

Bidirectional Forwarding Detection Routing

This chapter describes how to configure Firewall Threat Defense to use the Bidirectional Forwarding Detection (BFD) routing protocol.

- BFD routing protocol, on page 1
- Guidelines for BFD routing, on page 1
- Configure BFD, on page 3
- History for BFD routing, on page 6

BFD routing protocol

A BFD routing protocol is a detection protocol that

- provides fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols
- operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems, and
- carries packets in the payload of the encapsulating protocol appropriate for the media and the network.

Why BFD?

BFD provides a consistent failure detection method for network administrators in addition to fast forwarding path failure detection.

Network administrators can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms. This makes network profiling and planning easier, and reconvergence time is consistent and predictable.

Guidelines for BFD routing

Context mode guidelines

BFD is supported on all Firewall Threat Defense platforms and is available in multi-instance mode.

Firewall mode guidelines

BFD is supported in routed firewall mode and not in transparent mode.

Failover and cluster guidelines

- BFD is not supported on failover interfaces.
- In clustering, BFD is supported only on the control node.

Routing and protocol guidelines

- OSPFv2, OSPFv3, IS-IS, BGP IPv4, and BGP IPv6 protocol are supported.

  For BFD support on IS-IS, using FlexConfig CLI configure BFD on IS-IS interfaces (Physical Interfaces, Sub-Interfaces, Port-Channels only):

```
For IPv6
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  ipv6 router isis
  isis ipv6 bfd
exit

For IPv4
###Flex-config Appended CLI###

router isis
  net 11.1111.0000.0000.0001.00
exit
interface GigabitEthernet x/x
  isis
  isis bfd
exit
```

  EIGRP protocol is not supported.
- BFD for static routes is not supported. You can configure BFD on interfaces that belong only to virtual routers.
- Only named interfaces are supported.
- BFD on BVI, VTI, and loopback interfaces are not supported.

Single-hop guidelines

- Echo mode is disabled by default. You can enable echo mode on single-hop only.
- Echo mode is not supported for IPv6.
- Use only a single-hop template to configure a single-hop policy.
- Authentication of the single-hop template is optional.
- You cannot configure multiple BFDs on the same interface.

Multi-hop guidelines

- Do not configure the source IP address also as the destination IP address.

- Source and destination address should have same IP type—IPV4 or IPV6.
- Only network objects of host or network type are allowed.
- Use only a multi-hop template to configure a multi-hop policy.
- Authentication is mandatory for the multi-hop template.

Upgrade guidelines

When you upgrade to version 7.3 and the previous version has any FlexConfig BFD policies, the management center displays a warning message during deployment. However, it does not stop the deployment process. After post-upgrade deployment, to manage the BFD policies from the UI (**Device (Edit)** > **Routing** > **BFD**), you must configure BFD policies in the **Device (Edit)** > **Routing** > **BFD** page and remove the configuration from the FlexConfig policy for the device.

Configure BFD

This task enables and configures the Bidirectional Forwarding Detection (BFD) routing policy on your system to provide rapid detection of faults in the forwarding path.

Before you begin

Ensure you have access to the system where you want to configure BFD.

Follow these steps to configure BFD:

Procedure

Step 1 Create Configure a BFD template.

Step 2 Configure BFD policies, on page 3.

Step 3 Configure BFD support in the BGP neighbor settings; see, Configure BGP Neighbor Settings.

BFD is enabled and configured on your system.

Configure BFD policies

BFD policies are used to provide rapid failure detection for interfaces associated with virtual routers. Configuring BFD templates allows you to monitor connectivity and quickly identify link failures.

- Enable fast failure detection for routing interfaces.
- Support both single-hop and multi-hop BFD configurations.

You can bind a BFD template to an interface belonging to a virtual router, or to a source and destination address pair.

Before you begin

- BFD policy is configurable only on interfaces that belong to virtual routers. See Configure interfaces to a virtual router.

To configure BFD policies, complete these steps.

Procedure

Step 1 From the **Devices** > **Device Management** page, edit the virtual-router supported device. Navigate to **Routing**.

Step 2 From the drop-down list, select the desired virtual router, and then click **BFD**.

Step 3 To configure a BFD on the interface, click the **Single-Hop** tab or **Multi-Hop** tab.



Note For a single-hop policy, the BFD template is configured on an interface; for a multi-hop policy, the BFD template is configured on a source and destination address pair.

Step 4 Click **Add**. To modify the configured BFD policy, click **Edit** ( ).



Note When you edit the interface mapping with BFD template to replace it with a new BFD template, the Firewall Management Center uses a **no** command to remove the template mapping from interface and applies the new template to the interface which causes a BFD flap which may also lead to an OSPFv2, OSPFv3, or BGP flap. However, if the BFD intervals are higher, the BFD flap might not occur. Alternatively, to avoid the flapping, you can delete the existing BFD template mapping; deploy the interface, and then add the new BFD template to the interface and deploy the configuration.

- See Configure a single-hop BFD policy, on page 4.
- See Configure a multi-hop BFD policy, on page 5.

After completing this task, BFD policies are configured on the selected interfaces or address pairs.

Configure a single-hop BFD policy

You can configure a single-hop BFD policy only on an interface that belongs to a virtual router. This task is relevant when you need to apply BFD for rapid link failure detection on specific interfaces.

Before you begin

- Create single-hop BFD templates. You cannot configure single-hop BFD policy on interfaces that use a multi-hop template.

Follow these steps to configure a single-hop BFD policy:

Procedure

Step 1 In the **Single-Hop** tab, click **Add** or **Edit**.

Step 2 In the **Add BFD Single-Hop** dialog box, configure the following:

a) The **Interface** drop-down list displays interfaces belonging to virtual routers. Select the interface you want to configure with the BFD policy.

b) The **Template Name** drop-down list displays single-hop templates. Select the template that you want to apply.

If you have not created a single-hop template, use **Add** (+) and create a single-hop BFD template.

Step 3 Click **OK** and **Save** the configuration.

The single-hop BFD policy is applied to the selected interface. The interface will now use the specified BFD template for single-hop operations.

Configure a multi-hop BFD policy

Configure a multi-hop BFD policy to enable monitoring of connectivity between specific source and destination address pairs. This configuration helps to monitor links that traverse multiple hops in your network.

Before you begin

- Create multi-hop BFD templates. You cannot configure multi-hop BFD policy using a single-hop template.

Follow these steps to configure a multi-hop BFD policy:

Procedure

Step 1 In the **Add BFD Multi-Hop** dialog box, configure the following:

a) Click the BFD source address type:**IPv4** or **IPv6** radio button.

b) The **Source Address** drop-down list displays the network objects. Select the source address for the BFD policy; do not choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note The created network object's IP type should match with the selected source IP type.

c) The **Destination Address** drop-down list displays network objects. Select the destination address for the BFD; do not choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note The created network object's IP type should match with the selected source IP type.

Attention Do not select the network object that has the same IP address as that of the source address.

d) The **Template Name** drop-down list displays multi-hop templates. Select the template to apply to the BFD policy.

If you have not created a multi-hop template, use **Add** (+) and create a multi-hop BFD template.

Step 2 Click **OK** and **Save** the configuration.

The multi-hop map (table view) is displayed on the **Multi-Hop** tab page.

History for BFD routing

The History table summarizes the introduction and evolution of the BFD routing in Cisco Firewall Management Center across releases, enabling quick tracking of feature availability and changes.

Table 1: Feature history for BFD routing

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
BFD support for IS-IS	7.4	7.4	You can configure BFD on IS-IS interfaces using FlexConfig CLI.
BFD support for OSPF	7.4	7.4	You can enable BFD on interfaces that use OSPF version 2 and OSPF version 3. New/modified screens: • **Configuration** > **Device Setup** > **Routing** > **OSPFv2** • **Configuration** > **Device Setup** > **Routing** > **OSPFv3**
BFD configuration	7.4	7.4	In the previous releases, BFD was configurable on threat defense only through FlexConfig. FlexConfig no longer supports BFD configuration. You can now configure BFD policies for threat defense in the management center UI. In threat defense, BFD is supported only on the BGP protocol. New/modified screens: **Devices** > **Device Management** > **Routing** > **BFD**.