

IDR WorkGroup  
Internet-Draft  
Intended status: Standards Track  
Expires: September 12, 2019

M. Zheng  
A. Lindem  
Cisco Systems  
March 11, 2019

BGP BFD Strict-Mode  
draft-merciaz-ietf-idr-bgp-bfd-strict-mode-01

## Abstract

This document specifies extensions to [RFC4271](#) BGP-4 that enable a BGP speaker to signal additional Bidirectional Forwarding Detection (BFD) extensions using an optional parameter BFD 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, Otherwise, a BGP speaker and its peer should not require a BFD session for BGP session establishment.

## 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 <http://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 12, 2019.

## 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 (<http://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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Requirements Language . . . . .	<a href="#">3</a>
<a href="#">3.</a>	BGP BFD Capability . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Operation . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Backward Compatibility . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">7.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">8.</a>	Acknowledgement . . . . .	<a href="#">5</a>
<a href="#">9.</a>	Normative References . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">6</a>

## [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 neighbor 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 remote 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.](#) BGP BFD Capability

The BGP Capability [[RFC5492](#)] for BFD parameters will allow a BGP speaker's BFD capabilities including its support for BFD strict-mode. This capability is defined as follows:

Capability code: TBD

Capability length: 1 octet

Capability value: Consists of 1 octet BFD flags as follows:

```
+-----+
| BFD Flags (8 bits) |
+-----+
```

The use and meaning of the fields are as follows:

BFD Flags: This field contains bit flags relating to BFD.

```
0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+---+
```

|S| Reserved |  
+--+--+--+--+--+--+--+

The most significant bit is defined as state of Strict-Mode ("Strict-Mode", or "S") bit, which can be used by a BGP speaker to signal its support for BFD Strict-mode. When set (value 1), this bit indicates that the BGP speaker has the BFD "Strict-mode" enabled. If both local BGP speaker and its peer are enabled with BFD strict-mode, then BGP session establishment will be disallowed until a BFD session is

established. A BGP speaker with BFD strict-mode enabled MUST advertise the BFD capability with "S" bit value 1.

The remaining bits are reserved and SHOULD be set to zero by the sender and MUST be ignored by the receiver.

#### [4.](#) Operation

A BGP speaker that supports capabilities advertisement sends an OPEN message to its BGP peer, the message MAY include an Optional Parameter, called Capabilities. The parameter lists the capabilities supported by the speaker. By following BGP capabilities advertisement procedures defined in [[RFC5492](#)], BFD capability advertisement for strict-mode is advertised to BGP peers.

A BGP speaker which supports capabilities advertisement and has BFD strict-mode enabled MUST include the BGP BFD capability with the "S" Bit set in the BGP capabilities it advertises.

A BGP speaker which supports BFD capability advertisement, examines the list of capabilities present in the Capabilities BFD Parameter that the speaker receives from its peer. If both the local and remote BGP speakers BFD strict-mode enabled, then BGP session establishment will be prevented until a BFD session is up. If either peer has not advertised the BFD Capability with strict-mode enabled, then a BFD session SHOULD NOT be required prior to BGP session establishment. This does not preclude usage of BFD after BGP session establishment [[RFC5882](#)].

A BGP speaker which does not support or recognize BFD capability should ignore the BFD capability. If a BGP speaker advertising the capability receives the Unsupported Capability NOTIFICATION message, it MUST NOT be result in BGP session termination.

## [5.](#) Backward Compatibility

The new BFD capability will introduce any backward compatibility if the procedures defined in this document are followed. A BGP speaker which does not support BFD capability MUST ignore this capability. The Unsupported Capability NOTIFICATION message MUST NOT result in session termination by the BGP speaker advertising the capability.

## [6.](#) Security Considerations

This specification doesn't change the basic security model inherent in [[RFC4271](#)]. To the extent [[RFC4271](#)] might be said to help defend against denials of service by making the control plane more resilient, this extension may modestly increase that resilience;

however, there are enough confounding and deployment-specific factors that no general claims can be made.

## [7.](#) IANA Considerations

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

IANA is requested to establish a "BGP BFD Capability Flags" registry within the "Border Gateway Protocol (BGP) Parameters" grouping. The Registration Procedure should be Standards Action, the initial values as follows:

Bit Position	Name	Short Name	Reference
0	Strict-Mode	S	this document
1-7	Unassigned		this document

## 8. Acknowledgement

The authors would like to acknowledge the review and inputs from Shyam Sethuram and Mohammed Mirza.

## 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>>.

Zheng & Lindem

Expires September 12, 2019

[Page 5]

---

Internet-Draft

BGP BFD Strict-Mode

March 2019

- [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  
Cisco Systems  
821 Alder Drive,  
MILPITAS, CALIFORNIA 95035

UNITED STATES

Email: [merciaz@cisco.com](mailto:merciaz@cisco.com)

Acee Lindem  
Cisco Systems  
821 Alder Drive,  
MILPITAS, CALIFORNIA 95035  
UNITED STATES

Email: [acee@cisco.com](mailto:acee@cisco.com)