# Configuring Advanced BGP Features

**First Published: October 31, 2005**
**Last Updated: August 21, 2007**

This module describes configuration tasks to configure various advanced Border Gateway Protocol (BGP) features. BGP is an interdomain routing protocol designed to provide loop-free routing between organizations. This module contains tasks to configure BGP next-hop address tracking, BGP Nonstop Forwarding (NSF) awareness, route dampening and MIB support.

### Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring Advanced BGP Features" section on page 35.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents



CISCO SYSTEMS

**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for Configuring Advanced BGP Features

Before configuring advanced BGP features you should be familiar with the "Cisco BGP Overview" module and the "Configuring a Basic BGP Network" module.

# Restrictions for Configuring Advanced BGP Features

A router that runs Cisco IOS software can be configured to run only one BGP routing process and to be a member of only one BGP autonomous system. However, a BGP routing process and autonomous system can support multiple address family configurations.

# Information About Configuring Advanced BGP Features

To configure the BGP features in this module you should understand the following concepts:



## BGP Version 4

Border Gateway Protocol (BGP) is an interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems). The Cisco IOS software implementation of BGP version 4 includes multiprotocol extensions to allow BGP to carry routing information for IP multicast routes and multiple Layer 3 protocol address families including IP Version 4 (IPv4), IP Version 6 (IPv6), Virtual Private Networks version 4 (VPNv4), and Connectionless Network Services (CLNS). For more details about configuring a basic BGP network, see the "Configuring a Basic BGP Network" module.

BGP is mainly used to connect a local network to an external network to gain access to the Internet or to connect to other organizations. When connecting to an external organization, external BGP (eBGP) peering sessions are created. For more details about connecting to external BGP peers, see the "Connecting to a Service Provider Using External BGP" module.

Although BGP is referred to as an exterior gateway protocol (EGP) many networks within an organization are becoming so complex that BGP can be used to simplify the internal network used within the organization. BGP peers within the same organization exchange routing information through internal BGP (iBGP) peering sessions. For more details about internal BGP peers, see the "Configuring Internal BGP Features" chapter of the *Cisco IOS IP Routing Configuration Guide*, Release 12.4.

**Note** BGP requires more configuration than other routing protocols and the effects of any configuration changes must be fully understood. Incorrect configuration can create routing loops and negatively impact normal network operation.

# BGP Support for Next-Hop Address Tracking

To configure BGP next-hop address tracking you should understand the following concepts:



## BGP Next-Hop Address Tracking

The BGP next-hop address tracking feature is enabled by default when a supporting Cisco IOS software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a bestpath calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.

## Default BGP Scanner Behavior

BGP monitors the next hop of installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner is used to poll the RIB for this information every 60 seconds. During the 60 second time period between scan cycles, Interior Gateway Protocol (IGP) instability or other network failures can cause black holes and routing loops to temporarily form.

## Selective BGP Next-Hop Route Filtering

In Cisco IOS Release 12.4(4)T, 12.2(33)SRB, and later releases, BGP selective next-hop route filtering was implemented as part of the BGP Selective Address Tracking feature to support BGP next-hop address tracking. Selective next-hop route filtering uses a route map to selectively define routes to help resolve the BGP next hop.

The ability to use a route map with the **bgp nexthop** command allows the configuration of the length of a prefix that applies to the BGP Next_Hop attribute. The route map is used during the BGP bestpath calculation and is applied to the route in the routing table that covers the next-hop attribute for BGP prefixes. If the next-hop route fails the route map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

**Note** Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

# BGP Nonstop Forwarding Awareness

To configure BGP Nonstop Forwarding (NSF) awareness you should understand the following concepts:

## Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, EIGRP, OSPF, and IS-IS have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices.

In this document, a networking device is said to be NSF-aware if it is running NSF-compatible software. A device is said to be NSF-capable if it has been configured to support NSF; therefore, it would rebuild routing information from NSF-aware or NSF-capable neighbors.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF then updates the line cards with the new FIB information.

**Note** Currently, EIGRP supports only NSF awareness. SSO support for EIGRP will be integrated into a future release.

## Cisco Express Forwarding for NSF

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates for CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables.

**Note** For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

## BGP Graceful Restart for NSF

When an NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the NSF-capable or NSF-aware router has "graceful restart capability." Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable router and its BGP peer(s) (NSF-aware peers) need to exchange the graceful restart capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable router as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable router reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable router as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful restart capability in an OPEN message but will establish a BGP session with the NSF-capable device. This functionality will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart capable.

## BGP NSF Awareness

BGP support for NSF requires that neighbor routers are NSF-aware or NSF-capable. NSF awareness in BGP is also enabled by the graceful restart mechanism. A router that is NSF-aware functions like a router that is NSF-capable with one exception: an NSF-aware router is incapable of performing an SSO operation. However, a router that is NSF-aware is capable of maintaining a peering relationship with a NSF-capable neighbor during a NSF SSO operation, as well as holding routes for this neighbor during the SSO operation.

The BGP Nonstop Forwarding Awareness feature provides an NSF-aware router with the capability to detect a neighbor that is undergoing an SSO operation, maintain the peering session with this neighbor, retain known routes, and continue to forward packets for these routes. The deployment of BGP NSF awareness can minimize the affects of route-processor (RP) failure conditions and improve the overall network stability by reducing the amount of resources that are normally required for reestablishing peering with a failed router.

NSF awareness for BGP is not enabled by default. The **bgp graceful-restart** command is used to enable NSF awareness on a router that is running BGP. NSF-aware operations are also transparent to the network operator and BGP peers that do not support NSF capabilities.

**Note** NSF awareness is enabled automatically in supported software images for Interior Gateway Protocols, such as EIGRP, IS-IS, and OSPF. In BGP, NSF awareness is not enabled automatically and must be started by issuing the **bgp graceful-restart** command in router configuration mode.

# BGP Route Dampening

Route dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when its availability alternates repeatedly.

For example, consider a network with three BGP autonomous systems: autonomous system 1, autonomous system 2, and autonomous system 3. Suppose the route to network A in autonomous system 1 flaps (it becomes unavailable). Under circumstances without route dampening, the eBGP neighbor of autonomous system 1 to autonomous system 2 sends a withdraw message to autonomous system 2. The border router in autonomous system 2, in turn, propagates the withdraw message to autonomous system 3. When the route to network A reappears, autonomous system 1 sends an advertisement message to autonomous system 2, which sends it to autonomous system 3. If the route to network A repeatedly becomes unavailable, then available, many withdrawal and advertisement messages are sent. This is a problem in an internetwork connected to the Internet because a route flap in the Internet backbone usually involves many routes.

**Note** No penalty is applied to a BGP peer reset when route dampening is enabled. Although the reset withdraws the route, no penalty is applied in this instance, even if route flap dampening is enabled.

### Minimizing Flapping

The route dampening feature minimizes the flapping problem as follows. Suppose again that the route to network A flaps. The router in autonomous system 2 (where route dampening is enabled) assigns network A a penalty of 1000 and moves it to history state. The router in autonomous system 2 continues to advertise the status of the route to neighbors. The penalties are cumulative. When the route flaps so often that the penalty exceeds a configurable suppress limit, the router stops advertising the route to network A, regardless of how many times it flaps. Thus, the route is dampened.

The penalty placed on network A is decayed until the reuse limit is reached, upon which the route is once again advertised. At half of the reuse limit, the dampening information for the route to network A is removed.

### Understanding Route Dampening Terms

The following terms are used when describing route dampening:

- Flap—A route whose availability alternates repeatedly.
- History state—After a route flaps once, it is assigned a penalty and put into history state, meaning the router does not have the best path, based on historical information.
- Penalty—Each time a route flaps, the router configured for route dampening in another autonomous system assigns the route a penalty of 1000. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. At that point, the route state changes from history to damp.
- Damp state—In this state, the route has flapped so often that the router will not advertise this route to BGP neighbors.
- Suppress limit—A route is suppressed when its penalty exceeds this limit. The default value is 2000.

- Half-life—Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds.
- Reuse limit—As the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. The process of unsuppressing routes occurs at 10-second increments. Every 10 seconds, the router finds out which routes are now unsuppressed and advertises them to the world.
- Maximum suppress limit—This value is the maximum amount of time a route can be suppressed. The default value is four times the half-life.

The routes external to an autonomous system learned via iBGP are not dampened. This policy prevent the iBGP peers from having a higher penalty for routes external to the autonomous system.

# BFD for BGP

Bidirectional Forwarding Detection (BFD) support for BGP was introduced in Cisco IOS Releases 12.0(31)S, 12.4(4)T, 12.0(32)S, and 12.2(33)SXH, and later releases. 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. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable. The main benefit of implementing BFD for BGP is a marked decrease in reconvergence time.

One caveat exists for BFD; BFD and BGP graceful restart capability cannot both be configured on a router running BGP. If an interface goes down, BFD detects the failure and indicates that the interface cannot be used for traffic forwarding and the BGP session goes down, but graceful restart still allows traffic forwarding on platforms that support NSF even though the BGP session is down, allowing traffic forwarding using the interface that is down. Configuring both BFD and BGP graceful restart for NSF on a router running BGP may result in suboptimal routing.

For more details about BFD, see the Bidirectional Forwarding Detection chapter of the Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4(4)T.

# BGP MIB Support

The Management Information Base (MIB) to support BGP is the CISCO-BGP4-MIB. In Cisco IOS Release 12.0(26)S, 12.3(7)T, 12.2(25)S, 12.2(33SRA, and 12.2(33)SXH, and later releases the BGP MIB Support Enhancements feature introduced support in the CISCO-BGP4-MIB for new SNMP notifications. The following sections describe the objects and notifications (traps) that are supported:

- BGP FSM Transition Change Support, page 8
- BGP Route Received Route Support, page 8
- BGP Prefix Threshold Notification Support, page 8
- VPNv4 Unicast Address Family Route Support, page 9
- cbgpPeerTable Support, page 9

### BGP FSM Transition Change Support

The *cbgpRouteTable* supports BGP Finite State Machine (FSM) transition state changes.

The *cbgpFsmStateChange* object allows you to configure SNMP notifications (traps) for all FSM transition state changes. This notification contains the following MIB objects:

- *bgpPeerLastError*
- *bgpPeerState*
- *cbgpPeerLastErrorTxt*
- *cbgpPeerPrevState*

The *cbgpBackwardTransition* object supports all BGP FSM transition state changes. This object is sent each time the FSM moves to either a higher or lower numbered state. This notification contains the following MIB objects:

- *bgpPeerLastError*
- *bgpPeerState*
- *cbgpPeerLastErrorTxt*
- *cbgpPeerPrevState*

The **snmp-server enable bgp traps** command allows you to enable the traps individually or together with the existing FSM backward transition and established state traps as defined in *RFC 1657*.

### BGP Route Received Route Support

The *cbgpRouteTable* object supports the total number of routes received by a BGP neighbor. The following MIB object is used to query the CISCO-BGP4-MIB for routes that are learned from individual BGP peers:

- *cbgpPeerAddrFamilyPrefixTable*

Routes are indexed by the address-family identifier (AFI) or subaddress-family identifier (SAFI). The prefix information displayed in this table can also viewed in the output of the **show ip bgp** command.

### BGP Prefix Threshold Notification Support

The *cbgpPrefixMaxThresholdExceed* and *cbgpPrfefixMaxThresholdClear* objects were introduced to allow you to poll for the total number of routes received by a BGP peer.

The *cbgpPrefixMaxThresholdExceed* object allows you to configure SNMP notifications to be sent when the prefix count for a BGP session has exceeded the configured value. This notification is configured on a per address family basis. The prefix threshold is configured with the **neighbor maximum-prefix** command. This notification contains the following MIB objects:

- *cbgpPeerPrefixAdminLimit*
- *cbgpPeerPrefixThreshold*

The *cbgpPrfefixMaxThresholdClear* object allows you to configure SNMP notifications to be sent when the prefix count drops below the clear trap limit. This notification is configured on a per address family basis. This notification contains the following objects:

- *cbgpPeerPrefixAdminLimit*
- *cbgpPeerPrefixClearThreshold*

Notifications are sent when the prefix count drops below the clear trap limit for an address family under a BGP session after the *cbgpPrefixMaxThresholdExceed* notification is generated. The clear trap limit is calculated by subtracting 5 percent from the maximum prefix limit value configured with the **neighbor maximum-prefix** command. This notification will not be generated if the session goes down for any other reason after the *cbgpPrefixMaxThresholdExceed* is generated.

#### VPNv4 Unicast Address Family Route Support

The *cbgpRouteTable* object allows you to configure SNMP GET operations for VPNv4 unicast address-family routes.

The following MIB object allows you to query for multiple BGP capabilities (for example, route refresh, multiprotocol BGP extensions, and graceful restart):

- *cbgpPeerCapsTable*

The following MIB object allows you to query for IPv4 and VPNv4 address family routes:

- *cbgpPeerAddrFamilyTable*

Each route is indexed by peer address, prefix, and prefix length. This object indexes BGP routes by the AFI and then by the SAFI. The AFI table is the primary index, and the SAFI table is the secondary index. Each BGP speaker maintains a local Routing Information Base (RIB) for each supported AFI and SAFI combination.

#### cbgpPeerTable Support

The cbgpPeerTable has been modified to support the enhancements described in this document. The following new table objects are supported in the CISCO-BGP-MIB.my:

- *cbgpPeerLastErrorTxt*
- *cbgpPeerPrevState*

The following table objects are not supported. The status of theses objects is listed as deprecated, and these objects are not operational:

- *cbgpPeerPrefixAccepted*
- *cbgpPeerPrefixDenied*
- *cbgpPeerPrefixLimit*
- *cbgpPeerPrefixAdvertised*
- *cbgpPeerPrefixSuppressed*
- *cbgpPeerPrefixWithdrawn*

# How to Configure Advanced BGP Features

This section contains the following task groups:

# Configuring BGP Next-Hop Address Tracking

The tasks in this section show how configure BGP next-hop address tracking. BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP. For more details about configuring route dampening, see the "Configuring BGP Route Dampening" section on page 20.



## Disabling BGP Next-Hop Address Tracking

Perform this task to disable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default under the IPv4 and VPNv4 address families. Disabling next hop address tracking may be useful if you the network has unstable IGP peers and route dampening is not resolving the stability issues. To reenable BGP next-hop address tracking, use the **bgp nexthop** command with the **trigger** and **enable** keywords.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]
5. **no bgp nexthop trigger enable**
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router bgp as-number**<br><br>**Example:**<br>`Router(config)# router bgp 64512` | Enters router configuration mod to create or configure a BGP routing process. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **address-family ipv4** [**mdt** \| **multicast** \| **tunnel** \| **unicast** [**vrf** *vrf-name*] \| **vrf** *vrf-name*] \| **vpnv4** [**unicast**]<br><br>**Example:**<br>`Router(config-router-af)# address-family ipv4 unicast` | Enter address family configuration mode to configure BGP peers to accept address family-specific configurations.<br>• The example creates an IPv4 unicast address family session. |
| **Step 5** | **no bgp nexthop trigger enable**<br><br>**Example:**<br>`Router(config-router-af)# no bgp nexthop trigger enable` | Disables BGP next-hop address tracking.<br>• Next-hop address tracking is enabled by default for IPv4 and VPNv4 address family sessions.<br>• The example disables next-hop address tracking. |
| **Step 6** | **end**<br><br>**Example:**<br>`Router(config-router-af)# end` | Exits address-family configuration mode, and enters Privileged EXEC mode. |

## Adjusting the Delay Interval for BGP Next-Hop Address Tracking

Perform this task to adjust the delay interval between routing table walks for BGP next-hop address tracking.

### Delay Interval Tuning to Match the Interior Gateway Protocol

You can increase the performance of this feature by tuning the delay interval between full routing table walks to match the tuning parameters for the Interior Gateway protocol (IGP). The default delay interval is 5 seconds. This value is optimal for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

### Aggressive IGP Route Dampening

BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]
5. **bgp nexthop trigger delay** *delay-timer*
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router bgp as-number**<br><br>**Example:**<br>`Router(config)# router bgp 64512` | Enters router configuration mode to create or configure a BGP routing process. |
| **Step 4** | **address-family ipv4** [**mdt** \| **multicast** \| **tunnel** \| **unicast** [**vrf** *vrf-name*] \| **vrf** *vrf-name*] \| **vpnv4** [**unicast**]<br><br>**Example:**<br>`Router(config-router-af)# address-family ipv4 unicast` | Enter address family configuration mode to configure BGP peers to accept address family-specific configurations.<br>• The example creates an IPv4 unicast address family session. |
| **Step 5** | **bgp nexthop trigger delay delay-timer**<br><br>**Example:**<br>`Router(config-router-af)# bgp nexthop trigger delay 20` | Configures the delay interval between routing table walks for next-hop address tracking.<br>• The time period determines how long BGP will wait before starting a full routing table walk after notification is received.<br>• The value for the *delay-timer* argument is a number from 1 to 100 seconds. The default value is 5 second.<br>• The example configures a delay interval of 20 seconds. |
| **Step 6** | **end**<br><br>**Example:**<br>`Router(config-router-af)# end` | Exits address-family configuration mode, and enters privileged EXEC mode. |

## Configuring BGP Selective Next-Hop Route Filtering

Perform this task to configure selective next-hop route filtering using a route map to filter potential next-hop routes. This task uses prefix lists and route maps to match IP addresses or source protocols and can be used to avoid aggregate addresses and BGP prefixes being considered as next-hop routes.

For more examples of how to use the **bgp nexthop** command, see the "Configuring BGP Selective Next-Hop Route Filtering: Examples" section on page 29.

### BGP Next_Hop Attribute

The Next_Hop attribute identifies the next-hop IP address to be used as the BGP next hop to the destination. The router makes a recursive lookup to find the BGP next hop in the routing table. In external BGP (eBGP), the next hop is the IP address of the peer that sent the update. Internal BGP (iBGP) sets the next-hop address to the IP address of the peer that advertised the prefix for routes that originate internally. When any routes to iBGP that are learned from eBGP are advertised, the Next_Hop attribute is unchanged.

A BGP next-hop IP address must be reachable in order for the router to use a BGP route. Reachability information is usually provided by the IGP, and changes in the IGP can influence the forwarding of the next-hop address over a network backbone.

### Restrictions

Only **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **bgp nexthop route-map** *map-name*
6. **exit**
7. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
8. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
9. **match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*]
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **end**
13. **show ip bgp** [*network*] [*network-mask*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **router bgp** *autonomous-system-number*<br><br>**Example:**<br>`Router(config)# router bgp 45000` | Enters router configuration mode and creates a BGP routing process. |
| **Step 4** | **address-family ipv4** [**unicast** \| **multicast** \| **vrf** *vrf-name*]<br><br>**Example:**<br>`Router(config-router)# address-family ipv4 unicast` | Specifies the IPv4 address family and enters address family configuration mode.<br>• The **unicast** keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the **unicast** keyword is not specified with the **address-family ipv4** command.<br>• The **multicast** keyword specifies IPv4 multicast address prefixes.<br>• The **vrf** keyword and *vrf-name* argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands. |
| **Step 5** | **bgp nexthop route-map** *map-name*<br><br>**Example:**<br>`Router(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP` | Permits a route map to selectively define routes to help resolve the BGP next hop.<br>• In this example the route map named CHECK-NEXTHOP is created. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-router-af)# exit` | Exits address family configuration mode and enters router configuration mode. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-router)# exit` | Exits router configuration mode and enters global configuration mode. |
| **Step 8** | **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* \| **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]<br><br>**Example:**<br>`Router(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25` | Creates a prefix list for BGP next-hop route filtering.<br>• Selective next-hop route filtering supports prefix length matching or source protocol matching on a per address-family basis.<br>• The example creates a prefix list named FILTER25 that permits routes only if the mask length is more than 25; this will avoid aggregate routes being considered as the next-hop route. |
| **Step 9** | **route-map** *map-name* [**permit** \| **deny**] [*sequence-number*]<br><br>**Example:**<br>`Router(config)# route-map CHECK-NEXTHOP deny 10` | Configures a route map and enters route map configuration mode.<br>• In this example, a route map named CHECK-NEXTHOP is created. If there is an IP address match in the following **match** command, the IP address will be denied. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **match ip address prefix-list** *prefix-list-name* [*prefix-list-name...*]<br><br>**Example:**<br>`Router(config-route-map)# match ip address prefix-list FILTER25` | Matches the IP addresses in the specified prefix list.<br>• Use the *prefix-list-name* argument to specify the name of a prefix list. The ellipsis means that more than one prefix list can be specified.<br>**Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T. |
| **Step 11** | **exit**<br><br>**Example:**<br>`Router(config-route-map)# exit` | Exits route map configuration mode and enters global configuration mode. |
| **Step 12** | **route-map** *map-name* [**permit** \| **deny**] [*sequence-number*]<br><br>**Example:**<br>`Router(config)# route-map CHECK-NEXTHOP permit 20` | Configures a route map and enters route map configuration mode.<br>• In this example, all other IP addresses are permitted by route map CHECK-NEXTHOP. |
| **Step 13** | **end**<br><br>**Example:**<br>`Router(config-route-map)# end` | Exits route map configuration mode and enters privileged EXEC mode. |
| **Step 14** | **show ip bgp** [*network*] [*network-mask*]<br><br>**Example:**<br>`Router# show ip bgp` | Displays the entries in the BGP routing table.<br>• Enter this command to view the next-hop addresses for each route.<br>**Note** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T. |

## Examples

The following example from the **show ip bgp** command shows the next-hop addresses for each route:

```
BGP table version is 7, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.1.0/24      192.168.1.2              0             0 40000 i
*  10.2.2.0/24      192.168.3.2              0             0 50000 i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
*> 172.17.1.0/24    0.0.0.0                  0         32768
```

# Configuring BGP Nonstop Forwarding Awareness

The tasks in this section show how configure BGP Nonstop Forwarding (NSF) awareness. The first task enables BGP NSF and suggests a few troubleshooting options. The second task describes how to adjust the BGP graceful restart timers although the default settings are optimal for most network deployments, and the third task verifies the local and peer router configuration of BGP NSF.



## Enabling BGP NSF Awareness

Perform this task to enable BGP NSF awareness. BGP NSF awareness is part of the graceful restart mechanism and BGP NSF awareness is enabled by issuing the **bgp graceful-restart** command in router configuration mode. BGP NSF awareness allows NSF-aware routers to support NSF-capable routers during an SSO operation. NSF-awareness is not enabled by default and should be configured on all neighbors that participate in BGP NSF.

**Note** The configuration of the restart and stalepath timers is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

### Restrictions

Configuring both BFD and BGP graceful restart for NSF on a router running BGP may result in suboptimal routing. For more details, see the "BFD for BGP" section on page 7.

### SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart**
5. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure** {**terminal** \| **memory** \| **network**}<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router bgp** autonomous-system-*number*<br><br>**Example:**<br>`Router(config)# router bgp 101` | Enters router configuration mode and creates a BGP routing process. |
| **Step 4** | **bgp graceful-restart** [**restart-time** *seconds*] [**stalepath-time** *seconds*]<br><br>**Example:**<br>`Router(config-router)# bgp graceful-restart` | Enables the BGP graceful restart capability and BGP NSF awareness.<br>• If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor.<br>• Use this command on the restarting router and all of its peers (NSF-capable and NSF-aware). |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-router)# exit` | Exits router configuration mode and enters global configuration mode. |

### Troubleshooting Tips

To troubleshoot the NSF feature, use the following commands in privileged EXEC mode, as needed:

- **debug ip bgp**—Displays open messages that advertise the graceful restart capability.
- **debug ip bgp updates**—Displays sent and received EOR messages. The EOR message is used by the NSF-aware router to start the stalepath timer, if configured.
- **debug ip bgp event**—Displays graceful restart timer events, such as the restart timer and the stalepath timer.
- **show ip bgp**—Displays entries in the BGP routing table. The output from this command will display routes that are marked as stale by displaying the letter “S” next to each stale route.
- **show ip bgp neighbor**—Displays information about the TCP and BGP connections to neighbor devices. When enabled, the graceful restart capability is displayed in the output of this command.

### What to do next

If the **bgp graceful-restart** command has been issued after the BGP session has been established, you must reset by issuing the **clear ip bgp *** command or by reloading the router before graceful restart capabilities will be exchanged. For more information about resetting BGP sessions and using the **clear ip bgp** command, see the "Configuring a Basic BGP Network" module.

## Configuring BGP NSF Awareness Timers

Perform this task to adjust the BGP graceful restart timers.

### BGP Graceful Restart Timers

There are two BGP graceful restart timers that can be configured. The optional **restart-time** keyword and *seconds* argument determine how long peer routers will wait to delete stale routes before a BGP open message is received. The default value is 120 seconds. The optional **stalepath-time** keyword and *seconds* argument determine how long a router will wait before deleting stale routes after an end of record (EOR) message is received from the restarting router. The default value is 360 seconds.

**Note** The configuration of the restart and stalepath timers is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

### SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart restart-time** *seconds*
5. **bgp graceful-restart stalepath-time** *seconds*
6. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure** {**terminal** \| **memory** \| **network**}<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **router bgp** *as-number*<br><br>**Example:**<br>`Router(config)# router bgp 101` | Enters router configuration mode and creates a BGP routing process. |
| **Step 4** | **bgp graceful-restart** [**restart-time** seconds] [**stalepath-time** *seconds*]<br><br>**Example:**<br>`Router(config-router)# bgp graceful-restart restart-time 130` | Enables the BGP graceful restart capability and BGP NSF awareness.<br>• The **restart-time** argument determines how long peer routers will wait to delete stale routes before a BGP open message is received.<br>• The default value is 120 seconds. The configurable range is from 1 to 3600 seconds. |
| **Step 5** | **bgp graceful-restart** [**restart-time** seconds] [**stalepath-time** *seconds*]<br><br>**Example:**<br>`Router(config-router)# bgp graceful-restart stalepath-time 350` | Enables the BGP graceful restart capability and BGP NSF awareness.<br>• The **stalepath-time** argument determines how long a router will wait before deleting stale routes after an end of record (EOR) message is received from the restarting router.<br>• The default value is 360 seconds. The configurable range is from 1 to 3600 seconds. |
| **Step 6** | `Router(config-router)# end`<br><br>**Example:**<br>`Router(config-router)# end` | Exits router configuration mode and enters privileged EXEC mode. |

### What To Do Next

If the **bgp graceful-restart** command has been issued after the BGP session has been established, you must reset the peer sessions by issuing the **clear ip bgp *** command or by reloading the router before graceful restart capabilities will be exchanged. For more information about resetting BGP sessions and using the **clear ip bgp** command, see the "Configuring a Basic BGP Network" module.

## Verifying the Configuration of BGP Nonstop Forwarding Awareness

Use the following steps to verify the local configuration of BGP NSF awareness on a router and to verify the configuration NSF awareness on peer routers in a BGP network.

### SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]
3. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]

### DETAILED STEPS

**Step 1** **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

**Step 2** **show running-config** [*options*]

Displays the running configuration on the local router. The output will display the configuration of the **bgp graceful-restart** command in the BGP section. Repeat this command on all BGP neighbor routers to verify that all BGP peers are configured for BGP NSF awareness.

```
Router# show running-config

.
.
.
router bgp 45000
 bgp router-id 172.17.1.99
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 130
 bgp graceful-restart stalepath-time 350
 bgp graceful-restart
 timers bgp 70 120
 neighbor 192.168.1.2 remote-as 40000
```

**Step 3** **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]]

Displays information about TCP and BGP connections to neighbors. “Graceful Restart Capabilty:advertised and received” will be displayed for each neighbor that has exchanged graceful restart capabilities with this router.

The following partial output example displays the graceful restart information for BGP neighbor 192.168.1.2 at Router A in :

```
Router# show ip bgp neighbors 192.168.1.2

BGP neighbor is 192.168.1.2,  remote AS 40000, external link
  BGP version 4, remote router ID 10.1.1.99
  BGP state = Established, up for 00:00:47
  Last read 00:00:07, last write 00:00:05, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtims
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
```

# Configuring BGP Route Dampening

The tasks in this section configure and monitor BGP route dampening. Route dampening is designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when its availability alternates repeatedly.



## Enabling and Configuring BGP Route Dampening

Perform this task to enable and configure BGP route dampening.

## SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **bgp dampening** [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]
6. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure** {**terminal** \| **memory** \| **network**}<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router bgp** as-*number*<br><br>**Example:**<br>`Router(config)# router bgp 45000` | Enters router configuration mode and creates a BGP routing process. |
| **Step 4** | **address-family ipv4** [**unicast** \| **multicast** \| **vrf** *vrf-name*]<br><br>**Example:**<br>`Router(config-router)# address-family ipv4 unicast` | Specifies the IPv4 address family and enters address family configuration mode.<br>• The **unicast** keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the **unicast** keyword is not specified with the **address-family ipv4** command.<br>• The **multicast** keyword specifies IPv4 multicast address prefixes.<br>• The **vrf** keyword and *vrf-name* argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **bgp dampening** [half-life reuse suppress max-suppress-time] [**route-map** *map-name*]<br><br>**Example:**<br>`Router(config-router-af)# bgp dampening 30 1500 10000 120` | Enables BGP route dampening and changes the default values of route dampening factors.<br>• The *half-life*, *reuse*, *suppress*, and *max-suppress-time* arguments are all position dependent; if one argument is entered then all the arguments must be entered.<br>• Use the **route-map** keyword and *map-name* argument to control where BGP route dampening is enabled. |
| **Step 6** | **end**<br><br>**Example:**<br>`Router(config-router-af)# end` | Exits address family configuration mode and enters privileged EXEC mode. |

## Monitoring and Maintaining BGP Route Dampening

Perform the steps in this task as required to monitor and maintain BGP route dampening.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *access-list*} | {*ip-address mask* [**longer-prefix**]}]
3. **clear ip bgp flap-statistics** [*neighbor-address* [*ipv4-mask*]] [**regexp** *regexp* | **filter-list** *extcom-number*]
4. **show ip bgp dampened-paths**
5. **clear ip bgp** [**ipv4** {**multicast** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4** {**unicast**}] **dampening** [*neighbor-address*] [*ipv4-mask*]

### DETAILED STEPS

**Step 1** **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

**Step 2** **show ip bgp flap-statistics** [{**regexp** *regexp*} | {**filter-list** *access-list*} | {*ip-address mask* [**longer-prefix**]}]

Use this command to monitor the flaps of all the paths that are flapping. The statistics will be deleted once the route is not suppressed and is stable for at least one half-life.

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 172.17.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 10.0.0.0         172.17.232.177  4     00:13:31 00:18:10 100
*d 10.2.0.0         172.17.232.177  4     00:02:45 00:28:20 100
```

**Step 3** **clear ip bgp flap-statistics** [*neighbor-address* [*ipv4-mask*]] [**regexp** *regexp* | **filter-list** *extcom-number*]

Use this command to clear the accumulated penalty for routes that are received on a router that has BGP dampening enabled. If no arguments or keywords are specified, flap statistics are cleared for all routes. Flap statistics are also cleared when the peer is stable for the half-life time period. After the BGP flap statistics are cleared, the route is less likely to be dampened.

```
Router# clear ip bgp flap-statistics 172.17.232.177
```

**Step 4** **show ip bgp dampened-paths**

Use this command to monitor the flaps of all the paths that are flapping. The statistics will be deleted once the route is not suppressed and is stable for at least one half-life.

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 10.0.0.0         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

**Step 5** **clear ip bgp** [**ipv4** {**multicast** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpnv4** {**unicast**}] **dampening** [*neighbor-address*] [*ipv4-mask*]

Use this command to clear stored route dampening information. If no keywords or arguments are entered, route dampening information for the entire routing table is cleared. The following example clears route dampening information for VPNv4 address family prefixes from network 192.168.10.0/24, and unsuppresses its suppressed routes.

```
Router# clear ip bgp vpnv4 unicast dampening 192.168.10.0 255.255.255.0
```

# Decreasing BGP Convergence Time Using BFD

BFD support for BGP was introduced in Cisco IOS Releases 12.0(31)S, 12.4(4)T, 12.0(32)S, and 12.2(33)SXH, and later releases. You start a BFD process by configuring BFD on the interface. When the BFD process is started, no entries are created in the adjacency database, in other words, no BFD control packets are sent or received. The adjacency creation takes places once you have configured BFD support for the applicable routing protocols. The first two tasks must be configured to implement BFD support for BGP to reduce the BGP convergence time. The third task is an optional task to help monitor or troubleshoot BFD.


- Configuring BFD Session Parameters on the Interface, page 24
- Configuring BFD Support for BGP, page 25
- Monitoring and Troubleshooting BFD for Cisco 7600 Series Routers, page 26


## Prerequisites

- Cisco Express Forwarding (CEF) and IP routing must be enabled on all participating routers.
- BGP must be configured on the routers before BFD is deployed. You should implement fast convergence for the routing protocol that you are using. See the IP routing documentation for your version of Cisco IOS software for information on configuring fast convergence.

## Restrictions

- For the current Cisco implementation of BFD support for BGP in Cisco IOS Releases 12.0(31)S, 12.4(4)T, 12.0(32)S, and 12.2(33)SXH, only asynchronous mode is supported. In asynchronous mode, either BFD peer can initiate a BFD session.
- For the current Cisco implementation of BFD support for BGP in Cisco IOS Releases 12.0(31)S, 12.4(4)T, 12.0(32)S, and 12.2(33)SXH, BFD is supported only for IPv4 networks.
- BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away. Multihop configurations are not supported.
- Configuring both BFD and BGP graceful restart for NSF on a router running BGP may result in suboptimal routing. For more details, see the "BFD for BGP" section on page 7.

## 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.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface FastEthernet 6/0` | Enters interface configuration mode. |
| **Step 4** | **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*<br><br>**Example:**<br>`Router(config-if)# bfd interval 50 min_rx 50 multiplier 5` | Enables BFD on the interface. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Exits interface configuration mode. |

## Configuring BFD Support for BGP

Perform this task to configure BFD support for BGP, so that BGP is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD.

### Prerequisites

- BGP must be running on all participating routers.
- The baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured. See the "Configuring BFD Session Parameters on the Interface" section on page 24 for more information.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **fall-over bfd**
5. **end**
6. **show bfd neighbors** [**details**]
7. **show ip bgp neighbors**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router bgp** *autonomous-system-number*<br><br>*Example:*<br>`Router(config)# router bgp tag1` | Specifies a BGP process and enters router configuration mode. |
| **Step 4** | **neighbor** *ip-address* **fall-over bfd**<br><br>**Example:**<br>`Router(config-router)# neighbor 172.16.10.2 fall-over bfd` | Enables BFD support for fallover. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-router)# end` | Returns the router to privileged EXEC mode. |
| **Step 6** | **show bfd neighbors** [**details**]<br><br>**Example:**<br>`Router# show bfd neighbors detail` | Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered. |
| **Step 7** | **show ip bgp neighbor**<br><br>**Example:**<br>`Router# show ip bgp neighbor` | Displays information about BGP and TCP connections to neighbors. |

## Monitoring and Troubleshooting BFD for Cisco 7600 Series Routers

To monitor or troubleshoot BFD on Cisco 7600 series routers, perform one or more of the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **show bfd neighbors** [**details**]
3. **debug bfd** [**event** | **packet** | **ipc-error** | **ipc-event** | **oir-error** | **oir-event**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show bfd neighbors** [**details**]<br><br>**Example:**<br>`Router# show bfd neighbors details` | (Optional) Displays the BFD adjacency database.<br>• The **details** keyword shows all BFD protocol parameters and timers per neighbor. |
| **Step 3** | **debug bfd** [**event** \| **packet** \| **ipc-error** \| **ipc-event** \| **oir-error** \| **oir-event**]<br><br>**Example:**<br>`Router# debug bfd packet` | (Optional) Displays debugging information about BFD packets. |

### What to Do Next

For more information about configuring BFD support for another routing protocol, see the Bidirectional Forwarding Detection feature in Cisco IOS Release 12.4(4)T.

# Enabling BGP MIB Support

SNMP notifications can be configured on the router and GET operations can be performed from an external management station only after BGP SNMP support is enabled. Perform this task on a router to configure SNMP notifications for the BGP MIB.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps bgp** [**state-changes** {[**all**] [**backward-trans**] [**limited**]}] | [**threshold prefix**]
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **snmp-server enable traps bgp** [**state-changes** {[**all**] [**backward-trans**] [**limited**]}] \| [**threshold prefix**]<br><br>**Example:**<br>`Router# snmp-server enable traps bgp` | Enables BGP support for SNMP operations. Entering this command with no keywords or arguments enables support for all BGP events.<br>• The **state-changes** keyword is used to enable support for FSM transition events.<br>• The **all** keyword enables support for FSM transitions events.<br>• The **backward-trans** keyword enables support only for backward transition state change events.<br>• The **limited** keyword enables support for backward transition state changes and established state events.<br>• The **threshold** and **prefix** keywords are used to enable notifications when the configured maximum prefix limit is reached on the specified peer. |
| Step 4 | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode, and enters privileged EXEC mode. |

# Configuration Examples for Configuring Advanced BGP Features

This section contains the following examples:



## Enabling and Disabling BGP Next-Hop Address Tracking: Example

In the following example, next-hop address tracking is disabled under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
  no bgp nexthop trigger enable
```

# Adjusting the Delay Interval for BGP Next-Hop Address Tracking: Example

In the following example, the delay interval for next-hop tracking is configured to occur every 20 seconds under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
  bgp nexthop trigger delay 20
```

# Configuring BGP Selective Next-Hop Route Filtering: Examples

The following example shows how to configure BGP selective next-hop route filtering to avoid using a BGP prefix as the next-hop route. If the most specific route that covers the next hop is a BGP route, then the BGP route will be marked as unreachable. The next hop must be an IGP or static route.

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP
 exit
 exit
route-map CHECK-BGP deny 10
 match source-protocol bgp 1
 exit
route-map CHECK-BGP permit 20
 end
```

The following example shows how to configure BGP selective next-hop route filtering to avoid using a BGP prefix as the next-hop route and to ensure that the prefix is more specific than /25.

```
router bgp 45000
 address-family ipv4 unicast
 bgp nexthop route-map CHECK-BGP25
 exit
 exit
ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 le 25
route-map CHECK-BGP25 deny 10
 match ip address prefix-list FILTER25
 exit
route-map CHECK-BGP25 deny 20
 match source-protocol bgp 1
 exit
route-map CHECK-BGP25 permit 30
 end
```

# Configuring BGP NSF Awareness: Example

The following example configures BGP NSF awareness on a router that is running BGP:

```
configure terminal
 router bgp 45000
 bgp graceful-restart
```

# Configuring the Restart Time for BGP NSF Awareness: Example

The following example configures BGP NSF awareness on a router that is running BGP and sets the restart time to 130 seconds. The configuration of this timer is optional and the preconfigured default value is optimal for most network deployments.

```
configure terminal
 router bgp 45000
 bgp graceful-restart restart-time 130
```

# Configuring the Stalepath Time for BGP NSF Awareness: Example

The following example configures BGP NSF awareness on a router that is running BGP and sets the stale path time to 350 seconds. The configuration of this timer is optional and the preconfigured default value is optimal for most network deployments.

```
configure terminal
 router bgp 45000
 bgp graceful-restart stalepath-time 350
```

# Configuring BGP Route Dampening: Example

The following example configures BGP dampening to be applied to prefixes filtered through the route-map named ACCOUNTING:

```
ip prefix-list FINANCE permit 10.0.0.0/8
!
route-map ACCOUNTING
 match ip address ip prefix-list FINANCE
 exit
router bgp 50000
 address-family ipv4
 bgp dampening route-map ACCOUNTING
 end
```

# Configuring BFD on a BGP Network: Example

In the following example, the simple BGP network consists of Router A and Router B. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 in Router B. The example, starting in global configuration mode, shows the configuration of BFD.

### Configuration for Router A

```
!
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 3/0.1
ip address 172.17.0.1 255.255.255.0
!
!
router bgp 40000
 bgp log-neighbor-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
```

```
 !
 address-family ipv4
 neighbor 172.16.10.2 activate
 no auto-summary
 no synchronization
 network 172.18.0.0 mask 255.255.255.0
 exit-address-family
!
```

### Configuration for Router B

```
!
interface FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 6/1
 ip address 172.18.0.1 255.255.255.0
!
router bgp 45000
 bgp log-neighbor-changes
 neighbor 172.16.10.1 remote-as 40000
 neighbor 172.16.10.1 fall-over bfd
 !
 address-family ipv4
 neighbor 172.16.10.1 activate
 no auto-summary
 no synchronization
 network 172.17.0.0 mask 255.255.255.0
 exit-address-family
!
```

The output from the **show bfd neighbors details** command from Router A verifies that a BFD session has been created and that BGP is registered for BFD support. The relevant command output is shown in bold in the output.

### Router A

```
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   332  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(15491)
Rx Count: 9160, Rx Interval (ms) min/max/avg: 200/440/332 last: 268 ms ago
Tx Count: 15494, Tx Interval (ms) min/max/avg: 152/248/197 last: 32 ms ago
Registered protocols: BGP
Uptime: 00:50:45
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

The output from the **show bfd neighbors details** command from the line card on Router B verifies that a BFD session has been created:

**Note** Router B is a Cisco 12000 series router. The **show bfd neighbors details** command must be run on the line cards. The **show bfd neighbors details** command will not display the registered protocols when it is entered on a line card.

### Router B

```
RouterB# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session

Press RETURN to get started!

LC-Slot6> show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

The output of the **show ip bgp neighbors** command verifies that BFD has been enabled for the BGP neighbors:

### Router A

```
RouterA# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
 Using BFD to detect fast fallover
.
.
.
```

### Router B

```
RouterB# show ip bgp neighbors

BGP neighbor is 172.16.10.1,  remote AS 40000, external link
 Using BFD to detect fast fallover
.
```

.
.

## Enabling BGP MIB Support: Examples

The following example enables SNMP support for all supported BGP events:

```
Router(config)# snmp-server enable traps bgp
```

The following verification example shows that SNMP support for BGP is enabled and shown the running-config file:

```
Router# show run | include snmp-server

snmp-server enable traps bgp
```

# Where to Go Next

- If you want to connect to an external service provider and use other external BGP features, see the "Connecting to a Service Provider Using External BGP" module.
- If you want to configure some internal BGP features, see the "Configuring Internal BGP Features" chapter of the BGP section of the *Cisco IOS IP Routing Protocols Configuration Guide*, 12.4.
- If you want to configure BGP neighbor session options, see the "Configuring BGP Neighbor Session Options" module.

# Additional References

The following sections provide references related to configuring advanced BGP features.

## Related Documents

| Related Topic | Document Title |
|---|---|
| BGP commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples | • *Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols*, Release 12.3T<br>• *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T<br>• *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR |
| Overview of Cisco BGP conceptual information with links to all the individual BGP modules | "Cisco BGP Overview" module |
| Conceptual and configuration details for basic BGP tasks. | "Configuring a Basic BGP Network" module |
| Information about SNMP and SNMP operations. | "Configuring SNMP Support" section of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3. |

# Standards

| Standard | Title |
|---|---|
| MDT SAFI | *MDT SAFI* |

# MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-BGP4-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

# RFCs

| RFC | Title |
|---|---|
| RFC 1657 | *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2* |
| RFC 1771 | *A Border Gateway Protocol 4 (BGP-4)* |
| RFC 1772 | *Application of the Border Gateway Protocol in the Internet* |
| RFC 1773 | *Experience with the BGP Protocol* |
| RFC 1774 | *BGP-4 Protocol Analysis* |
| RFC 1930 | *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)* |
| RFC 2519 | *A Framework for Inter-Domain Route Aggregation* |
| RFC 2858 | *Multiprotocol Extensions for BGP-4* |
| RFC 2918 | *Route Refresh Capability for BGP-4* |
| RFC 3392 | *Capabilities Advertisement with BGP-4* |

# Technical Assistance

| Description | Link |
|---|---|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/techsupport |

# Feature Information for Configuring Advanced BGP Features

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1), 12.0(3)S, 12.2(33)SRA, 12.2(33)SXH, or later releases appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the "Cisco BGP Implementation Roadmap"

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note** Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

*Table 1 Feature Information for Configuring Advanced BGP Features*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| BGP MIB Support Enhancements | 12.0(26)S<br>12.2(25)S<br>12.3(7)T<br>12.2(33)SRA<br>12.2(33)SXH | The BGP MIB Support Enhancements feature introduced support in the CISCO-BGP4-MIB for new SNMP notifications.<br>The following sections provide information about this feature:<br>• BGP MIB Support, page 7<br>• Enabling BGP MIB Support, page 27<br>• Enabling BGP MIB Support: Examples, page 33<br>The following command was introduced in this feature: **snmp-server enable traps**. |
| BGP Nonstop Forwarding (NSF) Awareness | 12.2(15)T | Nonstop Forwarding (NSF) awareness allows a router to assist NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation. The BGP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running BGP to forward packets along routes that are already known for a router that is performing an SSO operation. This capability allows the BGP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.<br>The following sections provide information about this feature:<br>• BGP Nonstop Forwarding Awareness, page 3<br>• Configuring BGP Nonstop Forwarding Awareness, page 16<br>• Configuring BGP NSF Awareness: Example, page 29<br>• Configuring the Restart Time for BGP NSF Awareness: Example, page 30<br>• Configuring the Stalepath Time for BGP NSF Awareness: Example, page 30<br>The following commands were introduced or modified by this feature: **bgp graceful-restart**, **show ip bgp**, **show ip bgp neighbors**. |

*Table 1 Feature Information for Configuring Advanced BGP Features (continued)*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| BGP Selective Address Tracking | 12.4(4)T<br>12.2(33)SRB | The BGP Selective Address Tracking feature introduces the use of a route map for next-hop route filtering and fast session deactivation. Selective next-hop filtering uses a route map to selectively define routes to help resolve the BGP next hop, or a route map can be used to determine if a peering session with a BGP neighbor should be reset when a route to the BGP peer changes.<br>The following sections provide information about this feature:<br>• Selective BGP Next-Hop Route Filtering, page 3<br>• Configuring BGP Selective Next-Hop Route Filtering, page 12<br>• Configuring BGP Selective Next-Hop Route Filtering: Examples, page 29<br>The following commands were modified by this feature: **bgp nexthop**, **neighbor fall-over**. |

*Table 1 Feature Information for Configuring Advanced BGP Features (continued)*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| BGP Support for BFD | 12.0(31)S<br>12.4(4)T<br>12.2(33)SRA<br>12.2(33)SXH | Bidirectional Forwarding Detection (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. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable. The main benefit of implementing BFD for BGP is a significantly faster reconvergence time.<br><br>The following sections provide information about this feature:<br>• BFD for BGP, page 7<br>• Decreasing BGP Convergence Time Using BFD, page 23<br>• Configuring BFD on a BGP Network: Example, page 30<br><br>The following commands were introduced or modified by this feature: **bfd interval**, **neighbor fall-over bfd**, **show bfd neighbors**, **show ip bgp neighbors**. |
| BGP Support for Next-Hop Address Tracking | 12.0(29)S<br>12.3(14)T<br>12.2(33)SXH | The BGP Support for Next-Hop Address Tracking feature is enabled by default when a supporting Cisco IOS software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a bestpath calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.<br><br>The following sections provide information about this feature:<br>• BGP Support for Next-Hop Address Tracking, page 3<br>• Configuring BGP Next-Hop Address Tracking, page 10<br>• Enabling and Disabling BGP Next-Hop Address Tracking: Example, page 28<br>• Adjusting the Delay Interval for BGP Next-Hop Address Tracking: Example, page 29<br><br>The following command was introduced in this feature: **bgp nexthop**. |