Workgroup: Network Working Group
Internet-Draft:
draft-ietf-bfd-optimizing-authentication-15
Updates: 5880 (if approved)
Published: 20 March 2024
Intended Status: Standards Track
Expires: 21 September 2024
Authors: M. Jethanandani
Kloud Services
A. Mishra
Aalyria Technologies
A. Saxena
Ciena Corporation
M. Bhatia
Google

Optimizing BFD Authentication

Abstract

This document describes an optimization to BFD Authentication as described in Section 6.7 of BFD RFC 5880. This document updates RFC 5880.

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 21 September 2024.

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

Authenticating every BFD [RFC5880] control packet with MD5 Message-Digest Algorithm [RFC1321], or Secure Hash Algorithm (SHA-1) is a computationally intensive process. This makes it difficult, if not impossible to authenticate every packet - particularly at faster rates. Also, the recent escalating series of attacks on MD5 and SHA-1 described in Finding Collisions in the Full SHA-1 [SHA-1-attack1] and New Collision Search for SHA-1 [SHA-1-attack2] raise concerns about their remaining useful lifetime as outlined in Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithm [RFC6151] and Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithm [RFC6194]. If replaced by stronger algorithms, the computational overhead, will make the task of authenticating every packet even more difficult to achieve.

This document proposes that BFD control packets that signal a state change, a demand mode change (to D bit), a poll sequence change (P or F bit change) be categorized as a significant change. Control packets that do not require a poll sequence, such as

bfd.RequiredMinRxInterval or bfd.RequiredMinTxInterval, are also considered as a significant change. In other words, the contents of an Up packet MUST NOT change aside from the authentication section without stronger authentication to take advantage of the method described in this document.

In the Up state, most packets that are transmitted and received have no state change associated with them. Limiting authentication to packets that affect a BFD session's state allows more sessions to be supported with this optimized method of authentication.

Once the session has reached the Up state, the session can choose the Auth Type to be one of:

* No authentication, i.e., Authentication Present (A-bit) is zero. Having no authentication provides computational relief to the system. However, a malicious user can blindly inject traffic that will be accepted by the BFD session.

* NULL Auth Type (Section 3) as defined in this document. This type prevents blind injection, but is vulnerable to active attacks, where the attacker is aware of the sequence number, and potentially becomes the PITM. However, periodic check with stronger authentication can thwart that attack as described below.

* Meticulous Keyed ISAAC authentication as described in Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers]. This authentication type prevents the attack when the Up packets do not change, because only the paired devices know the shared secret, key, and sequence number to select the ISAAC result.

To detect a Person In the Middle (PITM) attack when the session is in Up state, implementations have two options. They can choose to use:

* Test periodic strong authentication using a Poll sequence. To perform a strong authentication, a Poll sequence SHOULD be initiated by the sender. If a Fin is not received within the Detect Interval, the session has been compromised, and should be brought down. The interval for initiating a Poll sequence can be configured depending on the capability of the system.

* Meticulous Keyed ISAAC as defined in Securing BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers].

Most packets transmitted on a BFD session are BFD Up packets. Authenticating a small subset of these packets with a Poll sequence as described above, for example every one minute, significantly

reduces the computational demand for the system while maintaining security of the session across the configured interval.

The rest of this document is structured as follows: Section 2 talks about the changes to authentication mode as described in BFD [RFC5880]. Section 3 goes into the details of the new Authentication Type.

1.1. Requirements Language

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Note to RFC Editor

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

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

2024-03-21 with the actual date of the publication of this document.

1.3. Terminology

The following terms used in this document have been defined in BFD [RFC5880].

*Detect Multiplier

*Detection Time

The following terms are introduced in this document.

Term	Meaning
significant change	State change, a demand mode change (to D bit) or a poll sequence change (P or F bit). Control packets that do not require a poll sequence, such as bfd.RequiredMinRxInterval bfd.RequiredMinTxInterval, or bfd.DetectMult are also considered as a significant change.
configured interval	Interval at which BFD control packets are retried with a stronger authentication.

Table 1

2. Authentication Mode

The cryptographic authentication mechanisms specified in BFD [RFC5880] describes enabling and disabling of authentication as a one time operation. As a security precaution, it mentions that authentication state be allowed to change at most once. Once enabled, every packet must have Authentication Bit set and the associated Authentication Type appended. In addition, it states that an implementation SHOULD NOT allow the authentication state to be changed based on the receipt of a BFD control packet.

This document proposes that the authentication mode be modified to be enabled on demand. Instead of authenticating every packet, BFD peers are configured for which packets need to be authenticated, and authenticate only those packets. The remaining packets MAY be transmitted and received without authentication, or use a less expensive authentication. For example, the two ends can be configured such that BFD control packets that indicate a significant change should be authenticated and enable authentication on those packets only. If the two ends have previously been configured as such, but at least one side decides not to authenticate a significant change packet, then the BFD session will fail to come up.

The proposal outlines which BFD control packets are required to be authenticated. A BFD control packet that fails authentication is discarded, or a BFD control packet that was supposed to be authenticated, but was not; e.g. a significant change packet, is discarded. However, there is no change to the state machine for BFD, as the decision of a significant change is still decided by how many valid consecutive packets were received, authenticated or otherwise.

The following table summarizes when the Auth Type should be set with a Auth or a OPT authentication type. The table should be read with the column indicating the BFD state the receiver is currently in, and the row indicating the BFD state the receiver might transition to based on the BFD control packet received. The intersection of the two indicates whether the received BFD control packet should have the Auth Type set to either Auth, or OPT. The BFD state refers to the states in BFD state machine described in Section 6.2 of BFD [RFC5880].

```
 Read   : On state change from <column> to <row>
 Auth   : Strongly authenticated BFD control packet
 OPT    : Any or no authentication, as configured.
 n/a    : Invalid state transition.
 Select : Most packets OPT AUTH. Selective (periodic)
          packets authenticated.
+--------+--------+--------+--------+
|        | DOWN   | INIT   | UP     |
+--------+--------+--------+--------+
| DOWN   |  OPT   |  Auth  |  Auth  |
+--------+--------+--------+--------+
| INIT   |  Auth  |  OPT   |  n/a   |
+--------+--------+--------+--------+
| UP     |  Auth  |  Auth  | Select |
+--------+--------+--------+--------+
```

Figure 1: Optimized Authentication Map

In other words, the contents of an Up packet MUST NOT change aside from the authentication section without stronger authentication.

Implementations supporting this feature can send BFD packets with or without authentication that carries a meticulously increasing sequence number. This meticulously increasing sequence number prevents replay attacks, and it supports BFD Stability [I-D.ietf-bfd-stability].

The NULL Authentication type is defined in NULL Authentication Type (Section 3). This authentication type does not provide any authentication of the BFD Control Up packets, but does carry a meticulously increasing sequence number compatible with this specification.

Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers] defines an authentication mechanism that does not provide any authentication of the BFD Control packets, carries a meticulously increasing sequence number, but provides for a stronger mechanism to prevent active attacks against these procedures for Up packets without requiring strong authentication.

3. NULL Auth Type

This section describes a new Authentication Type as:

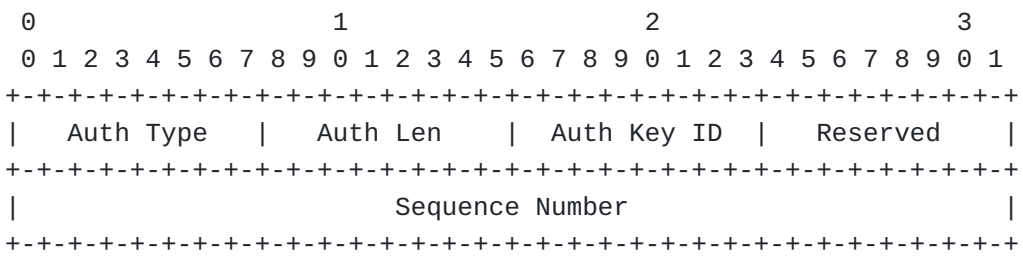

Figure 2: NULL Auth Type

where:

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

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

Auth Key ID: The authentication key ID in use for this packet. Must be set to zero.

Reserved: This byte MUST be set to zero on transmit and ignored on receive.

Sequence Number: The sequence number for this packet. Implementations will use sequence numbers (bfd.XmitAuthSeq) as defined in BFD [RFC5880].

4. Optimizing Authentication YANG Model

4.1. Data Model Overview

The YANG 1.1 [RFC7950] model defined in this document augments the "ietf-bfd" module to add configuration relevant to the management of the feature defined in this document. In particular, it adds crypto algorithms that are described in this model, and in Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers]. It adds a feature statement to enable optimized authentication. Finally, it adds a flag to enable optimized authentication, an interval value that specifies how often the BFD session should be re-authenticated once it is in the Up state, and the key chain that should be used in the Up state.

4.2. Tree Diagram

The tree diagram for the YANG modules defined in this document use annotations defined in YANG Tree Diagrams. [RFC8340].

```
module: ietf-bfd-opt-auth

  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:authentication:
    +--rw optimized-auth?      boolean {optimized-auth}?
    +--rw reauth-interval?     uint32
    +--rw up-auth-key-chain?   key-chain:key-chain-ref
  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:authentication:
    +--rw optimized-auth?    boolean {optimized-auth}?
    +--rw reauth-interval?   uint32
    +--rw up-auth-type?      key-chain:key-chain-ref
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-lag:lag
            /bfd-lag:sessions/bfd-lag:session/bfd-lag:authentication:
    +--rw optimized-auth?    boolean {optimized-auth}?
    +--rw reauth-interval?   uint32
    +--rw up-auth-type?      key-chain:key-chain-ref
  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:authentication:
    +--rw optimized-auth?    boolean {optimized-auth}?
    +--rw reauth-interval?   uint32
    +--rw up-auth-type?      key-chain:key-chain-ref
```

4.3. The YANG Model

This YANG module imports YANG Key Chain [RFC8177], 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-opt-auth@2024-03-21.yang"

module ietf-bfd-opt-auth {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-bfd-opt-auth";
  prefix "bfdoa";

  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)
            Manav Bhatia (mnvbhatia@google.com).";


description
  "This YANG module augments the base BFD YANG model to add
   attributes related to BFD Optimized Authentication.

   Copyright (c) 2024 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 "2024-03-21" {
  description
    "Initial Version.";
  reference
    "RFC XXXX: Optimizing BFD Authentication.";
}

feature optimized-auth {
```

```
  description
    "When enabled, this implementation supports optimized
     authentication as described in this document.";
}

identity no-auth {
  base key-chain:crypto-algorithm;
  description
    "No authentication will be used.";
}

identity null-auth {
  base key-chain:crypto-algorithm;
  description
    "BFD Null Auth type defined in this draft.";
  reference
    "RFC XXXX: Optimizing BFD Authentication.";
}

identity meticulous-keyed-isaac {
  base key-chain:crypto-algorithm;
  description
    "BFD ISAAC Keyed Meticulous Auth.";
  reference
    "I-D.ietf-bfd-secure-sequence-numbers: Securing BFD Sequence
                                           Numbers.";
}

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:authentication" {
  leaf optimized-auth {
    if-feature optimized-auth;
    type boolean;
    default false;
    description
      "If set to true, BFD Single Hop Sessions will be
       enabled for optimized authentication.";
  }

  leaf reauth-interval {
    when "../optimized-auth = 'true'";
    type uint32;
    units "seconds";
    default "60";
    description
      "Interval of time after which a strong authentication
       should be enabled to prevent a Person-In-The-Middle
```

```
        attack. Default is 1 minute.

        A value of zero means that we do not do periodic
        re-authorization using strong authentication; e.g.,
        when 'up-auth-type' is 'meticulous-keyed-isaac'.

        This value SHOULD have jitter applied to it to avoid
        self-synchronization during expensive authentication
        operations.";
    }

    leaf up-auth-key-chain {
      type key-chain:key-chain-ref;
      must "(../optimized-auth = 'true') and " +
           "(../bfd-ip-sh:meticulous = 'true')";
      description
        "The authentication type that should be used once the
         connection transitions to Up state. In case
         of optimized auth, the choices are Reserved (or no
         authentication), NULL Auth, or Meticulous Keyed ISAAC.";
    }
    description
      "Augment the 'authentication' container in BFD module to
       add attributes related to BFD optimized authentication.";
  }

  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:authentication" {
    leaf optimized-auth {
      if-feature optimized-auth;
      type boolean;
      default false;
      description
        "If set to true, BFD Multi Hop Sessions will be
         enabled for optimized authentication.";
    }

    leaf reauth-interval {
      when "../optimized-auth = 'true'";
      type uint32;
      units "seconds";
      default "60";
      description
        "Interval of time after which a strong authentication
         should be enabled to prevent a Person-In-The-Middle
         attack. Default is 1 minute.
```

```
        A value of zero means that we do not do periodic
        re-authorization using strong authentication; e.g.,
        when 'up-auth-type' is 'meticulous-keyed-isaac'.

        This value SHOULD have jitter applied to it to avoid
        self-synchronization during expensive authentication
        operations.";
    }

    leaf up-auth-type {
      type key-chain:key-chain-ref;
      must "(../optimized-auth = 'true') and " +
           "(../bfd-ip-mh:meticulous = 'true')";
      description
        "The authentication type that should be used once the
         connection transitions to Up state. In case
         of optimized auth, the choices are Reserved (or no
         authentication), NULL Auth, or Meticulous Keyed ISAAC.";
    }
    description
      "Augment the 'authentication' container in BFD module to
       add attributes related to BFD optimized authentication.";
  }

  augment "/rt:routing/rt:control-plane-protocols/" +
          "rt:control-plane-protocol/bfd:bfd/bfd-lag:lag/" +
          "bfd-lag:sessions/bfd-lag:session/" +
          "bfd-lag:authentication" {
    leaf optimized-auth {
      if-feature optimized-auth;
      type boolean;
      default false;
      description
        "If set to true, BFD LAG Sessions will be
         enabled for optimized authentication.";
    }

    leaf reauth-interval {
      when "../optimized-auth = 'true'";
      type uint32;
      units "seconds";
      default "60";
      description
        "Interval of time after which a strong authentication
         should be enabled to prevent a Person-In-The-Middle
         attack. Default is 1 minute.

         A value of zero means that we do not do periodic
         re-authorization using strong authentication; e.g.,
```

```
        when 'up-auth-type' is 'meticulous-keyed-isaac'.

        This value SHOULD have jitter applied to it to avoid
        self-synchronization during expensive authentication
        operations.";
    }

    leaf up-auth-type {
      type key-chain:key-chain-ref;
      must "(../optimized-auth = 'true') and " +
           "(../bfd-lag:meticulous = 'true')";
      description
        "The authentication type that should be used once the
         connection transitions to Up state. In case
         of optimized auth, the choices are Reserved (or no
         authentication), NULL Auth, or Meticulous Keyed ISAAC.";
    }
    description
      "Augment the 'authentication' container in BFD module to
       add attributes related to BFD optimized authentication.";
  }

  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:authentication" {
    leaf optimized-auth {
      if-feature optimized-auth;
      type boolean;
      default false;
      description
        "If set to true, BFD MPLS Sessions will be
         enabled for optimized authentication.";
    }

    leaf reauth-interval {
      when "../optimized-auth = 'true'";
      type uint32;
      units "seconds";
      default "60";
      description
        "Interval of time after which a strong authentication
         should be enabled to prevent a Person-In-The-Middle
         attack. Default is 1 minute.

         A value of zero means that we do not do periodic
         re-authorization using strong authentication; e.g.,
         when 'up-auth-type' is 'meticulous-keyed-isaac'.
```

```
          This value SHOULD have jitter applied to it to avoid
          self-synchronization during expensive authentication
          operations.";
      }

      leaf up-auth-type {
        type key-chain:key-chain-ref;
        must "(../optimized-auth = 'true') and " +
             "(../bfd-mpls:meticulous = 'true')";
        description
          "The authentication type that should be used once the
           connection transitions to Up state. In case
           of optimized auth, the choices are Reserved (or no
           authentication), NULL Auth, or Meticulous Keyed ISAAC.";
      }
      description
        "Augment the 'authentication' container in BFD module to
         add attributes related to BFD optimized authentication.";
    }
}

<CODE ENDS>
```

5. IANA Considerations

This documents requests two new authentication types, one URI, one YANG model, and an update to an existing IANA YANG model.

5.1. Auth Type

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

* NULL Auth Type (Section 3), with a suggested value of 6.

* Meticulous Keyed ISAAC Authentication [I-D.ietf-bfd-secure-sequence-numbers] (Part meticulous-keyed-isaac-authentication), with a suggested value of 7.

5.2. IETF XML Registry

This document registers one URIs in the "ns" subregistry of the "IETF XML" registry [RFC3688]. Following the format in [RFC3688], the following registration is requested:

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

5.3. The YANG Module Names Registry

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

```
name:         ietf-bfd-opt-auth
namespace:    urn:ietf:params:xml:ns:yang:ietf-bfd-opt-auth
prefix:       bfdoa
reference:    RFC XXXX
```

5.4. Updated IANA Module

This document also requests an update to an existing IANA YANG module described in Updated BFD IANA Module (Appendix A)

6. 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]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446]. 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.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. Some of the subtrees and data nodes and their sensitivity/vulnerability are described here.

*'optimized-auth' flag is used to enable optimized authentication for the session. If this was not intended, or the other end is not configured with the same flag, the BFD session will fail to come up.

*'reauth-interval' specifies the interval in Up state, after which a strong authentication SHOULD be performed to prevent a Person-In-The-Middle (PITM) attack. If this interval is set very low, or very high, then it will make optimization worthless.

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.

There are no read-only data nodes defined in this model.

Some of the RPC operations in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control access to these operations.

There are no RPC operations defined in this model.

The approach described in this document enhances the ability to authenticate a BFD session by taking away the onerous requirement that every BFD control packet be authenticated. By authenticating packets that affect the state of the session, the security of the BFD session is maintained. In this mode, packets that are a significant change but are not authenticated, are dropped by the

system. Therefore, a malicious user that tries to inject a non-authenticated packet; e.g. with a Down state to take a session down will fail. That combined with the proposal of using sequence number defined in Secure BFD Sequence Numbers [I-D.ietf-bfd-secure-sequence-numbers] further enhances the security of BFD sessions.

7. References

7.1. Normative References

[I-D.ietf-bfd-secure-sequence-numbers]
DeKok, A., Jethanandani, M., Agarwal, S., Mishra, A., and A. Saxena, "Meticulous Keyed ISAAC for BFD Authentication", Work in Progress, Internet-Draft, draft-ietf-bfd-secure-sequence-numbers-13, 4 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bfd-secure-sequence-numbers-13>.

[I-D.ietf-bfd-stability]
Mishra, A., Jethanandani, M., Saxena, A., Pallagatti, S., Chen, M., and P. Fan, "BFD Stability", Work in Progress, Internet-Draft, draft-ietf-bfd-stability-12, 31 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bfd-stability-12>.

[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>.

[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>.

[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>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[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>.

[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>.

[RFC8177] Lindem, A., Ed., Qu, Y., Yeung, D., Chen, I., and J. Zhang, "YANG Data Model for Key Chains", RFC 8177, DOI 10.17487/RFC8177, June 2017, <https://www.rfc-editor.org/info/rfc8177>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[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>.

[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>.

[RFC9127] Rahman, R., Ed., Zheng, L., Ed., Jethanandani, M., Ed., Pallagatti, S., and G. Mirsky, "YANG Data Model for Bidirectional Forwarding Detection (BFD)", RFC 9127, DOI 10.17487/RFC9127, October 2021, <https://www.rfc-editor.org/info/rfc9127>.

[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>.

7.2. Informative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <https://www.rfc-editor.org/info/rfc1321>.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, DOI 10.17487/RFC6151, March 2011, <https://www.rfc-editor.org/info/rfc6151>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <https://www.rfc-editor.org/info/rfc6194>.

[SHA-1-attack1] Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the Full SHA-1", 2005.

[SHA-1-attack2] Wang, X., Yao, A., and F. Yao, "New Collision Search for SHA-1", 2005.

Appendix A. Updated BFD IANA Module

This section carries the updated IANA BFD Module, iana-bfd-types.yang module, first defined in YANG Data Model for Bidirectional Forward Detection (BFD) [RFC9127]. The updated module carries two new authentication type enum definitions, 'null' with a suggested value of 6, and 'meticulous-keyed-isaac' with a suggested value of 7. This module should replace the version that currently exists in the IANA registry.

```
<CODE BEGINS> file "iana-bfd-types@2024-03-21.yang"

module iana-bfd-types {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:iana-bfd-types";
  prefix iana-bfd-types;

  organization
    "IANA";
  contact
    "Internet Assigned Numbers Authority

     Postal: ICANN
             12025 Waterfront Drive, Suite 300
             Los Angeles, CA 90094-2536
             United States of America
     Tel:    +1 310 301 5800
     <mailto:iana@iana.org>";
  description
    "This module defines YANG data types for IANA-registered
     BFD parameters.

     This YANG module is maintained by IANA and reflects the
     'BFD Diagnostic Codes' and 'BFD Authentication Types'
     registries.

     Copyright (c) 2021 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 Simplified 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 9127; see the
     RFC itself for full legal notices.";
  reference
    "RFC 9127: YANG Data Model for Bidirectional Forwarding
     Detection (BFD)";

  revision 2024-03-21 {
    description
      "Add NULL and Meticulous ISAAC authentication type.";
    reference
      "I-D.ietf-bfd-optimized-auth: Optimizing BFD Authentication.";
  }

  revision 2021-10-21 {
```

```
  description
    "Initial revision.";
  reference
    "RFC 9127: YANG Data Model for Bidirectional Forwarding
     Detection (BFD)";
}

/*
 * Type definitions
 */

typedef diagnostic {
  type enumeration {
    enum none {
      value 0;
      description
        "No Diagnostic.";
    }
    enum control-expiry {
      value 1;
      description
        "Control Detection Time Expired.";
    }
    enum echo-failed {
      value 2;
      description
        "Echo Function Failed.";
    }
    enum neighbor-down {
      value 3;
      description
        "Neighbor Signaled Session Down.";
    }
    enum forwarding-reset {
      value 4;
      description
        "Forwarding Plane Reset.";
    }
    enum path-down {
      value 5;
      description
        "Path Down.";
    }
    enum concatenated-path-down {
      value 6;
      description
        "Concatenated Path Down.";
    }
    enum admin-down {
```

```
      value 7;
      description
        "Administratively Down.";
    }
    enum reverse-concatenated-path-down {
      value 8;
      description
        "Reverse Concatenated Path Down.";
    }
    enum mis-connectivity-defect {
      value 9;
      description
        "Mis-connectivity defect.";
      reference
        "RFC 5880: Bidirectional Forwarding Detection (BFD)
         RFC 6428: Proactive Connectivity Verification, Continuity
         Check, and Remote Defect Indication for the MPLS
         Transport Profile";
    }
  }
  description
    "BFD diagnostic codes as defined in RFC 5880.  Values are
     maintained in the 'BFD Diagnostic Codes' IANA registry.
     Range is 0 to 31.";
  reference
    "RFC 5880: Bidirectional Forwarding Detection (BFD)";
}

typedef auth-type {
  type enumeration {
    enum reserved {
      value 0;
      description
        "Reserved.";
    }
    enum simple-password {
      value 1;
      description
        "Simple Password.";
    }
    enum keyed-md5 {
      value 2;
      description
        "Keyed MD5.";
    }
    enum meticulous-keyed-md5 {
      value 3;
      description
        "Meticulous Keyed MD5.";
```

```
      }
      enum keyed-sha1 {
        value 4;
        description
          "Keyed SHA1.";
      }
      enum meticulous-keyed-sha1 {
        value 5;
        description
          "Meticulous Keyed SHA1.";
      }
      enum null {
        value 6;
        description
          "NULL Auth.";
      }
      enum meticulous-keyed-isaac {
        value 7;
        description
          "Meticulous Keyed ISAAC.";
      }
    }
    description
      "BFD authentication type as defined in RFC 5880.  Values are
       maintained in the 'BFD Authentication Types' IANA registry.
       Range is 0 to 255.";
    reference
      "RFC 5880: Bidirectional Forwarding Detection (BFD)";
  }
}

<CODE ENDS>
```

Appendix B. Examples

This section tries to show some examples in how the model can be configured.

B.1. Single Hop BFD Configuration

This example demonstrates how a Single Hop BFD session can be configured for optimized authentication.

```
=============== 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">
  <key-chain>
    <name>bfd-auth-config</name>
    <description>"An example for BFD Optimized Auth configuration."\
</description>
    <key>
      <key-id>55</key-id>
      <lifetime>
        <send-lifetime>
          <start-date-time>2017-01-01T00:00:00Z</start-date-time>
          <end-date-time>2017-02-01T00:00:00Z</end-date-time>
        </send-lifetime>
        <accept-lifetime>
          <start-date-time>2016-12-31T23:59:55Z</start-date-time>
          <end-date-time>2017-02-01T00:00:05Z</end-date-time>
        </accept-lifetime>
      </lifetime>
      <crypto-algorithm xmlns:opt-auth=
      "urn:ietf:params:xml:ns:yang:ietf-bfd-opt-auth">opt-auth:meti\
culous-keyed-isaac</crypto-algorithm>
      <key-string>
        <keystring>testvector</keystring>
      </key-string>
    </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:iana-bfd-types="urn:ietf:params:xml:ns:yang:iana-bfd-type\
s"
    xmlns:opt-auth="urn:ietf:params:xml:ns:yang:ietf-bfd-opt-auth">
  <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>
              <authentication>
                <meticulous>true</meticulous>
                <opt-auth:optimized-auth>true</opt-auth:optimized-a\
uth>
                <opt-auth:reauth-interval>30</opt-auth:reauth-inter\
val>
                <opt-auth:up-auth-key-chain>bfd-auth-config</opt-au\
th:up-auth-key-chain>
              </authentication>
            </session>
          </sessions>
        </ip-sh>
      </bfd>
    </control-plane-protocol>
  </control-plane-protocols>
</routing>
```

Authors' Addresses

Mahesh Jethanandani
Kloud Services
United States of America

Email: mjethanandani@gmail.com

Ashesh Mishra
Aalyria Technologies

Email: ashesh@aalyria.com

Ankur Saxena
Ciena Corporation
3939 N 1st Street
San Jose, CA 95134
United States of America

Email: ankurpsaxena@gmail.com

Manav Bhatia
Google
Doddanekkundi
Bangalore 560048
India

Email: mnvbhatia@google.com