Seamless Bidirectional Forwarding Detection (BFD) for IP
draft-akiya-bfd-seamless-ip-01

Abstract

   This specification defines procedures to use Seamless Bidirectional
   Forwarding Detection (S-BFD) in IP and IP signalled MPLS
   environments.

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 June 8, 2014.

Table of Contents

1. Introduction

One application for Seamless Bidirectional Forwarding Detection
(S-BFD) [I-D.akiya-bfd-seamless-base] is to perform full and partial
reachability validations on IP and IP signalled MPLS environments.

This specification defines procedures to use Seamless BFD in IP and
IP signalled MPLS environments.

2. BFD Target Identifier Type

BFD target identifier type of value 1 is used for IPv4 addresses and
router IDs. This identifier type will cover Seamless BFD in
following scenarios:

o BFD control packets IPv4 routed.

o BFD control packets IPv6 routed.

o BFD control packets label switched in IPv4 signaled LSP.

o BFD control packets label switched in IPv6 signaled LSP.

   Not all IPv6 aspects are covered by this specification, and details
   are clarified in [Section 3](#).

3. Reserved BFD Discriminators

   With IPv4 based BFD, BFD target identifier type 1 is used. IPv4
   addresses are used as BFD discriminators. BFD discriminator values
   corresponding to all or subset of local IPv4 addresses are to be
   allocated from the discriminator pool for Seamless BFD.

   Example:

   o BFD Target Identifier Type 1: IPv4 address 3.3.2.1 maps to BFD
      discriminator 0x03030201.

   With IPv6 based BFD, BFD target identifier type 1 is used. Router
   IDs are used as BFD discriminators. BFD discriminator values
   corresponding to all or subset of local router IDs are to be
   allocated from the discriminator pool for Seamless BFD. IDs which
   are larger than 32 bits (ex: ISIS system ID) are not included as part
   of this identifier type, and is outside the scope of this document.

   Example:

   o BFD Target Identifier Type 1: Router-ID 3.3.4.5 maps to BFD
      discriminator 0x03030405.

   Note that it is acceptable for an IPv4 address and a router-ID to
   collide, mapping into a same BFD discriminator value. There will not
   be an issue as long as colliding BFD discriminator value is reserved
   for the Seamless BFD purpose.

4. BFD Target Identifier Table

   With IP identifier type, only locally reserved BFD discriminators and
   corresponding information are to be in this table. No inter-node
   communications are needed to exchange BFD discriminator and BFD
   target identifier mappings.

5. Full Reachability Validations

5.1. Initiator Behavior

   Any IP network node can attempt to perform a full reachability
   validation to any BFD target identifier of type 1 (IPv4 address or
   router-ID) on other network nodes, as long as destination BFD target
   identifier is provisioned to use this mechanism. Transmitted BFD
   control packet by the initiator is to have "your discriminator"
   corresponding to destination IPv4 address or router ID.

   Initiator is to use following procedures to construct BFD control
   packets to perform IP full reachability validations on BFD packets
   that are IP routed:

   o MUST set "your discriminator" to target IPv4 address or target
      router-ID.
   o If packet is to be explicitly label switched, then explicit label
      switching packet format described in [I-D.akiya-bfd-seamless-base]
      MUST be used. Otherwise IP routing packet format described in
      [I-D.akiya-bfd-seamless-base] MUST be used.

5.2. Responder Behavior

   To respond to received BFD control packet which was targeted to local
   BFD target identifier of type 1 (IP address or router-ID), response
   BFD control packet is targeted to IP address taken from received
   "source IP address". Responder MUST validate obtained IP address is
   in valid format (ex: not Martian address). Responder MUST consult
   local routing table to ensure obtained IP address is reachable.

6. Partial Reachability Validations

   Procedures described in [I-D.akiya-bfd-seamless-base] applies.

7. MPLS Label Verifications

   MPLS label verification mechanism is applicable to those IP based BFD
   which use explicit label switching techniques. However, details of
   what responder embeds in the lower 23 bits of localhost address, and
   how initiator determines correctness of label programming is outside
   the scope of this document.

8. Provisioning Active IP Sessions

   Active IP BFD sessions, single-hop, multi-hop or MPLS can be
   instantiated on any network node to any IPv4 target addresses and
   OSPFv3 router IDs using this mechanism. This style of usage is
   particularly useful only if one side is required to perform full
   reachability validations (ex: static route, uni-directional tunnel).

This style of usage is also particularly useful to perform
validations and verifications on just subset of LSPs (ex: inter-AS,
injection of partial BFD reachability validation packet on IPv4 RSVP
LSP nodes).

9. Security Considerations

Security considerations for BFD are discussed in [RFC5880] and
security considerations for S-BFD are discussed in
[I-D.akiya-bfd-seamless-base].

10. IANA Considerations

None

11. Acknowledgements

Authors would like to thank Marc Binderberger from Cisco Systems for
providing valuable comments.

12. Contributing Authors

Tarek Saad
Cisco Systems
Email: tsaad@cisco.com

Siva Sivabalan
Cisco Systems
Email: msiva@cisco.com

Nagendra Kumar
Cisco Systems
Email: naikumar@cisco.com

13. References

13.1. Normative References

[I-D.akiya-bfd-seamless-base]
          Akiya, N., Pignataro, C., Ward, D., Bhatia, M., and J.
          Networks, "Seamless Bidirectional Forwarding Detection
          (BFD) with MPLS Label Verification Extension", draft-
          akiya-bfd-seamless-base-02 (work in progress), October
          2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC5880]   Katz, D. and D. Ward, "Bidirectional Forwarding Detection
               (BFD)", RFC 5880, June 2010.

13.2. Informative References

   [RFC5881]   Katz, D. and D. Ward, "Bidirectional Forwarding Detection
               (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, June
               2010.

   [RFC5883]   Katz, D. and D. Ward, "Bidirectional Forwarding Detection
               (BFD) for Multihop Paths", RFC 5883, June 2010.

   [RFC5884]   Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow,
               "Bidirectional Forwarding Detection (BFD) for MPLS Label
               Switched Paths (LSPs)", RFC 5884, June 2010.

Authors' Addresses

   Nobo Akiya
   Cisco Systems

   Email: nobo@cisco.com

   Carlos Pignataro
   Cisco Systems

   Email: cpignata@cisco.com

   Dave Ward
   Cisco Systems

   Email: wardd@cisco.com