Configuring Bidirectional Forwarding Detection

About BFD

BFD is a detection protocol designed to provide fast forwarding-path failure detection times for media types, encapsulations, topologies, and routing protocols. You can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different protocol hello mechanisms. BFD makes network profiling and planning easier and reconvergence time consistent and predictable.

BFD provides subsecond failure detection between two adjacent devices and can be less CPU-intensive than protocol hello messages because some of the BFD load can be distributed onto the data plane on supported modules.

Asynchronous Mode

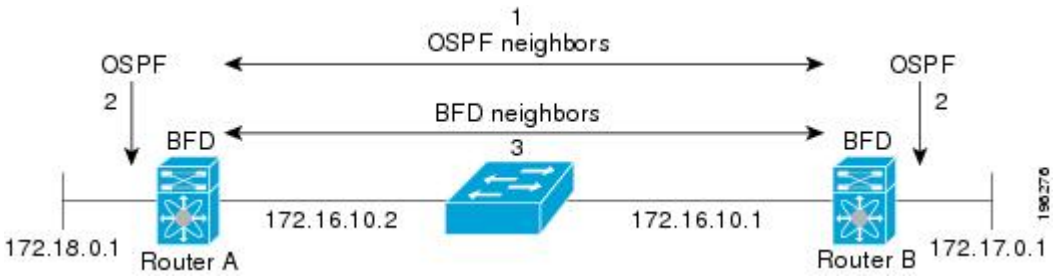
Cisco NX-OS supports the BFD asynchronous mode, which sends BFD control packets between two adjacent devices to activate and maintain BFD neighbor sessions between the devices. You configure BFD on both devices (or BFD neighbors). Once BFD has been enabled on the interfaces and on the appropriate protocols, Cisco NX-OS creates a BFD session, negotiates BFD session parameters, and begins to send BFD control packets to each BFD neighbor at the negotiated interval. The BFD session parameters include the following:

- Desired minimum transmit interval—The interval at which this device wants to send BFD hello messages.

- Required minimum receive interval—The minimum interval at which this device can accept BFD hello messages from another BFD device.
- Detect multiplier—The number of missing BFD hello messages from another BFD device before this local device detects a fault in the forwarding path.

The following figure shows how a BFD session is established. The figure shows a simple network with two routers running Open Shortest Path First (OSPF) and BFD. When OSPF discovers a neighbor (1), it sends a request to the local BFD process to initiate a BFD neighbor session with the OSPF neighbor router (2). The BFD neighbor session with the OSPF neighbor router is now established (3).

Figure 1: Establishing a BFD Neighbor Relationship



BFD Detection of Failures

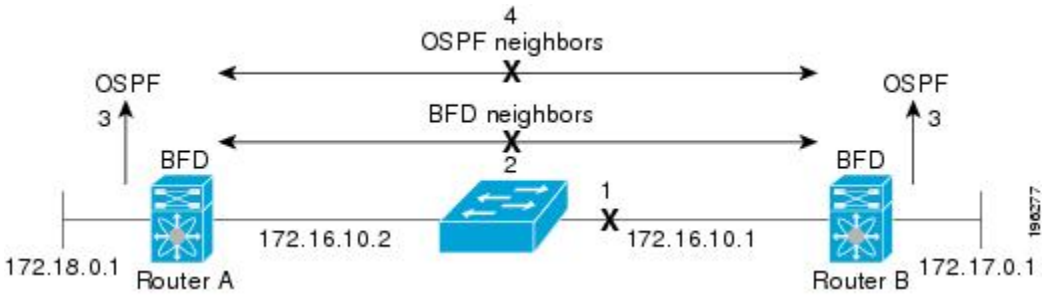
Once a BFD session has been established and timer negotiations are complete, BFD neighbors send BFD control packets that act in the same manner as an IGP hello protocol to detect liveliness, except at a more accelerated rate. BFD detects a failure, but the protocol must take action to bypass a failed peer.

BFD sends a failure detection notice to the BFD-enabled protocols when it detects a failure in the forwarding path. The local device can then initiate the protocol recalculation process and reduce the overall network convergence time.

The following figure shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor router is torn down (2). BFD notifies the local OSPF process that the BFD neighbor is no longer reachable (3). The local OSPF process tears down the OSPF neighbor relationship (4). If an alternative path is available, the routers immediately start converging on it.

Note Note The BFD failure detection occurs in less than a second, which is much faster than OSPF Hello messages could detect the same failure.

Figure 2: Tearing Down an OSPF Neighbor Relationship



Distributed Operation

Cisco NX-OS can distribute the BFD operation to compatible modules that support BFD. This process offloads the CPU load for BFD packet processing to the individual modules that connect to the BFD neighbors. All BFD session traffic occurs on the module CPU. The module informs the supervisor when a BFD failure is detected.

BFD Echo Function

Echo packets are defined and processed only by the transmitting system. For IPv4 and IPv6, the echo packets' destination address is that of the transmitting device. It is chosen in such a way as to cause the remote system to forward the packet back to the local system. This bypasses the routing lookup on the remote system and relies on the forwarding information base (FIB) instead. BFD can use the slow timer to slow down the asynchronous session when the echo function is enabled and reduce the number of BFD control packets that are sent between two BFD neighbors. The Echo function tests only the forwarding path of the remote system by having the remote (neighbor) system loop them back, so there is less inter-packet delay variability and faster failure detection times.

Security

Cisco NX-OS uses the packet Time to Live (TTL) value to verify that the BFD packets came from an adjacent BFD peer. For all asynchronous and echo request packets, the BFD neighbor sets the TTL value to 255 and the local BFD process verifies the TTL value as 255 before processing the incoming packet. For the echo response packet, BFD sets the TTL value to 254.

You can configure SHA-1 authentication of BFD packets.

High Availability

BFD supports stateless restarts. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration and BFD immediately sends control packets to the BFD peers.

Virtualization Support

BFD supports virtual routing and forwarding instances (VRFs). VRFs exist within virtual device contexts (VDCs). By default, Cisco NX-OS places you in the default VDC and default VRF.

Prerequisites for BFD

BFD has the following prerequisites:

- You must enable the BFD feature.
- Disable Internet Control Message Protocol (ICMP) redirect messages on BFD-enabled interfaces.
- Disable the IP packet verification check for identical IP source and destination addresses.
- See other detailed prerequisites that are listed with the configuration tasks.

Guidelines and Limitations

BFD has the following configuration guidelines and limitations:

- The QSFP 40/100-G BiDi comes up in the highest possible speed available on the port. For example, in the Cisco Nexus 93180LC-EX switch it comes up as 40 G in the first 28 ports and 100 G in the last 4 ports. If you need to connect to 40-G SR4 BiDi, the speed on the 40/100-G BiDi needs to be set to 40 G.
- Forming BFD neighbors on a vPC VLAN through an orphan port is not supported on Cisco Nexus 9000 Switches.
- Beginning with Cisco NX-OS Release 9.2(1), QSFP-40/100-SRBD comes up in the speed of 100-G and inter-operate with other QSFP-40/100-SRBD at either 40-G or 100-G speed on Cisco Nexus 9500 Switches with the N9K-X9636C-RX line card. The QSFP-40/100-SRBD can also inter-operate with QSFP-40G-SR-BD at 40G speeds. However to operate at 40G speed, you must configure the speed as 40G.
- **show** commands with the **internal** keyword are not supported.
- Cisco Nexus 9000 Series switches supports BFD per-member link.
- BFD per-member link support is added on Cisco Nexus 9000 Series switches.
- Beginning with Cisco NX-OS Release 9.3(3) BFD is supported on the following Cisco Nexus switches:
  - 9364C-GX
  - 9316D-GX
  - 93600CD-GX
- BFD supports BFD version 1.
- BFD supports IPv4 and IPv6.
- BFD supports OSPFv3.
- BFD supports IS-ISv6.
- If BFD is configured with IS-IS, use unique IP address on interfaces or disable echo function to prevent interface flapping.

- BFD supports BGPv6.
- BFD supports EIGRPv6.
- BFD supports only one session per address family, per Layer 3 interface.
- BFD supports only sessions which have unique (src_ip, dst_ip, interface/vrf) combination.
- BFD supports single-hop BFD.
  - Only single-hop static BFD is supported.
  - BFD for BGP supports single-hop EBGP and iBGP peers.
- BFD supports keyed SHA-1 authentication.
- BFD supports the following Layer 3 interfaces—physical interfaces, port channels, sub-interfaces, and VLAN interfaces.
- BFD depends on a Layer 3 adjacency information to discover topology changes, including Layer 2 topology changes. A BFD session on a VLAN interface (SVI) may not be up after the convergence of the Layer 2 topology if there is no Layer 3 adjacency information available.
- For BFD on a static route between two devices, both devices must support BFD. If one or both of the devices do not support BFD, the static routes are not programmed in the Routing Information Base (RIB).
- Both single-hop and multi-hop BFD features are supported with specific restrictions. For multi-hop BFD features restrictions, refer to section.
- Port channel configuration limitations:
  - For Layer 3 port channels used by BFD, you must enable LACP on the port channel.
  - For Layer 2 port channels used by SVI sessions, you must enable LACP on the port channel.
- SVI limitations:
  - An ASIC reset causes traffic disruption for other ports and it can cause the SVI sessions on the other ports to flap. For example, if the carrier interface is a virtual port channel (vPC), BFD is not supported over the SVI interface and it could cause a trigger for an ASIC reset. When a BFD session is over SVI using virtual port channel (vPC) Peer-Link, the BFD echo function is not supported. You must disable the BFD echo function for all sessions over SVI between vPC peer nodes.

    An SVI on the Cisco Nexus series switches should not be configured to establish a BFD neighbor adjacency with a device connected to it via a vPC. This is because the BFD keepalives from the neighbor, if sent over the vPC member link connected to the vPC peer-switch, do not reach this SVI causing the BFD adjacency to fail.
  - When you change the topology (for example, add or delete a link into a VLAN, delete a member from a Layer 2 port channel, and so on), the SVI session could be affected. It may go down first and then come up after the topology discovery is finished.
  - BFD over FEX HIF interfaces is not supported.
  - When a BFD session is over SVI using virtual port-channel (vPC) Peer-Link (either BCM or GEM based ports), the BFD echo function is not supported. You must disable the BFD echo function for all sessions over SVI between vPC peer nodes using the **no bfd echo** command at the SVI configuration level.

Tip If you do not want the SVI sessions to flap and you need to change the topology, you can disable the BFD feature before making the changes and re-enable BFD after the changes have been made. You can also configure the BFD timer to be a large value (for example, 5 seconds), and change it back to a fast timer after the above events complete.

- When you configure the BFD Echo function on the distributed Layer 3 port channels, reloading a member module flaps the BFD session hosted on that module, which results in a packet loss.

  If you connect the BFD peers directly without a Layer 2 switch in between, you can use the BFD per-link mode as an alternative solution.

Note Using BFD per-link mode and sub-interface optimization simultaneously on a Layer 3 port channel is not supported.

- When you specify a BFD neighbor prefix in the **clear** {**ip** | **ipv6**} **route** *prefix* command, the BFD echo session will flap.
- The **clear** {**ip** | **ipv6**} **route *** command causes BFD echo sessions to flap.
- HSRP for IPv4 is supported with BFD.
- BFD packets generated by the Cisco NX-OS device line cards are sent with COS 6/DSCP CS6. The DSCP/COS values for BFD packets are not user configurable.
- When configuring BFDv6 in no-bfd-echo mode, it is recommended to run with timers of 150 ms with a multiplier of 3.
- BFDv6 is not supported for VRRPv3 and HSRP for v6.
- IPv6 **eigrp bfd** cannot be disabled on an interface.
- IETF BFD is not supported on N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636C-RX and N9K-X9636Q-R line cards.
- Port channel configuration notes:
  - When the BFD per-link mode is configured, the BFD echo function is not supported. You must disable the BFD echo function using the **no bfd echo** command before configuring the **bfd per-link** command.
  - Before configuring BFD per-link, make sure there is no BFD session running on the port-channel. If there is any BFD session running already, remove it and then proceed with bfd per-link configuration.
  - Configuring BFD per-link with link-local is not supported.
  - The supported platforms include Cisco Nexus 9500 Series switches with N9K-X9636C-R, N9K-X9636Q-R, N9K-X9636C-RX line cards.
- Beginning with Cisco NX-OS Release 9.3(7), BFD is supported on unnumbered interfaces.

Note BFD over Unnumbered Switched Virtual Interfaces (SVIs) are not supported.

Downgrade compatibility for BFD on unnumbered interface support cannot be verified using **show incompatibility nxos bootflash:filename** command. The compatibility will be checked during **install all** command.

- When you configure BFD on a numbered interface along with OSPF and when the interface is converted to an unnumbered interface, the OSPF and BFD command remains in the running configuration but the BFD functionality may not work
- The following BFD command configurations are not supported for configuration replace:
  - **port-channel bfd track-member-link**
  - **port-channel bfd destination** *destination-ip-address*

Default Settings

The following table lists the default settings for BFD parameters.

Table 1: Default BFD Parameters

Parameters	Default
BFD feature	Disabled
Required minimum receive interval	50 milliseconds
Desired minimum transmit interval	50 milliseconds
Detect multiplier	3
Echo function	Enabled
Mode	Asynchronous
Port-channel	Logical mode (one session per source-destination pair address)
Slow timer	2000 milliseconds
Startup timer	5 seconds

Configuring BFD

Configuration Hierarchy

You can configure BFD at the global level and at the interface level. The interface configuration overrides the global configuration.

For physical ports that are members of a port channel, the member port inherits the primary port channel BFD configuration.

Task Flow for Configuring BFD

Follow these steps in the following sections to configure BFD:

- Enabling the BFD Feature.
- Configuring Global BFD Parameters or Configuring BFD on an Interface.

Enabling the BFD Feature

You must enable the BFD feature before you can configure BFD on an interface and protocol.

Note Use the **no feature bfd** command to disable the BFD feature and remove all associated configuration.

Command	Purpose
no feature bfd **Example:** `switch(config)# no feature bfd`	Disables the BFD feature and removes all associated configuration.

SUMMARY STEPS

1. **configure terminal**
2. **feature bfd**
3. **show feature** | **include bfd**
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

	Command or Action	Purpose
Step 2	**feature bfd** **Example:** `switch(config)# feature bfd`	Enables the BFD feature.
Step 3	**show feature** | **include bfd** **Example:** `switch(config)# show feature | include bfd`	(Optional) Displays enabled and disabled features.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring Global BFD Parameters

You can configure the BFD session parameters for all BFD sessions on the device. The BFD session parameters are negotiated between the BFD peers in a three-way handshake.

See the Configuring BFD on an Interface section to override these global session parameters on an interface.

Before you begin

Enable the BFD feature.

SUMMARY STEPS

1. **configure terminal**
2. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
3. **bfd slow-timer** [*interval*]
4. [**no**] **bfd startup-timer** [*seconds*]
5. **bfd echo-interface loopback** *interface number*
6. **show running-config bfd**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:**	Configures the BFD session parameters for all BFD sessions on the device. This command overrides these values by configuring the BFD session parameters on an interface.

	Command or Action	Purpose
	`switch(config)# bfd interval 50 min_rx 50 multiplier 3`	The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 3	**bfd slow-timer** [*interval*] **Example:** `switch(config)# bfd slow-timer 2000`	Configures the slow timer used in the echo function. This value determines how fast BFD starts up a new session and at what speed the asynchronous sessions use for BFD control packets when the echo function is enabled. The slow-timer value is used as the new control packet interval, while the echo packets use the configured BFD intervals. The echo packets are used for link failure detection, while the control packets at the slower rate maintain the BFD session. The range is from 1000 to 30000 milliseconds. The default is 2000.
Step 4	[**no**] **bfd startup-timer** [*seconds*] **Example:** `switch(config)# bfd startup-timer 20`	Configures the BFD startup timer, which delays the startup time for BFD sessions in order to give the routes that are being used by local and remote routers time to settle down in the hardware. Using this feature can prevent BFD flaps in higher scale scenarios. The range is from 0 to 30 seconds. The default is 5 seconds. The **bfd startup-timer 0** command disables the BFD startup timer. The **no bfd startup-timer** command sets the BFD startup timer to 5 seconds (the default value).
Step 5	**bfd echo-interface loopback** *interface number* **Example:** `switch(config)# bfd echo-interface loopback 1 3`	Configures the interface used for Bidirectional Forwarding Detection (BFD) echo frames. This command changes the source address for the echo packets to the one configured on the specified loopback interface. The interface number range is from 0 to 1023.
Step 6	**show running-config bfd** **Example:** `switch(config)# show running-config bfd`	(Optional) Displays the BFD running configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on an Interface

You can configure the BFD session parameters for all BFD sessions on an interface. The BFD session parameters are negotiated between the BFD peers in a three-way handshake.

This configuration overrides the global session parameters for the configured interface.

Before you begin

Ensure that Internet Control Message Protocol (ICMP) redirect messages are disabled on BFD-enabled interfaces. Use the **no ip redirects** command or the **no ipv6 redirects** command on the interface.

Enable the BFD feature. See the Enabling the BFD Feature section.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *int-if*
3. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
4. **bfd authentication keyed-sha1 keyid** *id* **key** *ascii_key*
5. **show running-config bfd**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface** *int-if*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the ? keyword to display the supported interfaces.

Step 3	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Configures the BFD session parameters for all BFD sessions on the device. This command overrides these values by configuring the BFD session parameters on an interface. The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3. Beginning with Cisco NX-OS Release 9.3(5), configuring BFD session parameters under interface with default timer values using the **bfd interval 50 min_rx 50 multiplier 3** command is functionally equivalent to **no bfd interval** command. Once BFD session parameters under interface are set to default values, those BFD sessions running on that interface will inherit global session parameters, if present.
Step 4	**bfd authentication keyed-sha1 keyid** *id* **key** *ascii_key* **Example:** `switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123`	(Optional) Configures SHA-1 authentication for all BFD sessions on the interface. The *ascii_key* string is a secret key shared among BFD peers. The *id* value, a number between 0 and 255, is assigned to this particular *ascii_key*. BFD packets specify the key by *id*, allowing the use of multiple active keys.

	Command or Action	Purpose
		To disable SHA-1 authentication on the interface, use the **no** form of the command.
Step 5	**show running-config bfd** **Example:** `switch(config-if)# show running-config bfd`	(Optional) Displays the BFD running configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on a Port Channel

You can configure the BFD session parameters for all BFD sessions on a port channel. If per-link mode is used for Layer 3 port channels, BFD creates a session for each link in the port channel and provides an aggregate result to client protocols. For example, if the BFD session for one link on a port channel is up, BFD informs client protocols, such as OSPF, that the port channel is up. The BFD session parameters are negotiated between the BFD peers in a three-way handshake.

This configuration overrides the global session parameters for the configured port channel. The member ports of the port channel inherit the port channel BFD session parameters.

Before you begin

Ensure that you enable LACP on the port channel before you enable BFD.

Ensure that Internet Control Message Protocol (ICMP) redirect messages are disabled on BFD-enabled interfaces. Use the **no ip redirects** command on the interface.

Enable the BFD feature. See the Enabling the BFD Feature section.

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **bfd per-link**
4. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
5. **bfd authentication keyed-sha1 keyid** *id* **key** *ascii_key*
6. **show running-config bfd**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

Step 2	**interface port-channel** *number*
	Example:
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		Enters port-channel configuration mode. Use the **?** keyword to display the supported number range.

Step 3	**bfd per-link** **Example:** `switch(config-if)# bfd per-link`	Configures the BFD sessions for each link in the port channel.
Step 4	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	(Optional) Configures the BFD session parameters for all BFD sessions on the port channel. This command overrides these values by configuring the BFD session parameters. The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 5	**bfd authentication keyed-sha1 keyid** *id* **key** *ascii_key* **Example:** `switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123`	(Optional) Configures SHA-1 authentication for all BFD sessions on the interface. The *ascii_key* string is a secret key shared among BFD peers. The *id* value, a number between 0 and 255, is assigned to this particular *ascii_key*. BFD packets specify the key by *id*, allowing the use of multiple active keys. To disable SHA-1 authentication on the interface, use the **no** form of the command.
Step 6	**show running-config bfd** **Example:** `switch(config-if)# show running-config bfd`	(Optional) Displays the BFD running configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring the BFD Echo Function

You can configure the BFD echo function on one or both ends of a BFD-monitored link. The echo function slows down the required minimum receive interval, based on the configured slow timer. The RequiredMinEchoRx BFD session parameter is not set to zero if the echo function is disabled in compliance with RFC 5880. The slow timer becomes the required minimum receive interval if the echo function is enabled.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section on or the Configuring BFD on an Interface section.

Ensure that Internet Control Message Protocol (ICMP) redirect messages are disabled on BFD-enabled interfaces. Use the **no ip redirects** command on the interface.

Ensure that the IP packet verification check for identical IP source and destination addresses is disabled. Use the **no hardware ip verify address identical** command. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information about this command.

SUMMARY STEPS

1. **configure terminal**
2. **bfd slow-timer** *echo-interval*
3. **interface** *int-if*
4. **bfd echo**
5. **show running-config bfd**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**bfd slow-timer** *echo-interval* **Example:** `switch(config)# bfd slow-timer 2000`	Configures the slow timer used in the echo function. This value determines how fast BFD starts up a new session and is used to slow down the asynchronous sessions when the BFD echo function is enabled. This value overwrites the required minimum receive interval when the echo function is enabled. The range is from 1000 to 30000 milliseconds. The default is 2000.

Step 3	**interface** *int-if*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the ? keyword to display the supported interfaces.

Step 4	**bfd echo** **Example:** `switch(config-if)# bfd echo`	Enables the echo function. The default is enabled.
Step 5	**show running-config bfd** **Example:** `switch(config-if)# show running-config bfd`	(Optional) Displays the BFD running configuration.

	Command or Action	Purpose
Step 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring Per-Member Link BFD Sessions

BFD per-member link support is added on Cisco Nexus 9000 Series switches. See the following sections for more information.

BFD Enhancement to Address Per-link Efficiency

The Bidirectional Forwarding (BFD) enhancement to address per-link efficiency, called as IETF Micro BFD, lets you configure the individual BFD sessions on every Link Aggregation Group (LAG) member interfaces (as defined in RFC 7130).

With this enhancement, the BFD sessions run on each member link of the port-channel. If BFD detects a link failure, the member link is removed from the forwarding table. This mechanism delivers faster failure detection as the BFD sessions are created on an individual port-channel interface.

The BFD sessions running on member links of the port-channel are called as Micro BFD sessions. You can configure RFC 7130 BFD over main port-channel interface, that performs bandwidth monitoring over LAG by having one Micro BFD session over each member. If any of the member port goes down, the port is removed from the forwarding table and this prevents traffic disruption on that member.

Micro BFD sessions are supported for both LACP and non-LACP based-port channels. For more information on how to configure Micro BFD sessions, see *Configuring Micro BFD Sessions*.

Limitations of the IETF Bidirectional Forwarding Detection

See the following limitations of the IETF Bidirectional Forwarding Detection:

- BFD Limitations
  - It cannot co-exist with BFD over logical port-channels or proprietary BFD per-member links. BFD IPv6 logical/proprietary per-link session is also not supported when BFD IETF IPv4 is configured on PC.
  - When you configure logical BFD session under any routing protocol, make sure that is not applied to any IETF port-channel. Having both logical and IETF configuration for same port-channel results in undefined behavior during ISSU/reloads.
  - IETF BFD IPv6 is not supported.
  - Echo functionality is not supported for Micro-BFD sessions.
  - Port-channel interfaces should be directly connected between two switches that are running the BFD sessions. No intermediate Layer 2 switches are expected.

- EthPCM/LACP Limitations

- If a LACP port-channel has members in hot-standby state, BFD failure in one of the active links may not cause the hot-standby link to come up directly. Once the active link with BFD failure goes down, the hot-standby member becomes active. However, it may not be able to prevent the port-channel from going down before the hot-standby link comes up, in cases where port-channel min-link condition is hit.

- General Limitations:
  - It is supported only on Layer 3 port-channels.
  - It is not supported on the following:
    - vPC
    - Layer 3 sub-interfaces
    - Layer 2 port-channels/Layer 2 Fabric Path
    - FPC/HIF PC
    - Layer 3 sub-interfaces
    - SVI over port-channels

Guidelines for Migration/Configuration of IETF Per-Member Sessions:

See the following guidelines for migration/configuration of IETF per-member sessions:

- The logical BFD sessions that are created using the routing protocols over port-channel sub-interfaces (where RFC 7130 cannot run) are still supported. The main port-channel interface however does not support both logical and RFC 7130 sessions that co-exist. It can support only either of them.
- You can configure RFC 7130 BFD over the main port-channel interface that perform bandwidth monitoring over the LAG by having one Micro-BFD session over each member. If any of the member port goes down, BFD notifies it to the port-channel manager that removes the port from the LTL, thereby preventing blackholing of the traffic on that member.
- If the minimum number of links required to have the port-channel operationally *up* is not met in the above case, the port-channel is brought down by the port-channel manager. This in turn brings down the port-channel sub-interfaces if they are configured and thereby the logical BFD session also comes down notifying the routing protocol.
- When you are using RFC 7130 on the main port-channel and logical BFD on the sub-interfaces, the logical BFD session should be run with lesser aggressive timers than the RFC 7130 BFD session. You can have RFC 7130 configured on the port-channel interface or you can have it configured in conjunction with the logical BFD sessions on the port-channel sub-interfaces.
- When a proprietary per-link is configured, enabling IETF Micro-BFD sessions is not allowed on a port channel and vice-versa. You have to remove the proprietary per-link configuration. Current implementation of proprietary per-link does not allow changing the configuration (no per-link), if there is any BFD session that is bootstrapped by the applications. You need to remove the BFD tracking on the respective applications and remove per-link configuration. The migration path from the proprietary per-link to IETF Micro-BFD is as follows:
  - Remove the BFD configuration on the applications.

- Remove the per-link configuration.
- Enable the IETF Micro-BFD command.
- Enable BFD on the applications.

The same migration path can be followed for proprietary BFD to IETF Micro-BFD on the main port-channel interface.

Configuring Port Channel Interface

Before you begin

Ensure that the BFD feature is enabled.

SUMMARY STEPS

1. switch(config)# **interface port-channel** *port-number*
2. switch(config-if)# **no switchport**

DETAILED STEPS

Step 1 switch(config)# **interface port-channel** *port-number*

Configures interface port-channel.

Step 2 switch(config-if)# **no switchport**

Configures interface as Layer 3 port-channel.

What to do next

- Configuring BFD Start Timer
- Enabling IETF Per-link BFD

(Optional) Configuring BFD Start Timer

Complete the following steps to configure the BFD start timer:

SUMMARY STEPS

1. switch(config-if)# **port-channel bfd start** *60*

DETAILED STEPS

switch(config-if)# **port-channel bfd start** *60*

Configures the BFD start timer for a port-channel.

Note The default value is infinite (that is no timer is running). The range of BFD Start Timer value for port-channel is from 60 to 3600 seconds. For start timer to work, configure start timer value before completing the port-channel BFD configurations (that is before port-channel bfd track-member-link and port-channel bfd destination are configured for Layer 3 port-channel interface with the active members).

What to do next

- Enabling IETF Per-link BFD
- Configuring BFD Destination IP Address

Enabling IETF Per-link BFD

SUMMARY STEPS

1. switch(config-if)# **port-channel bfd track-member-link**

DETAILED STEPS

switch(config-if)# **port-channel bfd track-member-link**

Enables IETF BFD on port-channel interface.

What to do next

- Configuring BFD Destination IP Address
- Verifying Micro BFD Session Configurations

Configuring BFD Destination IP Address

Complete the following steps to configure the BFD destination IP address:

SUMMARY STEPS

1. switch(config-if)# **port-channel bfd destination***ip-address*

DETAILED STEPS

switch(config-if)# **port-channel bfd destination***ip-address*

Configures an IPv4 address to be used for the BFD sessions on the member links.

What to do next

- Verifying Micro BFD Sessions Configuration

Verifying Micro BFD Session Configurations

Use the following commands to verify the Micro BFD session configurations.

SUMMARY STEPS

1. Displays the port-channel and port-channel member operational state.
2. switch# **show bfd neighbors**
3. switch# **show bfd neighbors details**
4. switch# **show tech-support bfd**
5. switch# **show tech-support lacp all**
6. switch# **show running-config interface port-channel** *port-channel-number*

DETAILED STEPS

Step 1 Displays the port-channel and port-channel member operational state.

switch# **show port-channel summary**

Step 2 switch# **show bfd neighbors**

Displays Micro BFD sessions on port-channel members.

Step 3 switch# **show bfd neighbors details**

Displays BFD session for a port channel interface and the associated Micro BFD sessions on members.

Step 4 switch# **show tech-support bfd**

Displays the technical support information for BFD.

Step 5 switch# **show tech-support lacp all**

Displays the technical support information for Ethernet Port Manager, Ethernet Port-channel Manager, and LACP.

Step 6 switch# **show running-config interface port-channel** *port-channel-number*

Displays the running configuration information of the port-channel interface.

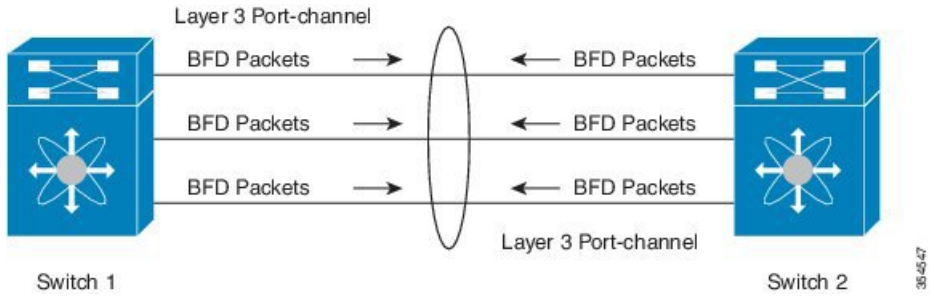
Examples: Configuring Micro BFD Sessions

See the following examples for configuring Micro BFD sessions.

Configuring Micro BFD Sessions

In this example, the following topology is used.

Figure 3: Configuring Micro BFD Session



The sample configuration of switch 1 is as follows:

```
feature bfd
configure terminal
    interface port-channel 10
       port-channel bfd track-member-link
       port-channel bfd destination 10.1.1.2
       port-channel bfd start 60
       ip address 10.1.1.1/24
```

The sample configuration of switch 2 is as follows:

```
feature bfd
configure terminal
     interface port-channel 10
           port-channel bfd track-member-link
           port-channel bfd destination 10.1.1.1
           port-channel bfd start 60
             ip address 10.1.1.2/24
```

Verifying Micro BFD Sessions Configuration

The following example displays the show output of the **show running-config interface port-channel**<*port-channel*>, **show port-channel summary**, **show bfd neighbors vrf internet_routes**, and **show bfd neighbors interface port-channel** <*port-channel*> **vrf internet_routes details** commands.

```
switch# show running-config interface port-channel 1001

!Command: show running-config interface port-channel1001
!Time: Fri Oct 21 09:08:00 2016

version 7.0(3)I5(1)

interface port-channel1001
  no switchport
  vrf member internet_routes
  port-channel bfd track-member-link
  port-channel bfd destination 40.4.1.2
  ip address 40.4.1.1/24
  ipv6 address 2001:40:4:1::1/64

switch# show por
port-channel   port-profile
switch# show port-channel summary
```

```
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1001  Po1001(RU)  Eth      LACP      Eth1/11/1(P)  Eth1/11/2(P)  Eth1/12/1(P)
                                     Eth1/12/2(P)
switch# show bfd neighbors vrf internet_routes

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519041/0          Up              N/A(3)            Up
          Po1001                internet_routes
40.4.1.1        40.4.1.2        1090519042/1090519051 Up              819(3)            Up
          Eth1/12/1             internet_routes
40.4.1.1        40.4.1.2        1090519043/1090519052 Up              819(3)            Up
          Eth1/12/2             internet_routes
40.4.1.1        40.4.1.2        1090519044/1090519053 Up              819(3)            Up
          Eth1/11/1             internet_routes
40.4.1.1        40.4.1.2        1090519045/1090519054 Up              819(3)            Up
          Eth1/11/2             internet_routes
switch#

switch# show bfd neighbors interface port-channel 1001 vrf internet_routes details

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519041/0          Up              N/A(3)            Up
          Po1001                internet_routes

Session state is Up
Local Diag: 0
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 8 secs
Hosting LC: 0, Down reason: None, Reason not-hosted: None
Parent session, please check port channel config for member info
switch#

switch# show bfd neighbors interface ethernet 1/12/1 vrf internet_routes details

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519042/1090519051 Up              604(3)            Up
          Eth1/12/1             internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holdown (hits): 900 ms (0), Hello (hits): 300 ms (458317)
Rx Count: 427188, Rx Interval (ms) min/max/avg: 19/1801/295 last: 295 ms ago
Tx Count: 458317, Tx Interval (ms) min/max/avg: 275/275/275 last: 64 ms ago
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 24 secs
Last packet: Version: 1               - Diagnostic: 0
             State bit: Up            - Demand bit: 0
             Poll bit: 0              - Final bit: 0
```

```
            Multiplier: 3             - Length: 24
            My Discr.: 1090519051     - Your Discr.: 1090519042
            Min tx interval: 300000   - Min rx interval: 300000
            Min Echo interval: 300000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001


switch# show bfd neighbors interface ethernet 1/12/2 vrf internet_routes details

OurAddr         NeighAddr       LD/RD                 RH/RS           Holdown(mult)
State       Int                   Vrf
40.4.1.1        40.4.1.2        1090519043/1090519052 Up              799(3)            Up
          Eth1/12/2             internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holdown (hits): 900 ms (0), Hello (hits): 300 ms (458336)
Rx Count: 427207, Rx Interval (ms) min/max/avg: 19/1668/295 last: 100 ms ago
Tx Count: 458336, Tx Interval (ms) min/max/avg: 275/275/275 last: 251 ms ago
Registered protocols:  eth_port_channel
Uptime: 1 days 11 hrs 4 mins 30 secs
Last packet: Version: 1               - Diagnostic: 0
             State bit: Up            - Demand bit: 0
             Poll bit: 0              - Final bit: 0
             Multiplier: 3            - Length: 24
             My Discr.: 1090519052    - Your Discr.: 1090519043
             Min tx interval: 300000  - Min rx interval: 300000
             Min Echo interval: 300000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001
switch#
```

Configuring BFD Support for Routing Protocols

Configuring BFD on BGP

You can configure BFD for the Border Gateway Protocol (BGP).

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the BGP feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** (*ip-address* | *ipv6-address*) **remote-as** *as-number*

4. **bfd** [**multihop** | **singlehop**]
5. **update-source** *interface*
6. **show running-config bgp**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**router bgp** *as-number*
	Example:
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		Enables BGP and assigns the AS number to the local BGP speaker. The AS number can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format.

Step 3	**neighbor** (*ip-address* | *ipv6-address*) **remote-as** *as-number*
	Example:
	`switch(config-router)# neighbor 209.165.201.1 remote-as 64497`
	`switch(config-router-neighbor)#`
		Configures the IPv4 or IPv6 address and AS number for a remote BGP peer. The *ip-address* format is x.x.x.x. The *ipv6-address* format is A:B::C:D.

Step 4	**bfd** [**multihop** | **singlehop**] **Example:** `switch(config-router-neighbor)# bfd multiihop`	Configures the BFD multi hop or single hop session on the device. The default is with no keyword. When you do not specify any keyword and if the peer is directly connected then a single hop session is selected, if the peer is not connected then a multi hop session type is selected. When you specify a "multihop" or "singlehop" option, the session type is forced in a device according to the CLI option.
Step 5	**update-source** *interface* **Example:** `switch(config-router-neighbor)# update-source ethernet 2/1`	Allows BGP sessions to use the primary IP address from a particular interface as the local address when forming a BGP session with a neighbor and enables BGP to register as a client with BFD.
Step 6	**show running-config bgp** **Example:** `switch(config-router-neighbor)# show running-config bgp`	(Optional) Displays the BGP running configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config-router-neighbor)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on EIGRP

You can configure BFD for the Enhanced Interior Gateway Routing Protocol (EIGRP).

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the EIGRP feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **router eigrp** *instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface** *int-if*
5. **ip eigrp** *instance-tag* **bfd**
6. **show ip eigrp** [**vrf** *vrf-name*] [**interfaces** *if*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**router eigrp** *instance-tag*
	Example:
	`switch(config)# router eigrp Test1`
	`switch(config-router)#`
		Creates a new EIGRP process with the configured instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
		If you configure an instance-tag that does not qualify as an AS number, you must use the **autonomous-system** to configure the AS number explicitly or this EIGRP instance will remain in the shutdown state.

Step 3	**bfd** [**ipv4**	**ipv6**] **Example:** `switch(config-router-neighbor)# bfd ipv4`	(Optional) Enables BFD for all EIGRP interfaces.

Step 4	**interface** *int-if*
	Example:
	`switch(config-router-neighbor)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

	Command or Action	Purpose
Step 5	**ip eigrp** *instance-tag* **bfd** **Example:** `switch(config-if)# ip eigrp Test1 bfd`	(Optional) Enables or disables BFD on an EIGRP interface. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters. The default is disabled.
Step 6	**show ip eigrp** [**vrf** *vrf-name*] [**interfaces** *if*] **Example:** `switch(config-if)# show ip eigrp`	(Optional) Displays information about EIGRP. The *vrf-name* can be any case-sensitive, alphanumeric string up to 32 characters.
Step 7	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on OSPF

You can configure BFD for the Open Shortest Path First.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the OSPF feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **router ospf** *instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface** *int-if*
5. **ip ospf bfd**
6. **show ip ospf** [**vrf** *vrf-name*] [**interfaces** *if*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**router ospf** *instance-tag*
	Example:
	`switch(config)# router ospf 200`
	`switch(config-router)#`
		Creates a new OSPF instance with the configured instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.

Step 3	**bfd** [**ipv4** | **ipv6**] **Example:** `switch(config-router)# bfd`	(Optional) Enables BFD for all OSPF interfaces.

Step 4	**interface** *int-if*
	Example:
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

Step 5	**ip ospf bfd** **Example:** `switch(config-if)# ip ospf bfd`	(Optional) Enables or disables BFD on an OSPF interface. The default is disabled.
Step 6	**show ip ospf** [**vrf** *vrf-name*] [**interfaces** *if*] **Example:** `switch(config-if)# show ip ospf`	(Optional) Displays information about OSPF. The *vrf-name* can be any case-sensitive, alphanumeric string up to 32 characters.
Step 7	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Example Configurations for BFD on OSPF

Example configuration where BFD is enabled under a non-default VRF (OSPFv3 neighbors in vrf3).

```
configure terminal
  router ospfv3 10
    vrf vrf3
    bfd
```

Configuring BFD on IS-IS

You can configure BFD for the Intermediate System-to-Intermediate System (IS-IS) protocol.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the IS-IS feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **router isis** *instance-tag*
3. **bfd** [**ipv4** | **ipv6**]
4. **interface** *int-if*
5. **isis bfd**
6. **show isis** [**vrf** *vrf-name*] [**interface** *if*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**router isis** *instance-tag*
	Example:
	`switch(config)# router isis 100`
	`switch(config-router)# net 49.0001.1720.1600.1001.00`
	`switch(config-router)# address-family ipv6 unicast`
		Creates a new IS-IS instance with the configured *instance tag*.

Step 3	**bfd** [**ipv4**	**ipv6**] **Example:** `switch(config-router)# bfd`	(Optional) Enables BFD for all OSPF interfaces.

Step 4	**interface** *int-if*
	Example:
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

Step 5	**isis bfd** **Example:** `switch(config-if)# isis bfd`	(Optional) Enables or disables BFD on an IS-IS interface. The default is disabled.
Step 6	**show isis** [**vrf** *vrf-name*] [**interface** *if*] **Example:** `switch(config-if)# show isis`	(Optional) Displays information about IS-IS. The *vrf-name* can be any case-sensitive, alphanumeric string up to 32 characters.

	Command or Action	Purpose
Step 7	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Example Configurations for BFD on IS-IS

Example configuration for IS-IS where BFD is enabled under IPv4 and an IPv6 address family.

```
configure terminal
  router isis isis-1
    bfd
    address-family ipv6 unicast
    bfd
```

Configuring BFD on HSRP

You can configure BFD for the Hot Standby Router Protocol (HSRP). The active and standby HSRP routers track each other through BFD. If BFD on the standby HSRP router detects that the active HSRP router is down, the standby HSRP router treats this event as an active time rexpiry and takes over as the active HSRP router.

The **show hsrp detail** command shows this event as BFD@Act-down or BFD@Sby-down.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the HSRP feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **hsrp bfd all-interfaces**
3. **interface** *int-if*
4. **hsrp bfd**
5. **show running-config hsrp**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**hsrp bfd all-interfaces** **Example:** `switch# hsrp bfd all-interfaces`	(Optional) Enables or disables BFD on all HSRP interfaces. The default is disabled.

Step 3	**interface** *int-if*
	Example:
	`switch(config-router)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

Step 4	**hsrp bfd** **Example:** `switch(config-if)# hsrp bfd`	(Optional) Enables or disables BFD on an HSRP interface. The default is disabled.
Step 5	**show running-config hsrp** **Example:** `switch(config-if)# show running-config hsrp`	(Optional) Displays the HSRP running configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on VRRP

You can configure BFD for the Virtual Router Redundancy Protocol (VRRP). The active and standby VRRP routers track each other through BFD. If BFD on the standby VRRP router detects that the active VRRP router is down, the standby VRRP router treats this event as an active time rexpiry and takes over as the active VRRP router.

The **show vrrp detail** command shows this event as BFD@Act-down or BFD@Sby-down.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Configure the BFD session parameters. See the Configuring Global BFD Parameters section or the Configuring BFD on an Interface section.

Enable the VRRP feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *int-if*
3. **vrrp** *group-no*
4. **vrrp bfd** *address*
5. **show running-config vrrp**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *int-if*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

Step 3	**vrrp** *group-no* **Example:** `switch(config-if)# vrrp 2`	Specifies the VRRP group number.
Step 4	**vrrp bfd** *address* **Example:** `switch(config-if)# vrrp bfd`	Enables or disables BFD on a VRRP interface. The default is disabled.
Step 5	**show running-config vrrp** **Example:** `switch(config-if)# show running-config vrrp`	(Optional) Displays the VRRP running configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on PIM

You can configure BFD for the Protocol Independent Multicast (PIM) protocol.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

Enable the PIM feature. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information.

SUMMARY STEPS

1. **configure terminal**
2. **ip pim bfd**
3. **interface** *int-if*
4. **ip pim bfd-instance** [**disable**]
5. **show running-config pim**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim bfd** **Example:** `switch(config)# ip pim bfd`	Enables BFD for PIM.

Step 3	**interface** *int-if*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.

Step 4	**ip pim bfd-instance** [**disable**] **Example:** `switch(config-if)# ip pim bfd-instance`	(Optional) Enables or disables BFD on a PIM interface. The default is disabled.
Step 5	**show running-config pim** **Example:** `switch(config)# show running-config pim`	(Optional) Displays the PIM running configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuring BFD on Static Routes

You can configure BFD for static routes on an interface. You can optionally configure BFD on a static route within a virtual routing and forwarding (VRF) instance.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip route** *route interface* {*nh-address* | *nh-prefix*}
4. **ip route static bfd** *interface* {*nh-address* | *nh-prefix*}
5. **show ip route static** [**vrf** *vrf-name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**vrf context** *vrf-name*
	Example:
	`switch(config)# vrf context Red`
	`switch(config-vrf)#`
		(Optional) Enters VRF configuration mode.

Step 3	**ip route** *route interface* {*nh-address*	*nh-prefix*} **Example:** `switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4`	Creates a static route Use the **?** keyword to display the supported interfaces.
Step 4	**ip route static bfd** *interface* {*nh-address*	*nh-prefix*} **Example:** `switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4`	Enables BFD for all static routes on an interface. Use the**?** keyword to display the supported interfaces.
Step 5	**show ip route static** [**vrf** *vrf-name*] **Example:** `switch(config-vrf)# show ip route static vrf Red`	(Optional) Displays the static routes.
Step 6	**copy running-config startup-config** **Example:** `switch(config-vrf)# copy running-config startup-config`	(Optional) Saves the configuration change.

Disabling BFD on an Interface

You can selectively disable BFD on an interface for a routing protocol that has BFD enabled at the global or VRF level.

To disable BFD on an interface, use one of the following commands in interface configuration mode:

Command	Purpose
ip eigrp *instance-tag* **bfd disable** **Example:** `switch(config-if)# ip eigrp Test1 bfd disable`	Disables BFD on an EIGRP interface. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
ip ospf bfd disable **Example:** `switch(config-if)# ip ospf bfd disable`	Disables BFD on an OSPFv2 interface.
isis bfd disable **Example:** `switch(config-if)# isis bfd disable`	Disables BFD on an IS-IS interface.

Disabling BFD on an Interface

Example configuration where BFD is disabled per interface.

```
configure terminal
  interface port-channel 10
    no ip redirects
    ip address 22.1.10.1/30
    ipv6 address 22:1:10::1/120
    no ipv6 redirects
    ip router ospf 10 area 0.0.0.0
    ip ospf bfd disable        /*** disables IPv4 BFD session for OSPF
    ospfv3 bfd disable         /*** disables IPv6 BFD session for OSPFv3
```

Configuring BFD Interoperability

Configuring BFD Interoperability in Cisco NX-OS Devices in a Point-to-Point Link

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *int-if*
3. **ip ospf bfd**
4. **no ip redirects**

5. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface port-channel** *int-if* **Example:** `switch(config-if)# interface ethernet 2/1`	Enters interface configuration mode. Use the **?** keyword to display the supported interfaces.
Step 3	**ip ospf bfd** **Example:** `switch(config-if)# ip ospf bfd`	Enables BFD on an OSPFv2 interface. The default is disabled. OSPF is used as an example. You can enable BFD of any of the supported protocols.
Step 4	**no ip redirects** **Example:** `switch(config-if)# no ip redirects`	Prevents the device from sending redirects.
Step 5	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Configures the BFD session parameters for all BFD sessions on the port channel. This command overrides these values by configuring the BFD session parameters. The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 6	**exit** **Example:** `switch(config-if)# exit`	Exits interface configuration mode and returns to EXEC mode.

Configuring BFD Interoperability in Cisco NX-OS Devices in a Switch Virtual Interface

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *vlan vlan-id*
3. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
4. **no ip redirects**
5. **ip address** *ip-address/length*
6. **ip ospf bfd**

7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface port-channel** *vlan vlan-id*
	Example:
	`switch(config)# interface vlan 998`
	`switch(config-if)#`
		Creates a dynamic Switch Virtual Interface (SVI).

Step 3	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Configures the BFD session parameters for all BFD sessions on the device. The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 4	**no ip redirects** **Example:** `switch(config-if)# no ip redirects`	Prevents the device from sending redirects.
Step 5	**ip address** *ip-address/length* **Example:** `switch(config-if)# ip address 10.1.0.253/24`	Configures an IP address for this interface.
Step 6	**ip ospf bfd** **Example:** `switch(config-if)# ip ospf bfd`	Enables BFD on an OSPFv2 interface. The default is disabled.
Step 7	**exit** **Example:** `switch(config-if)# exit`	Exits interface configuration mode and returns to EXEC mode.

Configuring BFD Interoperability in Cisco NX-OS Devices in Logical Mode

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *type number.subinterface-id*
3. **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value*
4. **no ip redirects**
5. **ip ospf bfd**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface port-channel** *type number.subinterface-id* **Example:** `switch(config-if)# interface port-channel 50.2`	Enters port channel configuration mode. Use the **?** keyword to display the supported number range.
Step 3	**bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Configures the BFD session parameters for all BFD sessions on the port channel. The *mintx* and *msec* range is from 50 to 999 milliseconds and the default is 50. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 4	**no ip redirects** **Example:** `switch(config-if)# no ip redirects`	Prevents the device from sending redirects.
Step 5	**ip ospf bfd** **Example:** `switch(config-if)# ip ospf bfd`	Enables BFD on an OSPFv2 interface. The default is disabled. OSPF is used as an example. You can enable BFD of any of the supported protocols.
Step 6	**exit** **Example:** `switch(config-if)# exit`	Exits interface configuration mode and returns to EXEC mode.

Verifying BFD Interoperability in a Cisco Nexus 9000 Series Device

The following example shows how to verify BFD interoperability in a Cisco Nexus 9000 Series device.

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.1.1.1 10.1.1.2 1140850707/2147418093 Up 6393(4) Up Vlan2121
default
Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 4
Holdown (hits): 8000 ms (0), Hello (hits): 2000 ms (108)
Rx Count: 92, Rx Interval (ms) min/max/avg: 347/1996/1776 last: 1606 ms ago
Tx Count: 108, Tx Interval (ms) min/max/avg: 1515/1515/1515 last: 1233 ms ago
Registered protocols: ospf
Uptime: 0 days 0 hrs 2 mins 44 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
```

```
Poll bit: 0 - Final bit: 0
Multiplier: 4 - Length: 24
My Discr.: 2147418093 - Your Discr.: 1140850707
Min tx interval: 2000000 - Min rx interval: 2000000
Min Echo interval: 1000 - Authentication bit: 0
Hosting LC: 10, Down reason: None, Reason not-hosted: None


switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
Vrf
10.0.2.1 10.0.2.2 1140850695/131083 Up 270(3) Up Po14.121
default
Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
Received MinRxInt: 100000 us, Received Multiplier: 3
Holdown (hits): 300 ms (0), Hello (hits): 100 ms (3136283)
Rx Count: 2669290, Rx Interval (ms) min/max/avg: 12/1999/93 last: 29 ms ago
Tx Count: 3136283, Tx Interval (ms) min/max/avg: 77/77/77 last: 76 ms ago
Registered protocols: ospf
Uptime: 2 days 21 hrs 41 mins 45 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 131083 - Your Discr.: 1140850695
Min tx interval: 100000 - Min rx interval: 100000
Min Echo interval: 0 - Authentication bit: 0
Hosting LC: 8, Down reason: None, Reason not-hosted: None
```

Verifying the BFD Configuration

To display BFD configuration information, perform one of the following:

Command	Purpose
show running-config bfd	Displays the running BFD configuration.
show startup-config bfd	Displays the BFD configuration that will be applied on the next system startup.

Monitoring BFD

Use the following commands to display BFD:

Command	Purpose
show bfd neighbors [**application** *name*] [**details**]	Displays information about BFD for a supported application, such as BGP or OSPFv2.
show bfd neighbors [**interface** *int-if*] [**details**]	Displays information about BGP sessions on an interface.

Command	Purpose
show bfd neighbors [**dest-ip** *ip-address*] [**src-ip** *ip-address*][**details**]	Displays information about the specified BGP session on an interface.
show bfd neighbors [**vrf** *vrf-name*] [**details**]	Displays information about BFD for a VRF.
show bfd [**ipv4** | **ipv6**] [**neighbors**]	Displays information about IPv4 neighbors or IPv6 neighbors.

BFD Multihop

BFD multihop for IPv4 and BFD multihop for IPv6 are supported in compliance with RFC5883. BFD multihop sessions are set up between a unique source and destination address pair. A multihop BFD session is associated with the link between a source and destination rather than with an interface, as with single-hop BFD sessions.

BFD Multihop Number of Hops

BFD multihop sets the TTL field to the maximum limit, and it does not check the value on reception. The BFD code has no impact on the number of hops a BFD multihop packet can traverse. However, in most of the systems, it limits the number of hops to 255.

Guidelines and Limitations for BFD Multihop

BFD multihop has the following configuration guidelines and limitations:

- Beginning with Cisco NX-OS Release 9.3(6), BFD multihop is only supported in BGP IPv4 on Cisco Nexus 9200, 9300-EX/FX/GX platform switches and Cisco Nexus 9500 platform switches with N9K-X9700-EX line cards.
- In a dynamic BGP configuration, both the single and multihop BGP peers accepts BFD multihop configuration.
- BFD multihop is only supported with BGP.
- BFD multihop is supported for BGP IPv6 multihop neighbors on the following devices:
  - Cisco Nexus 9200YC-X, 9300-EX, 9300-FX and 9300-GX switches
  - Cisco Nexus 9500 platform switches with N9K-X9736C-EX, N9K-X97160YC-EX, N9K-X9732C-EX, N9K-X9732C-EXM, or N9K-X9736C-FX line cards

Note You must enable the **system routing template-mpls-heavy** command in order to use BFD multihop for BGP IPv6 with Cisco Nexus 9500 platform switches with -EX and -FX line cards.

- Multihop BFD is identified with UDP Destination port 4784.
- The default interval timer for multihop BFD is 250 ms with multiplier 3.

- The maximum number of supported multihop BFD sessions is 100.
- Existing BFD authentication support is extended for multihop sessions.
- Echo mode is not supported for multihop BFD.
- Multihop with segment routing underlay is not supported.
- On unsupported platforms, BFD commands are accepted when configuring BGPv6 multihop neighbors. However, the sessions will not be created or installed.
- When Multihop BFD session is installed in port-channel, the following points must be taken care:
  - If all the sessions are hosted on a single line card of Cisco Nexus 9500 family switches, during reloading of hosted line cards all the sessions will be hosted on another line card. BFD and BGP sessions may flap in this case.
  - Multihop BFD session for BGP over cross modules port-channel doesn't provide full redundancy.

Configuring BFD Multihop Session Global Interval Parameters

You can configure the BFD session global parameters for all BFD sessions on the device. Different BFD session parameters for each session can be achieved using the per session configuration commands .

Before you begin

Enable the BFD feature.

SUMMARY STEPS

1. **configure terminal**
2. **[no] bfd multihop interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
3. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**[no] bfd multihop interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `switch(config)# bfd multihop interval 250 min_rx 250 multiplier 3`	Configures the BFD multihop session global parameters for all BFD sessions on the device. This command overrides the default values. The *Required Minimum Receive Interval* and *Desired Minimum Transmit Interval* are 250. The multiplier default is 3.
Step 3	**end** **Example:** `switch(config)# end`	Saves the configuration change and ends the configuration session.

Configuring Per Multihop Session BFD Parameters

You can configure per multihop session BFD parameters.

Before you begin

Enable the BFD feature. See the Enabling the BFD Feature section.

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** (*ip-address* | *ipv6-address*) **remote-as** *as-number*
4. **update-source** *interface*
5. **bfd**
6. **bfd multihop interval** *mintx* **min_rx** *msec* **multiplier** *value*
7. **bfd multihop authentication keyed-sha1 keyid** *id* **key** *ascii_key*
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**router bgp** *as-number*
	Example:
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		Enables BGP and assigns the AS number to the local BGP speaker. The AS number can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format.

Step 3	**neighbor** (*ip-address* | *ipv6-address*) **remote-as** *as-number*
	Example:
	`switch(config-router)# neighbor 209.165.201.1 remote-as 64497`
	`switch(config-router-neighbor)#`
		Configures the IPv4 or IPv6 address and AS number for a remote BGP peer. The *ip-address* format is x.x.x.x. The *ipv6-address* format is A:B::C:D.

Step 4	**update-source** *interface*
	Example:
	`switch(config-router-neighbor)# update-source Ethernet1/4`
	`switch(config-router-neighbor)#`
		Retrieves the source IP address of the BFD session from the interface.

Step 5	**bfd** **Example:** `switch(config-router-neighbor)# bfd multihop`	Enables BFD for this BGP peer.

	Command or Action	Purpose
Step 6	**bfd multihop interval** *mintx* **min_rx** *msec* **multiplier** *value* **Example:** `switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 3`	Configures Multihop BFD interval values for this neighbor. The *mintx* and *msec* range is from 250 to 999 milliseconds and the default is 250. The multiplier range is from 1 to 50. The multiplier default is 3.
Step 7	**bfd multihop authentication keyed-sha1 keyid** *id* **key** *ascii_key* **Example:** `switch(config-router-neighbor)# bfd multihop authentication keyed-sha1 keyid 1 ascii_key cisco123`	(Optional) Configures SHA-1 authentication for BFDs on Multihop BFD session over this neighbor. The *ascii_key* string is a secret key shared among BFD peers. The *id* value, a number between 0 and 255, is assigned to this particular *ascii_key*. BFD packets specify the key by *id*, allowing the use of multiple active keys. To disable SHA-1 authentication on the interface, use the **no** form of the command.
Step 8	**copy running-config startup-config** **Example:** `switch(config-router-neighbor)# copy running-config startup-config`	(Optional) Saves the configuration change.

Configuration Examples for BFD

This example shows how to configure BFD for OSPFv2 on Ethernet 2/1, using the default BFD session parameters:

```
feature bfd
feature ospf
router ospf Test1
interface ethernet 2/1
ip ospf bfd
no shutdown
```

This example shows how to configure BFD for all EIGRP interfaces, using the default BFD session parameters:

```
feature bfd
feature eigrp
bfd interval 100 min_rx 100 multiplier 4
router eigrp Test2
bfd
```

This example shows how to configure BFDv6:

```
feature bfd
feature ospfv3
router ospfv3 Test1
interface Ethernet2/7
  ipv6 router ospfv3 Test1 area 0.0.0.0
  ospfv3 bfd
```

```
  no shutdown
```

Show Example for BFD

This example shows results of the **show bfd ipv6 neighbors details** command.

```
#show bfd ipv6 neighbors details

OurAddr                           NeighAddr
 LD/RD                 RH/RS           Holdown(mult)     State       Int
 Vrf
cc:10::2                          cc:10::1
 1090519335/1090519260 Up              5692(3)           Up          Po1
 default


Session state is Up and using echo function with 250 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 250000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 3
Holdown (hits): 6000 ms (4), Hello (hits): 2000 ms (205229)
Rx Count: 227965, Rx Interval (ms) min/max/avg: 124/1520/1510 last: 307 ms ago
Tx Count: 205229, Tx Interval (ms) min/max/avg: 1677/1677/1677 last: 587 ms ago
Registered protocols:  bgp
Uptime: 3 days 23 hrs 31 mins 13 secs
Last packet: Version: 1               - Diagnostic: 0
             State bit: Up            - Demand bit: 0
             Poll bit: 0              - Final bit: 0
             Multiplier: 3            - Length: 24
             My Discr.: 1090519260    - Your Discr.: 1090519335
             Min tx interval: 250000  - Min rx interval: 2000000
             Min Echo interval: 250000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
```

Related Documents

Related Topic	Document Title
BFD commands	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*

RFCs

RFC	Title
RFC 5880	*Bidirectional Forwarding Detection (BFD)*
RFC 5881	*BFD for IPv4 and IPv6 (Single Hop)*
RFC 7130	*Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*