Example

This example shows how to create a VLAN interface:

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

Configuring a Static MAC Address on a Layer 3 Interface

You can configure static MAC addresses on Layer 3 interfaces. You cannot configure broadcast or multicast addresses as static MAC addresses.

Note You cannot configure static MAC addresses on tunnel interfaces.

Note This configuration is limited to 16 VLAN interfaces. Applying the configuration to additional VLAN interfaces results in a down state for the interface with a `Hardware prog failed.` status.

SUMMARY STEPS

1. **config t**
2. **interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
3. **mac-address** *mac-address*
4. **exit**
5. (Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:**	Specifies the Layer 3 interface and enters the interface configuration mode. **Note**

	Command or Action	Purpose
	`switch(config)# interface ethernet 7/3`	You must create the Layer 3 interface before you can assign the static MAC address.

Step 3	**mac-address** *mac-address*
	Example:
	`switch(config-if)# mac-address 22ab.47dd.ff89`
	`switch(config-if)#`
		Specified a static MAC address to add to the Layer 3 interface.

Step 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface mode.

Step 5	(Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:** `switch# show interface ethernet 7/3`	Displays information about the Layer 3 interface.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the Layer 3 interface on slot 7, port 3 with a static MAC address:

```
switch# config t
switch(config)# interface ethernet 7/3
switch(config-if)# mac-address 22ab.47dd.ff89
switch(config-if)#
```

Configuring a Loopback Interface

You can configure a loopback interface to create a virtual interface that is always up.

Before you begin

Ensure that the IP address of the loopback interface is unique across all routers on the network.

SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *instance*
3. [**ip address** *ip-address/length* | **ipv6 address** *ipv6-address/length*]
4. **show interface loopback** *instance*
5. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**interface loopback** *instance*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		Creates a loopback interface. The range is from 0 to 1023.

Step 3	[**ip address** *ip-address/length* | **ipv6 address** *ipv6-address/length*]
	Example:
	`switch(config-if)# ip address 192.0.2.1/8`
	Example:
	`switch(config-if)# ipv6 address 2001:0DB8::1/8`
		• Configures an IP address for this interface. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information about IP addresses.
		• Configures an IPv6 address for this interface. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information about IPv6 addresses.

Step 4	**show interface loopback** *instance* **Example:** `switch(config-if)# show interface loopback 0`	(Optional) Displays the loopback interface statistics.

Step 5	**copy running-config startup-config**
	Example:
	`switch(config-if)# copy running-config`
	`startup-config`
		(Optional) Saves the configuration change.

Example

This example shows how to create a loopback interface:

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

Configuring PBR on SVI on the Gateway

This procedure configures PBR on the primary SVI interface in the gateway.

Note Steps 2 through 6 are needed if you want to configure a PBR policy on the unnumbered Primary/Secondary VLAN interfaces. This is not mandatory for IP unnumbered on the SVI feature.

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *list-name*
3. **permit tcp host** *ipaddr* **host** *ipaddr* **eq** *port-number*
4. **exit**
5. **route-map** *route-map-name*
6. **match ip address** *access-list-name*
7. **set ip next-hop** *addr1*
8. **exit**
9. **interface vlan** *vlan-id*
10. **ip address** *ip-addr*
11. **no ip redirects**
12. (Optional) **ip policy route-map pbr-sample**
13. **exit**
14. **hsrp version 2**
15. **hsrp***group-num*
16. **name** *name-val*
17. **ip** *ip-addr*
18. **no shutdown**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enter global configuration mode.
Step 2	**ip access-list** *list-name* **Example:** `switch(config)# ip access-list pbr-sample`	Configure access list.
Step 3	**permit tcp host** *ipaddr* **host** *ipaddr* **eq** *port-number* **Example:** `switch(config-acl)# permit tcp host 10.1.1.1 host 192.168.2.1 eq 80`	Specify the packets to forward on a specific port.

	Command or Action	Purpose
Step 4	**exit** **Example:** `switch(config-acl)# exit`	Exit configuration mode.
Step 5	**route-map** *route-map-name* **Example:** `switch(config)# route-map pbr-sample`	Create a route-map or enter route-map command mode.
Step 6	**match ip address** *access-list-name* **Example:** `switch(config-route-map)# match ip address pbr-sample`	Match values from the routing table.
Step 7	**set ip next-hop** *addr1* **Example:** `switch(config-route-map)# set ip next-hop 192.168.1.1`	Set IP address of the next hop.
Step 8	**exit** **Example:** `switch(config-route-map)# exit`	Exit command mode.
Step 9	**interface vlan** *vlan-id* **Example:** `switch(config)# interface vlan 2003`	Creates a VLAN interface and enters interface configuration mode. The range is from 1 and 4094.This is the primary VLAN.
Step 10	**ip address** *ip-addr* **Example:** `switch(config-if)# ip address 10.0.0.1/8`	Configures an IP address for the interface.
Step 11	**no ip redirects** **Example:** `switch(config-if)# no ip redirects`	Needs to be configured on all unnumbered primary and secondary VLAN interfaces.
Step 12	(Optional) **ip policy route-map pbr-sample** **Example:** `switch(config-if)# ip policy route-map pbr-sample`	Enter this command if you want to apply a PBR policy on the unnumbered Primary/Secondary VLAN interface.
Step 13	**exit** **Example:** `switch(config-if)# exit`	Exit command mode.
Step 14	**hsrp version 2** **Example:** `switch(config-if)# hsrp version 2`	Set the HSRP version.

	Command or Action	Purpose
Step 15	**hsrp***group-num* **Example:** `switch(config-if)# hsrp 200`	Set the HSRP group number.
Step 16	**name** *name-val* **Example:** `switch(config-if-hsrp)# name primary`	Configure the redundancy name string.
Step 17	**ip** *ip-addr* **Example:** `switch(config-if-hsrp)# ip 10.0.0.100`	Configures an IP address.
Step 18	**no shutdown** **Example:** `switch(config-if-hsrp)# no shutdown`	Negates shutdown.

Configuring IP Unnumbered on SVI Secondary VLAN on the Gateway

This procedure configures IP unnumbered on the secondary SVI in the gateway. Beginning Cisco NX-OS Release 9.3(6), this feature is supported on Cisco Nexus N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX switches.

SUMMARY STEPS

1. **configure terminal**
2. **interface vlan** *vlan-list*
3. **ip unnumbered vlan** *primary-vlan-id*
4. (Optional) **ip policy route-map pbr-sample**
5. **no ip redirects**
6. **hsrp version 2**
7. **hsrp** *group-num*
8. **follow** *name*
9. **ip** *ip-addr*
10. **no shutdown**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enter configuration mode.

	Command or Action	Purpose
Step 2	**interface vlan** *vlan-list* **Example:** `switch(config)# interface vlan 2001`	Creates a VLAN interface and enters interface configuration mode. The range is from 1 to 4094. This is the secondary VLAN.
Step 3	**ip unnumbered vlan** *primary-vlan-id* **Example:** `switch(config-if)# ip unnumbered vlan 2003`	Enables IP processing on an interface without assigning an explicit IP address to an interface.
Step 4	(Optional) **ip policy route-map pbr-sample** **Example:** `switch(config-if)# ip policy route-map pbr-sample`	Enter this command if you want to apply a PBR policy on the unnumbered Primary/Secondary VLAN interface.
Step 5	**no ip redirects** **Example:** `switch(config-if)# no ip redirects`	Needs to be configured on all unnumbered primary and secondary VLAN interfaces.
Step 6	**hsrp version 2** **Example:** `switch(config-if)# hsrp version 2`	Set the HSRP version.
Step 7	**hsrp** *group-num* **Example:** `switch(config-if)# hsrp 200`	Set the HSRP group number.
Step 8	**follow** *name* **Example:** `switch(config-if-hsrp)# follow primary`	Configure the group to be followed.
Step 9	**ip** *ip-addr* **Example:** `switch(config-if-hsrp)# ip 10.0.0.100`	Enters HRSP IPv4 and sets the virtual IP address.
Step 10	**no shutdown** **Example:** `switch(config-if-hsrp)# no shutdown`	Negate shutdown.

Configuring SVI TCAM Region

Beginning Cisco NX-OS Release 9.3(3), you can display Layer 3 statistics on SVI interfaces on Cisco Nexus 3100 Series switches. You can change the size of the SVI ternary content addressable memory (TCAM) regions in the hardware to display the Layer 3 incoming unicast counters on SVI interfaces.

SUMMARY STEPS

1. **hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** | **svi** } *tcam_size*
2. **copy running-config startup-config**
3. switch(config)# **show hardware profile tcam region**
4. switch(config)# **reload**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** | **svi** } *tcam_size*	Changes the ACL TCAM region size. • **arpacl**—Configures the size of the Address Resolution Protocol (ARP) ACL (ARPACL) TCAM region. • **e-racl**—Configures the size of the egress router ACL (ERACL) TCAM region. • **e-vacl**—Configures the size of the egress VLAN ACL (EVACL) TCAM region. • **ifacl**—Configures the size of the interface ACL (ifacl) TCAM region. The maximum number of entries is 1500. • **nat**—Configures the size of the NAT TCAM region. • **qos**—Configures the size of the quality of service (QoS) TCAM region. • **qoslbl**—Configures the size of the QoS Label (qoslbl) TCAM region. • **racl**—Configures the size of the router ACL (RACL) TCAM region. • **vacl**—Configures the size of the VLAN ACL (VACL) TCAM region. • *svi*—Configures the size of the SVI TCAM region. The default size of SVI TCAM size is 0. • *tcam_size*—TCAM size. The range is from 0 to 2,14,74, 83, 647 entries. **Note** **vacl** and **e-vacl** TCAM regions should be set to the same size.

	Command or Action	Purpose
Step 2	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 3	switch(config)# **show hardware profile tcam region** **Example:** `switch(config)# show hardware profile tcam region`	Displays the TCAM sizes that will be applicable on the next reload of the switch.
Step 4	switch(config)# **reload** **Example:** `switch(config)# reload`	Copies the running configuration to the startup configuration. **Note** The new size values are effective only upon the next reload after saving the **copy running-config to startup-config**.

Example

The following example shows how to change the size of the SVI TCAM region:

```
switch(config)# hardware profile tcam region svi 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

Assigning an Interface to a VRF

You can add a Layer 3 interface to a VRF.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type number*
3. **vrf member** *vrf-name*
4. **ip address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *interface-type number*
	Example:
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	**vrf member** *vrf-name* **Example:** `switch(config-if)# vrf member RemoteOfficeVRF`	Adds this interface to a VRF.
Step 4	**ip address** *ip-prefix/length* **Example:** `switch(config-if)# ip address 192.0.2.1/16`	Configures an IP address for this interface. You must do this step after you assign this interface to a VRF.
Step 5	**show vrf** [*vrf-name*] **interface** *interface-type number* **Example:** `switch(config-vrf)# show vrf Enterprise interface loopback 0`	(Optional) Displays VRF information.
Step 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Saves the configuration change.

Example

This example shows how to add a Layer 3 interface to the VRF:

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

Configuring a DHCP Client on an Interface

You can configure the DHCP client on an SVI, a management interface, or a physical Ethernet interface for IPv4 or IPv6 address

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *type slot/port* | **mgmt** *mgmt-interface-number* | **vlan** *vlan id*
3. switch(config-if)# [**no**] **ipv6 address use-link-local-only**
4. switch(config-if)# [**no**] [**ip** | **ipv6] address dhcp**
5. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *type slot/port* | **mgmt** *mgmt-interface-number* | **vlan** *vlan id*	Creates a physical Ethernet interface, a management interface, or a VLAN interface. The range of *vlan id* is from 1 to 4094.
Step 3	switch(config-if)# [**no**] **ipv6 address use-link-local-only**	Prepares for request to the DHCP server. **Note** This command is only required for an IPv6 address.
Step 4	switch(config-if)# [**no**] [**ip** | **ipv6] address dhcp**	Requests the DHCP server for an IPv4 or IPv6 address. The **no** form of this command removes any address that was acquired.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure the IP address of a DHCP client on an SVI:

```
switch# configure terminal
switch(config)# interface vlan 15
switch(config-if)# ip address dhcp
```

This example shows how to configure an IPv6 address of a DHCP client on a management interface:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ipv6 address use-link-local-only
switch(config-if)# ipv6 address dhcp
```

Configuring SVI and Subinterface Ingress/Egress Unicast Counters

Beginning Cisco NX-OS Release 9.3(3), SVI and subinterface unicast counters are supported on Cisco Nexus 9300-EX, 9300-FX/FX2 switches; and Cisco Nexus 9500 series switches with X9700-EX and X9700-FX line cards.

Beginning Cisco NX-OS Release 9.3(5), SVI and subinterface unicast counters are supported on Cisco Nexus N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX switches.

Beginning Cisco NX-OS Release 10.5(2)F, if the **hardware profile svi-and-si flex stats enable flex-stats** command is enabled, SVI statistics rate is supported on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1 Series ToR switches and 9500 Series EoR switches with 9700-EX, FX, FX3, and GX line cards.

Note

- Enabling this feature disables VXLAN, MPLS, Tunnel, Multicast, and ERSPAN counters. Reload the switch for the changes to take effect.
- For a vPC setup, the **peer-gateway** feature must be enabled under the **vpc domain** on both vPC peers. Otherwise, SVI counters may be inconsistent.
- Multicast counters are not supported.
- In EOR switches, the statistics rate is supported only for ports in the first ASIC (ASIC 0). If ingress or egress ports are in a different ASIC other than the first ASIC, then the statistics rate is not supported.

To configure SVI and subinterface ingress and/or egress unicast counters on a device, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **[no] hardware profile svi-and-si flex-stats-enable**
3. **copy running-config startup-config**
4. **reload**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**[no] hardware profile svi-and-si flex-stats-enable**
	Example:
	`switch(config)# hardware profile svi-and-si flex-stats-enable`
	`switch(config-if)#`
		Configures the ingress/egress unicast counters on SVI and subinterface.
		Note
		You must save the configuration and reload the switch for this command to work.

	Command or Action	Purpose
Step 3	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves this configuration.
Step 4	**reload** **Example:** `switch(config-if)# reload`	Reload the switch.

Configuring Subinterface Multicast and Broadcast Counters

Beginning Cisco NX-OS Release 9.3(6), subinterface multicast and broadcast counters are supported on Cisco Nexus N9K-C9336C-FX2 and N9K-C93240YC-FX2 switches.

To configure multicast and broadcast counters on a device, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **[no] hardware profile sub-interface flex-stats**
3. **copy running-config startup-config**
4. **reload**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	**[no] hardware profile sub-interface flex-stats**
	Example:
	`switch(config)# hardware profile sub-interface flex-stats`
	`switch(config-if)#`
		Enables subinterface flex stats for multicast and broadcast counters.

Step 3	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Saves this configuration.

	Command or Action	Purpose
Step 4	**reload** **Example:** `switch(config-if)# reload`	Reload the switch.

Example

The following example displays the subinterface multicast and broadcast counters as a result of show interface counters command:

```
switch(config)# show int ethernet 1/31/4.1 counters
--------------------------------------------------------------------------------
Port                                          InOctets                InUcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                       InMcastPkts                InBcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                      InIPv4Octets            InIPv4UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                   InIPv4McastPkts            InIPv4BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                      InIPv6Octets            InIPv6UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                   InIPv6McastPkts            InIPv6BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                         OutOctets               OutUcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                      OutMcastPkts               OutBcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                     OutIPv4Octets           OutIPv4UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                          0                          0

--------------------------------------------------------------------------------
Port                                  OutIPv4McastPkts           OutIPv4BcastPkts
--------------------------------------------------------------------------------
```

```
Eth1/31/4.1                                    0                               0

--------------------------------------------------------------------------------
Port                               OutIPv6Octets                OutIPv6UcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0

--------------------------------------------------------------------------------
Port                            OutIPv6McastPkts                OutIPv6BcastPkts
--------------------------------------------------------------------------------
Eth1/31/4.1                                    0                               0
```

Verifying the Layer 3 Interfaces Configuration

To display the Layer 3 configuration, perform one of the following tasks:

Command	Purpose
show interface ethernet *slot/port*	Displays the Layer 3 interface configuration, status, and counters (including the 5-minute exponentially decayed moving average of inbound and outbound packet and byte rates).
show interface ethernet *slot/port* **brief**	Displays the Layer 3 interface operational status.
show interface ethernet *slot/port* **capabilities**	Displays the Layer 3 interface capabilities, including port type, speed, and duplex.
show interface ethernet *slot/port* **description**	Displays the Layer 3 interface description.
show interface ethernet *slot/port* **status**	Displays the Layer 3 interface administrative status, port mode, speed, and duplex.
show interface ethernet *slot/port.number*	Displays the subinterface configuration, status, and counters (including the f-minute exponentially decayed moving average of inbound and outbound packet and byte rates).
show interface port-channel *channel-id.number*	Displays the port-channel subinterface configuration, status, and counters (including the 5-minute exponentially decayed moving average of inbound and outbound packet and byte rates).
show interface loopback *number*	Displays the loopback interface configuration, status, and counters.
show interface loopback *number* **brief**	Displays the loopback interface operational status.
show interface loopback *number* **description**	Displays the loopback interface description.
show interface loopback *number* **status**	Displays the loopback interface administrative status and protocol status.

Command	Purpose
show interface vlan *number*	Displays the VLAN interface configuration, status, and counters.
show interface vlan *number* **brief**	Displays the VLAN interface operational status.
show interface vlan *number* **description**	Displays the VLAN interface description.
show interface vlan *number* **status**	Displays the VLAN interface administrative status and protocol status.

Monitoring the Layer 3 Interfaces

Use the following commands to display Layer 3 statistics:

Command	Purpose
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	Cisco Nexus 9000 Series devices set three different sampling intervals to bit-rate and packet-rate statistics. The range for VLAN network interface is 60 to 300 seconds, and the range for Layer interfaces is 30 to 300 seconds.
show interface ethernet *slot/port* **counters**	Displays the Layer 3 interface statistics (unicast, multicast, and broadcast).
show interface ethernet *slot/port* **counters brief**	Displays the Layer 3 interface input and output counters.
show interface ethernet errors *slot/port* **detailed** [**all**]	Displays the Layer 3 interface statistics. You can optionally include all 32-bit and 64-bit packet and byte counters (including errors).
show interface ethernet errors *slot/port* **counters errors**	Displays the Layer 3 interface input and output errors.
show interface ethernet errors *slot/port* **counters snmp**	Displays the Layer 3 interface counters reported by SNMP MIBs.
show interface ethernet *slot/port.number* **counters**	Displays the subinterface statistics (unicast, multicast, and broadcast).
show interface port-channel *channel-id.number* **counters**	Displays the port-channel subinterface statistics (unicast, multicast, and broadcast).
show interface loopback *number* **counters**	Displays the loopback interface input and output counters (unicast, multicast, and broadcast).
show interface loopback *number* **detailed** [**all**]	Displays the loopback interface statistics. You can optionally include all 32-bit and 64-bit packet and byte counters (including errors).

Command	Purpose
show interface loopback *number* **counters errors**	Displays the loopback interface input and output errors.
show interface vlan *number* **counters**	Displays the VLAN interface input and output counters (unicast, multicast, and broadcast).
show interface vlan *number* **counters detailed** [**all**]	Displays the VLAN interface statistics. You can optionally include all Layer 3 packet and byte counters (unicast and multicast).
show interface vlan *number* **counters snmp**	Displays the VLAN interface counters reported by SNMP MIBs.

Configuration Examples for Layer 3 Interfaces

This example shows how to configure Ethernet subinterfaces:

```
interface ethernet 2/1.10
description Layer 3
ip address 192.0.2.1/8
```

This example shows how to configure a loopback interface:

```
interface loopback 3
ip address 192.0.2.2/32
```

The following examples shows the output of the SVI counters and SVI statistics rate details when **hardware profile svi-and-si flex-stats-enable** command is enabled.

In the **show interface** command, the statistics rate or polling interval of 60 seconds and 300 seconds are added starting with Cisco NX-OS Release 10.5(2)F release.

```
show interface  vlan 2406
Vlan2406 is up, line protocol is up, autostate enabled
  Hardware is EtherSVI, address is  3c13.ccc9.a397
  Internet Address is 20.0.0.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA
  Last clearing of "show interface" counters 00:11:03
  Load-Interval #1: 1 minute (60 seconds)
  60 seconds input rate 5492528 bits/sec, 10096 packets/sec
  60 seconds output rate 0 bits/sec, 0 packets/sec
    input rate 5.49 Mbps, 10.10 Kpps; output rate 0 bps, 0 pps
  Load-Interval #2: 5 minute (300 seconds)
  300 seconds input rate 5448741 bits/sec, 10016 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
    input rate 5.45 Mbps, 10.02 Kpps; output rate 0 bps, 0 pps
  L3 Switched:
    input: 0 pkts, 0 bytes - output: 0 pkts, 0 bytes
  L3 in Switched:
    ucast: 6643884 pkts, 451784112 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes
```

Related Documents

Related Documents	Document Title
IP	*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*
VLANs	*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*

CHAPTER 6

Configuring Bidirectional Forwarding Detection

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a protocol designed to quickly identify faults in the forwarding path between two devices. BFD simplifies network profiling and planning by offering predictable reconvergence time.

BFD detects forwarding path failures across various media types, encapsulations, topologies, and routing protocols. It provides subsecond failure detection between two adjacent devices, distributing some load onto the data plane on supported modules. BFD can be less CPU-intensive than protocol hello messages.

Asynchronous mode

BFD asynchronous mode is a BFD session mode that:

- involves the exchange of periodic control packets to monitor connectivity,
- establishes and maintains BFD neighbor sessions, and
- negotiates session parameters.

BFD session parameters

The table lists the BFD session parameters and the intervals.

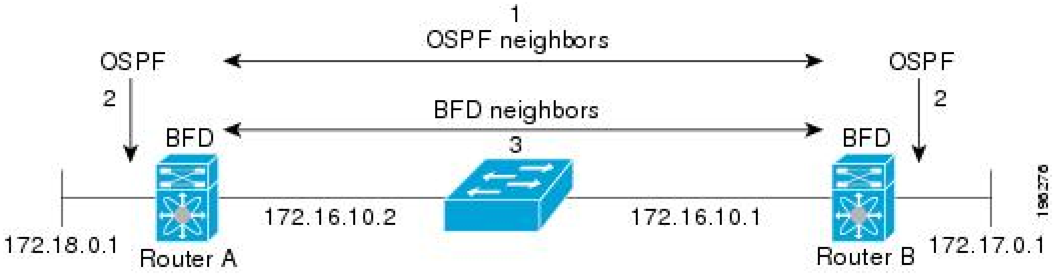
Table 11: BFD session parameters

Session Parameters	Description
Desired minimum transmit interval	The interval at which the device is configured to send BFD hello messages.
Required minimum receive interval	The minimum interval at which the device can accept BFD hello messages from another BFD device.
Detect multiplier	The number of missing BFD hello messages required to detects a fault in the forwarding path.

BFD neighbor workflow

The figure details the BFD neighbor sessions establishment between two routers.

Figure 6: Establishing a BFD Neighbor Relationship



The stages that establish a BFD neighbor session are:

1. The OSPF process discovers a BFD neighbor.
2. The local BFD process gets a request to start a session BFD neighbor session with the OSPF neighbor router.
3. The session is established between the BFD neighbor with the OSPF neighbor router.

BFD Detection of Failures

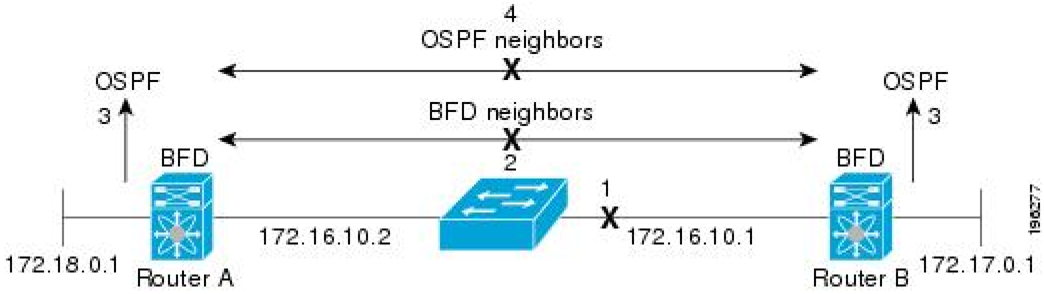
Once a BFD session has been established and timer negotiations are complete, BFD neighbors send BFD control packets that act in the same manner as an IGP hello protocol to detect liveliness, except at a more accelerated rate. BFD detects a failure, but the protocol must take action to bypass a failed 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 7: 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

Ensure you meet these prerequisites before you configure BFD.

- Enable the BFD feature.
- Disable ICMP redirect messages on interfaces where BFD is enabled.
- Disable the IP packet verification check for identical IP source and destination addresses.
- Review the detailed prerequisites in 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.
- BFD over private-vlan is not supported Cisco Nexus 9000 Switches.
- Beginning with Cisco NX-OS Release 10.2(1q)F, Layer 3 Unicast BFD is supported on Cisco Nexus N9K-C9332D-GX2B platform switches.
- 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.
- BFD per-member link support is added on Cisco Nexus 9000 Series switches.
- BFD supports BFD version 1.
- BFD supports IPv4 and IPv6.
- BFD supports OSPFv3.
- BFD supports IS-ISv6.
- When configuring BFD over IP unnumbered interfaces, use these guidelines:

    - Disable the BFD echo function to prevent the interface from flapping.
    - Enable BFD multihop when configuring BGP over IP unnumbered interface.

- Set the **ipv6 nd ns-interval** command range to 15 under the Layer 3 interface configuration to prevent BFD sessions from flapping, when there are a large number of IPv6 adjacencies.

  Alternatively, increase the BFD echo interval to avoid session instability that might occur due to CoPP drops of NS/NA packets.
- BFD supports BGPv6.
- BFD supports EIGRPv6.
- 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 Guidelines and Limitations for BFD Multihop, on page 188 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 flaps.
- 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.

- Beginning with Cisco NX-OS Release 10.5(2)F, BFD over IP unnumbered is *not* supported on Cisco Nexus 9808 and 9804 switches.
- 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*
- Cisco Nexus 9800 platform switches have the following limitation for BFD IPv6 sessions:
  - Each ASIC unit in supervisor switch mode of line card supports a maximum of 256 BFD IPv6 sessions. If more BFD IPv6 sessions are required, sessions must be spread across ASIC units or line cards.
- Beginning with Cisco NX-OS Release 10.3(1)F, BFD supports single-hop BFD on routed port, routed-sub interface, and breakout port of Cisco Nexus 9808 platform switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, BFD supports single-hop BFD on routed port, routed-sub interface, and breakout port of Cisco Nexus 9804 platform switches.
- Beginning with Cisco NX-OS Release 10.4(2)F the following are applicable for Cisco Nexus C9232E-B1 switch:
  - Single-hop BFD on routed port, routed-sub interface, and breakout ports are supported.
  - BFD Authentication is not supported.
- Beginning with Cisco NX-OS Release 10.5(3)F, the Cisco Nexus 93C64E-SG2-Q switch supports these features.
  - Single-hop BFD on Layer 3 physical interfaces and physical subinterfaces
  - Single-hop BFD on Layer 3 port channel and port channel subinterfaces

  - Single-hop BFD on routed port and breakout ports
  - Single-hop BFD on IPv4 and IPv6 address
  - Minimum BFD timer with 50ms
  - BFD asynchronous mode
  - BFD echo function

- Use the **bfd authentication interop** command to configure BFD authentication interoperability between Nexus and non-Nexus platforms. If you do not configure this command, BFD authentication fails due to an invalid authentication sequence number field format.
- BFD Authentication is not supported on Cisco Nexus 9800 platform switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, BFD supports single-hop BFD on N9KX98900CD-A and N9KX9836DM-A line cards with Cisco Nexus 9808 and 9804 switches.
- Beginning with Cisco NX-OS Release 10.4(3)F, single hop BFD is supported on Cisco Nexus 9808 and 9804 L3 port-channel interfaces and port-channel sub-interfaces with the following limitations:
  - Per Port-channel interface, only 128 sessions are supported.
  - BFD authentication is not supported.
- Beginning with Cisco NX-OS Release 10.4(3)F, single-hop BFD is supported on Layer 3 port channel on Cisco Nexus 9800 switches. The BFD server selects the hosting line card for the session among the available online line cards. However, this feature has the following limitations:
  - If the hosting line card changes, the ongoing session gets deleted on that line card, and the hosting is created on another line card that is available.
  - If the source IP of the BFD session changes, the ongoing session gets deleted and recreated with the new source IP.

BFD Support on Nexus Switches

BFD support is available on the Nexus platforms in these releases. For more information, see platform support matrix.

Table 12: BFD Support on Nexus Switches

Platform	Introduced in Cisco NX-OS Release
N93-C64E-SG2-Q	10.5.3F
N9K-C9364C-H1	10.4.3F
N9K-C93400LD-H1 N9K-C9232E-B1	10.4.2F
Nexus 9804 N9K-C9332D-H2R	10.4.1F

Platform	Introduced in Cisco NX-OS Release
Nexus 9808	10.3.1F
N9K-C9348D-GX2A N9K-C9364D-GX2A N9K-C9332D-GX2B Cisco Nexus 9300-EX, 9300-FX, 9300-FX2, 9300-FX3, and 9300-GX	10.2.3F
9364C-GX 9316D-GX 93600CD-GX N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636C-RX and N9K-X9636Q-R	9.3.3F

Default Settings

The following table lists the default settings for BFD parameters.

Table 13: 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

Configuring BFD

Best Practices for BFD configuration hierarchy and inheritance

Consider these points when you configure BFD at:

- Interface-level configuration versus global configuration
- Member ports and port channels

Interface-level configuration versus global configuration

Configure BFD at both the global level and at the interface level.

Note Interface-level configuration overrides the global configuration.

Inheritance for member ports and port channels

Configure the member port to inherit the BFD configuration of the primary port channel.

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.

Enable BFD feature

Enable the BFD feature to configure BFD on an interface and protocol.

Procedure

Step 1 Enter the configuration mode with the **configure terminal** command.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Enable BFD with the **feature bfd** command.

Example:

```
switch(config)# feature bfd
```

Step 3 (Optional) View the status of features with the **show feature | include bfd** command.

Example:

```
switch(config)# show feature | include
bfd
```

Step 4 (Optional) Save the configuration with the **copy running-config startup-config** command.

Example:

```
switch(config)# copy running-config startup-config
```

Disable BFD

Procedure

	Command or Action	Purpose
Step 1	Disable the BFD feature and remove all associated configurations with the **no feature bfd** command. **Example:** `switch(config)# no feature bfd`	

Configure global BFD parameters

Configure default session behaviors for all BFD (Bidirectional Forwarding Detection) sessions on your device.

BFD global parameters set the timer and detection characteristics for all BFD sessions. You can override these parameters at the interface.

You can configure these settings for all BFD sessions on the device. Both BFD peers negotiate the session parameters in a three-way handshake.

To override these global session parameters on an interface, see Configuring BFD on an Interface.

Use these steps to configure global BFD parameters.

Before you begin

Enable the BFD feature, see Configure global BFD parameters, on page 157

Procedure

Step 1 Enter configuration mode using the **configure terminal** command.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Configure the BFD session parameters for all BFD sessions using the **bfd interval** *mintx* **min_rx** *msec* **multiplier** *value* command.

Example:

```
switch(config)# bfd interval 50 min_rx 50 multiplier 3
```

This command overrides the values you configure for BFD session parameters on individual interfaces.

The intervals *mintx* and *msec* range from 50 milliseconds to 999 milliseconds, with a default of 50 milliseconds.

The multiplier ranges from 1 to 50. The default is 3.

Step 3 Configure the slow timer used in the echo function using the **bfd slow-timer** [*interval*] command.

Example:

```
switch(config)# bfd slow-timer 2000
```

This value determines how quickly BFD starts a new session. It specifies the rate at which asynchronous sessions send BFD control packets when the echo function is enabled.

The **slow-timer** value sets the interval for control packets. Echo packets use the configured BFD intervals for link failure detection. Control packets at the slower rate maintain the BFD session.

The range is from 1000 to 30,000 milliseconds. The default is 2000.

Step 4 Configure the interface used for Bidirectional Forwarding Detection (BFD) echo frames **bfd echo-interface loopback** *interface number*

Example:

```
switch(config)# bfd echo-interface loopback 1 3
```

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 5 (Optional) Display the BFD running configuration using the **show running-config bfd** command.

Example:

```
switch(config)# show running-config bfd
```

Step 6 (Optional) Save the configuration using the **copy running-config startup-config** command.

Example:

```
switch(config)# copy running-config startup-config
```

Your device uses the specified default BFD parameters for all BFD sessions unless you override them on an interface.

Example

Configure 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.

Procedure

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.

To disable SHA-1 authentication on the interface, use the **no** form of the command.

Step 5 Use the **bfd authentication interop** command to configure BFD authentication interoperability between Nexus and non-Nexus platforms.

Example:

```
switch(config-if)# bfd authentication interop
```

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.

Example

What to do next

-

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

Procedure

	Command or Action	Purpose

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

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.

	Command or Action	Purpose
		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.

Configure the BFD Echo function (task)

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 remains nonzero if you disable the echo function to comply with RFC 5880 When you enable the echo function, the slow timer value becomes the required minimum receive interval.

Before you begin

Enable the BFD feature. See the Enable BFD feature.

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

Disable Internet Control Message Protocol (ICMP) redirect messages on BFD-enabled interfaces using the **no ip redirects** command on the interface.

Procedure

Step 1 Enter the configuration mode using the **configure terminal** command.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Set the slow timer to determine when BFD starts a new sesion using the **bfd slow-timer** *echo-interval* command.

Example:

```
switch(config)# bfd slow-timer 2000
```

When the BFD echo function is enabled, this value also slows down the asynchronous sessions.

This value overwrites the required minimum receive interval when the echo function is enabled. The range is from 1000 to 30,000 milliseconds. The default is 2000 milliseconds.

Step 3 Enters interface configuration mode using the **interface** *int-if* command.

Example:

```
switch(config)# interface ethernet 2/1
switch(config-if)#
```

Use the ? keyword to display the supported interfaces.

Step 4 Enable the echo function using the **bfd echo** command.

Example:

```
switch(config-if)# bfd echo
```

The default is enabled.

Step 5 (Optional) Display the BFD running configuration using the **show running-config bfd** command.

Example:

```
switch(config-if)# show running-config bfd
```

Step 6 (Optional) Saves the configuration using the **copy running-config startup-config** command.

Example:

```
switch(config-if)# copy running-config startup-config
```

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

    - IETF Micro-BFD sessions supports only single-hop BFD sessions. We recommend that you do *not* configure IPs from different subnets to establish the Micro-BFD sessions.
    - 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

Procedure

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

Procedure

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

Procedure

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

Procedure

---

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

Procedure

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.

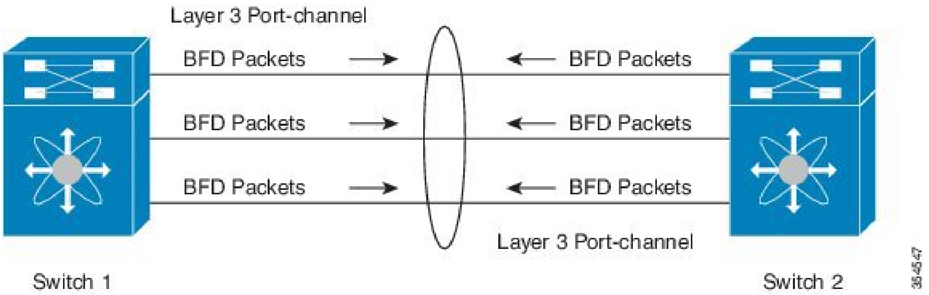
Examples: Configuring Micro BFD Sessions

See the following examples for configuring Micro BFD sessions.

Configuring Micro BFD Sessions

In this example, the following topology is used.

Figure 8: 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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

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

Procedure

	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.

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.

	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.

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

Procedure

	Command or Action	Purpose

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

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:**	(Optional) Enables BFD for all OSPF interfaces.

	Command or Action	Purpose
	`switch(config-router)# bfd`	

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

Procedure

	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.

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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
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*