Internet Engineering Task Force (IETF)
Request for Comments: 7881
Category: Standards Track
ISSN: 2070-1721

C. Pignataro
D. Ward
Cisco
N. Akiya
Big Switch Networks

July 2016

Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS

Abstract

This document defines procedures for using Seamless Bidirectional Forwarding Detection (S-BFD) in IPv4, IPv6, and MPLS environments.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Seamless Bidirectional Forwarding Detection (S-BFD) [RFC7880] defines a generalized mechanism to allow network nodes to seamlessly perform continuity checks to remote entities. This document defines necessary procedures for using S-BFD in IPv4, IPv6, and MPLS environments.

The reader is expected to be familiar with the IP [RFC791] [RFC2460], BFD [RFC5880], MPLS BFD [RFC5884], and S-BFD [RFC7880] terms and protocol constructs.

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].

2. S-BFD UDP Port

A new UDP port is defined for use by S-BFD in IPv4, IPv6, and MPLS environments: 7784.

In S-BFD Control packets from the SBFDInitiator to the SBFDReflector, the SBFDReflector session MUST listen for incoming S-BFD Control packets on port 7784. SBFDInitiator sessions MUST transmit S-BFD Control packets with destination port 7784. The source port of the S-BFD Control packets transmitted by SBFDInitiator sessions can be any port, with one exception: it MUST NOT be 7784. The same UDP source port number MUST be used for all S-BFD Control packets associated with a particular SBFDInitiator session. The source port number is unique among all SBFDInitiator sessions on the system.

In S-BFD Control packets from the SBFDReflector to the SBFDInitiator, the SBFDInitiator session MUST listen for reflected S-BFD Control packets at its source port.

3. S-BFD Echo UDP Port

The BFD Echo port defined by [RFC5881], port 3785, is used for the S-BFD Echo function in IPv4, IPv6, and MPLS environments. SBFDInitiator sessions MUST transmit S-BFD Echo packets with destination port 3785. The setting of the UDP source port [RFC5881] and the procedures [RFC7880] for the S-BFD Echo function are outside the scope of this document.

4. S-BFD Control Packet Demultiplexing

S-BFD Control packet demultiplexing follows the procedure specified in Section 7.1 of [RFC7880]. A received S-BFD Control packet MUST be demultiplexed with the destination UDP port field.

This procedure for an S-BFD packet is executed on both the initiator and the reflector. If the port is 7784 (i.e., an S-BFD packet for the SBFDReflector), then the packet MUST be looked up to locate a corresponding SBFDReflector session based on the value from the Your Discriminator field in the table describing S-BFD Discriminators. If the port is not 7784 but the packet is demultiplexed to be for an SBFDInitiator, then the packet MUST be looked up to locate a corresponding SBFDInitiator session based on the value from the Your Discriminator field in the table describing BFD Discriminators. In that case, the destination IP address of the packet SHOULD be validated to be for itself. If the packet demultiplexes to a classical BFD session, then the procedures from [RFC5880] apply.

5. Initiator Procedures

S-BFD Control packets are transmitted with an IP header, UDP header, and BFD Control packet ([RFC5880]). When S-BFD Control packets are explicitly label switched (i.e., not IP routed and forwarded over a Label Switched Path (LSP), but explicitly sent on a specific LSP), the former is prepended with a label stack. Note that this document does not make a distinction between a single-hop S-BFD scenario and a multi-hop S-BFD scenario; both scenarios are supported.

The necessary values in the BFD control headers are described in [RFC7880]. Section 5.1 describes necessary values in the MPLS header, IP header, and UDP header when an SBFDInitiator on the initiator is sending S-BFD Control packets.

5.1. Details of S-BFD Control Packets Sent by SBFDInitiator

- Specifications common to both IP-routed S-BFD Control packets and explicitly label-switched S-BFD Control packets:
  - The Source IP Address field of the IP header MUST be set to a local IP address that is expected to be routable by the target (i.e., not an IPv6 link-local address when the target is multiple hops away).
  - The UDP destination port MUST be set to a well-known UDP destination port assigned for S-BFD, i.e., 7784.
  - The UDP source port MUST NOT be set to 7784.
- Specifications for IP-routed S-BFD Control packets:
  - The Destination IP Address field of the IP header MUST be set to an IP address of the target.
  - The TTL / Hop Limit field of the IP header SHOULD be set to 255.
- Specifications for explicitly label-switched S-BFD Control packets:
  - S-BFD Control packets MUST have the label stack that is expected to reach the target.
  - The TTL field of the topmost label SHOULD be 255.
  - The destination IP address MUST be chosen from the 127/8 range for IPv4 and from the 0:0:0:0:0:ffff:7f00:0/104 range for IPv6, as per [RFC5884].
  - The TTL / Hop Limit field of the IP header MUST be set to 1.

5.1.1. Target versus Remote Entity (S-BFD Discriminator)

Typically, an S-BFD Control packet will have the Your Discriminator field corresponding to an S-BFD Discriminator of the remote entity located on the target network node defined by the destination IP address or the label stack. It is, however, possible for an

SBFDInitiator to carefully set the Your Discriminator and TTL fields to perform a continuity test in the direction towards a target, but destined to a transit network node and not to the target itself.

Section 5.1 intentionally uses the word "target" instead of "remote entity" to accommodate this possible S-BFD usage through TTL expiry. This also requires that S-BFD Control packets not be dropped by the responder node due to TTL expiry. Thus, implementations on the responder MUST allow received S-BFD Control packets taking a TTL expiry exception path to reach the corresponding SBFDReflector session. This is an existing packet-processing exception practice for Operations, Administration, and Maintenance (OAM) packets, where the control plane further identifies the type of OAM by the protocol and port numbers.

6. Responder Procedures

S-BFD Control packets are IP routed back to the initiator and will have an IP header, UDP header, and BFD control header. If an SBFDReflector receives an S-BFD Control packet with a UDP source port of 7784, the packet MUST be discarded. Necessary values in the BFD control header are described in [RFC7880]. Section 6.1 describes necessary values in the IP header and UDP header when an SBFDReflector on the responder is sending S-BFD Control packets.

6.1. Details of S-BFD Control Packets Sent by SBFDReflector

- The Destination IP Address field of the IP header MUST be copied from the Source IP Address field of the received S-BFD Control packet.

- The Source IP Address field of the IP header MUST be set to a local IP address that the initiator expects to be visible (i.e., not an IPv6 link-local address when the initiator is multiple hops away). The source IP address SHOULD be copied from the Destination IP Address field of the received S-BFD Control packet, except when it is from the 127/8 range for IPv4 or from the 0:0:0:0:0:ffff:7f00:0/104 range for IPv6.

- The TTL / Hop Limit field of the IP header MUST be set to 255.

- The UDP destination port MUST be copied from the received UDP source port.

- The UDP source port MUST be copied from the received UDP destination port.

7. Security Considerations

Security considerations for S-BFD are discussed in [RFC7880]. Additionally, implementing the following measures will strengthen security aspects of the mechanism described by this document:

- Implementations MUST provide filtering capability based on source IP addresses of received S-BFD Control packets; see [RFC2827].

- Implementations MUST NOT act on received S-BFD Control packets containing source Martian IP addresses (i.e., addresses that, by application of the current forwarding tables, would not have their return traffic routed back to the sender).

- Implementations MUST ensure that response S-BFD Control packets generated by the SBFDReflector and sent to the initiator have a reachable target (e.g., destination IP address).

8. IANA Considerations

A new port number value, 7784, was allocated from the "Service Name and Transport Protocol Port Number Registry". The allocated registry entry is:

Service Name (REQUIRED)
s-bfd

Transport Protocol(s) (REQUIRED)
udp

Assignee (REQUIRED)
IESG <iesg@ietf.org>

Contact (REQUIRED)
IETF Chair <chair@ietf.org>

Description (REQUIRED)
Seamless Bidirectional Forwarding Detection (S-BFD)

Reference (REQUIRED)
RFC 7881

Port Number (OPTIONAL)
7784

9. References

9.1. 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>.

[RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, DOI 10.17487/RFC5881, June 2010, <http://www.rfc-editor.org/info/rfc5881>.

[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>.

9.2. Informative References

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <http://www.rfc-editor.org/info/rfc2827>.

[RFC5884] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)", RFC 5884, DOI 10.17487/RFC5884, June 2010, <http://www.rfc-editor.org/info/rfc5884>.

Acknowledgements

The authors would like to thank the BFD WG members for helping to shape the contents of this document. In particular, significant contributions were made by the following people: Marc Binderberger, Jeffrey Haas, Santosh Pallagatti, Greg Mirsky, Sam Aldrin, Vengada Prasad Govindan, Mallik Mudigonda, and Srihari Raghavan.

Contributors

The following are key contributors to this document:

Tarek Saad, Cisco Systems, Inc.
Siva Sivabalan, Cisco Systems, Inc.
Nagendra Kumar, Cisco Systems, Inc.

Authors' Addresses

Carlos Pignataro
Cisco Systems, Inc.

Email: cpignata@cisco.com

Dave Ward
Cisco Systems, Inc.

Email: wardd@cisco.com

Nobo Akiya
Big Switch Networks

Email: nobo.akiya.dev@gmail.com