Stream: Internet Engineering Task Force (IETF)
RFC: 9978
Category: Experimental
Published: May 2026
ISSN: 2070-1721
Authors:
A. Mishra, *Aalyria Technologies*
M. Jethanandani, *Arrcus, Inc.*
A. Saxena, *Ciena Corporation*
S. Pallagatti, *Zscaler*
M. Chen, *Huawei*

RFC 9978
Bidirectional Forwarding Detection (BFD) Stability

Abstract

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

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9978.

Copyright Notice

Table of Contents

1. Introduction

The Bidirectional Forwarding Detection (BFD) [RFC5880] protocol operates by transmitting and receiving BFD control packets, generally at a 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 [RFC5880] is set to the smallest feasible value.

A BFD session [RFC5880] will remain in the Up state as long as it receives at least one BFD packet within the Detection Time interval. However, additional packet loss within that time interval is not noted by the BFD state machinery. Noting the other missed packets provides a valuable indicator of systemic issues or a deteriorating network that may warrant preventive action.

This document proposes an experimental mechanism to detect lost packets in a BFD session in addition to the datapath fault detection mechanisms of BFD. Such a mechanism, combined with 'received-packet-count' defined in "YANG Data Model for Bidirectional Forwarding Detection (BFD)" [RFC9314] permits operators to measure the stability of BFD sessions. The details of the motivation for the Experimental status of this document can be found in Appendix A. Implementations may also do additional analysis of the packet loss over a time interval. Such an analysis is outside the scope of this document.

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**", "**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.

The reader is expected to be familiar with BFD [RFC5880]. In particular, the term "meticulous" as specified in "Meticulous Keyed ISAAC for BFD Optimized Authentication" [BFD-ISAAC] means that the sequence number is incremented on every new packet that is sent.

3. Use Cases

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

This proposal enables BFD implementations to generate diagnostic information on the health of each BFD session. This information could be used to preempt the probability of 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 the delay and loss measurement Operations, Administration, and Maintenance (OAM) protocol Connectivity Fault Management (CFM) [Y-1731] or packet loss and delay measurement for MPLS networks [RFC6374] to further isolate the issue.

4. Functionality

BFD stability measurement requires that a BFD Meticulous authentication type be configured.

The "ietf-bfd-stability" YANG data model, defined in this document, provides the ability to configure the BFD stability measurement for BFD sessions by configuring the 'stability' flag. The 'lost-packet-count' leaf permits monitoring of stability issues as defined in this document for BFD sessions that have the 'stability' flag enabled.

The configuration of the BFD stability measurement and monitoring using other methods than the attached YANG data model is out of scope of this document.

5. NULL Auth Type

The NULL authentication type, defined in this document, can be used to provide a meticulously increasing sequence number BFD [RFC5880] for stability measurement. It provides none of the protections desired for authentication and is used only to provide BFD stability services to BFD sessions that otherwise have no authentication in use.

If the Authentication Present (A) bit is set in the header as defined in Section 4 of [RFC5880], and the Authentication Type field contains 6, the Authentication Section has the following format:

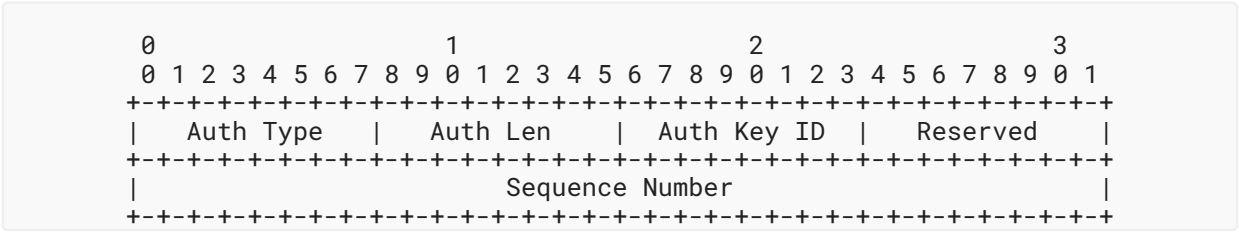

Figure 1: NULL Auth Type

where:

Auth Type (8 bits): The Authentication Type, which in this case is 6 (NULL).

Auth Len (8 bits): The length of the NULL Auth Type in bytes (i.e., 8 bytes).

Auth Key ID (8 bits): The authentication key ID in use for this packet. It **MUST** be set to zero and **MUST** be ignored on receipt.

Reserved (8 bits): This byte **MUST** be set to zero on transmit and **MUST** be ignored on receipt.

Sequence Number (32 bits): The sequence number for this packet. This value is incremented for each successive packet transmitted for a session. Implementations will use sequence numbers (bfd.XmitAuthSeq) as defined in [RFC5880].

If bfd.AuthSeqKnown is 1, and the received Sequence Number field is not equal to bfd.RcvAuthSeq + 1 (in a circular number space), then the loss count is incremented by the difference between the received sequence number and bfd.RcvAuthSeq, and bfd.RcvAuthSeq is set to the received sequence number.

Otherwise (bfd.AuthSeqKnown is 0), bfd.AuthSeqKnown **MUST** be set to 1, and bfd.RcvAuthSeq **MUST** be set to the value of the received Sequence Number field as defined in [RFC5880], Section 6.8.1, and the packet **MUST** be accepted.

According to Section 6.7.3 of [RFC5880], a receiver **MUST** discard a received packet that lies outside the range of bfd.RcvAuthSeq and bfd.RcvAuthSeq + (3 * Detect Multi). If it is within that range, but is missing a packet, it can be used to detect a loss. In case of NULL authentication where packets containing sequence numbers are accepted on receipt, an attacker with an unauthenticated sequence number could move the sequence number forward. Meanwhile, the actual BFD neighbor that continues to send packets will find them discarded and the session would drop. To prevent such an attack, the received sequence number **MUST NOT** be compared with bfd.RcvAuthSeq for the purpose of discarding the BFD packets.

6. Theory of Operation

This mechanism allows operators to measure the loss of BFD control packets. A BFD authentication type carrying a meticulously increasing sequence number is required to support this loss measurement. Authentication types that provide for meticulously increasing sequence numbers include:

- Meticulously Keyed MD5 and SHA1, defined in [RFC5880].
- Meticulously Keyed ISAAC, defined in [BFD-ISAAC].
- The NULL authentication mechanism, which does not provide for authentication but carries a meticulously increasing sequence number, is defined in this document.

Other authentication types that provide for meticulously increasing sequence numbers appropriate for this mechanism may be defined in future specifications.

6.1. Loss Measurement

Loss measurement counts the number of BFD control packets missed at the receiver during any Detection Time period (see [RFC5880], Section 6.8.4). The loss is detected by comparing the Sequence Number field 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. This loss count can then be exposed using the YANG module defined in the subsequent section. See discussion on out-of-order packets in Section 6.2 of this document.

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.

6.2. Out-of-Order Packets

Some transmission mechanisms, for example, Link Aggregate Groups (LAGs) or Equal Cost Multipath (ECMP), can result in out-of-order packet delivery. In circumstances where BFD packets are not lost, but are delivered out of order, strict comparison of increasing sequence numbers may result in classifying the out-of-order packets as packet loss.

Implementations **MAY** provide mechanisms wherein all expected packets received across an expected interval, but delivered out of order, are not considered lost packets.

7. Stability YANG Module

7.1. Data Model Overview

This YANG module augments the base BFD YANG module to add attributes such as the 'stability' flag related to the experiment of BFD stability. The feature statement 'stability' needs to be enabled to indicate that BFD stability is supported by the implementation. In addition, a loss count per-session or lsp for BFD packets that are lost has also been added in this model.

```
module: ietf-bfd-stability

  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh
            /bfd-ip-sh:sessions/bfd-ip-sh:session:
    +--rw stability?   boolean {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-mh:ip-mh
            /bfd-ip-mh:session-groups/bfd-ip-mh:session-group:
    +--rw stability?   boolean {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-lag:lag
            /bfd-lag:sessions/bfd-lag:session:
    +--rw stability?   boolean {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-mpls:mpls
            /bfd-mpls:session-groups/bfd-mpls:session-group:
    +--rw stability?   boolean {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh
            /bfd-ip-sh:sessions/bfd-ip-sh:session
            /bfd-ip-sh:session-statistics:
    +--ro lost-packet-count?   yang:counter64 {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-mh:ip-mh
            /bfd-ip-mh:session-groups/bfd-ip-mh:session-group
            /bfd-ip-mh:sessions/bfd-ip-mh:session-statistics:
    +--ro lost-packet-count?   yang:counter64 {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-lag:lag
            /bfd-lag:sessions/bfd-lag:session/bfd-lag:member-links
            /bfd-lag:micro-bfd-ipv4/bfd-lag:session-statistics:
    +--ro lost-packet-count?   yang:counter64 {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-lag:lag
            /bfd-lag:sessions/bfd-lag:session/bfd-lag:member-links
            /bfd-lag:micro-bfd-ipv6/bfd-lag:session-statistics:
    +--ro lost-packet-count?   yang:counter64 {stability}?
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-mpls:mpls
            /bfd-mpls:session-groups/bfd-mpls:session-group
            /bfd-mpls:sessions/bfd-mpls:session-statistics:
    +--ro lost-packet-count?   yang:counter64 {stability}?
```

7.2. YANG Module

This YANG module imports modules defined in "Common YANG Data Types" [RFC6991], "A YANG Data Model for Routing Management (NMDA Version)" [RFC8349], and "YANG Data Model for Bidirectional Forwarding Detection (BFD)" [RFC9314].

```
<CODE BEGINS> file "ietf-bfd-stability@2026-05-05.yang"

module ietf-bfd-stability {
  yang-version 1.1;
```

```
namespace "urn:ietf:params:xml:ns:yang:ietf-bfd-stability";
prefix bfd-s;

import ietf-yang-types {
  prefix yang;
  reference
    "RFC 6991: Common YANG Data Types";
}
import ietf-routing {
  prefix rt;
  reference
    "RFC 8349: A YANG Data Model for Routing Management
     (NMDA Version)";
}
import ietf-bfd {
  prefix bfd;
  reference
    "RFC 9314: YANG Data Model for Bidirectional
     Forwarding Detection.";
}
import ietf-bfd-ip-sh {
  prefix bfd-ip-sh;
  reference
    "RFC 9314: YANG Data Model for Bidirectional
     Forwarding Detection (BFD)";
}
import ietf-bfd-ip-mh {
  prefix bfd-ip-mh;
  reference
    "RFC 9314: YANG Data Model for Bidirectional
     Forwarding Detection (BFD)";
}
import ietf-bfd-lag {
  prefix bfd-lag;
  reference
    "RFC 9314: YANG Data Model for Bidirectional
     Forwarding Detection (BFD)";
}
import ietf-bfd-mpls {
  prefix bfd-mpls;
  reference
    "RFC 9314: YANG Data Model for Bidirectional
     Forwarding Detection (BFD)";
}
import ietf-key-chain {
  prefix key-chain;
  reference
    "RFC 8177: YANG Data Model for Key Chains";
}

organization
  "IETF BFD Working Group";
contact
  "WG Web:   <http://tools.ietf.org/wg/bfd>
   WG List:  <rtg-bfd@ietf.org>

   Authors: Mahesh Jethanandani (mjethanandani@gmail.com)
            Ashesh Mishra (mishra.ashesh@gmail.com)
```

```
              Ankur Saxena (ankurpsaxena@gmail.com)
              Santosh Pallagatti (santosh.pallagati@gmail.com)
              Mach Chen (mach.chen@huawei.com).";
  description
    "This YANG module augments the base BFD YANG data model to add
     experimental attributes related to BFD stability.
     In particular, it adds a per-session count for BFD packets
     that are lost.

     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 (RFC 2119) (RFC 8174) when, and only when,
     they appear in all capitals, as shown here.

     Copyright (c) 2026 IETF Trust and the persons identified as
     authors of the code.  All rights reserved.

     Redistribution and use in source and binary forms, with or
     without modification, is permitted pursuant to, and subject to
     the license terms contained in, the Revised BSD License set
     forth in Section 4.c of the IETF Trust's Legal Provisions
     Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     This version of this YANG module is part of RFC 9978; see the
     RFC itself for full legal notices.";

  revision 2026-05-05 {
    description
      "Initial version.";
    reference
      "RFC 9978: Bidirectional Forwarding Detection (BFD) Stability";
  }

  feature stability {
    description
      "This feature enables BFD sessions to be monitored for lost
       packets.";
  }

  identity null-auth {
    base key-chain:crypto-algorithm;
    description
      "BFD NULL Auth type defined in this document.";
    reference
      "RFC 9978: Bidirectional Forwarding Detection (BFD) Stability";
  }

  grouping lost-packet-count {
    leaf lost-packet-count {
      if-feature "stability";
      type yang:counter64;
      description
        "Number of BFD packets that were lost, where loss is
         determined by the fact that the sequence number is
         not consecutive.  This counter should be present only if
         stability is configured.";
```

```
    }
    description
      "Grouping of statistics related to BFD stability.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh/"
        + "bfd-ip-sh:sessions/bfd-ip-sh:session" {
    leaf stability {
      if-feature "stability";
      type boolean;
      must "../bfd-ip-sh:authentication/bfd-ip-sh:meticulous = "
         + "'true'";
      default "false";
      description
        "If set to true, this enables the BFD session to monitor
         for stability, i.e., to watch how many packets are getting
         dropped.";
    }
    description
      "Augment the 'bfd' container to add attributes related to BFD
       stability for IP Single Hop sessions.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-ip-mh:ip-mh/"
        + "bfd-ip-mh:session-groups/bfd-ip-mh:session-group" {
    leaf stability {
      if-feature "stability";
      type boolean;
      must "../bfd-ip-mh:authentication/bfd-ip-mh:meticulous = "
         + "'true'";
      default "false";
      description
        "If set to true, this enables the BFD session to monitor
         for stability, i.e., to watch how many packets are getting
         dropped.";
    }
    description
      "Augment the 'bfd' container to add attributes related to BFD
       stability for Multi Hop sessions.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-lag:lag/"
        + "bfd-lag:sessions/bfd-lag:session" {
    leaf stability {
      if-feature "stability";
      type boolean;
      must "../bfd-lag:authentication/bfd-lag:meticulous = "
         + "'true'";
      default "false";
      description
        "If set to true, this enables the BFD session to monitor
         for stability, i.e., to watch how many packets are getting
         dropped.";
    }
    description
```

```
      "Augment the 'bfd' container to add attributes related to BFD
       stability for LAG session.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-mpls:mpls/"
        + "bfd-mpls:session-groups/bfd-mpls:session-group" {
    leaf stability {
      if-feature "stability";
      type boolean;
      must "../bfd-mpls:authentication/bfd-mpls:meticulous = "
         + "'true'";
      default "false";
      description
        "If set to true, this enables the BFD session to monitor
         for stability, i.e., to watch how many packets are getting
         dropped.";
    }
    description
      "Augment the 'bfd' container to add attributes related to BFD
       stability for MPLS.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh/"
        + "bfd-ip-sh:sessions/bfd-ip-sh:session/"
        + "bfd-ip-sh:session-statistics" {
    uses lost-packet-count;
    description
      "Augment the 'bfd' container to add statistics related to BFD
       stability for IP Single Hop sessions.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-ip-mh:ip-mh/"
        + "bfd-ip-mh:session-groups/bfd-ip-mh:session-group/"
        + "bfd-ip-mh:sessions/bfd-ip-mh:session-statistics" {
    uses lost-packet-count;
    description
      "Augment the 'bfd' container to add statistics related to BFD
       stability for IP Multi Hop sessions.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-lag:lag/"
        + "bfd-lag:sessions/bfd-lag:session/bfd-lag:member-links/"
        + "bfd-lag:micro-bfd-ipv4/bfd-lag:session-statistics" {
    uses lost-packet-count;
    description
      "Augment the 'bfd' container to add statistics related to BFD
       stability for Micro BFD sessions for IPv4.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-lag:lag/"
        + "bfd-lag:sessions/bfd-lag:session/bfd-lag:member-links/"
        + "bfd-lag:micro-bfd-ipv6/bfd-lag:session-statistics" {
    uses lost-packet-count;
```

```
    description
      "Augment the 'bfd' container to add statistics related to BFD
       stability for Micro BFD sessions for IPv6.";
  }

  augment "/rt:routing/rt:control-plane-protocols/"
        + "rt:control-plane-protocol/bfd:bfd/bfd-mpls:mpls/"
        + "bfd-mpls:session-groups/bfd-mpls:session-group/"
        + "bfd-mpls:sessions/bfd-mpls:session-statistics" {
    uses lost-packet-count;
    description
      "Augment the 'bfd' container to add statistics related to BFD
       stability for MPLS sessions.";
  }
}
<CODE ENDS>
```

8. IANA Considerations

This document registers a new authentication type in the "BFD Authentication Types" registry, a new URI in the "ns" registry within the "IETF XML" registry group [RFC3688], and a YANG module in the "YANG Module Names" registry.

8.1. Auth Type

IANA has registered the following BFD Auth Type in the "BFD Authentication Types" registry:

Address: 6
BFD Authentication Type Name: NULL
Reference RFC 9978

8.2. IETF XML Registry

IANA has registered the following URI in the "ns" registry [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-bfd-stability
Registrant Contact: The IESG
XML: N/A; the requested URI is an XML namespace.

8.3. The "YANG Module Names" Registry

IANA has registered the following YANG module in the "YANG Module Names" registry [RFC6020]:

Name: ietf-bfd-stability
Namespace: urn:ietf:params:xml:ns:yang:ietf-bfd-stability
Prefix: bfd-s
Reference: RFC 9978

9. Security Considerations

9.1. BFD NULL Auth Security Considerations

The use of a BFD authentication mechanism that protects the BFD packets is **RECOMMENDED**.

The security considerations of [RFC5880] for unauthenticated BFD all apply to the new NULL authentication type. The NULL authentication type, defined in this document, provides none of the properties desired for authenticating BFD packets. It is intended to provide BFD sessions that otherwise would not use authentication with a sequence number that can be used for the purpose of detecting lost packets.

The lack of a computed AuthKey/Digest over the BFD packet, but the presence of a sequence number, makes this authentication type susceptible to injection attacks. BFD without authentication is vulnerable to session resets; the NULL Auth type does not change this.

When the NULL authentication type is used for BFD stability purposes, maliciously injected packets that do not reset the BFD session can resemble high packet loss. Sessions such as multi-hop routed paths, tunnels without authentication, or MPLS Label Switched Paths (LSPs), therefore, have security guarantees that are identical to situations where BFD is run without authentication.

9.2. YANG Security Considerations

This section is modeled after the template described in Section 3.7.1 of [RFC9907].

The "ietf-bfd-stability" YANG module defines a data model that is designed to be accessed via YANG-based management protocols, such as Network Configuration Protocol (NETCONF) [RFC6241] and RESTCONF [RFC8040]. These YANG-based management protocols (1) have to use a secure transport layer (e.g., Secure Shell (SSH) [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and (2) have to use mutual authentication.

The Network Configuration Access Control Model (NACM) [RFC8341] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

The YANG module does not define any writeable/creatable/deletable data nodes that can have an adverse impact on a BFD session.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. Specifically, the following subtrees and data nodes have particular sensitivities/vulnerabilities:

The model defines a read-only node to indicate the number of packets that were lost. Access to this information may allow a malicious user information on which links are experiencing issues. In addition, and as stated in Section 6.2, on links such as LAG or ECMP, there is a possibility of packets being delivered out-of-order. A strict comparison of increasing sequence numbers may result in classifying those out-of-order packets as packet loss.

The YANG module does not define any RPC operations.

10. Contributors

The authors would like to acknowledge Jeff Haas as a contributor to this document. His contribution lead to significant improvements of the document. In addition, Manav Bhatia contributed to this document.

11. Acknowledgements

The authors would like to thank Nobo Akiya, Dileep Singh, Basil Saji, Sagar Soni, Albert Fu, Peng Fang, and Mallik Mudigonda for contributing to this document. Thanks to Christian Huitema for the SECDIR review and Ebben Aries for the YANG Doctors review.

Thanks to Reshad Rehman for being the shepherd of the document.

12. References

12.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC4252] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, DOI 10.17487/RFC4252, January 2006, <https://www.rfc-editor.org/info/rfc4252>.

[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>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[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>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8349] Lhotka, L., Lindem, A., and Y. Qu, "A YANG Data Model for Routing Management (NMDA Version)", RFC 8349, DOI 10.17487/RFC8349, March 2018, <https://www.rfc-editor.org/info/rfc8349>.

[RFC9314] Jethanandani, M., Ed., Rahman, R., Ed., Zheng, L., Ed., Pallagatti, S., and G. Mirsky, "YANG Data Model for Bidirectional Forwarding Detection (BFD)", RFC 9314, DOI 10.17487/RFC9314, September 2022, <https://www.rfc-editor.org/info/rfc9314>.

12.2. Informative References

[BFD-ISAAC] DeKok, A., Jethanandani, M., Agarwal, S., Mishra, A., and J. Haas, "Meticulous Keyed ISAAC for BFD Optimized Authentication", Work in Progress, Internet-Draft, draft-ietf-bfd-secure-sequence-numbers-27, 16 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-bfd-secure-sequence-numbers-27>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9907] Bierman, A., Boucadair, M., Ed., and Q. Wu, "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", BCP 216, RFC 9907, DOI 10.17487/RFC9907, March 2026, <https://www.rfc-editor.org/info/rfc9907>.

[Y-1731] ITU-T, "OAM functions and mechanisms for Ethernet based networks", ITU-T Recommendation G.8013/Y.1731, November 2013, <https://www.itu.int/rec/T-REC-G.8013-201311-S/en>.

Appendix A. Experimental Status

This document describes an experiment that will present a candidate solution to predict whether a given BFD [RFC5880] session will continue to be stable. The experiment will use the packet lost count and the 'received-packet-count' defined in "YANG Data Model for Bidirectional Forwarding Detection (BFD)" [RFC9314] to determine how stable the session is. The reason this document is on the Experimental track is because there are no known implementations or proof of concept. As a result, the authors are not clear whether a simple lost count is enough to predict the stability or if there will be a need to be a more granular count.

This document is classified as Experimental and is not part of the IETF Standards Track.

Appendix B. Examples

This section tries to show some examples of how the model can be configured for stability.

B.1. Single-Hop BFD Configuration

This example demonstrates how a single-hop BFD session can be configured to enable monitoring of a session for stability.

```
=============== NOTE: '\' line wrapping per RFC 8792 ===============

<?xml version="1.0" encoding="UTF-8"?>
<key-chains
    xmlns="urn:ietf:params:xml:ns:yang:ietf-key-chain"
    xmlns:kc="urn:ietf:params:xml:ns:yang:ietf-key-chain">
  <key-chain>
    <name>bfd-stability-config</name>
    <description>"An example for BFD stabilized configuration."</de\
scription>
    <key>
      <key-id>55</key-id>
      <lifetime>
        <send-lifetime>
          <start-date-time>2025-01-01T00:00:00Z</start-date-time>
          <end-date-time>2025-02-01T00:00:00Z</end-date-time>
        </send-lifetime>
        <accept-lifetime>
          <start-date-time>2024-12-31T23:59:55Z</start-date-time>
          <end-date-time>2025-02-01T00:00:05Z</end-date-time>
        </accept-lifetime>
      </lifetime>
      <crypto-algorithm>kc:sha-1</crypto-algorithm>
    </key>
  </key-chain>
</key-chains>
<interfaces
    xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces"
    xmlns:if-type="urn:ietf:params:xml:ns:yang:iana-if-type">
```

```
  <interface>
    <name>eth0</name>
    <type>if-type:ethernetCsmacd</type>
  </interface>
</interfaces>
<routing
    xmlns="urn:ietf:params:xml:ns:yang:ietf-routing"
    xmlns:bfd-types="urn:ietf:params:xml:ns:yang:ietf-bfd-types"
    xmlns:stability="urn:ietf:params:xml:ns:yang:ietf-bfd-stability\
">
  <control-plane-protocols>
    <control-plane-protocol>
      <type>bfd-types:bfdv1</type>
      <name>name:BFD</name>
      <bfd xmlns="urn:ietf:params:xml:ns:yang:ietf-bfd">
        <ip-sh xmlns="urn:ietf:params:xml:ns:yang:ietf-bfd-ip-sh">
          <sessions>
            <session>
              <interface>eth0</interface>
              <dest-addr>2001:db8:0:113::101</dest-addr>
              <desired-min-tx-interval>10000</desired-min-tx-interv\
al>
              <required-min-rx-interval>
                10000
              </required-min-rx-interval>
              <stability:stability>true</stability:stability>
              <authentication>
                <key-chain>bfd-stability-config</key-chain>
                <meticulous>true</meticulous>
              </authentication>
            </session>
          </sessions>
        </ip-sh>
      </bfd>
    </control-plane-protocol>
  </control-plane-protocols>
</routing>
```

B.2. Use of NULL Auth

This example demonstrates how to configure NULL Auth to enable monitoring of a session for stability.

```
=============== NOTE: '\' line wrapping per RFC 8792 ===============

<?xml version="1.0" encoding="UTF-8"?>
<key-chains
    xmlns="urn:ietf:params:xml:ns:yang:ietf-key-chain"
    xmlns:stability="urn:ietf:params:xml:ns:yang:ietf-bfd-stability\
">
  <key-chain>
    <name>bfd-stability-config</name>
    <description>"An example for BFD stability configuration."</des\
cription>
    <key>
```

```
      <key-id>55</key-id>
      <lifetime>
        <send-lifetime>
          <start-date-time>2025-01-01T00:00:00Z</start-date-time>
          <end-date-time>2025-02-01T00:00:00Z</end-date-time>
        </send-lifetime>
        <accept-lifetime>
          <start-date-time>2024-12-31T23:59:55Z</start-date-time>
          <end-date-time>2025-02-01T00:00:05Z</end-date-time>
        </accept-lifetime>
      </lifetime>
      <crypto-algorithm>stability:null-auth</crypto-algorithm>
    </key>
  </key-chain>
</key-chains>
<interfaces
    xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces"
    xmlns:if-type="urn:ietf:params:xml:ns:yang:iana-if-type">
  <interface>
    <name>eth0</name>
    <type>if-type:ethernetCsmacd</type>
  </interface>
</interfaces>
<routing
    xmlns="urn:ietf:params:xml:ns:yang:ietf-routing"
    xmlns:bfd-types="urn:ietf:params:xml:ns:yang:ietf-bfd-types"
    xmlns:stability="urn:ietf:params:xml:ns:yang:ietf-bfd-stability\
">
  <control-plane-protocols>
    <control-plane-protocol>
      <type>bfd-types:bfdv1</type>
      <name>name:BFD</name>
      <bfd xmlns="urn:ietf:params:xml:ns:yang:ietf-bfd">
        <ip-sh xmlns="urn:ietf:params:xml:ns:yang:ietf-bfd-ip-sh">
          <sessions>
            <session>
              <interface>eth0</interface>
              <dest-addr>2001:db8:0:113::101</dest-addr>
              <desired-min-tx-interval>10000</desired-min-tx-interv\
al>
              <required-min-rx-interval>
                10000
              </required-min-rx-interval>
              <stability:stability>true</stability:stability>
              <authentication>
                <key-chain>bfd-stability-config</key-chain>
                <meticulous>true</meticulous>
              </authentication>
            </session>
          </sessions>
        </ip-sh>
      </bfd>
    </control-plane-protocol>
  </control-plane-protocols>
</routing>
```

Authors' Addresses

Ashesh Mishra
Aalyria Technologies
Email: ashesh@aalyria.com

Mahesh Jethanandani
Arrcus, Inc.
United States of America
Email: mjethanandani@gmail.com

Ankur Saxena
Ciena Corporation
3939 North 1st Street
San Jose, CA 95134
United States of America
Email: ankurpsaxena@gmail.com
URI: www.ciena.com

Santosh Pallagatti
Zscaler
Bangalore 560103
Karnataka
India
Email: santosh.pallagatti@gmail.com

Mach Chen
Huawei
Email: mach.chen@huawei.com