Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 22, 2022

E. Chen
Palo Alto Networks
N. Shen
Zededa
R. Raszuk
NTT Network Innovations
R. Rahman

October 19, 2021

Unsolicited BFD for Sessionless Applications
draft-ietf-bfd-unsolicited-05

Abstract

For operational simplification of "sessionless" applications using BFD, in this document we present procedures for "unsolicited BFD" that allow a BFD session to be initiated by only one side, and be established without explicit per-session configuration or registration by the other side (subject to certain per-interface or per-router policies).

Requirements Language

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Status of This Memo

Table of Contents

1. Introduction

The current implementation and deployment practice for BFD ([RFC5880] and [RFC5881]) usually requires BFD sessions be explicitly configured or registered on both sides. This requirement is not an issue when an application like BGP [RFC4271] has the concept of a "session" that involves both sides for its establishment. However, this requirement can be operationally challenging when the prerequisite "session" does not naturally exist between two endpoints in an application. Simultaneous configuration and coordination may be required on both sides for BFD to take effect. For example:

o When BFD is used to keep track of the "liveness" of the nexthop of static routes. Although only one side may need the BFD functionality, currently both sides need to be involved in

specific configuration and coordination and in some cases static routes are created unnecessarily just for BFD.

o When BFD is used to keep track of the "liveness" of the third-pary nexthop of BGP routes received from the Route Server [RFC7947] at an Internet Exchange Point (IXP). As the third-party nexthop is different from the peering address of the Route Server, for BFD to work, currently two routers peering with the Route Server need to have routes and nexthops from each other (although indirectly via the Router Server), and the nexthop of each router must be present at the same time. These issues are also discussed in [I-D.ietf-idr-rs-bfd].

Clearly it is beneficial and desirable to reduce or eliminate unnecessary configurations and coordination in these "sessionless" applications using BFD.

In this document we present procedures for "unsolicited BFD" that allow a BFD session to be initiated by only one side, and be established without explicit per-session configuration or registration by the other side (subject to certain per-interface or per-router policies).

With "unsolicited BFD" there is potential risk for excessive resource usage by BFD from "unexpected" remote systems. To mitigate such risks, several mechanisms are recommended in the Security Considerations section.

Compared to the "Seamless BFD" [RFC7880], this proposal involves only minor procedural enhancements to the widely deployed BFD itself. Thus we believe that this proposal is inherently simpler in the protocol itself and deployment. As an example, it does not require the exchange of BFD discriminators over an out-of-band channel before the BFD session bring-up.

When BGP Add-Path [RFC7911] is deployed at an IXP using the Route Server, multiple BGP paths (when exist) can be made available to the clients of the Router Server as described in [RFC7947]. The "unsolicited BFD" can be used in BGP route selection by these clients to eliminate paths with "inaccessible nexthops".

2. Procedures for Unsolicited BFD

With "unsolicited BFD", one side takes the "Active role" and the other side takes only the "Passive role" as described in [RFC5880].

On the passive side, the "unsolicited BFD" SHOULD be explicitly configured on an interface or globally (apply to all interfaces). The BFD parameters can be either per-interface or per-router based.

It MAY also choose to use the parameters that the active side uses in its BFD Control packets. The "My Discriminator", however, MUST be chosen to allow multiple unsolicited BFD sessions.

The active side starts sending the BFD Control packets as specified in [RFC5880]. The passive side does not send BFD Control packets.

When the passive side receives a BFD Control packet from the active side with 0 as "Your Discriminator" and does not find an existing BFD session, the passive side MAY create a matching BFD session toward the active side, if permitted by local configuration.

It would then start sending the BFD Control packets and perform necessary procedure for bringing up, maintaining and tearing down the BFD session. If the BFD session fails to get established within certain specified time, or if an established BFD session goes down, the passive side would stop sending BFD Control packets and MAY delete the BFD session created until the BFD Control packets is initiated by the active side again.

When an Unsolicited BFD session goes down, an implementation MAY retain the session state for a period of time, which may be configurable. Retaining this state can be useful for operational purposes.

The "Passive role" may change to the "Active role" when a local client registers for the same BFD session, and from the "Active role" to the "Passive role" when there is no longer any locally registered client for the BFD session.

3. State Variables

This document defines a new state variable called Unsolicited Role.

bfd.UnsolicitedRole

The operational mode of BFD interface when configured for unsolicited behaviour. Options can be either PASSIVE, ACTIVE or NULL (NULL - not initialized) for unsolicited BFD sessions. Default (not configured for unsolicited behaviour) MUST be set to NULL if present on the interface.

4. YANG Data Model

This section extends the YANG data model for BFD [I-D.ietf-bfd-yang] to cover the unsolicited BFD.

4.1. Unsolicited BFD Hierarchy

```
module: ietf-bfd-unsolicited
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh:
    +--rw unsolicited {bfd-unsol:unsolicited-params-global}?
       +--rw enable?                          boolean
       +--rw local-multiplier?                multiplier
       +--rw (interval-config-type)?
          +--:(tx-rx-intervals)
          |  +--rw desired-min-tx-interval?    uint32
          |  +--rw required-min-rx-interval?   uint32
          +--:(single-interval) {single-minimum-interval}?
             +--rw min-interval?               uint32
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh
            /bfd-ip-sh:interfaces:
    +--rw unsolicited {bfd-unsol:unsolicited-params-per-interface}?
       +--rw enable?                          boolean
       +--rw local-multiplier?                multiplier
       +--rw (interval-config-type)?
          +--:(tx-rx-intervals)
          |  +--rw desired-min-tx-interval?    uint32
          |  +--rw required-min-rx-interval?   uint32
          +--:(single-interval) {single-minimum-interval}?
             +--rw min-interval?               uint32
  augment /rt:routing/rt:control-plane-protocols
            /rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh
            /bfd-ip-sh:sessions/bfd-ip-sh:session:
    +--ro unsolicited
       +--ro role?   bfd-unsol:unsolicited-role
```

4.2. Unsolicited BFD Module

```
<CODE BEGINS> file "ietf-bfd-unsolicited@2021-10-15.yang"

module ietf-bfd-unsolicited {

  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:ietf-bfd-unsolicited";

  prefix "bfd-unsol";

  // RFC Ed.: replace occurences of YYYY with actual RFC numbers
  // and remove this note
```

```
   import ietf-bfd-types {
     prefix "bfd-types";
     reference "RFC 9127: YANG Data Model for BFD";
   }

   import ietf-bfd {
     prefix "bfd";
     reference "RFC 9127: YANG Data Model for BFD";
   }

   import ietf-bfd-ip-sh {
     prefix "bfd-ip-sh";
     reference "RFC 9127: YANG Data Model for BFD";
   }

   import ietf-routing {
     prefix "rt";
     reference
       "RFC 8349: A YANG Data Model for Routing Management
        (NMDA version)";
   }

   organization "IETF BFD Working Group";

   contact
     "WG Web:   <http://tools.ietf.org/wg/bfd>
      WG List:  <rtg-bfd@ietf.org>

      Editors:  Enke Chen (enchen@paloaltonetworks.com),
                Naiming Shen (naiming@zededa.com),
                Robert Raszuk (robert@raszuk.net),
                Reshad Rahman (reshad@yahoo.com)";

   description
     "This module contains the YANG definition for BFD unsolicited
      as per RFC YYYY.

      Copyright (c) 2021 IETF Trust and the persons
      identified as authors of the code.  All rights reserved.

      Redistribution and use in source and binary forms, with or
      without modification, is permitted pursuant to, and subject
      to the license terms contained in, the Simplified BSD License
      set forth in Section 4.c of the IETF Trust's Legal Provisions
      Relating to IETF Documents
      (http://trustee.ietf.org/license-info).

      This version of this YANG module is part of RFC YYYY; see
```

```
      the RFC itself for full legal notices.";

   reference "RFC YYYY";

   revision 2021-10-15 {
     description "Initial revision.";
     reference "RFC 9127: A YANG data model for BFD unsolicited";
   }

   /*
    * Feature definitions
    */
    feature unsolicited-params-global {
      description
        "This feature indicates that the server supports global
         parameters for unsolicited sessions.";
    }

   feature unsolicited-params-per-interface {
     description
       "This feature indicates that the server supports per-interface
        parameters for unsolicited sessions.";
   }

   /*
    * Type Definitions
    */
   typedef unsolicited-role {
     type enumeration {
       enum unsolicited-active {
         description "Active role";
       }
       enum unsolicited-passive {
         description "Passive role";
       }
     }
     description "Unsolicited role";
   }

   /*
    * Augments
    */
    augment "/rt:routing/rt:control-plane-protocols/"
          + "rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh" {
      description
        "Augmentation for BFD unsolicited parameters";
      container unsolicited {
        if-feature bfd-unsol:unsolicited-params-global;
```

```
        description
          "BFD unsolicited top level container";
        leaf enable {
          type boolean;
          default false;
          description
            "Enable BFD unsolicited globally for IP single-hop.";
        }
        uses bfd-types:base-cfg-parms;
      }
    }

    augment "/rt:routing/rt:control-plane-protocols/"
          + "rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh/"
          + "bfd-ip-sh:interfaces" {
      description
        "Augmentation for BFD unsolicited on IP single-hop interface";
      container unsolicited {
        if-feature bfd-unsol:unsolicited-params-per-interface;
        description
          "BFD IP single-hop interface unsolicited top level container";
        leaf enable {
          type boolean;
          default false;
          description "Enable BFD unsolicited on this interface.";
        }
        uses bfd-types:base-cfg-parms;
      }
    }

   augment "/rt:routing/rt:control-plane-protocols/"
         + "rt:control-plane-protocol/bfd:bfd/bfd-ip-sh:ip-sh/"
         + "bfd-ip-sh:sessions/bfd-ip-sh:session" {
     description
       "Augmentation for BFD unsolicited on IP single-hop session";
     container unsolicited {
       config false;
       description
         "BFD IP single-hop session unsolicited top level container";
       leaf role {
         type bfd-unsol:unsolicited-role;
         description "Role.";
       }
     }
   }
 }

 <CODE ENDS>
```

5. IANA Considerations

This documents makes no IANA requests.

6. Acknowledgments

Authors would like to thank Acee Lindem, Greg Mirsky, Jeffrey Haas and Raj Chetan for their review and valuable input.

7. Security Considerations

7.1. BFD Protocol Security Considerations

The same security considerations and protection measures as those described in [RFC5880] and [RFC5881] normatively apply to this document. With "unsolicited BFD" there is potential risk for excessive resource usage by BFD from "unexpected" remote systems. To mitigate such risks, the following measures are mandatory:

- Limit the feature to specific interfaces, and to a single-hop BFD with "TTL=255" [RFC5082]. For numbered interfaces source address of an incoming BFD packet should belongs to the subnet of the interface from which the BFD packet is received. For unnumbered interfaces the above check should be aligned with routing protocol addresses running on such pair of interfaces.
- Apply "access control" to allow BFD packets only from certain subnets or hosts.
- Deploy the feature only in certain "trustworthy" environment, e.g., at an IXP, or between a provider and its customers.
- Adjust BFD parameters as needed for the particular deployment and scale.
- Use BFD authentication.

7.2. YANG Module Security Considerations

The YANG module specified in this document defines a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC5246].

The NETCONF access control model [RFC6536] provides the means to restrict access for particular NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

/routing/control-plane-protocols/control-plane-protocol/bfd/ip-sh
/unsolicited:

- o data node "enable" enables creation of unsolicited BFD IP single-hop sessions globally, i.e. on all interfaces. See Section 7.1.
- o data nodes local-multiplier, desired-min-tx-interval, required-min-rx-interval and min-interval all impact the parameters of the unsolicited BFD IP single-hop sessions.

/routing/control-plane-protocols/control-plane-protocol/bfd/ip-sh
/interfaces/interface/unsolicited:

- o data node "enable" enables creation of unsolicited BFD IP single-hop sessions on a specific interface. See Section 7.1.
- o data nodes local-multiplier, desired-min-tx-interval, required-min-rx-interval and min-interval all impact the parameters of the unsolicited BFD IP single-hop sessions on the interface.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

/routing/control-plane-protocols/control-plane-protocol/bfd/ip-sh
/sessions/session/unsolicited: access to this information discloses the role of the local system in the creation of the unsolicited BFD session.

8. References

8.1. Normative References

[I-D.ietf-bfd-yang]
Rahman, R., Zheng, L., Jethanandani, M., Pallagatti, S., and G. Mirsky, "YANG Data Model for Bidirectional Forwarding Detection (BFD)", draft-ietf-bfd-yang-17 (work in progress), August 2018.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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, <https://www.rfc-editor.org/info/rfc5082>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://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, <https://www.rfc-editor.org/info/rfc5881>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <https://www.rfc-editor.org/info/rfc6536>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[I-D.ietf-idr-rs-bfd]
Bush, R., Haas, J., Scudder, J. G., Nipper, A., and C. Dietzel, "Making Route Servers Aware of Data Link Failures at IXPs", draft-ietf-idr-rs-bfd-09 (work in progress), September 2020.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[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, <https://www.rfc-editor.org/info/rfc7880>.

[RFC7911] Walton, D., Retana, A., Chen, E., and J. Scudder, "Advertisement of Multiple Paths in BGP", RFC 7911, DOI 10.17487/RFC7911, July 2016, <https://www.rfc-editor.org/info/rfc7911>.

[RFC7947] Jasinska, E., Hilliard, N., Raszuk, R., and N. Bakker, "Internet Exchange BGP Route Server", RFC 7947, DOI 10.17487/RFC7947, September 2016, <https://www.rfc-editor.org/info/rfc7947>.

Authors' Addresses

Enke Chen
Palo Alto Networks

Email: enchen@paloaltonetworks.com

Naiming Shen
Zededa

Email: naiming@zededa.com

Robert Raszuk
NTT Network Innovations
940 Stewart Dr
Sunnyvale, CA 94085
USA

Email: robert@raszuk.net

Reshad Rahman

Email: reshad@yahoo.com