BFD IPv6 Encapsulation Support

Bidirectional Forwarding Detection for IPv6 encapsulations are described within a session information structure. These session information structures are defined by BFDv6 for the protocols supported. BFDv6 uses information from the session information structures to determine the correct encapsulation for BFDv6 packets on that session.

Prerequisites for BFD IPv6 Encapsulation Support

- When using Bidirectional Forwarding Detection over IPv6 (BFDv6), IPv6 Cisco Express Forwarding and IPv6 unicast routing must be enabled on all participating routers.
- When you configure BFD IPv6 software sessions, you should configure the following CLI command:

  no ipv6 nd nud igp

  If the peer is also an ASR device, the above command should be configured on the peer device too.

Restrictions for BFD IPv6 Encapsulation Support

- BFDv6 supports only global IPv6 neighbor addresses if a global IPv6 address is configured on the interface.
- Only asynchronous mode is supported. In asynchronous mode, either BFDv6 peer can initiate a BFDv6 session.

Information About BFD IPv6 Encapsulation Support

Overview of the BFDv6 Protocol

This section describes the BFDv6 protocol, how it is different from BFD for IPv4, and how it works with BFD for IPv4. BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. BFDv6 provides IPv6 support by accommodating IPv6 addresses and provides the ability to create BFDv6 sessions.

BFDv6 Registration

BFD clients register with BFD using a registry application program interface (API). The registry arguments include protocol type and the address and interface description block (IDB) of the route to be monitored. These APIs and arguments are all assumed by BFD to be IPv4.

BFDv6 has registries from which these arguments have been removed, and the protocol and encapsulation are described within a session information structure. These session information structures are defined by BFDv6 for the protocols supported. BFDv6 uses information from the session information structures to determine the correct encapsulation for BFDv6 packets on that session.

BFDv6 Global and Link-Local Addresses

BFDv6 supports both global and link-local IPv6 addresses for neighbor creation. BFDv6 sessions select source addresses to match the neighbor address types (for example, global IPv6 address neighbors must be paired with global IPv6 source addresses and link-local IPv6 address neighbors must be paired with link-local IPv6 source addresses). The table below shows the address pairings that BFDv6 supports.

Table 1: BFDv6 Address Pairings for Neighbor Creation

Source Address	Destination Address	Status
Global	Global	Supported
Global	Link local	Not supported
Link local	Global	Not supported
Link local	Link local	Supported

Because all IPv6-enabled interfaces have a link-local address and BFDv6 selects the source address, link-local address neighbors are always paired with a link-local interface address. The link-local source address with global destination address is not supported by Cisco Express Forwarding. Therefore, a global IPv6 address must be configured on an interface before a session with a global address neighbor may be established in BFDv6. BFDv6 rejects any sessions in which the neighbor address is global and no global address is configured on the interface.

Note The behavior of a unique local address (ULA) in BFDv6 is the same as a global address.

BFD for IPv4 and IPv6 on the Same Interface

BFD supports multiple IPv4 and IPv6 sessions per interface, with no restriction on the protocol of those sessions.

How to Configure BFD IPv6 Encapsulation Support

Configuring BFD Session Parameters on the Interface

The steps in this procedure show how to configure BFD on the interface by setting the baseline BFD session parameters on an interface. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to BFD neighbors.

Note RSP3 Module eysupports only the following BFD interval timers:

3.3ms, 6.6ms, 10ms, 20ms, 50ms, 100ms, 200ms ,999ms. It is recommended that peer should also configure the same timer values.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **bfd-template single-hop** *template-name*

Example:

```
Router(config)# bfd-template single-hop bfdtemplate1
```

Creates a single-hop BFD template and enters BFD configuration mode.

Step 4 **interval min-tx** *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier-value*

Example:

```
Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
```

Configures the transmit and receive intervals between BFD packets, and specifies the number of consecutive BFD control packets that must be missed before BFD declares that a peer is unavailable.

Step 5 **interface** *type number*

Example:

```
Device(config)# interface FastEthernet 6/0
```

Enters interface configuration mode.

Step 6 **interface gigabitethernet** *number*

Example:

```
Device(config)# interface gigabitethernet 0/0/0
```

Specifies the Gigabit Ethernet interface and enters interface configuration mode.

Step 7 Perform one of the following steps:

- **ip address** *ipv4-address mask*
- **ipv6 address** *ipv6-address*/*mask*

Example:

Configuring an IPv4 address for the interface:

```
Device(config-if)# ip address 10.201.201.1 255.255.255.0
```

Configuring an IPv6 address for the interface:

```
Device(config-if)# ipv6 address 2001:DB8::/32
```

Configures an IP address for the interface.

Step 8 **bfd template** *template name*

Enables the BFD template.

Step 9 **end**

Example:

```
Device(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for BFD IPv6 Encapsulation Support

Example: Configuring BFD Session Parameters on the Interface

```
Device# show ipv6 ospf neighbor detail

 Neighbor 172.16.3.3
    In the area 1 via interface GigabitEthernet0/0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following is a sample configuration where interface 0/0/7 of Router A is connected to interface 0/4/6 of router B.

Configuration on Router A

```
bfd-template single-hop BFDM
interval min-tx 50 min-rx 50 multiplier 3

router ospfv3 1
router-id 2.2.2.2
!
address-family ipv6 unicast
  bfd all-interfaces
exit-address-family
!
!
interface TenGigabitEthernet0/0/7
ipv6 address 19:1:1::1/64
ospfv3 1 ipv6 area 0
bfd template BFDM
```

Configuration on Router B

```
bfd-template single-hop BFDM
interval min-tx 50 min-rx 50 multiplier 3
!
interface TenGigabitEthernet0/4/6
ipv6 address 19:1:1::2/64
ospfv3 1 ipv6 area 0
bfd template BFDM
end
!
router ospfv3 1
router-id 3.3.3.3
!
address-family ipv6 unicast
```

```
  bfd all-interfaces
exit-address-family
```