Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 18, 2021

A. Mishra
SES
M. Jethanandani
Kloud Services
A. Saxena
Ciena Corporation
S. Pallagatti
VmWare
M. Chen
Huawei
P. Fan
China Mobile
Jan 14, 2021

BFD Stability
draft-ietf-bfd-stability-07

Abstract

This document describes extensions to the Bidirectional Forwarding Detection (BFD) protocol to measure BFD stability. Specifically, it describes a mechanism for detection of BFD packet loss.

Table of Contents

1. Introduction

The Bidirectional Forwarding Detection (BFD) [RFC5880] protocol operates by transmitting and receiving BFD control packets, generally at high frequency, over the datapath being monitored. In order to prevent significant data loss due to a datapath failure, BFD session detection time as defined in BFD [RFC5880] is set to the smallest feasible value.

This document proposes a mechanism to detect lost packets in a BFD session in addition to the datapath fault detection mechanisms of BFD. Such a mechanism presents significant value to measure the stability of BFD sessions and provides data to the operators for the cause of a BFD failure.

This document does not propose any BFD extension to measure data traffic loss or delay on a link or tunnel and the scope is limited to BFD packets.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] and RFC 8174 [RFC8174].

The reader is expected to be familiar with the BFD [RFC5880], Optimizing BFD Authentication [I-D.ietf-bfd-optimizing-authentication] and BFD Secure Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers].

3. Use Cases

Bidirectional Forwarding Detection as defined in BFD [RFC5880] cannot detect any BFD packet loss if the loss does not last for detection time. This document proposes a method to detect a dropped packet on the receiver. For example, if the receiver receives BFD control packet k at time t but receives packet k+3 at time t+10ms, and never receives packet k+1 and/or k+2, then it has experienced a drop.

This proposal enables BFD implementations to generate diagnostic information on the health of each BFD session that could be used to preempt a failure on a datapath that BFD was monitoring by allowing time for a corrective action to be taken.

In a faulty datapath scenario, an operator can use BFD health information to trigger delay and loss measurement OAM protocol (Connectivity Fault Management (CFM) or Loss Measurement (LM)-Delay Measurement (DM)) to further isolate the issue.

4. BFD Null-Authentication Type

The functionality proposed for BFD stability measurement is achieved by appending an authentication section with the NULL Authentication type (as defined in Optimizing BFD Authentication [I-D.ietf-bfd-optimizing-authentication]) to the BFD control packets that do not have authentication enabled.

5. Theory of Operation

This mechanism allows operators to measure the loss of BFD control packets.

When using MD5 or SHA authentication, BFD uses an authentication section that carries the Sequence Number. However, if non-meticulous authentication is being used, or no authentication is in use, then the non-authenticated BFD control packets MUST include an authentication section with the NULL Authentication type.

5.1. Loss Measurement

Loss measurement counts the number of BFD control packets missed at the receiver during any Detection Time period. The loss is detected by comparing the Sequence Number field in the Auth TLV (NULL or

otherwise) in successive BFD control packets. The Sequence Number in each successive control packet generated on a BFD session by the transmitter is incremented by one.

The first BFD authentication section with a non-zero sequence number, in a valid BFD control packet, processed by the receiver is used for bootstrapping the logic. When using secure sequence numbers, if the expected values are pre-calculated, the value must be matched to detect lost packets as defined in BFD secure sequence numbers [I-D.ietf-bfd-secure-sequence-numbers].

6. IANA Considerations

This document has no actions for IANA.

7. Security Consideration

Other than concerns raised in BFD [RFC5880], Optimizing BFD Authentication [I-D.ietf-bfd-optimizing-authentication] and BFD Secure Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers]. There are no new concerns with this proposal.

8. Contributors

Manav Bhatia

9. Acknowledgements

Authors would like to thank Nobo Akiya, Jeffery Haas, Peng Fan, Dileep Singh, Basil Saji, Sagar Soni and Mallik Mudigonda who also contributed to this document.

10. Normative References

[I-D.ietf-bfd-optimizing-authentication]
Jethanandani, M., Mishra, A., Saxena, A., and M. Bhatia, "Optimizing BFD Authentication", draft-ietf-bfd-optimizing-authentication-11 (work in progress), July 2020.

[I-D.ietf-bfd-secure-sequence-numbers]
Jethanandani, M., Agarwal, S., Mishra, A., Saxena, A., and A. DeKok, "Secure BFD Sequence Numbers", draft-ietf-bfd-secure-sequence-numbers-07 (work in progress), December 2020.

[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>.

[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>.

[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

Ashesh Mishra
SES

Email: mishra.ashesh@gmail.com

Mahesh Jethanandani
Kloud Services
CA
USA

Email: mjethanandani@gmail.com

Ankur Saxena
Ciena Corporation
3939 North 1st Street
San Jose, CA 95134
USA

Email: ankurpsaxena@gmail.com
URI: www.ciena.com

Santosh Pallagatti
VmWare
Bangalore, Karnataka 560103
India

Email: santosh.pallagatti@gmail.com

Mach Chen
Huawei

Email: mach.chen@huawei.com

Peng Fan
China Mobile
32 Xuanwumen West Street
Beijing, Beijing
China

Email: fanp08@gmail.com