Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 6 February 2026

M. Jethanandani
Arrcus
A. Mishra
Aalyria Technologies
A. Saxena
Ciena Corporation
M. Bhatia
Google
J. Haas
Juniper Networks
5 August 2025

Optimizing BFD Authentication
draft-ietf-bfd-optimizing-authentication-28

Abstract

This document describes an experimental optimization to BFD Authentication. It provides procedure where BFD state transitions require strong authentication and permits the majority of BFD Control Packets to use a less computationally intensive authentication mechanism. This enables BFD to scale better when there is a desire to use strong authentication.

Status of This Memo

Copyright Notice

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 BFD packet at high session scale and at faster rates.

This document describes an experimental procedure whereby only BFD state transitions and some other changes (as described later in this document) require strong authentication. The majority of BFD Control Packets use a less computationally intensive authentication mechanism. The details of the motivation for experimental status are given in Appendix B.

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.

2025-08-05 with the actual date of the publication of this document.

2. Terminology

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

* Auth Type

* 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). Changes to BFD control packets that do not require a poll sequence, such as bfd.DetectMult are also considered as a significant change.
configured strong reauthentication interval	Interval at which BFD control packets are retried with strong authentication.

Table 1

3. BFD Control Packets That Require Strong Authentication

For purposes of this document, "strong authentication" refers to BFD authentication mechanisms such as those already defined for use with BFD. For example, MD5 and SHA1 (Section 6.7 of [RFC5880]). The use of stronger cryptographic mechanisms such as SHA2 while using optimized BFD authentication is left for future study.

The intention of these optimized procedures is to permit strong authentication for BFD state changes and utilize the less computationally intensive authentication mechanisms to provide protection for the session in the Up state while performing less overall work. Such procedures will aid BFD session scaling without compromising BFD session security.

All BFD Control Packets with the states AdminDown, Down, and Init require strong authentication.

Once the BFD state machine has reached the Up state, it will continue to send BFD Control Packets in the Up state for a period as discussed in Section 7.2. If optimized authentication mechanisms are in use, the session MAY switch to the less computationally intensive mode.

The contents of an Up packet MUST NOT change aside from the Authentication Section without strong authentication.

In addition to these requirements, BFD "significant changes" require strong authentication.

3.1. Protecting BFD Significant Changes with Strong Authentication

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

Such significant changes are intended to be protected by strong authentication.

4. Using Less Computationally Intensive Auth Types

The majority of packets exchanged on a BFD session in the Up state are not significant changes. This document proposes a new optimized authentication mode where packets that are not significant changes may use a less computationally intensive authentication mechanism.

Once the session has reached the Up state, the session can use a less computationally intensive Auth Type. Currently, this includes:

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

5. Periodic Strong Reauthentication

When using the less computationally intensive authentication mechanism, BFD should periodically test the session using the strong authentication mechanism. Strong authentication is tested using a Poll sequence. To test strong authentication, a Poll sequence SHOULD be initiated by the sender using the strong authentication mode rather than the less computationally intensive mechanism. If a control packet with the Final (F) bit is not received within the Detect Interval, the session has been compromised, and MUST be brought down.

This "strong reauthentication interval" for performing such periodic tests using the strong authentication mechanism can be configured depending on the capability of the system.

Most packets transmitted on a BFD session are BFD Up packets. Strongly 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 strong reauthentication interval.

6. Optimized Authentication Modes

The cryptographic authentication mechanisms specified in Section 6.7 of 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 an "optimized" authentication mode that permits both a strong authentication mode and a less computationally intensive mode to be used within the same BFD session. This pairing of a strong and an less computationally intensive mode of authentication is carried in new BFD authentication types representing a given optimized authentication type pairing.

This document defines in Section 3.1 which BFD control packets are required to be strongly authenticated. A BFD control packet that fails authentication is discarded, or a BFD control packet that was supposed to be strongly 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.

In this specification, the contents of an Up packet MUST NOT change aside from the Authentication Section without strong authentication. The full procedure is documented in the following sections.

7. Signaling Optimized Authentication

When the Authentication Present (A) bit is set and the Auth Type is a type supporting Optimized BFD Authentication, the Auth Type signals a pairing of a strong authentication type and a less computationally intensive authentication type. This pairing is advertised in a single Auth Type value in order to permit implementations to be aware that:

* Optimized BFD procedures will be in use.

* The pairing of the strong and less computationally intensive authentication mechanisms will be used for that session.

* The requirement to carry a Sequence Number.

* The current strong or less computationally intensive mode will be carried as described below:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Auth Type   |   Auth Len    | Auth Key ID  |   Opt. Mode   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Authentication Specific Data                ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Common BFD Authentication Section

The Meticulous Keyed MD5 (Section 6.7.3 of [RFC5880]), Meticulous Keyed SHA-1 (Section 6.7.4 of [RFC5880]), and Meticulous Keyed ISAAC Authentication (Section 5 of [I-D.ietf-bfd-secure-sequence-numbers]) Sections define the fourth octet as "Reserved". This document repurposes the "Reserved" field as the "Optimized Authentication Mode" field when used for authentication types for optimized BFD procedures.

The values of the Optimized Authentication Mode field are:

1. When using the strong authentication type for optimized BFD Auth Types.

2. When using the less computationally intensive authentication type for optimized BFD Auth Types.

Authentication Specific Data: When using the strong authentication type, the remainder of the Authentication Section carries that type’s data.

For example, for Auth Type "Optimized MD5 Meticulous Keyed ISAAC Authentication" (type TBD):

When Optimized Authentication Mode is 1, the format of the authentication section is the same as Section 4.3 of [RFC5880], excepting that Auth Type is still TBD and that Reserved is set to 1.

When Optimized Authentication Mode is 2, the format of the authentication section is the same as Section 5 of [I-D.ietf-bfd-secure-sequence-numbers], excepting that Auth Type is still TBD and that Reserved is set to 2.

7.1. Transmitting and Receiving Using Optimized Authentication

The procedures for authenticating BFD Control packets using Optimized Authentication is similar to the existing procedures covered in Section 6.7 of [RFC5880]. Optimized Authentication modes have common procedural requirements for authentication regardless of which strong and less computationally intensive authentication modes are used.

The required value of the Auth Len field for a given Optimized Authentication mode is defined in the respective specifications for the strong mode and less computationally intensive mode.

The following common procedures apply to authenticating BFD Control packets utilizing Optimized Authentication:

If the received BFD Control packet does not contain an Authentication Section ([RFC5880], Section 4.1), or the Auth Type is not a supported Optimized Authentication Auth Type, then the received packet MUST be discarded.

If the received BFD Control packet contains an optimized authentication type using these procedures and the Optimized Authentication Mode field is not 1 or 2, then the received packet MUST be discarded.

If bfd.SessionState is AdminDown, Down, or Init and the Optimized Authentication Mode field is not 1, then the received packet MUST be discarded.

If bfd.SessionState is Up and there is a significant change as defined Section 3.1, and the Optimized Authentication Mode field is not 1, then the received packet MUST be discarded.

If the Auth Len field is not equal to a value appropriate for the Optimized Authentication Mode field, the packet MUST be discarded.

If bfd.AuthSeqKnown is 1, examine the Sequence Number field. If the sequence number lies outside of the range of bfd.RcvAuthSeq+1 to bfd.RcvAuthSeq+(3*Detect Mult) inclusive (when treated as an unsigned 32-bit circular number space) the received packet MUST be discarded.

Otherwise (bfd.AuthSeqKnown is 0), bfd.AuthSeqKnown MUST be set to 1, bfd.RcvAuthSeq MUST be set to the value of the received Sequence Number field, and the received packet MUST be accepted.

For the specified Auth Type and Optimized Authentication Mode, perform the appropriate authentication procedures. If authentication succeeds, the received packet MUST be accepted. Otherwise, the received packet MUST be discarded.

7.2. Optimized Authentication Operations

As noted in Section 3.1, when using optimized BFD procedures, strong authentication is used in the BFD state machine to bring a BFD session to the Up state or to make any change of the BFD parameters as carried in the BFD Control packet when in the Up state.

Once the BFD session has reached the Up state, the BFD Up state MUST be signaled to the remote BFD system using the strong authentication mode for an interval that is at least the Detection Time before switching to the less computationally intensive authentication mode. This is to permit mechanisms such as Meticulous Keyed ISAAC for BFD Authentication [I-D.ietf-bfd-secure-sequence-numbers] to be bootstrapped before switching to the less computationally intensive mode.

It is RECOMMENDED that when using optimized authentication that implementations switch from strong authentication to the less computationally intensive authentication mode after an interval that is at least the Detection Time. In the circumstances where a BFD session successfully reaches the Up state with strong authentication, but there are problems with the optimized authentication, this will permit the remote system to tear down the session as quickly as possible.

BFD sessions using optimized authentication that succeed in reaching the Up state using strong authentication and fail using the optimized authentication SHOULD bring the issue to the attention of the operator. Further, implementations MAY wish to throttle session restarts.

It is further RECOMMENDED that BFD implementations using optimized authentication defer notifying their client that the session has reached the Up state until it has transitioned to using the optimized authentication mode. In the event where optimized authentication is failing in the protocol, this avoids propagating the failed transitions to the optimized mode to their clients.

8. Optimizing Authentication YANG Model

8.1. 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 Meticulous Keyed ISAAC for BFD Authentication [I-D.ietf-bfd-secure-sequence-numbers]. It adds a feature statement to enable optimized authentication. Finally, it adds an interval value that specifies how often the BFD session should be re-authenticated once it is in the Up state.

8.2. 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 reauth-interval?   uint32
  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 reauth-interval?   uint32
  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 reauth-interval?   uint32
  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 reauth-interval?   uint32
```

8.3. 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].

Implementations supporting the optimization procedures defined in this document enable optimization by using one of the newly defined key-chain crypto-algorithms defined in this YANG module.

```
<CODE BEGINS> file "ietf-bfd-opt-auth@2025-08-05.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 (BFD).";
  }

  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 (ashesh@aalyria.com)
                 Ankur Saxena (ankurpsaxena@gmail.com)
                 Manav Bhatia (mnvbhatia@google.com)
                 Jeffrey Haas (jhaas@juniper.net).";


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

        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 "2025-08-05" {
       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 optimized-md5-meticulous-keyed-isaac {
       base key-chain:crypto-algorithm;
       description
         "BFD Optimized Authentication using Meticulous Keyed MD5 as the
          strong authentication and Meticulous Keyed ISAAC Keyed as the
          less computationally intensive authentication.";
       reference
         "RFC XXXX: Meticulous Keyed ISAAC for BFD Authentication.";
     }

     identity optimized-sha1-meticulous-keyed-isaac {
       base key-chain:crypto-algorithm;
       description
         "BFD Optimized Authentication using Meticulous Keyed SHA-1 as
         the strong authentication and Meticulous Keyed ISAAC Keyed as
         the less computationally intensive authentication.";
       reference
         "RFC XXXX: Meticulous Keyed ISAAC for BFD Authentication.";
     }

     grouping bfd-opt-auth-config {
       description
         "Grouping for BFD Optimized Authentication Parameters.";
       leaf reauth-interval {
         type uint32;
         units "seconds";
         default "60";
         description
           "Interval of time after which strong authentication
            should be utilized to prevent an on-path-attacker attack.
            Default is 1 minute.

            A value of zero means that we do not do periodic
            reauthentication using the strong authentication method.
```

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

     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" {
       uses bfd-opt-auth-config;

       description
         "Augment the 'authentication' container for single hop 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" {
       uses bfd-opt-auth-config;

       description
         "Augment the 'authentication' container for multi-hop 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" {
       uses bfd-opt-auth-config;

       description
         "Augment the 'authentication' container for BFD over LAG
          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" {
       uses bfd-opt-auth-config;
```

```
       description
         "Augment the 'authentication' container for BFD over MPLS
          module to add attributes related to BFD optimized
          authentication.";
     }
   }
   <CODE ENDS>
```

9. IANA Considerations

This documents requests the assignment of one URI and one YANG model.

9.1. 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.

9.2. 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
```

10. Security Considerations

10.1. Protocol Security Considerations

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 strongly authenticated. By strongly 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 strongly 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 Meticulous Keyed ISAAC for BFD Authentication [I-D.ietf-bfd-secure-sequence-numbers] further enhances the security of BFD sessions.

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.

The procedures described in this document provide a mechanism which could enable implementations to leverage stronger security to address the concerns above when strong authentication is required. However, this requires operators to evaluate the tradeoffs of the less computationally intensive mechanisms adequately address their desired security stance.

10.2. 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]. 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.

* '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, the utility of these optimization procedures is lessened. If this interval is set very high, attacks detected by the strong authentication mechanisms may happen overly late.

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.

11. Contributors

The authors of this document would like to acknowledge Reshad Rahman as a contributor to this document.

12. Acknowledgments

The authors would like to thank Qiufang Ma and Stephen Farrell for providing directorate review of this document.

13. References

13.1. Normative 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-22, 6 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-bfd-secure-sequence-numbers-22>.

[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>.

[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>.

[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>.

13.2. 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>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[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>.

[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>.

[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. Examples

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

A.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:opti\
mized-sha1-meticulous-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>
                    <key-chain>bfd-auth-config</key-chain>
                    <opt-auth:reauth-interval>30</opt-auth:reauth-inter\
   val>
                  </authentication>
                </session>
              </sessions>
            </ip-sh>
          </bfd>
        </control-plane-protocol>
      </control-plane-protocols>
    </routing>
```


Appendix B. Experimental Status

This document describes an experiment that presents a candidate solution to update BFD Authentication that is currently specified in [RFC5880]. This experiment is intended to provide additional insights into what happens when the optimized authentication method defined in this document is used. Here are the reasons why this document is on the Experimental track:

* In the initial stages of the document, there were significant participation and reviews from the working group. Since then, there has been considerable changes to the document, e.g. the use of ISAAC, allowing for ISAAC bootstrapping when a BFD session comes up and use of a single Auth Type to indicate use of optimized authentication etc. These changes did not get significant review from the working group and therefore does not meet the bar set in Section 4.1.1 of [RFC2026]

* There are no known implementations (even proof-of-concept) or implementation plans. As a result, we do not currently know if there will be interop issues with legacy implementations or what exactly are the performance benefits of the optimization method.

* The work in this document could become very valuable in the future, especially if the need for deploying BFD authentication at scale becomes a reality.

This document is classified as Experimental and is not part of the IETF Standards Track. Implementations based on this document should not be considered as compliant with BFD [RFC5880].

Authors' Addresses

Mahesh Jethanandani
Arrcus
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

Jeffrey Haas
Juniper Networks
Email: jhaas@pfrc.org