CHAPTER 18

SSO-BFD

To establish alternative paths, networking equipment are designed to rapidly detect communication failures between adjacent systems. The Bidirectional Forwarding Detection (BFD) protocol detects failures that occur for short durations in the path between adjacent forwarding engines. BFD is a protocol that help the underlying networking protocols to detect failures in the forwarding path.

The stateful switchover (SSO)-BFD feature helps achieve high resiliency and availability by allowing peer switches to start communicating, upon supervisor switchover. This is a high-availability feature that can be used to mitigate the impact of both planned and unplanned supervisor switchover in a system by minimizing network disruption.

This SSO-BFD feature is described in the following topics:

Feature History of SSO-BFD

Cisco IOS Release	Description	Required PRE
12.2(33)XNE	This feature was introduced in the Cisco 10000 series routers	PRE3 and PRE4

Information about SSO-BFD

Network deployments have dual route processor (RP) routers and switches to provide redundancy. These routers have a graceful restart mechanism that protects the forwarding state across switchovers. These dual RP platforms have varying switchover times depending on the hardware that can detect failure and propagate it. When the BFD protocol runs on the RP, certain platforms, called fast switchover platforms, are able to detect a switchover before the BFD protocol times out. However, certain platforms, called slow switchover platforms, are unable to detect a switchover before the BFD protocol times out. The Cisco 10000 series router is a slow switchover platform. For the BFD protocol to maintain the up state

across a switchover, the Cisco 10000 series router needs the addition of SSO support for the BFD protocol. With this addition, a planned or an unplanned switchover does not result in the peer router declaring a failure in the forwarding path.

For configuring the SSO-BFD feature, see the How to Configure Bidirectional Forwarding Detection section in the *Bidirectional Forwarding Detection* guide at the following link:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html#wp1054190

The SSO-BFD feature is dependent on the following three modules for its execution.

- Enhanced Timers
- BFD HA Process
- Early Packet Send

Enhanced Timers

After the switchover on the active RP, the BFD protocol needs a periodic signal to continue sending packets to its peer router in the absence of its pseudo preemptive process. The enhanced timers infrastructure sends the BFD protocol packets until the RP is completely active. This infrastructure allows the clients to register to it, and specify the interval at which the clients are to be called. The enhanced timers infrastructure runs until the control plane on the Cisco 10000 series router comes up which can take upto 17 seconds. After the control plane is operational, the BFD protocol deregisters from the enhanced timers infrastructure and spawns its own pseudo preemptive process.

The enhanced timers infrastructure is a mechanism for the BFD protocol to perform the add or register, and callback or notification functions that are invoked at regular intervals. The callback or notification function starts when the data path is established and packets can be transmitted out of an interface.

BFD HA Process

The BFD High Availability (HA) process is a platform-independent effort for the SSO-BFD feature to enhance the BFD protocol to be stateful. The BFD HA process maintains sessions on the standby RP, if those sessions are in the up state. After the switchover, the process on the newly active RP begin to transmit the BFD packets. The BFD clients need to create or reclaim those sessions after the standby RP becomes active. The BFD HA process starts a timer for reclaiming sessions after switchover, and any session that is not reclaimed before the timer expires is deleted.

Early Packet Send

The early packet send routine is specific to the Cisco 10000 series router, and takes care of the BFD protocol. It sends keep-alive packets using the data plane, before the control plane is up. Therefore, when the standby RP is signaled of a switchover and becomes active, the active RP performs platform-specific tasks and brings up the enhanced timers infrastructure. At regular time intervals, this infrastructure invokes the BFD protocol that sends keep-alive packets. At this stage, the Interface Descriptor Block (IDB) state on newly active RP is not up; so, it is not possible to send packets out through the Cisco Express Forwarding (CEF) path that is normally used by the BFD protocol. As a result, the platform provides a specific send path to the BFD protocol until the CEF path is able to send packets out. When the CEF path is able to send packets, the BFD protocol deregisters from the enhanced timers infrastructure, spawns its own pseudo preemptive process, and uses the CEF path for sending and receiving packets.

The following line cards support the early packet send routine:

- 1-port Channelized OC12 line card.
- 4-port channelized OC3/STM-1 line card.
- Half-height Gigabit Ethernet line card.
- Asynchronous Transfer Mode (ATM) line cards.

To summarize the three modules, the sequence of steps before and after a switchover is as follows:

1. The BFD protocol checkpoint the sessions on the standby RP, and retain these sessions until the sessions on the active RP are down or deleted. Checkpointing of sessions happen before the switchover occurs. This is a continuous process each time a session comes up. The BFD protocol registers with the enhanced timers infrastructure; the interval, at which the protocol is invoked by the enhanced timers infrastructure, is specified depending on platform limitations.
2. When a planned or unplanned switchover event occurs, the standby RP is notified by the platform. When the data plane on the standby RP is activated, it activates the enhanced timers infrastructure.
3. When the enhanced timers infrastructure is activated, the BFD process is invoked on the new active RP. The BFD process goes through the queue of active sessions and sends packets using the early packet send platform-specific path.
4. The enhanced timers infrastructure signals its registered client to send the next set of packets, at regular intervals that is set earlier. This process continues until the control plane on the new active RP is activated and the BFD protocol receives the RF_PROG_ACTIVE_FAST event. Once that occurs, the BFD spawns its own pseudo preemptive process. The BFD protocol does not start the detect timers and echo timers for sessions, when its starts receiving packets. If it has not received packets from peer routers, the sessions begin to timeout.

Note The BFD control packets are sent when the platform starts receiving the BFD packets from peer routers.

Restrictions of SSO-BFD

The SSO-BFD feature has the following restrictions:

- The timeout interval on PRE2 is slightly higher than PRE4 and PRE4, and can offset the utility of BFD per session. The SSO-BFD feature is not supported on PRE2.
- The Cisco 10000 series router needs about 1.6 seconds for packet express forwarder (PXF) to loop the echo packets again after switchover.
- In an non-Echo mode, when the ISSU is issued with minimum disruption, in about 700ms, the BFD sessions resumes sending packets.
- No error messages are displayed, if the user configures a timer lower than that can be supported for the SSO-BFD feature in the Cisco 10000 series router.
- If there is a link failure at the same time when a switchover occurs, there will be a delay in detecting the forwarding failure on the local router that has just gone through a switchover. The platform cannot receive packets during the delta time when the control plane has not come up.
- When the BFD detection time is configured greater or equal to 5 seconds, the maximum number of BFD HA sessions that the Cisco 10000 series router can support is 1100.

Monitoring and Maintaining SSO-BFD

The BFD packets are dropped if there is a problem on the link and the BFD signals its client. A corresponding action occurs to bring down the feature. However, during a switchover, if the peer router goes down, the router undergoing the switchover detects the failure when the CEF path comes up.

To monitor and maintain the SSO-BFD feature, enter any of the following commands in privileged EXEC mode:

Command	Purpose
Router# **show enhanced-timers**	Displays status of the values set on the timers. This command is used on the standby PRE.
Router# **show bfd neighbour detail**	Displays complete details of the BFD neighbor including the routing protocol registered with it. This command is used on the active PRE.
Router# **debug bfd ha**	Displays logs specific to the BFD HA process. The command can also be used to check whether there is a failure in transmission of BFD packets during a switchover causing the peer router to detect a failure. This command can be enabled on the standby PRE also.
Router# **debug bfd event**	Checks for packets received or lost from the router undergoing a switchover.
Router# **debug bfd packet**	Checks whether the router undergoing a switchover failed to transmit BFD packets.

Configuration Examples of SSO-BFD

This section explains the following configuration examples:

- SSO-BFD with Static: Example, page 18-73
- SSO-BFD with BGP: Example, page 18-75
- SSO-BFD with EIGRP: Example, page 18-79
- SSO-BFD with ISIS: Example, page 18-82
- SSO-BFD with OSPF: Example, page 18-84

Note The following BFD timers are supported for the SSO-BFD feature:

- bfd interval 999 min_rx 999 multiplier 5
- bfd interval 999 min_rx 999 multiplier 6
- bfd interval 500 min_rx 500 multiplier 8

Note The [**no**] **bfd echo** command is configured to enable or disable the echo mode. When the echo mode is enabled, the **no ip redirect** command must be configured under interfaces that are enabled with the BFD protocol.

SSO-BFD with Static: Example

Example 18-1 and Example 18-2 show the configuration example of the SSO-BFD feature with a static client in a VPN scenario:

Example 18-1 SSO-BFD with a Static Client on the CE1 Router

CE1

```
interface GigabitEthernet1/1/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip address 20.1.1.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface GigabitEthernet1/1/0.5
 no ip redirect
 encapsulation dot1q 105
 ip address 20.1.5.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface ATM4/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip address 20.1.2.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
interface serial5/0/0/1:1
 ip address 20.1.4.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
ip route static bfd GigabitEthernet1/1/0.1 20.1.1.2
ip route static bfd ATM4/0/0.1 20.1.2.2
ip route static bfd serial5/0/0/1:1 20.1.4.2
ip route static bfd GigabitEthernet1/1/0.5 20.1.5.2
!
ip route 10.1.1.0 255.255.255.0 GigabitEthernet1/1/0.1 20.1.1.2
ip route 10.1.2.0 255.255.255.0 ATM4/0/0.1 20.1.2.2
ip route 10.1.4.0 255.255.255.0 serial5/0/0/1:1 20.1.4.2
ip route 10.1.5.0 255.255.255.0 GigabitEthernet1/1/0.5 20.1.5.2
!
end
```

Example 18-2 SSO-BFD with a Static Client on the PE1 Router

PE1

```
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet2/0/0
 ip address 50.0.0.1 255.0.0.0
```

```
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
!
router ospf 50
 router-id 1.1.1.1
 log-adjacency-changes
 nsf ietf
 network 1.1.1.1 0.0.0.0 area 0
 network 50.0.0.0 0.255.255.255 area 0
!
mpls ldp router-id Loopback0 force
!
 ip vrf vpn1001
  rd 75:1001
  route-target export 75:1001
  route-target import 75:1001
 !
 ip vrf vpn1002
  rd 75:1002
  route-target export 75:1002
  route-target import 75:1002
 !
 ip vrf vpn1004
  rd 75:1004
  route-target export 75:1004
  route-target import 75:1004
 !
 ip vrf vpn1005
  rd 75:1005
  route-target export 75:1005
  route-target import 75:1005
 !
 interface GigabitEthernet1/0/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip vrf forwarding vpn1001
 ip address 20.1.1.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
 interface GigabitEthernet1/0/0.5
 no ip redirect
 encapsulation dot1q 105
 ip vrf forwarding vpn1005
 ip address 20.1.5.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
 interface ATM8/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip vrf forwarding vpn1002
 ip address 20.1.2.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
interface serial5/0/0/1:1
 ip vrf forwarding vpn1004
 ip address 20.1.4.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
```

```
 !
ip route static bfd GigabitEthernet1/0/0.1 20.1.1.1
ip route static bfd ATM4/0/0.1 20.1.2.1
ip route static bfd serial5/0/0/1:1 20.1.4.1
ip route static bfd GigabitEthernet1/0/0.5 20.1.5.1
!
ip route vrf vpn1001 20.1.1.0 255.255.255.0 GigabitEthernet1/0/0.1 20.1.1.1
ip route vrf vpn1002 20.1.2.0 255.255.255.0 ATM4/0/0.1 20.1.2.1
ip route vrf vpn1004 20.1.4.0 255.255.255.0 serial5/0/0/1:1 20.1.4.1
ip route vrf vpn1005 20.1.5.0 255.255.255.0 GigabitEthernet1/0/0.5 20.1.5.1
!
router bgp 75
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 2.2.2.2 remote-as 75
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  redistribute connected
  neighbor 2.2.2.2 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
address-family ipv4 vrf vpn1001
redistribute static
redistribute connected
exit-address-family
 !
address-family ipv4 vrf vpn1002
redistribute static
redistribute connected
exit-address-family
 !
address-family ipv4 vrf vpn1004
redistribute static
redistribute connected
 !
address-family ipv4 vrf vpn1005
redistribute static
redistribute connected
!
end
```

SSO-BFD with BGP: Example

Example 18-3 and Example 18-4 show the configuration example of the SSO-BFD feature with the Border Gateway Protocol (BGP) client in a VPN scenario:

Example 18-3 SSO-BFD with a BGP Client on the CE1 Router

CE1:

```
interface GigabitEthernet1/1/0.1
  no ip redirect
 encapsulation dot1Q 1001 second-dot1q 500
 ip address 20.1.1.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface GigabitEthernet1/1/0.2
 no ip redirect
 encapsulation dot1Q 1002
 ip address 20.1.2.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface ATM4/0/0.1 point-to-point
 no ip redirect
 ip address 20.1.3.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 pvc 1/100
  encapsulation aal5snap
 !
interface Serial5/0/0/1:1
 no ip redirect
 ip address 20.1.4.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
router bgp 71
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 network 30.1.1.0 mask 255.255.255.0
 neighbor 20.1.1.2 remote-as 75
 neighbor 20.1.1.2 ha-mode sso
 neighbor 20.1.1.2 fall-over bfd
 neighbor 20.1.2.2 remote-as 75
 neighbor 20.1.2.2 ha-mode sso
 neighbor 20.1.2.2 fall-over bfd
 neighbor 20.1.3.2 remote-as 75
 neighbor 20.1.3.2 ha-mode sso
 neighbor 20.1.3.2 fall-over bfd
 neighbor 20.1.4.2 remote-as 75
 neighbor 20.1.4.2 ha-mode sso
 neighbor 20.1.4.2 fall-over bfd
 no auto-summary
!
```

Example 18-4 SSO-BFD with a BGP Client on the PE1 Router

PE1

```
ip vrf vpn1001
 rd 75:1001
 route-target export 75:1001
 route-target import 75:1001
!
```

```
ip vrf vpn1002
 rd 75:1002
 route-target export 75:1002
 route-target import 75:1002
!
ip vrf vpn1003
 rd 75:1003
 route-target export 75:1003
 route-target import 75:1003
!
!
ip vrf vpn1004
 rd 75:1004
 route-target export 75:1004
 route-target import 75:1004
!
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!

interface GigabitEthernet1/0/0
  no ip redirect
 no ip address
 negotiation auto
!
interface GigabitEthernet1/0/0.1
 no ip redirect
 encapsulation dot1Q 1001 second-dot1q 500
 ip vrf forwarding vpn1001
 ip address 20.1.1.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface GigabitEthernet1/0/0.2
 no ip redirect
 encapsulation dot1Q 1002
 ip vrf forwarding vpn1002
 ip address 20.1.2.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!

!
interface ATM8/0/0.1 point-to-point
 no ip redirect
 ip vrf forwarding vpn1003
 ip address 20.1.3.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 pvc 1/100
  encapsulation aal5snap
!
interface Serial5/0/0/1:1
 no ip redirect
 ip vrf forwarding vpn1004
 ip address 20.1.4.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface GigabitEthernet2/0/0
```

```
 ip address 50.0.0.1 255.0.0.0
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
!
router ospf 50
 router-id 1.1.1.1
 log-adjacency-changes
 nsf ietf
 network 1.1.1.1 0.0.0.0 area 0
 network 50.0.0.0 0.255.255.255 area 0
!
router bgp 75
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 2.2.2.2 remote-as 75
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  redistribute connected
  neighbor 2.2.2.2 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
 address-family ipv4 vrf vpn1001
  no synchronization
  redistribute connected
  neighbor 20.1.1.1 remote-as 71
  neighbor 20.1.1.1 ha-mode sso
  neighbor 20.1.1.1 fall-over bfd
  neighbor 20.1.1.1 activate
 exit-address-family
!
 address-family ipv4 vrf vpn1002
  no synchronization
  redistribute connected
  neighbor 20.1.2.1 remote-as 71
  neighbor 20.1.2.1 ha-mode sso
  neighbor 20.1.2.1 fall-over bfd
  neighbor 20.1.2.1 activate
 exit-address-family
!
 address-family ipv4 vrf vpn1003
  no synchronization
  redistribute connected
  neighbor 20.1.3.1 remote-as 71
  neighbor 20.1.3.1 ha-mode sso
  neighbor 20.1.3.1 fall-over bfd
  neighbor 20.1.3.1 activate
 exit-address-family
!
 address-family ipv4 vrf vpn1004
  no synchronization
  redistribute connected
```

```
  neighbor 20.1.4.1 remote-as 71
  neighbor 20.1.4.1 ha-mode sso
  neighbor 20.1.4.1 fall-over bfd
  neighbor 20.1.4.1 activate
 exit-address-family
!
!
mpls ldp router-id Loopback0 force
!
```

SSO-BFD with EIGRP: Example

Example 18-5 and Example 18-6 show the configuration example of the SSO-BFD feature with an Enhanced Interior Gateway Routing Protocol (EIGRP) client in a VPN scenario:

Example 18-5 SSO-BFD with an EIGRP Client on the CE1 Router

CE1

```
interface GigabitEthernet1/1/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip address 20.1.1.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface GigabitEthernet1/1/0.5
 no ip redirect
 encapsulation dot1q 105
 ip address 20.1.5.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
interface ATM4/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip address 20.1.2.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
interface serial5/0/0/1:1
 ip address 20.1.4.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
router eigrp 1
 nsf
 network 20.1.1.0 0.0.0.255
 bfd all-interfaces
!
router eigrp 2
nsf
bfd all-interfaces
network 20.1.2.0 0.0.0.255
!
router eigrp 4
nsf
bfd all-interfaces
network 20.1.4.0 0.0.0.255
!
```

```
router eigrp 5
nsf
bfd all-interfaces
network 20.1.5.0 0.0.0.255
!
end
```

Example 18-6 SSO-BFD with an EIGRP Client on the PE1 Router

PE1

```
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet2/0/0
 ip address 50.0.0.1 255.0.0.0
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
!
router ospf 50
 router-id 1.1.1.1
 log-adjacency-changes
 nsf ietf
 network 1.1.1.1 0.0.0.0 area 0
 network 50.0.0.0 0.255.255.255 area 0
!
mpls ldp router-id Loopback0 force
!
 ip vrf vpn1001
  rd 75:1001
  route-target export 75:1001
  route-target import 75:1001
 !
 ip vrf vpn1002
  rd 75:1002
  route-target export 75:1002
  route-target import 75:1002
 !
 ip vrf vpn1004
  rd 75:1004
  route-target export 75:1004
  route-target import 75:1004
 !
 ip vrf vpn1005
  rd 75:1005
  route-target export 75:1005
  route-target import 75:1005
 !
 interface GigabitEthernet1/0/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip vrf forwarding vpn1001
 ip address 20.1.1.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
 interface GigabitEthernet1/0/0.5
```

```
 no ip redirect
 encapsulation dot1q 105
 ip vrf forwarding vpn1005
 ip address 20.1.5.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
 interface ATM8/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip vrf forwarding vpn1002
 ip address 20.1.2.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
interface serial5/0/0/1:1
 ip vrf forwarding vpn1004
 ip address 20.1.4.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
router eigrp 1
nsf
 address-family ipv4 vrf vpn1001 autonomous-system 1
 nsf
 redistribute bgp 75 metric 10000 100 255 1 1500
 network 20.1.1.0 0.0.0.255
 bfd all-interfaces
!
router eigrp 2
nsf
 address-family ipv4 vrf vpn1002 autonomous-system 2
 nsf
 redistribute bgp 75 metric 10000 100 255 1 1500
 network 20.1.2.0 0.0.0.255
 bfd all-interfaces
!
router eigrp 4
nsf
 address-family ipv4 vrf vpn1004 autonomous-system 4
 nsf
 redistribute bgp 75 metric 10000 100 255 1 1500
 network 20.1.4.0 0.0.0.255
 bfd all-interfaces
!
router eigrp 5
nsf
 address-family ipv4 vrf vpn1005 autonomous-system 5
 nsf
 redistribute bgp 75 metric 10000 100 255 1 1500
 network 20.1.5.0 0.0.0.255
 bfd all-interfaces
!
router bgp 75
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 2.2.2.2 remote-as 75
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
```

```
  no synchronization
  redistribute connected
  neighbor 2.2.2.2 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
address-family ipv4 vrf vpn1001
redistribute eigrp 1
exit-address-family
 !
address-family ipv4 vrf vpn1002
redistribute eigrp 2
exit-address-family
 !
address-family ipv4 vrf vpn1004
redistribute eigrp 4
exit-address-family
 !
address-family ipv4 vrf vpn1005
redistribute eigrp 5
exit-address-family
!
end
```

SSO-BFD with ISIS: Example

Example 18-7 and Example 18-8 show the configuration example of the SSO-BFD feature with an Integrated Intermediate System-to-Intermediate system (ISIS) client in a non VPN scenario:

Note The SSO-BFD feature with ISIS is supported only on non VPN scenarios.

Example 18-7 SSO-BFD with an ISIS Client on Router 1

Router 1

```
router isis
 net 99.0000.0000.0001.00
 nsf ietf
 nsf interval 0
 bfd all-interfaces
!
!
int g1/1/0.1
 no ip redirect
 encap dot1q 101
 ip address 192.168.1.1 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int g1/1/0.2
 no ip redirect
 encap dot1q 102 second-dot1q 200
```

```
 ip address 192.168.2.1 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int atm4/0/0.1 point
 no ip redirect
 pvc 1/101
  encap aal5snap
  ip address 192.168.3.1 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
!
int s5/0/0/1:1
 no ip redirect
 ip address 192.168.5.1 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int l0
 ip address 1.1.1.1 255.255.255.255
 ip router isis
!
```

Example 18-8 SSO-BFD with an ISIS Client on Router 2

Router 2

```
router isis
 net 99.0000.0000.0002.00
 nsf ietf
 nsf interval 0
 bfd all-interfaces
!
int g1/0/0.1
 no ip redirect
 encap dot1q 101
 ip address 192.168.1.2 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int g1/0/0.2
 no ip redirect
 encap dot1q 102 second-dot1q 200
 ip address 192.168.2.2 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int atm8/0/0.1 point
 no ip redirect
 pvc 1/101
  encap aal5snap
  ip address 192.168.3.2 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
```

```
!
int s5/0/0/1:1
 no ip redirect
 ip address 192.168.5.2 255.255.255.0
 ip router isis
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
int l0
 ip address 2.2.2.2 255.255.255.255
 ip router isis
!
```

SSO-BFD with OSPF: Example

Example 18-9 and Example 18-10 show the configuration example of the SSO-BFD feature with an Open Shortest Path First (OSPF) client in a VPN scenario:

Example 18-9 SSO-BFD with an OSPF Client on the CE1 Router

CE1

```
!Qinq interface
 interface GigabitEthernet1/1/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip address 20.1.1.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
!
!dot1q interface
 interface GigabitEthernet1/1/0.5
 no ip redirect
 encapsulation dot1q 105
 ip address 20.1.5.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
  no bfd echo
!
!ATM interface
!
interface ATM4/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip address 20.1.2.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
  no bfd echo
 !
 ! Serial interface
interface serial5/0/0/1:1
 no ip redirect
 ip address 20.1.4.1 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
  no bfd echo
 !
! 4 ospf process for 4 different interfaces
!
router ospf 1
nsf ietf
```

```
bfd all-interfaces
network 20.1.1.0 0.0.0.255 area 0
!
router ospf 2
nsf ietf
bfd all-interfaces
network 20.1.2.0 0.0.0.255 area 0
!
router ospf 4
nsf ietf
bfd all-interfaces
network 20.1.4.0 0.0.0.255 area 0
!
router ospf 5
nsf ietf
bfd all-interfaces
network 20.1.5.0 0.0.0.255 area 0
!
end
```

Example 18-10 SSO-BFD with an OSPF Client on the CE1 Router

PE1

```
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet2/0/0
 ip address 50.0.0.1 255.0.0.0
 negotiation auto
 mpls ip
 mpls label protocol ldp
!
!
router ospf 50
 router-id 1.1.1.1
 log-adjacency-changes
 nsf ietf
 network 1.1.1.1 0.0.0.0 area 0
 network 50.0.0.0 0.255.255.255 area 0
!
mpls ldp router-id Loopback0 force
!
!4 vpns for 4 different interfaces
!
 ip vrf vpn1001
  rd 75:1001
  route-target export 75:1001
  route-target import 75:1001
 !
 ip vrf vpn1002
  rd 75:1002
  route-target export 75:1002
  route-target import 75:1002
 !
 ip vrf vpn1004
  rd 75:1004
  route-target export 75:1004
  route-target import 75:1004
```

```
 !
 ip vrf vpn1005
  rd 75:1005
  route-target export 75:1005
  route-target import 75:1005
 !
! Qinq interface
 !
 interface GigabitEthernet1/0/0.1
 no ip redirect
 encapsulation dot1q 101 second-dot1q 500
 ip vrf forwarding vpn1001
 ip address 20.1.1.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
  no bfd echo
 !
! dot1q interface
!
interface GigabitEthernet1/0/0.5
 no ip redirect
 encapsulation dot1q 105
 ip vrf forwarding vpn1005
 ip address 20.1.5.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
! ATM interface
!
 interface ATM8/0/0.1 point
 no ip redirect
 pvc 1/101
 encapsulation aal5snap
 ip vrf forwarding vpn1002
 ip address 20.1.2.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
!Serial interface
 !
interface serial5/0/0/1:1
 no ip redirect
 ip vrf forwarding vpn1004
 ip address 20.1.4.2 255.255.255.0
 bfd interval 999 min_rx 999 multiplier 5
 no bfd echo
 !
router ospf 1 vrf vpn1001
nsf ietf
redistribute bgp 75 metric 20 subnets
network 20.1.1.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 2 vrf vpn1002
nsf ietf
redistribute bgp 75 metric 20 subnets
network 20.1.2.0 0.0.0.255 area 0
bfd all-interfaces
!
router ospf 4 vrf vpn1004
nsf ietf
redistribute bgp 75 metric 20 subnets
network 20.1.4.0 0.0.0.255 area 0
bfd all-interfaces
!
```

```
router ospf 5 vrf vpn1005
nsf ietf
redistribute bgp 75 metric 20 subnets
network 20.1.5.0 0.0.0.255 area 0
bfd all-interfaces
!
!
router bgp 75
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 2.2.2.2 remote-as 75
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  redistribute connected
  neighbor 2.2.2.2 activate
  no auto-summary
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community both
 exit-address-family
 !
address-family ipv4 vrf vpn1001
redistribute ospf 1 vrf vpn1001
exit-address-family
 !
address-family ipv4 vrf vpn1002
redistribute ospf 2 vrf vpn1002
exit-address-family
 !
address-family ipv4 vrf vpn1004
redistribute ospf 4 vrf vpn1004
exit-address-family
 !
address-family ipv4 vrf vpn1005
redistribute ospf 5 vrf vpn1005
exit-address-family
 !
end
```