConfirm state [RFC4271] until the BFD session is in the Up state (see below for AdminDown state). This means that a KEEPALIVE message is not sent nor is the KeepaliveTimer set.

If the BFD session does not transition to the Up state, and the HoldTimer has been negotiated to a non-zero value, the BGP FSM will close the session appropriately. If the HoldTimer has been negotiated to a zero value, the session should be closed after a time of X. This time X is referred as "BGP BFD Hold time". The proposed default BGP BFD Hold time value is 30 seconds. The BGP BFD Hold time value is configurable.

If BFD session is in the AdminDown state, then the BGP finite state machine will proceed normally without input from BFD. This means that BFD session "AdminDown" state WILL NOT prevent the BGP state transition to Established state from OpenConfirm.

Once the BFD session has transitioned to the Up state, the BGP FSM may proceed to transition to the Established state from the OpenSent or OpenConfirm state appropriately. I.e. a KEEPALIVE message is sent, and the KeepaliveTimer is started.

If either BGP peer has not advertised the BFD Strict-Mode Capability, then a BFD session WILL NOT be required for the BGP session to reach Established state. This does not preclude usage of BFD after BGP session establishment [RFC5882].

If BFD is disabled for a BGP peer and the BGP session state is being held in OpenSent or OpenConfirm state, then the BGP will close session, and start a new TCP connect.

5. Manageability Considerations

Auto-configuration is possible for the enabling BGP BFD Strict-Mode. However, the configuration automation is out of the scope of this document.

A BGP NOTIFICATION message Subcode indicating BFD Hold timer expiration may be required for network management. (To be discussed in the next revision of this document.)

6. Security Considerations

The mechanism defined in this document interacts with the BGP finite state machine when so configured. The security considerations of BFD thus, become considerations for BGP-4 [RFC4271] so used. Given that a BFD session is required for a BGP session, a Denial-of-Service (DoS) attack on BGP can now be mounted by preventing a BFD session between the BGP peers from being established or interrupting an existing BFD session. The use of the BFD Authentication mechanism defined in [RFC5880] is thus RECOMMENDED when used to protect BGP-4 [RFC4271].

7. IANA Considerations

This document defines a new BGP capability - BFD Capability. The Capability Code for BFD Capability is TBD.

8. Acknowledgement

The authors would like to acknowledge the review and inputs from Shyam Sethuram, Mohammed Mirza, Bruno Decraene, Carlos Pignataro, and Enke Chen.

9. 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>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC5882] Katz, D. and D. Ward, "Generic Application of Bidirectional Forwarding Detection (BFD)", RFC 5882, DOI 10.17487/RFC5882, June 2010, <https://www.rfc-editor.org/info/rfc5882>.

[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>.

Authors' Addresses

Mercia Zheng
Individual Contributor

Email: merciaz.ietf@gmail.com

Acee Lindem
Cisco Systems
301 Midenhall Way
GARY, NC 27513
UNITED STATES

Email: acee@cisco.com

Jeffrey Haas
Juniper Networks, Inc.
1133 Innovation Way
SUNNYVALE, CALIFORNIA 94089
UNITED STATES

Email: jhaas@juniper.net

Albert Fu
Bloomberg L.P.

Email: afu14@bloomberg.net