Chapter 5
Configuring BFD

This chapter describes how to configure bidirectional forwarding detection (BFD) on your E-series router; it contains the following sections:

Overview

Fast failure detection is a high priority feature for any network element. Some media, like Ethernet, do not provide remote end failure. Networks must often rely on internal gateway protocol (IGP) hello messages to detect any failure and, in some cases (for example, static routes), even these hello messages are not used.

IGP hellos have their own limitations—it often takes one second or more to detect a remote end failure and processing IGP hello messages takes precious processing time. BFD overcomes IGP detection time and processing limitations in detecting any data path failures.

When configured for various protocols like OSPF and IS-IS, BFD employs rapid, periodic and inexpensive hello messages to detect path activity. You can also configure BFD to function with static routes, combining with the BFD poll bit to detect path activity.

You can also configure a BFD session with a BGP neighbor or peer group to determine relatively quickly whether the neighbor or peer group is reachable. For information about configuring BFD for EBGP routes, see *JUNOSe BGP and MPLS Configuration Guide, Chapter 1, Configuring BGP Routing*.

How BFD Works

In a BFD-configured network, when a client launches a BFD session with a peer, BFD begins sending slow, periodic BFD control packets that contain the interval values that you specified when you configured the BFD peers. This is known as the initialization state and BFD does not generate any up or down notifications in this state.

When another BFD interface acknowledges the BFD control packets, the session moves into an up state and begins to more rapidly send periodic control packets.

If a data path failure occurs and BFD does not receive a control packet within the configured amount of time, the data path is declared down and BFD notifies the BFD client. The BFD client can then perform the necessary actions to reroute traffic. This process can be different for different BFD clients. All BFD-configured IGP clients (like IS-IS, OSPF, PIM, and RIP) launch BFD sessions when they detect neighbors through their own hello protocols. However, a static BFD client launches a BFD session when it detects that its next hop is resolved.

Negotiation of the BFD Liveness Detection Interval

When you issue the appropriate **bfd-liveness-detection** command on an IS-IS, OSPF, RIP, or PIM interface, BFD liveness detection is established with all of its BFD-enabled peers. When an update is received from a peer—if BFD is enabled and if the session is not already present—the local peer attempts to create a BFD session to the remote peer.

Each pair of peers negotiates acceptable transmit and receive intervals for BFD packets. These values can be different on each peer.

The negotiated transmit interval for a peer is the interval between the BFD packets that it sends to its peers. The receive interval for a peer is the minimum time that it requires between packets sent from its peer; the receive interval is not negotiated between peers.

To determine the transmit interval, each peer compares its configured minimum transmit interval with its peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.

Consider the following example. Router A and Router B are peers, with the following BFD liveness detection values configured.

Router	Configured Transmit Interval (ms)	Configured Receive Interval (ms)
A	400	500
B	450	450

- For Router A, the negotiated transmit interval is the greater of its transmit interval (400 ms) and the Router B receive interval (450 ms), or 450 ms.
- For Router B, the negotiated transmit interval is the greater of its transmit interval (450 ms) and the Router A receive interval (500 ms), or 500 ms.

The liveness detection interval is the period a peer waits for a BFD packet from its peer before declaring the BFD session to be down. The detection interval is determined independently by each peer and can be different for each. The detection interval for the local peer is calculated as the remote peer's negotiated transmit interval times the detection multiplier value configured on the remote peer.

Router	Negotiated Transmit Interval (ms)	Detection Multiplier	Liveness Detection Interval (ms)
A	450	2	1500
B	500	3	900

- For Router A, the detection interval is Router B's negotiated transmit interval times the Router B detection multiplier: 500 ms x 3 = 1500 ms.
- For Router B, the detection interval is Router A's negotiated transmit interval times the Router A detection multiplier: 450 ms x 2 = 900 ms.

If Router A fails to receive a BFD packet from Router B within 1500 milliseconds, Router A declares the BFD session to be down. Similarly, if Router B fails to receive a BFD packet from Router A within 900 milliseconds, Router B declares the BFD session to be down. In either case, all routes learned from the failed peer are purged immediately.

NOTE: Before the router can use any **bfd-liveness-detection** command, you must specify a BFD license key. To view an already configured license, use the **show license bfd** command.

Platform Considerations

For information about modules that support BFD on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support BFD.

For information about modules that support BFD on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support BFD.

References

For information about BFD, see the following:

- BFD for IPv4 and IPv6 (Single Hop)—draft-ietf-bfd-v4v6-1hop-00.txt (January 2005 expiration)
- Bidirectional Forwarding Detection—draft-ietf-bfd-base-00.txt. (January 2005 expiration)

Configuring a BFD License

You must configure a BFD license before the router configuration can use any BFD commands.

license bfd

- Use to specify a BFD license.
- Purchase a BFD license to allow BFD configuration on the E-series router.

NOTE: Acquire the BFD license from Juniper Networks Customer Service or your Juniper Networks sales representative.

- Example

  host1(config)#**license bfd** *license-value*

- Use the **no** version to disable the license.

BFD Version Support

The JUNOSe software supports both BFD Version 0 and BFD Version 1. When establishing a BFD neighbor session, the E-series router attempts to establish version 0 or version 1 sessions based on the capability of the BFD neighbor. Table 8 indicates how the routers establish sessions based on BFD version support:

Table 8: Determining BFD Versions

		E-series Routers Running JUNOSe 7.2.x (and later)	**E-series Routers Running Software Versions Earlier than JUNOSe 7.2.x**
	BFD Version Support	Version 0 and Version 1	Version 0 Only
E-series Routers Running JUNOSe 7.2.x (and later) and Other Routers	Version 0 and Version 1	Result = Version 1	Result = Version 0
E-series Routers Running Software Versions Earlier than JUNOSe 7.2.x and Other Routers	Version 0 Only	Result = Version 0	Result = Version 0
Other Routers	Version 1 Only	Result = Version 1	No session (version mismatch)

NOTE: You cannot configure the JUNOSe software to send BFD Version 0 or BFD Version 1 packets. The JUNOSe software determines the BFD version through auto-negotiation.

Configuring BFD

You configure BFD on routing protocols that use BFD for fast failure detection. BFD does not require any stand-alone configuration; it works in conjunction with the application that it is supporting. Applications on which you configure BFD pass configuration information to BFD when they need fast failure detection.

BFD works with a wide variety of routing protocols. The JUNOSe software currently supports only a few of these protocols. All BFD supported clients provide the ability to configure session parameters for each interface. Refer to the following table for added configuration information:

Configuration Topic	See
EBGP	*JUNOSe BGP and MPLS Configuration Guide, Chapter 1, Configuring BGP Routing*
IPv4 static routes	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*
IS-IS	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 6, Configuring IS-IS*
OSPF	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 5, Configuring OSPF*
OSPFv3	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 5, Configuring OSPF*
PIM	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 7, Configuring PIM for IPv4 Multicast* and *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 12, Configuring PIM for IPv6 Multicast*
RIP	*JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 4, Configuring RIP*
RSVP-TE	*JUNOSe BGP and MPLS Configuration Guide, Chapter 2, Configuring MPLS*

Managing BFD Adaptive Timer Intervals

The **bfd adapt** command enables timer intervals to adapt for all BFD sessions on all virtual routers on the router.

Enabling BFD adaptive timers avoids BFD session flaps that might occur because of misconfiguration or other errors. When enabled, BFD attempts to adapt timer intervals on the router by making them less restrictive and increasing the survival chances for the session.

NOTE: Enabling BFD adaptive timers targets only rapidly flapping events and not genuine BFD down events. If BFD down events occur in intervals longer than 5 seconds, the session does not attempt to adapt.

Disabling BFD adaptive timers does not affect current adaptive timer intervals for sessions. Disabling adaptive timers prohibits BFD from further adapting timer intervals for existing sessions or for new sessions.

To reset adapted intervals for all BFD sessions on the router, use the **clear bfd adapted-intervals** command.

bfd adapt

- Use to enable all BFD sessions to adapt timer intervals on all virtual routers on the router.
- Example

  host1(config)#**bfd adapt**

- Use the **no** version to disable subsequent BFD sessions from adapting timer intervals without resetting any already adapted intervals.

clear bfd adapted-intervals

- Use to reset adapted timer intervals for all BFD sessions on the router.
- Does not disable the state of the BFD adaptive timer interval feature.
- Example

  host1#**clear bfd adapted-intervals**

- There is no **no** version.

Clearing BFD Sessions

You can use the **clear bfd session** or **clear ipv6 bfd session** commands to clear one or more BFD sessions for IPv4 or IPv6 (respectively).

clear bfd session

- Use to restart all IPv4 BFD sessions or a specified IPv4 BFD session.
- Use the **address** keyword to indicate the IPv4 address of the destination to which the session has been established.
- Use the **discriminator** keyword to clear the BFD session associated with the unique system-wide identifier.
- Example 1

  host1#**clear bfd session**

- Example 2

  host1#**clear bfd session address 10.10.5.24**

- Example 3

  host1#**clear bfd session discriminator 4**

- There is no **no** version.

clear ipv6 bfd session

- Use to restart all IPv6 BFD sessions or a specified IPv6 BFD session.
- Use the **address** keyword to indicate the IPv6 address of the destination to which the session has been established.
- Example 1

  host1#**clear ipv6 bfd session**

- Example 2

  host1#**clear ipv6 bfd session address 1::4**

- There is no **no** version.

Monitoring BFD

This section lists the system event logs associated with the BFD protocol and describes the **show** commands you can use to view BFD-related information.

System Event Logs

To troubleshoot and monitor BFD, use the following system event logs:

- bfdGeneral
- bfdSession
- bfdEvents
- bgpConnections
- isisBfdEvents
- ospfEvents
- ospfv3General
- ripBfdLog

For more information about using event logs, see the *JUNOSe System Event Logging Reference Guide*.

Viewing BFD Information

You can monitor the following aspects of BFD by using the following **show** commands:

To Display	Command
BFD session information	**show bfd session**
BFD license key information	**show license bfd**

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string that you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

show license bfd

- Use to display the bfd license key configured on the router.
- Example

```
host1#show license bfd
BFD license is bfd_license
```

show bfd session

- Use to display BFD protocol session information.
- Use the **address** keyword to specify an IPv4 or IPv6 session that you want to view.
- Use the **detail** keyword to view more detailed information about the BFD session.
- Field descriptions
  - Address—IP address of the remote interface with which the session is established. In unnumbered cases, the remote interface provides its reference IP address.
  - State—State of the BFD session, Up or Down
  - Interface—Interface on which the BFD session has been established
  - Detect/Detection Time—Time (in seconds) taken to declare the remote interface down when no packets are received from that interface
  - Local discriminator—Value used to identify the session at the local end
  - Remote discriminator—Value used to identify the session at the remote end
  - Session up time—Amount of time the session has been operational since the last session down event in *days:hours:minutes:seconds* format.
  - Up/Down count—Number of times up/down transitions have occurred on the session
  - Adaptivity—Number of times this session has adapted its intervals, or that additional adaptivity is disabled for this BFD session on the router

- Local
  - min tx interval—Minimum transmit interval (in seconds) configured on the session at the local end
  - min rx interval—Minimum receive interval (in seconds) configured on the session at the local end
  - multiplier—Multiplier configured on the session at the local end
- (Adapted)
  - min tx interval—Minimum transmit interval (in seconds) to which the session is adapted at the local end
  - min rx interval—Minimum receive interval (in seconds) to which the session is adapted at the local end
  - multiplier—Multiplier to which the session is adapted at the local end
- Remote
  - min tx interval—Minimum transmit interval (in seconds) configured on the session at the remote end
  - min rx interval—Minimum receive interval (in seconds) configured on the session at the remote end
  - multiplier—Multiplier configured on the session at the remote end
- Up/Down count—Number of up/down transitions that have occurred on the session
- Local diagnostic—Reason at the local end for the last session down event
- Remote diagnostic—Reason at the remote end for the last session down event
- Remote heard/Remote not heard—Whether the local end is receiving packets from the remote end
- hears us/doesn't hear us—Whether the remote end is receiving packets from the local end
- Min async interval—Minimum interval (in seconds) between packets sent when in asynchronous mode
- min slow interval—Minimum interval (in seconds) between packets when the remote end is first being detected
- Echo mode—State of echo mode (enabled or disabled; active or inactive)
- Client—Name of the client
  - desired tx—Minimum transmit interval (in seconds) requested by the client
  - required rx—Minimum required receive interval (in seconds) specified by the client
  - multiplier—Multiplier requested by the client

- Example 1

```
host1#show bfd session
Address               State     Interface         Detect    Interval   Mx
                                                  Time
------------------------------------------------------------------------
172.16.1.2             Up        FastEthernet1/4   0.900     0.300      3
172.16.1.1             Up        FastEthernet1/5   0.900     0.300      3
```

- Example 2—IPv4 version

```
host1#show bfd session detail
Address: 172.16.1.2
  State UP on Interface FastEthernet1/4
  Detection Time0.900, version v0
  Local discriminator 3, Remote discriminator 1
  Session up time 00:00:01:04, Up/Down count 1, Adapted 3 times
  Local: min tx interval 0.3, min rx interval 0.3, multiplier 1
  (Adapted) min tx interval 0.6, min rx interval 0, multiplier 3
  Remote: min tx interval 0.3, min rx interval 0.3, multiplier 3
  Local diagnostic: None, Remote diagnostic: None
  Remote heard, hears us
  Min async interval 0.3, min slow interval 0.3
  Echo mode disabled/inactive
2 Clients:
  Client OSPFv2, desired tx: 0.3, required rx: 0.3, multiplier 3
  Client ISIS, desired tx: 0.3, required rx: 0.3, multiplier 3
```

- Example 3—IPv6 version

```
host1#show bfd session detail
Address fe80:1234::abcd
  State UP on Interface FastEthernet1/3
  Detection Time0.900, version v1
  Local discriminator 3, Remote discriminator 1
  Session up time 00:00:01:04, Up/Down count 1, Adaptivity disabled
  Local: min tx interval 0.3, min rx interval 0.3, multiplier 3
  (Adapted) min tx interval 0, min rx interval 0, multiplier 4
  Remote: min tx interval 0.3, min rx interval 0.3, multiplier 3
  Local diagnostic: None, Remote diagnostic: None
  Remote heard, hears us
  Min async interval 0.3, min slow interval 0.3
  Echo mode disabled/inactive
1 Client:
  Client OSPFv3, desired tx: 0.3, required rx: 0.3, multiplier 3
```