

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 23, 2017

M. Jethanandani  
S. Agarwal  
Cisco Systems, Inc  
A. Mishra  
03b Networks  
A. Saxena  
Ciena Corporation  
A. Dekok  
Network RADIUS SARL  
May 22, 2017

**Secure BFD Sequence Numbers**  
**draft-ietf-bfd-secure-sequence-numbers-00**

Abstract

This document describes a security enhancements for the BFD packet's sequence number.

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 [RFC 2119](#) [[RFC2119](#)].

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 <http://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 November 23, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Theory of operations . . . . .	<a href="#">2</a>
<a href="#">3.</a>	Impact of using a hash . . . . .	<a href="#">4</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">6.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">7.</a>	References . . . . .	<a href="#">4</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">4</a>
	Authors' Addresses . . . . .	<a href="#">5</a>

## [1.](#) Introduction

BFD [\[RFC5880\]](#) [section 6.7](#) describes the use of monotonically incrementing 32-bit sequence numbers for use in authentication of BFD packets. While this method protects against simple replay attacks, the monotonically incrementing sequence numbers are predictable and vulnerable to more complex attack vectors. This document proposes the use of non-monotonically-incrementing sequence numbers in BFD authentication TLVs to enhance the security of BFD sessions. Specifically, the document presents a method to generate pseudo-random sequence numbers on the frame by algorithmically hashing monotonically increasing sequence numbers. Further security may be introduced by resetting un-encrypted sequence to a random value when the 32-bit sequence number rolls-over.

## [2.](#) Theory of operations

Instead of monotonically increasing the sequence number or even occasionally monotonically increasing the sequence number, the next sequence number is generated by computing a hash on what would have been the next sequence number using a shared key. That computed hash is then inserted into the sequence number field of the packet. In case of BFD Authentication [\[I-D.ietf-bfd-optimizing-authentication\]](#), the sequence number used in computing an authenticated packet would be this new computed hash. Even though the BFD Authentication



[I-D.ietf-bfd-optimizing-authentication] sequence number is independent of this enhancement, it would benefit by using the computed hash.

A normal BFD packet with authentication will undergo the following steps, where:

[O]: original [RFC 5880](#) packet with monotonically increasing sequence number

[S]: psuedo random sequence number

[A]: Authentication

Sender	Receiver
[O] [S] [A] -----	[A] [S] [O]

In order to encode a sequence number, the sender would identify a hash algorithm (symmetric) that would create a 32 bit hash. The hashing key is provisioned securely on the sender and receiver of the BFD session. The mechanism of provisioning such a key is outside the scope of this draft. Instead of using the sequence number, the sender encodes the sequence number with the hashing key to produce a hash. Upon receiving the BFD Control packet, the receiver decodes the hash with the provisioned hashing key by performing a reverse hash. Note: The first sequence number can be obtained using the same logic as the My Discriminator value.

k: hashing key

s: sequence number

O: original [RFC 5880](#) packet with monotonically increasing sequence number

R: remainder of packet

H1: hash of s

H2: hash of entire packet

A: H2 + insertion in packet

$\text{hash}(s, k) = H1$

$\text{hash}((H1 + R), k) = H2$



hash'((Packet - H2), k) == H2 ? Good packet : bad packet

hash'(H1, k) == s ? Good sequence number : bad sequence number

Sender

Receiver

[0] [H1] [A] ----- [A] [H1] [0]

### **3. Impact of using a hash**

Under this proposal, every packet's sequence number is encoded within a hash. Therefore there is some impact on the system and its performance while encoding/decoding the hash. As security measures go, this enhancement greatly increases the security of the packet with or without authentication of the entire packet.

### **4. IANA Considerations**

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

### **5. Security Considerations**

### **6. Acknowledgements**

### **7. References**

#### **7.1. 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, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", [RFC 5880](#), DOI 10.17487/RFC5880, June 2010, <<http://www.rfc-editor.org/info/rfc5880>>.

#### **7.2. Informative References**

[I-D.ietf-bfd-optimizing-authentication]  
Jethanandani, M., Mishra, A., Saxena, A., and M. Bhatia, "Optimizing BFD Authentication", [draft-ietf-bfd-optimizing-authentication-02](#) (work in progress), January 2017.



## Authors' Addresses

Mahesh Jethanandani  
Cisco Systems, Inc  
170 West Tasman Drive  
San Jose, CA 95070  
USA

Email: [mjethanandani@gmail.com](mailto:mjethanandani@gmail.com)

Sonal Agarwal  
Cisco Systems, Inc  
170 W. Tasman Drive  
San Jose, CA 95070  
USA

Email: [agarwaso@cisco.com](mailto:agarwaso@cisco.com)  
URI: [www.cisco.com](http://www.cisco.com)

Ashesh Mishra  
03b Networks

Email: [mishra.ashesh@gmail.com](mailto:mishra.ashesh@gmail.com)

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

Email: [ankurpsaxena@gmail.com](mailto:ankurpsaxena@gmail.com)

Alan DeKok  
Network RADIUS SARL  
100 CentrepoinTE Drive #200  
Ottawa, ON K2G 6B1  
Canada

Email: [aland@networkradius.com](mailto:aland@networkradius.com)

