Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 7 May 2026

A. Mishra
Aalyria Technologies
M. Jethanandani
Arrcus, Inc.
A. Saxena
Ciena Corporation
S. Pallagatti
Zscaler
M. Chen
Huawei

3 November 2025

BFD Stability
draft-ietf-bfd-stability-21

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 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 7 May 2026.

Copyright Notice

Copyright (c) 2025 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 2
1.1. Note to the RFC Editor 3
2. Terminology 3
3. Use Cases 4
4. Functionality 4
5. NULL Auth Type 4
6. Theory of Operation 6
6.1. Loss Measurement 6
6.2. Out of Order Packets 7
7. Stability YANG Module 7
7.1. Data Model Overview 7
7.2. YANG Module 9
8. IANA Considerations 14
8.1. Auth Type 14
8.2. IETF XML Registry 14
8.3. The "YANG Module Names" Registry 15
9. Security Considerations 15
9.1. BFD NULL Auth Security Considerations 15
9.2. YANG Security Considerations 16
10. Contributors 16
11. Acknowledgements 16
12. References 17
12.1. Normative References 17
12.2. Informative References 18
Appendix A. Experimental Status 19
Appendix B. Examples 19
B.1. Single Hop BFD Configuration 19
B.2. Use of NULL Auth 21
Authors' Addresses 22

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.

A BFD [RFC5880] session 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 the YANG Data Model for Bidirectional Forward Detection (BFD) [RFC9314] permits operators to measure the stability of BFD sessions. The details of the motivation for experimental status 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.

1.1. Note to the RFC Editor

This document uses several placeholder values throughout the document. Please replace them as follows and remove this section before publication.

RFC XXXX, where XXXX is the number assigned to this document at the time of publication.

2025-10-30, with the actual date of the publication of this document.

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 RFC 2119 [RFC2119] and RFC 8174 [RFC8174].

The reader is expected to be familiar with the BFD [RFC5880]. In particular, the term 'meticulous' specified in Meticulous Keyed ISAAC for BFD Optimized Authentication [I-D.ietf-bfd-secure-sequence-numbers] means that the Sequence number is incremented on every new packet that is sent.

3. Use Cases

Bidirectional Forwarding Detection, as defined in BFD [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+10ms, 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 that could be used to preempt 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 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 is configured.

The ietf-bfd-stability YANG model, defined in this document, provides the ability to configure 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 BFD stability measurement and monitoring using other methods than the attached YANG model is out of scope from 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 BFD [RFC5880], and the Authentication Type field contains TBD, the Authentication section has the following format:

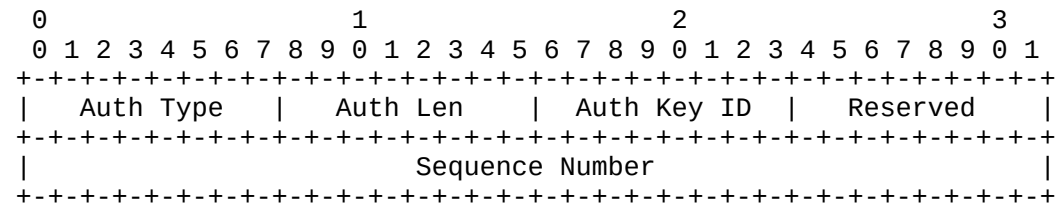

Figure 1: NULL Auth Type

where:

Auth Type (8 bits): The Authentication Type, which in this case is TBD (NULL, to be assigned by IANA, with a suggested value of 6).

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. 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 BFD [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 BFD [RFC5880], Section 6.8.1, and the packet MUST be accepted.

According to BFD [RFC5880], Section 6.7.3 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 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 purposes 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 [I-D.ietf-bfd-secure-sequence-numbers].

* The NULL authentication mechanism, which does not provide for authentication but carries a meticulously increasing sequence number, 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 BFD [RFC5880], Section 6.8.4 period. 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 (Section 6.2) later in the 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 (LAG), 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 flag ’stability’ 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 Types [RFC6991], A YANG Data Model for Routing [RFC8349], and YANG Data Model for Bidirectional Forwading Detection (BFD) [RFC9314].

```
<CODE BEGINS> file "ietf-bfd-stability@2025-10-30.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.";
  }

  import ietf-bfd-ip-mh {
    prefix bfd-ip-mh;
    reference
      "RFC 9314: YANG Data Model for Bidirectional
       Forwarding Detection.";
  }

  import ietf-bfd-lag {
    prefix bfd-lag;
```

```
    reference
      "RFC 9314: YANG Data Model for Bidirectional
       Forwarding Detection.";
  }

  import ietf-bfd-mpls {
    prefix bfd-mpls;
    reference
      "RFC 9314: YANG Data Model for Bidirectional
       Forwarding Detection.";
  }

  import ietf-key-chain {
    prefix key-chain;
    reference
      "RFC 8177: YANG Key Chain.";
  }

  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 model to add
     experimental attributes related to BFD Stability.
     In particular, it adds a per-session count for BFD packets
     that are lost.

     Copyright (c) 2025 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 XXXX
        (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
        for full legal notices.

        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.";

    revision "2025-10-30" {
      description
        "Initial Version.";
      reference
        "RFC XXXX: 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 draft.";
      reference
        "RFC XXXX: 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 requests one new authentication type and registers one URIs in the "ns" subregistry of the "IETF XML" registry [RFC3688].

8.1. Auth Type

This document requests an update to the registry titled "BFD Authentication Types". IANA is requested to assign a new BFD AuthType:

* NULL Auth Type, with a suggested value of 6.

8.2. IETF XML Registry

Following the format in [RFC3688], the following registrations are requested:

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

This document registers one YANG module in the "YANG Module Names" registry [RFC6020]. Following the format in [RFC6020], the following registrations are requested:

```
name:         ietf-bfd-stability
namespace:    urn:ietf:params:xml:ns:yang:ietf-bfd-stability
prefix:       bfd-s
reference:    RFC XXXX
```

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, a sequence number that can be used for purposes 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 LSP, therefore, have security guarantees that are identical to situations where BFD is run without authentication.

9.2. YANG Security Considerations

The YANG module specified in this document defines a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. These YANG-based management protocols have to use a secure transport layer (e.g., SSH [RFC4252], TLS [RFC8446], and QUIC [RFC9000]) and have to use mutual authentication.

The NETCONF 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.

The only readable data nodes in 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.

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 Out of Order Packets (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 of this document would like to acknowledge Jeff Haas as a contributor to this document. His contribution lead to a significant improvement of the document. In addition, Manav Bhatia contributed to this document.

11. Acknowledgements

Authors would like to thank Nobo Akiya, Dileep Singh, Basil Saji, Sagar Soni, Albert Fu, Peng Fang, and Mallik Mudigonda who contributed to this document. Thanks to Christian Huitema for the SECDIR 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

[I-D.ietf-bfd-secure-sequence-numbers] 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>.

[Y-1731] ITU-T, "OAM Functions and Mechanisms for Ethernet-based Networks", Recommendation G.8013/Y.1731, November 2013.

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 the YANG Data Model for Bidirectional Forward Detection (BFD) [RFC9314] to determine how stable is the session. The reason why this document is on an 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 there will be a need to have 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 in 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 Stabalized 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