Internet Engineering Task Force (IETF)
Request for Comments: 7885
Updates: 5885
Category: Standards Track
ISSN: 2070-1721

V. Govindan
C. Pignataro
Cisco

July 2016

Seamless Bidirectional Forwarding Detection (S-BFD) for Virtual Circuit Connectivity Verification (VCCV)

Abstract

This document defines Seamless BFD (S-BFD) for VCCV by extending the procedures and Connectivity Verification (CV) types already defined for Bidirectional Forwarding Detection (BFD) for Virtual Circuit Connectivity Verification (VCCV).

This document updates RFC 5885 by extending the CV Type values and the capability selection.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7885.

Table of Contents

1. Background

Bidirectional Forwarding Detection (BFD) for Virtual Circuit Connectivity Verification (VCCV) [RFC5885] defines the CV Types for BFD using VCCV, protocol operation, and the required packet encapsulation formats. This document extends those procedures and CV Type values to enable Seamless BFD (S-BFD) [RFC7880] operation for VCCV.

The new S-BFD CV Types are Pseudowire (PW) demultiplexer agnostic and hence are applicable for both MPLS and Layer Two Tunneling Protocol version 3 (L2TPv3) PW demultiplexers. This document concerns itself with the S-BFD VCCV operation over Single-Segment PWs (SS-PWs). The scope of this document is as follows:

- This specification describes procedures for S-BFD asynchronous mode only.
- S-BFD Echo mode is outside the scope of this specification.
- S-BFD operation for fault detection and status signaling is outside the scope of this specification.

This document specifies the use of a single S-BFD Discriminator per PW. There are cases where multiple S-BFD Discriminators per PW can be useful. One such case involves using different S-BFD Discriminators per Flow within a Flow-Aware Transport (FAT) PW [RFC6391]; however, the mapping between Flows and discriminators is a prerequisite. FAT PWs can be supported as described in Section 7 of [RFC6391], which details Operations, Administration, and Maintenance (OAM) considerations for FAT PWs.

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 [RFC2119].

2. S-BFD Connectivity Verification

The S-BFD protocol provides continuity check services by monitoring the S-BFD Control packets sent and received over the VCCV channel of the PW. The term "Connectivity Verification" (CV) is used throughout this document to be consistent with [RFC5885].

This section defines the CV Types to be used for S-BFD. It also defines the procedures for the S-BFD reflector and S-BFD initiator operation.

Two CV Types are defined for S-BFD. Table 1 summarizes the S-BFD CV Types, grouping them by encapsulation (i.e., with IP/UDP headers, without IP/UDP headers) for fault detection only. S-BFD for fault detection and status signaling is outside the scope of this specification.

	Fault Detection Only	Fault Detection and Status Signaling
S-BFD IP/UDP encapsulation (with IP/UDP headers)	0x40	N/A
S-BFD PW-ACH encapsulation when using MPLS PW or S-BFD L2-Specific Sublayer (L2SS) encapsulation when using L2TP PW (without IP/UDP headers)	0x80	N/A

Table 1: Bitmask Values for S-BFD CV Types

IANA has assigned two new bits to indicate S-BFD operation.

2.1. Co-existence of S-BFD and BFD Capabilities

Since the CV Types for S-BFD and BFD are unique, BFD and S-BFD capabilities can be advertised concurrently.

2.2. S-BFD CV Operation

2.2.1. S-BFD Initiator Operation

The S-BFD initiator SHOULD bootstrap S-BFD sessions after it learns the discriminator of the remote target identifier. This can be achieved, for example, through one or more of the following methods. (This list is not exhaustive.)

1. Advertisements of S-BFD Discriminators made through a PW signaling protocol -- for example, AVPs/TLVs defined in L2TP/LDP.

2. Provisioning of S-BFD Discriminators by manual configuration of the Provider Edge (PE) or L2TP Control Connection Endpoints (LCCEs).

3. Assignment of S-BFD Discriminators by a controller.

4. Probing remote S-BFD Discriminators through a mechanism such as S-BFD Alert Discriminators [SBFD-ALERT-DISCRIM].

The S-BFD initiator operation MUST be done as specified in Section 7.3 of [RFC7880].

2.2.2. S-BFD Reflector Operation

When a PW signaling protocol such as LDP or L2TPv3 is in use, the S-BFD reflector can advertise its target discriminators using that signaling protocol. When static PWs are in use, the target discriminator of S-BFD needs to be provisioned on the S-BFD initiator nodes.

All point-to-point PWs are bidirectional; the S-BFD reflector therefore reflects the S-BFD packet back to the initiator using the VCCV channel of the reverse direction of the PW on which it was received.

The reflector has enough information to reflect the S-BFD Async packet received by it back to the S-BFD initiator using the PW context (e.g., fields of the L2TPv3 headers).

The S-BFD reflector operation for BFD protocol fields MUST be performed as specified in [RFC7880].

2.2.2.1. Demultiplexing

Demultiplexing of S-BFD is achieved using the PW context, following the procedures in Section 7.1 of [RFC7880].

2.2.2.2. Transmission of Control Packets

S-BFD reflector procedures as described in [RFC7880] apply for S-BFD using VCCV.

2.2.2.3. Advertisement of Target Discriminators Using LDP

The advertisement of the target discriminator using LDP is left for further study. It should be noted that S-BFD can still be used with signaled PWs over an MPLS Packet Switched Network (PSN) by provisioning the S-BFD Discriminators or by learning the S-BFD Discriminators via some other means.

2.2.2.4. Advertisement of Target Discriminators Using L2TP

The S-BFD reflector MUST use the AVP defined in [RFC7886] for advertising its target discriminators using L2TP.

2.2.2.5. Provisioning of Target Discriminators

S-BFD target discriminators MAY be provisioned when static PWs are used.

2.3. S-BFD Encapsulation

Unless specified differently below, the encapsulation of S-BFD packets is identical to the method specified in Section 3.2 of [RFC5885] and in [RFC5880] for the encapsulation of BFD packets.

- IP/UDP BFD encapsulation (BFD with IP/UDP headers):
  - The destination UDP port for the IP-encapsulated S-BFD packet MUST be 7784 [RFC7881].
  - The contents of the S-BFD Control packets MUST be set according to Section 7.3.2 of [RFC7880].
  - The Time to Live (TTL) (IPv4) or Hop Limit (IPv6) is set to 255.
- PW-ACH/L2SS BFD encapsulation (BFD without IP/UDP headers):
  - The encapsulation of S-BFD packets using this format MUST be performed according to Section 3.2 of [RFC5885], with the exception of the value for the PW-ACH/L2SS type.
  - When VCCV carries PW-ACH/L2SS-encapsulated S-BFD (i.e., "raw" S-BFD), the Channel Type of PW-ACH (the PW Control Word (CW)) or L2SS MUST be set to 0x0008 to indicate "S-BFD Control, PW-ACH/L2SS-encapsulated" (i.e., S-BFD without IP/UDP headers; see Section 5.3). This is done to allow the identification of the encapsulated S-BFD payload when demultiplexing the VCCV control channel.

3. Capability Selection

When multiple S-BFD CV Types are advertised, and after applying the rules in [RFC5885], the set that both ends of the PW have in common is determined. If the two ends have more than one S-BFD CV Type in common, the following list of S-BFD CV Types is considered in order, from the lowest list number CV Type to the highest list number CV Type, and the CV Type with the lowest list number is used:

1. 0x40 - S-BFD IP/UDP-encapsulated, for PW Fault Detection only.

2. 0x80 - S-BFD PW-ACH/L2SS-encapsulated (without IP/UDP headers), for PW Fault Detection only.

The order of capability selection between S-BFD and BFD is defined as follows:

Advertised capabilities of PE1/PE2	BFD Only	S-BFD Only	Both S-BFD and BFD
BFD Only	BFD	None	BFD Only
S-BFD Only	None	S-BFD	S-BFD Only
Both S-BFD and BFD	BFD Only	S-BFD Only	Both S-BFD and BFD

Table 2: Capability Selection Matrix for BFD and S-BFD

4. Security Considerations

Security considerations for VCCV are addressed in Section 10 of [RFC5085]. The introduction of the S-BFD CV Types does not present any new security risks for VCCV. Implementations of the additional CV Types defined herein are subject to the same security considerations as those defined in [RFC5085] as well as [RFC7880].

The IP/UDP encapsulation of S-BFD makes use of the TTL / Hop Limit procedures described in the Generalized TTL Security Mechanism (GTSM) specification [RFC5082] as a security mechanism.

This specification does not raise any additional security issues beyond these.

5. IANA Considerations

5.1. MPLS CV Types for the VCCV Interface Parameters Sub-TLV

The VCCV Interface Parameters Sub-TLV codepoint is defined in [RFC4446], and the "MPLS VCCV Connectivity Verification (CV) Types" registry is defined in [RFC5085].

This section lists the new S-BFD CV Types.

IANA has augmented the "MPLS VCCV Connectivity Verification (CV) Types" registry in the "Pseudowire Name Spaces (PWE3)" registry [IANA-PWE3]. These are bitfield values. CV Type values are specified in Section 2 of this document.

MPLS VCCV Connectivity Verification (CV) Types:

Bit (Value)	Description	Reference
6 (0x40)	S-BFD IP/UDP-encapsulated, for PW Fault Detection only	RFC 7885
7 (0x80)	S-BFD PW-ACH-encapsulated, for PW Fault Detection only	RFC 7885

5.2. L2TPv3 CV Types for the VCCV Capability AVP

This section lists the new S-BFD "L2TPv3 Connectivity Verification (CV) Types" that have been added to the existing "VCCV Capability AVP (Attribute Type 96) Values" registry in the "Layer Two Tunneling Protocol 'L2TP'" registry [IANA-L2TP]. IANA has assigned the following L2TPv3 Connectivity Verification (CV) Types in the "VCCV Capability AVP (Attribute Type 96) Values" registry.

VCCV Capability AVP (Attribute Type 96) Values

L2TPv3 Connectivity Verification (CV) Types:

Bit (Value)	Description	Reference
6 (0x40)	S-BFD IP/UDP-encapsulated, for PW Fault Detection only	RFC 7885
7 (0x80)	S-BFD L2SS-encapsulated, for PW Fault Detection only	RFC 7885

5.3. PW Associated Channel Type

As per the IANA considerations in [RFC5586], IANA has allocated a Channel Type in the "MPLS Generalized Associated Channel (G-ACh) Types (including Pseudowire Associated Channel Types)" registry [IANA-G-ACh].

IANA has assigned a new Pseudowire Associated Channel Type value, as follows:

Value	Description	Reference
0x0008	S-BFD Control, PW-ACH/L2SS encapsulation (without IP/UDP Headers)	RFC 7885

6. References

6.1. 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>.

[RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, DOI 10.17487/RFC4446, April 2006, <http://www.rfc-editor.org/info/rfc4446>.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <http://www.rfc-editor.org/info/rfc5082>.

[RFC5085] Nadeau, T., Ed., and C. Pignataro, Ed., "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, DOI 10.17487/RFC5085, December 2007, <http://www.rfc-editor.org/info/rfc5085>.

[RFC5586] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, DOI 10.17487/RFC5586, June 2009, <http://www.rfc-editor.org/info/rfc5586>.

[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>.

[RFC5885] Nadeau, T., Ed., and C. Pignataro, Ed., "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", RFC 5885, DOI 10.17487/RFC5885, June 2010, <http://www.rfc-editor.org/info/rfc5885>.

[RFC7880] Pignataro, C., Ward, D., Akiya, N., Bhatia, M., and S. Pallagatti, "Seamless Bidirectional Forwarding Detection (S-BFD)", RFC 7880, DOI 10.17487/RFC7880, July 2016, <http://www.rfc-editor.org/info/rfc7880>.

[RFC7881] Pignataro, C., Ward, D., and N. Akiya, "Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS", RFC 7881, DOI 10.17487/RFC7881, July 2016, <http://www.rfc-editor.org/info/rfc7881>.

[RFC7886] Govindan, V. and C. Pignataro, "Advertising Seamless Bidirectional Forwarding Detection (S-BFD) Discriminators in the Layer Two Tunneling Protocol Version 3 (L2TPv3)", RFC 7886, DOI 10.17487/RFC7886, July 2016, <http://www.rfc-editor.org/info/rfc7886>.

6.2. Informative References

[IANA-G-ACh]
Internet Assigned Numbers Authority, "MPLS Generalized Associated Channel (G-ACh) Types (including Pseudowire Associated Channel Types)", <http://www.iana.org/assignments/g-ach-parameters>.

[IANA-L2TP]
Internet Assigned Numbers Authority, "Layer Two Tunneling Protocol 'L2TP'", <http://www.iana.org/assignments/l2tp-parameters>.

[IANA-PWE3]
Internet Assigned Numbers Authority, "Pseudowire Name Spaces (PWE3)", <http://www.iana.org/assignments/pwe3-parameters>.

[RFC6391] Bryant, S., Ed., Filsfils, C., Drafz, U., Kompella, V., Regan, J., and S. Amante, "Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network", RFC 6391, DOI 10.17487/RFC6391, November 2011, <http://www.rfc-editor.org/info/rfc6391>.

[SBFD-ALERT-DISCRIM] Akiya, N., Pignataro, C., and D. Ward, "Seamless Bidirectional Forwarding Detection (S-BFD) Alert Discriminator", Work in Progress, draft-akiya-bfd-seamless-alert-discrim-03, October 2014.

Acknowledgements

The authors would like to thank Nobo Akiya, Stewart Bryant, Greg Mirsky, Pawel Sowinski, Yuanlong Jiang, Andrew Malis, and Alexander Vainshtein for providing input to this document, performing thorough reviews, and providing useful comments.

Contributors

Mallik Mudigonda
Cisco Systems, Inc.

Email: mmudigon@cisco.com

Authors' Addresses

Vengada Prasad Govindan
Cisco Systems, Inc.

Email: venggovi@cisco.com

Carlos Pignataro
Cisco Systems, Inc.

Email: cpignata@cisco.com