Seamless Bidirectional Forwarding Detection (S-BFD)
draft-ietf-bfd-seamless-base-05

Abstract

   This document defines a simplified mechanism to use Bidirectional
   Forwarding Detection (BFD) with large portions of negotiation aspects
   eliminated, thus providing benefits such as quick provisioning as
   well as improved control and flexibility to network nodes initiating
   the path monitoring.

   This document updates RFC5880.

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].

Copyright Notice

Table of Contents

1. Introduction

   Bidirectional Forwarding Detection (BFD), [RFC5880] and related
   documents, has efficiently generalized the failure detection
   mechanism for multiple protocols and applications. There are some
   improvements which can be made to better fit existing technologies.
   There is a possibility of evolving BFD to better fit new
   technologies. This document focuses on several aspects of BFD in
   order to further improve efficiency, to expand failure detection
   coverage and to allow BFD usage for wider scenarios. This document
   extends BFD to provide solutions to use cases listed in
   [I-D.ietf-bfd-seamless-use-case].

   One key aspect of the mechanism described in this document eliminates
   the time between a network node wanting to perform a continuity test
   and completing the continuity test. In traditional BFD terms, the
   initial state changes from DOWN to UP are virtually nonexistent.
   Removal of this seam (i.e., time delay) in BFD provides applications
   a smooth and continuous operational experience. Therefore, "Seamless
   BFD" (S-BFD) has been chosen as the name for this mechanism.

2. Terminology

   The reader is expected to be familiar with the BFD, IP and MPLS
   terminologies and protocol constructs. This section describes
   several new terminologies introduced by S-BFD.

   o Classical BFD - BFD session types based on [RFC5880].

   o S-BFD - Seamless BFD.

   o S-BFD control packet - a BFD control packet for the S-BFD
      mechanism.

   o S-BFD echo packet - a BFD echo packet for the S-BFD mechanism.

   o S-BFD packet - a BFD control packet or a BFD echo packet.

   o Entity - a function on a network node that S-BFD mechanism allows
      remote network nodes to perform continuity test to. An entity can
      be abstract (e.g., reachability) or specific (e.g., IP addresses,
      router-IDs, functions).

o SBFDInitiator - an S-BFD session on a network node that performs a
   continuity test to a remote entity by sending S-BFD packets.

o SBFDReflector - an S-BFD session on a network node that listens
   for incoming S-BFD control packets to local entities and generates
   response S-BFD control packets.

o Reflector BFD session - synonymous with SBFDReflector.

o S-BFD discriminator - a BFD discriminator allocated for a local
   entity and is being listened by an SBFDReflector.

o BFD discriminator - a BFD discriminator allocated for an
   SBFDInitiator.

o Initiator - a network node hosting an SBFDInitiator.

o Responder - a network node hosting an SBFDReflector.

Below figure describes the relationship between S-BFD terminologies.

```
 +---------------------+                  +------------------------+
 |      Initiator      |                  |       Responder        |
 | +----------------+  |                  |    +----------------+  |
 | |  SBFDInitiator  |---S-BFD ctrl pkt----->|  SBFDReflector  | |
 | | +-------------+ |<--S-BFD ctrl pkt------| +-------------+ | |
 | | | BFD discrim | | |                  |   | |S-BFD discrim| | |
 | | |             | |---S-BFD echo pkt---+  | |             | | |
 | | +-------------+ | |                  | | | +----------^--+ | |
 | +----------------+<------------------+  +-----------|----+ |
 |                   |                  |              |      |
 |                   |                  |          +---v----+ |
 |                   |                  |          | Entity | |
 |                   |                  |          +--------+ |
 +---------------------+                  +------------------------+
```
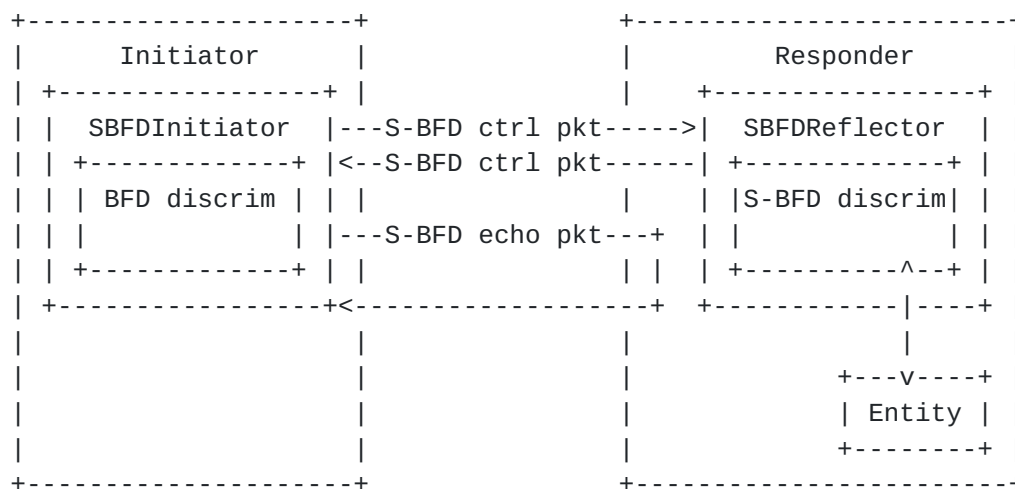
                 Figure 1: S-BFD Terminology Relationship

[3](#). Seamless BFD Overview

An S-BFD module on each network node allocates one or more S-BFD
discriminators for local entities, and creates a reflector BFD
session. Allocated S-BFD discriminators may be advertised by
applications (e.g., OSPF/IS-IS). Required result is that
applications, on other network nodes, possess the knowledge of the
mapping from remote entities to S-BFD discriminators. The reflector
BFD session is to, upon receiving an S-BFD control packet targeted to

one of local S-BFD discriminator values, transmit a response S-BFD
control packet back to the initiator.

Once above setup is complete, any network nodes, having the knowledge
of the mapping from a remote entity to an S-BFD discriminator, can
quickly perform a continuity test to the remote entity by simply
sending S-BFD control packets with corresponding S-BFD discriminator
value in the "your discriminator" field.

For example:

```
   <------- IS-IS Network ------->

            +---------+
            |         |
   A---------B---------C---------D
    ^                        ^
    |                        |
 SystemID                 SystemID
   xxx                       yyy
 BFD Discrim              BFD Discrim
   123                       456
```
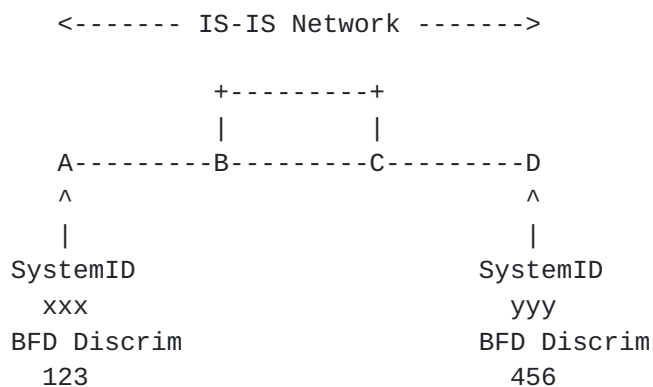
          Figure 2: S-BFD for IS-IS Network

The IS-IS with SystemID xxx (node A) allocates an S-BFD discriminator
123, and advertises the S-BFD discriminator 123 in an IS-IS TLV. The
IS-IS with SystemID yyy (node D) allocates an S-BFD discriminator
456, and advertises the S-BFD discriminator 456 in an IS-IS TLV. A
reflector BFD session is created on both network nodes (node A and
node D). When network node A wants to check the reachability to
network node D, node A can send an S-BFD control packet, destined to
node D, with "your discriminator" field set to 456. When the
reflector BFD session on node D receives this S-BFD control packet,
then response S-BFD control packet is sent back to node A, which
allows node A to complete the continuity test.

4. S-BFD Discriminators

4.1. S-BFD Discriminator Uniqueness

One important characteristics of an S-BFD discriminator is that it
MUST be unique within an administrative domain. If multiple network
nodes allocated a same S-BFD discriminator value, then S-BFD control
packets falsely terminating on a wrong network node can result in a
reflector BFD session to generate a response back, due to "your
discriminator" matching. This is clearly not desirable. If only IP
based S-BFD is considered, then it is possible for the reflector BFD

session to require demultiplexing of incoming S-BFD control packets
with combination of destination IP address and "your discriminator".
Then S-BFD discriminator only has to be unique within a local node.
However, S-BFD is a generic mechanism defined to run on wide range of
environments: IP, MPLS, etc. For other transports like MPLS, because
of the need to use non-routable IP destination address, it is not
possible for reflector BFD session to demultiplex using IP
destination address. With PHP, there may not be any incoming label
stack to aid in demultiplexing either. Thus, S-BFD imposes a
requirement that S-BFD discriminators MUST be unique within an
administrative domain.

4.2. Discriminator Pools

This subsection describes a discriminator pool implementation
technique to minimize S-BFD discriminator collisions. The result
will allow an implementation to better satisfy the S-BFD
discriminator uniqueness requirement defined in Section 4.1.

o SBFDInitiator is to allocate a discriminator from the BFD
   discriminator pool. If the system also supports classical BFD
   that runs on [RFC5880], then the BFD discriminator pool SHOULD be
   shared by SBFDInitiator sessions and classical BFD sessions.

o SBFDReflector is to allocate a discriminator from the S-BFD
   discriminator pool. The S-BFD discriminator pool SHOULD be a
   separate pool than the BFD discriminator pool.

Remainder of this subsection describes the reasons for above
suggestions.

Locally allocated S-BFD discriminator values for entities, listened
by SBFDReflector sessions, may be arbitrary allocated or derived from
values provided by applications. These values may be protocol IDs
(e.g., System-ID, Router-ID) or network targets (e.g., IP address).
To avoid derived S-BFD discriminator values already being assigned to
other BFD sessions (i.e., SBFDInitiator sessions and classical BFD
sessions), it is RECOMMENDED that discriminator pool for
SBFDReflector sessions be separate from other BFD sessions.

Even when following the separate discriminator pool approach,
collision is still possible between one S-BFD application to another
S-BFD application, that may be using different values and algorithms
to derive S-BFD discriminator values. If the two applications are
using S-BFD for a same purpose (e.g., network reachability), then the
colliding S-BFD discriminator value can be shared. If the two
applications are using S-BFD for a different purpose, then the

collision must be addressed. How such collisions are addressed is
outside the scope of this document.

5. Reflector BFD Session

Each network node creates one or more reflector BFD sessions. This
reflector BFD session is a session which transmits S-BFD control
packets in response to received S-BFD control packets with "your
discriminator" having S-BFD discriminators allocated for local
entities. Specifically, this reflector BFD session is to have
following characteristics:

o MUST NOT transmit any S-BFD packets based on local timer expiry.

o MUST transmit an S-BFD control packet in response to a received
   S-BFD control packet having a valid S-BFD discriminator in the
   "your discriminator" field, unless prohibited by local policies
   (e.g., administrative, security, rate-limiter, etc).

o MUST be capable of sending only two states: UP and ADMINDOWN.

One reflector BFD session may be responsible for handling received
S-BFD control packets targeted to all locally allocated S-BFD
discriminators, or few reflector BFD sessions may each be responsible
for subset of locally allocated S-BFD discriminators. This policy is
a local matter, and is outside the scope of this document.

Note that incoming S-BFD control packets may be IPv4, IPv6 or MPLS
based. How such S-BFD control packets reach an appropriate reflector
BFD session is also a local matter, and is outside the scope of this
document.

6. State Variables

S-BFD introduces new state variables, and modifies the usage of
existing ones.

6.1. New State Variables

A new state variable is added to the base specification in support of
S-BFD.

o bfd.SessionType: This is a variable introduced by
   [I-D.ietf-bfd-multipoint] and describes the type of this session.
   Allowable values for S-BFD sessions are:

> * SBFDInitiator - an S-BFD session on a network node that
>   performs a continuity test to a target entity by sending S-BFD
>   packets.
>
> * SBFDReflector - an S-BFD session on a network node that listens
>   for incoming S-BFD control packets to local entities and
>   generates response S-BFD control packets.

bfd.SessionType variable MUST be initialized to the appropriate type
when an S-BFD session is created.

6.2. State Variable Initialization and Maintenance

Some state variables defined in section 6.8.1 of the BFD base
specification need to be initialized or manipulated differently
depending on the session type.

o bfd.DemandMode: This variable MUST be initialized to 1 for session
   type SBFDInitiator, and MUST be initialized to 0 for session type
   SBFDReflector.

7. S-BFD Procedures

7.1. Demultiplexing of S-BFD Control Packet

S-BFD packet MUST be demultiplexed with lower layer information
(e.g., dedicated destination UDP port, associated channel type).
Following procedure SHOULD be executed on both initiator and
reflector.

    If S-BFD packet

        If S-BFD packet is for SBFDReflector

            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.

        Else

            Packet MUST be looked up to locate a corresponding
            SBFDInitiator session or classical BFD session based on the
            value from the "your discriminator" field in the table
            describing BFD discriminators.

            If session is SBFDInitiator

                    Destination of the packet (i.e., destination IP address)
                    SHOULD be validated to be for self.

               Else

                    Packet MUST be discarded

          Else

               Procedure described in [RFC5880] MUST be applied.

   More details on S-BFD control packet demultiplexing are described in
   relevant S-BFD data plane documents.

7.2. Initiator Procedures

   S-BFD control packets transmitted by an SBFDInitiator MUST set "your
   discriminator" field to an S-BFD discriminator corresponding to the
   remote entity.

   Every SBFDInitiator MUST have a locally unique "my discriminator"
   allocated from the BFD discriminator pool.

   Below ASCII art describes high level concept of continuity test using
   S-BFD. R2 allocates XX as the S-BFD discriminator for its network
   reachability purpose, and advertises XX to neighbors. ASCII art
   shows R1 and R4 performing a continuity test to R2.

```
 +--- md=50/yd=XX (ping) ----+
 |                           |
 |+-- md=XX/yd=50 (pong) --+ |
 ||                        | |
 |v                        | v
 R1 =================== R2[*] ======== R3 ======== R4
                         | ^                      |^
                         | |                      ||
                         | +-- md=60/yd=XX (ping) --+|
                         |                        |
                         +---- md=XX/yd=60 (pong) ---+
```

   [*] Reflector BFD session on R2.
   === Links connecting network nodes.
   --- S-BFD control packet traversal.

                 Figure 3: S-BFD Continuity Test

7.2.1. **SBFDInitiator State Machine**

   An SBFDInitiator may be a persistent session on the initiator with a
   timer for S-BFD control packet transmissions (stateful
   SBFDInitiator). An SBFDInitiator may also be a module, a script or a
   tool on the initiator that transmits one or more S-BFD control
   packets "when needed" (stateless SBFDInitiator). For stateless
   SBFDInitiators, a complete BFD state machine may not be applicable.
   For stateful SBFDInitiators, the states and the state machine
   described in [RFC5880] will not function due to SBFDReflector session
   only sending UP and ADMINDOWN states (i.e., SBFDReflector session
   does not send INIT state). The following diagram provides the
   RECOMMENDED state machine for stateful SBFDInitiators. The notation
   on each arc represents the state of the SBFDInitiator (as received in
   the State field in the S-BFD control packet) or indicates the
   expiration of the Detection Timer.

```
                 +--+
     ADMIN DOWN, |  |
     TIMER       |  V
                 +------+   UP                    +------+
                 |      |-------------------->|       |----+
                 | DOWN |                         |  UP  |    | UP
                 |      |<--------------------|       |<---+
                 +------+    ADMIN DOWN,          +------+
                             TIMER
```
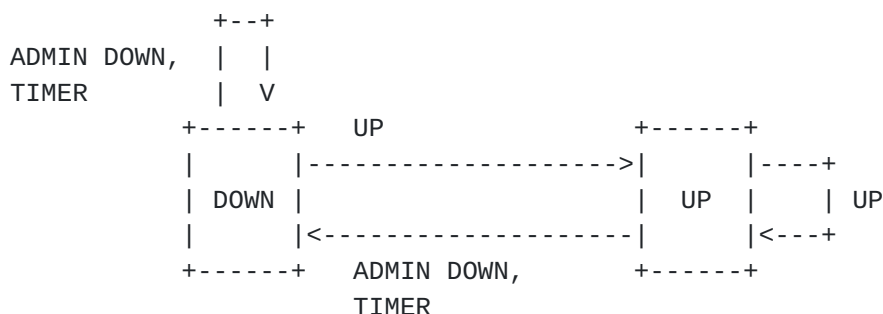
              Figure 4: SBFDInitiator FSM

   Note that the above state machine is different from the base BFD
   specification[RFC5880]. This is because the INIT state is no longer
   applicable for the SBFDInitiator. Another important difference is
   the transition of the state machine from the DOWN state to the UP
   state when a packet with State UP is received by the SBFDInitiator.
   The definitions of the states and the events have the same meaning as
   in the base BFD specification [RFC5880].

7.2.2. **Transmission of S-BFD Control Packet by SBFDInitiator**

   Contents of S-BFD control packets sent by an SBFDInitiator MUST be
   set as follows:

      Version

         Set to the current version number (1).

      Diagnostic (Diag)

   MAY be set to appropriate value for communicating with peer.

State (Sta)

   Set to the value indicated by local state.

Poll (P)

   Set to 1 if the local system is sending a Poll Sequence.

Final (F)

   Set to 1 if the local system is responding to a Control packet
   received with the Poll (P) bit set, or 0 if not.

Control Plane Independent (C)

   Set to 1 if the local system's BFD implementation is
   independent of the control plane (it can continue to function
   through a disruption of the control plane.)

Authentication Present (A)

   Set to 1 if authentication is in use on this session
   (bfd.AuthType is nonzero), or 0 if not.

Demand (D)

   MUST be set always.

Multipoint (M)

   MUST be set to 0.

Detect Mult

   MUST be set to a value describing locally used multiplier
   value.

Length

   Set to the appropriate length, based on the fixed header length
   (24) plus any Authentication Section.

My Discriminator

   Set to value assigned by local node.

   Your Discriminator

      Set to value corresponding to remote entity.

   Desired Min TX Interval

      MUST be set to a value describing local desired minimum
      transmit interval.

   Required Min RX Interval

      MUST be set to 0.

   Required Min Echo RX Interval

      MUST be set to 0.

7.3. Responder Procedures

   A network node which receives S-BFD control packets transmitted by an
   initiator is referred as responder. The responder, upon reception of
   S-BFD control packets, is to perform necessary relevant validations
   described in [RFC5880], [RFC5881], [RFC5883], [RFC5884] and
   [RFC5885].

7.3.1. Responder Demultiplexing

   S-BFD packet MUST be demultiplexed with lower layer information
   (e.g., dedicated destination UDP port, associated channel type).
   Following procedure SHOULD be executed by responder:

   If "your discriminator" not one of the entry allocated for local
   entities

      Packet MUST NOT be considered for this mechanism.

   Else

      Packet is determined to be handled by a reflector BFD session
      responsible for that S-BFD discriminator.

      If local policy allows (e.g., administrative, security, rate-
      limiter, etc)

         Chosen reflector BFD session SHOULD transmit a response BFD
         control packet using procedures described in Section 7.3.2.

7.3.2. **Transmission of S-BFD Control Packet by SBFDReflector**

   Contents of S-BFD control packets sent by an SBFDReflector MUST be
   set as follows:

      Version

         Set to the current version number (1).

      Diagnostic (Diag)

         MAY be set to appropriate value for communicating with peer.

      State (Sta)

         MUST be set to UP or ADMINDOWN. Clarification of reflector BFD
         session state is described in Section 7.8.

      Poll (P)

         Set to 1 if the local system is sending a Poll Sequence, or 0
         if not.

      Final (F)

         Set to 1 if the local system is responding to a Control packet
         received with the Poll (P) bit set, or 0 if not.

      Control Plane Independent (C)

         Set to 1 if the local system's BFD implementation is
         independent of the control plane (it can continue to function
         through a disruption of the control plane.)

      Authentication Present (A)

         Set to 1 if authentication is in use on this session
         (bfd.AuthType is nonzero), or 0 if not.

      Demand (D)

         MUST be cleared.

      Multipoint (M)

         MUST be set to 0.

      Detect Mult

MUST be copied from received "Detection Multiplier".

Length

Set to the appropriate length, based on the fixed header length
(24) plus any Authentication Section.

My Discriminator

MUST be copied from received "your discriminator".

Your Discriminator

MUST be copied from received "my discriminator".

Desired Min TX Interval

MUST be copied from received "Desired Min TX Interval".

Required Min RX Interval

MUST be set to a value describing how many incoming control
packets this reflector BFD session can handle. Further details
are described in Section 7.8.

Required Min Echo RX Interval

If device supports looping back S-BFD echo packets

MUST set non-zero value desired by local device.

Else

MUST be set to 0.

7.4. Diagnostic Values

Diagnostic value in both directions MAY be set to a certain value, to
attempt to communicate further information to both ends. However,
details of such are outside the scope of this specification.

7.5. The Poll Sequence

Poll sequence MAY be used in both directions. The Poll sequence MUST
operate in accordance with [RFC5880]. An SBFDReflector MAY use the
Poll sequence to slow down that rate at which S-BFD control packets
are generated from an SBFDInitiator. This is done by the
SBFDReflector using procedures described in Section 7.8 and setting

the Poll (P) bit in the reflected S-BFD control packet. The
SBFDInitiator is to then send the next S-BFD control packet with the
Final (F) bit set. If an SBFDReflector receives an S-BFD control
packet with Poll (P) bit set, then the SBFDReflector MUST respond
with an S-BFD control packet with Poll (P) bit cleared and Final (F)
bit set.

7.6. Control Plane Independent (C)

Control plane independent (C) bit for an SBFDInitiator sending S-BFD
control packets to a reflector BFD session MUST work according to
[RFC5880]. Reflector BFD session also MUST work according to
[RFC5880]. Specifically, if reflector BFD session implementation
does not share fate with control plane, then response S-BFD control
packets transmitted MUST have control plane independent (C) bit set.
If reflector BFD session implementation shares fate with control
plane, then response S-BFD control packets transmitted MUST NOT have
control plane independent (C) bit set.

7.7. Additional SBFDInitiator Behaviors

o If the SBFDInitiator receives a valid S-BFD control packet in
   response to transmitted S-BFD control packet to a remote entity,
   then the SBFDInitiator SHOULD conclude that S-BFD control packet
   reached the intended remote entity.

o When a sufficient number of S-BFD packets have not arrived as they
   should, the SBFDInitiator SHOULD declare loss of reachability to
   the remote entity. The criteria for declaring loss of
   reachability and the action that would be triggered as a result
   are outside the scope of this document.

o Relating to above bullet item, it is critical for an
   implementation to understand the latency to/from the reflector BFD
   session on the responder. In other words, for very first S-BFD
   packet transmitted by the SBFDInitiator, an implementation MUST
   NOT expect response S-BFD packet to be received for time
   equivalent to sum of latencies: initiator to responder and
   responder back to initiator.

o If the SBFDInitiator receives an S-BFD control packet with Demand
   (D) bit set, the packet MUST be discarded.

7.8. Additional SBFDReflector Behaviors

o S-BFD control packets transmitted by the SBFDReflector MUST have
   "Required Min RX Interval" set to a value which expresses how many
   incoming S-BFD control packets this SBFDReflector can handle. The

SBFDReflector can control how fast SBFInitiators will be sending
S-BFD control packets to self by ensuring "Required Min RX
Interval" indicates a value based on the current load.

o If the SBFDReflector wishes to communicate to some or all
   SBFDInitiators that monitored local entity is "temporarily out of
   service", then S-BFD control packets with "state" set to ADMINDOWN
   are sent to those SBFDInitiators. The SBFDInitiators, upon
   reception of such packets, MUST NOT conclude loss of reachability
   to corresponding remote entity, and MUST back off packet
   transmission interval for the remote entity to an interval no
   faster than 1 second. If the SBFDReflector is generating a
   response S-BFD control packet for a local entity that is in
   service, then "state" in response BFD control packets MUST be set
   to UP.

o If an SBFDReflector receives an S-BFD control packet with Demand
   (D) bit cleared, the packet MUST be discarded.

8. Scaling Aspect

This mechanism brings forth one noticeable difference in terms of
scaling aspect: number of SBFDReflector. This specification
eliminates the need for egress nodes to have fully active BFD
sessions when only one side desires to perform continuity tests.
With introduction of reflector BFD concept, egress no longer is
required to create any active BFD session per path/LSP/function
basis. Due to this, total number of BFD sessions in a network is
reduced.

9. Co-existence with Classical BFD Sessions

Initial packet demultiplexing requirement is described in
Section 7.1. Because of this, S-BFD mechanism can co-exist with
classical BFD sessions.

10. S-BFD Echo Function

The concept of the S-BFD Echo function is similar to the BFD Echo
function described in [RFC5880]. S-BFD echo packets have the
destination of self, thus S-BFD echo packets are self-generated and
self-terminated after traversing a link/path. S-BFD echo packets are
expected to u-turn on the target node in the data plane and MUST NOT
be processed by any reflector BFD sessions on the target node.

When using the S-BFD Echo function, it is RECOMMENDED that:

o Both S-BFD control packets and S-BFD echo packets be sent.

o Both S-BFD control packets and S-BFD echo packets have the same
   semantics in the forward direction to reach the target node.

In other words, it is not preferable to send just S-BFD echo packets
without also sending S-BFD control packets. There are two reasons
behind this suggestion:

o S-BFD control packets can verify the reachability to intended
   target node, which allows one to have confidence that S-BFD echo
   packets are u-turning on the expected target node.

o S-BFD control packets can detect when the target node is going out
   of service (i.e., via receiving back ADMINDOWN state).

The usage of the "Required Min Echo RX Interval" field is described
in Section 7.2.2 and Section 7.3.2. Because of the stateless nature
of SBFDReflector sessions, a value specified the "Required Min Echo
RX Interval" field in both directions is not very meaningful. Thus
it is RECOMMENDED that the "Required Min Echo RX Interval" field
simply be set to zero in both directions.

Following aspects of S-BFD Echo functions are left as implementation
details, and are outside the scope of this document:

o Format of the S-BFD echo packet (e.g., data beyond UDP header).

o Procedures on when and how to use the S-BFD Echo function.

11. Security Considerations

Same security considerations as [RFC5880], [RFC5881], [RFC5883],
[RFC5884] and [RFC5885] apply to this document. Additionally,
implementing the following measures will strengthen security aspects
of the mechanism described by this document:

o SBFDInitiator MAY pick crypto sequence number based on
   authentication mode configured.

o SBFDReflector MUST NOT look at the crypto sequence number before
   accepting the packet.

o SBFDReflector MAY look at the Key ID
   [I-D.ietf-bfd-generic-crypto-auth] in the incoming packet and
   verify the authentication data.

o SBFDReflector MUST accept the packet if authentication is
   successful.

o SBFDReflector MUST compute the Authentication data and MUST use
   the same sequence number that it received in the S-BFD control
   packet that it is responding to.

o SBFDInitiator MUST accept the S-BFD control packet if it either
   comes with the same sequence number as it had sent or it's within
   the window that it finds acceptable (described in detail in
   [I-D.ietf-bfd-generic-crypto-auth])

Using the above method,

o SBFDReflector continue to remain stateless despite using security.

o SBFDReflector are not susceptible to replay attacks as they always
   respond to S-BFD control packets irrespective of the sequence
   number carried.

o An attacker cannot impersonate the responder since the
   SBFDInitiator will only accept S-BFD control packets that come
   with the sequence number that it had originally used when sending
   the S-BFD control packet.

12. IANA Considerations

No action is required by IANA for this document.

13. Acknowledgements

Authors would like to thank Jeffrey Haas, Greg Mirsky and Marc
Binderberger for performing thorough reviews and providing number of
suggestions. Authors would like to thank Girija Raghavendra Rao, Les
Ginsberg, Srihari Raghavan, Vanitha Neelamegam and Vengada Prasad
Govindan from Cisco Systems for providing valuable comments. Authors
would also like to thank John E. Drake and Pablo Frank for providing
comments and suggestions.

14. 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

    Mallik Mudigonda
    Cisco Systems
    Email: mmudigon@cisco.com

    Sam Aldrin
    Google
    Email: aldrin.ietf@gmail.com

15. References

15.1. Normative References

    [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.

    [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.

15.2. Informative References
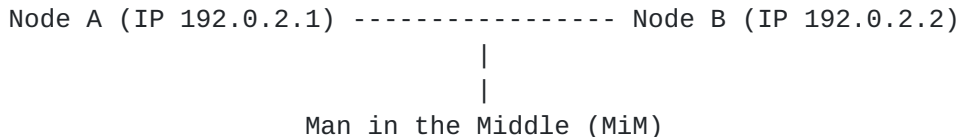
    [I-D.ietf-bfd-generic-crypto-auth]
                Bhatia, M., Manral, V., Zhang, D., and M. Jethanandani,
                "BFD Generic Cryptographic Authentication", draft-ietf-
                bfd-generic-crypto-auth-06 (work in progress), April 2014.

    [I-D.ietf-bfd-multipoint]
                Katz, D., Ward, D., and J. Networks, "BFD for Multipoint
                Networks", draft-ietf-bfd-multipoint-06 (work in
                progress), May 2015.

    [I-D.ietf-bfd-seamless-use-case]
                Bhatia, M., Matsushima, S., Mirsky, G., and N. Kumar,
                "Seamless Bidirectional Forwarding Detection (BFD) Use
                Case", draft-ietf-bfd-seamless-use-case-02 (work in
                progress), April 2015.

   [RFC5885]   Nadeau, T. and C. Pignataro, "Bidirectional Forwarding
               Detection (BFD) for the Pseudowire Virtual Circuit
               Connectivity Verification (VCCV)", RFC 5885, June 2010.

Appendix A. Loop Problem

   Consider a scenario where we have two nodes and both are S-BFD
   capable.

```
      Node A (IP 192.0.2.1) ----------------- Node B (IP 192.0.2.2)
                                 |
                                 |
                        Man in the Middle (MiM)
```

   Assume node A reserved a discriminator 0x01010101 for target
   identifier 192.0.2.1 and has a reflector session in listening mode.
   Similarly node B reserved a discriminator 0x02020202 for its target
   identifier 192.0.2.2 and also has a reflector session in listening
   mode.

   Suppose MiM sends a spoofed packet with MyDisc = 0x01010101, YourDisc
   = 0x02020202, source IP as 192.0.2.1 and dest IP as 192.0.2.2. When
   this packet reaches Node B, the reflector session on Node B will swap
   the discriminators and IP addresses of the received packet and
   reflect it back, since YourDisc of the received packet matched with
   reserved discriminator of Node B. The reflected packet that reached
   Node A will have MyDdisc=0x02020202 and YourDisc=0x01010101. Since
   YourDisc of the received packet matched the reserved discriminator of
   Node A, Node A will swap the discriminators and reflects the packet
   back to Node B. Since reflectors MUST set the TTL of the reflected
   packets to 255, the above scenario will result in an infinite loop
   with just one malicious packet injected from MiM.

   FYI: Packet fields do not carry any direction information, i.e., if
   this is Ping packet or reply packet.

   Solutions

   The current proposals to avoid the loop problem are:

   o Overload "D" bit (Demand mode bit): Initiator always sets the 'D'
      bit and reflector clears it. This way we can identify if a
      received packet was a reflected packet and avoid reflecting it
      back. However this changes the interpretation of 'D' bit.

   o Use of State field in the BFD control packets: Initiator will
      always send packets with State set to DOWN and reflector will send
      back packets with state field set to UP. Reflectors will never

reflect any received packets with state as UP. However the only
issue is the use of state field differently i.e., state in the
S-BFD control packet from initiator does not reflect the local
state which is anyway not significant at reflector.

o Use of local discriminator as My Disc at reflector: Reflector will
   always fill in My Discriminator with a locally allocated
   discriminator value (not reserved discriminators) and will not
   copy it from the received packet.

Authors' Addresses

Nobo Akiya
Big Switch Networks

Email: nobo.akiya.dev@gmail.com

Carlos Pignataro
Cisco Systems

Email: cpignata@cisco.com

Dave Ward
Cisco Systems

Email: wardd@cisco.com

Manav Bhatia
Ionos Networks

Email: manav@ionosnetworks.com

Santosh Pallagatti
Juniper Networks

Email: santoshpk@juniper.net