The BGP Support for Next-Hop Address Tracking feature is enabled by default when a supporting Cisco 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.

• Finding Feature Information, on page 1
• Information About BGP Support for Next-Hop Address Tracking, on page 1
• How to Configure BGP Support for Next-Hop Address Tracking, on page 3
• Configuration Examples for BGP Support for Next-Hop Address Tracking, on page 13
• Additional References, on page 14
• Feature Information for BGP Support for Next-Hop Address Tracking, on page 15

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About BGP Support for Next-Hop Address Tracking

BGP Next-Hop Address Tracking

The BGP next-hop address tracking feature is enabled by default when a supporting Cisco 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 best-path calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.
BGP Next-Hop Dampening Penalties

If the penalty threshold value is higher than 950, then the delay is calculated as the reuse time using the dampening calculations. The dampening calculations use the following parameters:

- Penalty
- Half-life time
- Reuse time
- max-suppress-time

The values for the dampening parameters used are a max-suppress-time of 60 seconds, the half-life of 8 seconds, and the reuse-limit of 100.

For example, if the original penalty of 1600 is added, then after 16 seconds it becomes 800, and after 40 seconds, the penalty becomes 100. Hence, for the route update penalty of 1600, a delay of 40 seconds is used to schedule the BGP scanner.

These parameters (penalty threshold and any of the dampening parameters) cannot be modified.

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.

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 device 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 device 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.

Selective BGP Next-Hop Route Filtering

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.
Use route map on ASR series devices to set the next hop as BGP peer for the route and apply that route map in outbound direction towards the peer.

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 Support for Fast Peering Session Deactivation

BGP Hold Timer

By default, the BGP hold timer is set to run every 180 seconds in Cisco software. This timer value is set as the default to protect the BGP routing process from instability that can be caused by peering sessions with other routing protocols. BGP devices typically carry large routing tables, so frequent session resets are not desirable.

BGP Fast Peering Session Deactivation

BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. This feature is event driven and configured on a per-neighbor basis. When this feature is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

Selective Address Tracking for BGP Fast Session Deactivation

In Cisco IOS XE Release 2.1 and later releases, the BGP Selective Address Tracking feature introduced the use of a route map with BGP fast session deactivation. The `route-map` keyword and `map-name` argument are used with the `neighbor fall-over` BGP neighbor session command to determine if a peering session with a BGP neighbor should be reset when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset. The route map is not used for session establishment.

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.

How to Configure BGP Support for Next-Hop Address Tracking

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 “Configuring BGP Route Dampening.”

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

For more examples of how to use the *bgp nexthop* command, see the “Examples: Configuring BGP Selective Next-Hop Route Filtering” section in this module.

**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. exit
8. ip prefix-list list-name [seq seq-value] [deny network / length | permit network/length] [ge ge-value] [le le-value]
9. route-map map-name [permit | deny] [sequence-number]
10. match ip address prefix-list prefix-list-name [prefix-list-name...]
11. exit
12. route-map map-name [permit | deny] [sequence-number]
13. end
14. show ip bgp [network] [network-mask]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
Example:  
Device> enable |
| Step 2 | configure terminal | Enters global configuration mode.  
Example:  
Device# configure terminal |
| Step 3 | router bgp autonomous-system-number | Enters router configuration mode and creates a BGP routing process.  
Example: |
### Command or Action

Device(config)# router bgp 45000

### Purpose

Specifies the IPv4 address family and enters address family configuration mode.

- 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.

- The `multicast` keyword specifies IPv4 multicast address prefixes.

- 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 4

**Example:**

Device(config-router)# address-family ipv4 unicast

### Step 5

**Example:**

Device(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP

Permits a route map to selectively define routes to help resolve the BGP next hop.

- In this example the route map named CHECK-NEXTHOP is created.

### Step 6

**Example:**

Device(config-router-af)# exit

Exits address family configuration mode and enters router configuration mode.

### Step 7

**Example:**

Device(config-router)# exit

Exits router configuration mode and enters global configuration mode.

### Step 8

**Example:**

Device(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.

- Selective next-hop route filtering supports prefix length matching or source protocol matching on a per address-family basis.

- 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

**Example:**

- In this example, a route map named CHECK-NEXTHOP is created. If there is an IP
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# route-map CHECK-NEXTHOP deny 10</td>
<td>address match in the following <strong>match</strong> command, the IP address will be denied.</td>
</tr>
</tbody>
</table>

**Step 10**

**match ip address prefix-list** *prefix-list-name*

*Example:*

Device(config-route-map)# match ip address prefix-list FILTER25

**Matches the IP addresses in the specified prefix list.**

- 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.

**Note**

Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.

**Step 11**

**exit**

*Example:*

Device(config-route-map)# exit

**Exits route map configuration mode and enters global configuration mode.**

**Step 12**

**route-map** *map-name* *[permit | deny]*

*sequence-number*

*Example:*

Device(config)# route-map CHECK-NEXTHOP permit 20

**Configures a route map and enters route map configuration mode.**

- In this example, all other IP addresses are permitted by route map CHECK-NEXTHOP.

**Step 13**

**end**

*Example:*

Device(config-route-map)# end

**Exits route map configuration mode and enters privileged EXEC mode.**

**Step 14**

**show ip bgp** *network* *network-mask*

*Example:*

Device# show ip bgp

**Displays the entries in the BGP routing table.**

- Enter this command to view the next-hop addresses for each route.

**Note**

Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.

---

**Example**

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
```
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.

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.

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 autonomous-system-number
4. address-family ipv4 [multicast | tunnel | unicast [vrf vrf-name] | vrf vrf-name] [vpnv4 [unicast]]
5. bgp nexthop trigger delay delay-timer
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>router bgp autonomous-system-number</td>
<td>Enters router configuration mode to create or configure a BGP routing process.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# router bgp 64512</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family ipv4 [multicast</td>
<td>tunnel</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• The example creates an IPv4 unicast address family session.</td>
</tr>
<tr>
<td></td>
<td>Device(config-router)# address-family ipv4 unicast</td>
<td></td>
</tr>
</tbody>
</table>
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. Beginning with Cisco IOS Release 12.2(33)SB6, BGP next-hop address tracking is also enabled by default under the VPNv6 address family whenever the next hop is an IPv4 address mapped to an IPv6 next-hop address.

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 autonomous-system-number`
4. `address-family ipv4 [[mdt | multicast | tunnel | unicast [vrf vrf-name] | vrf vrf-name] | vpnv4 [unicast] | vpnv6 [unicast]]`
5. `no bgp nexthop trigger enable`
6. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### BGP Support for Next-Hop Address Tracking

#### Configuring Fast Session Deactivation

The tasks in this section show how to 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 route dampening, see the "Configuring Internal BGP Features" module.

### Configuring Fast Session Deactivation for a BGP Neighbor

Perform this task to establish a peering session with a BGP neighbor and then configure the peering session for fast session deactivation to improve the network convergence time if the peering session is deactivated.

Enabling fast session deactivation for a BGP neighbor can significantly improve BGP convergence time. However, unstable IGP peers can still 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 **autonomous-system-number**
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable** | Enables privileged EXEC mode.  
  Example:
  ```
  Device> enable
  ``` |
| **Step 2** | **configure terminal** | Enters global configuration mode.  
  Example:
  ```
  Device# configure terminal
  ``` |
| **Step 3** | **router bgp** *autonomous-system-number* | Enters router configuration mode to create or configure a BGP routing process.  
  Example:
  ```
  Device(config)# router bgp 50000
  ``` |
| **Step 4** | **address-family ipv4** [mdt | multicast | tunnel | unicast [vrf vrf-name] | vrf vrf-name] | Enters address family configuration mode to configure BGP peers to accept address family-specific configurations.  
  Example:
  ```
  Device(config-router)# address-family ipv4 unicast
  ```  
  • The example creates an IPv4 unicast address family session. |
| **Step 5** | **neighbor** *ip-address* remote-as *autonomous-system-number* | Establishes a peering session with a BGP neighbor.  
  Example:
  ```
  Device(config-router-af)# neighbor 10.0.0.1 remote-as 50000
  ``` |
| **Step 6** | **neighbor** *ip-address* fall-over | Configures the BGP peering to use fast session deactivation.  
  Example:
  ```
  Device(config-router-af)# neighbor 10.0.0.1 fall-over
  ```  
  • BGP will remove all routes learned through this peer if the session is deactivated. |
| **Step 7** | **end** | Exits configuration mode and returns to privileged EXEC mode.  
  Example:
  ```
  Device(config-router-af)# end
  ``` |
Configuring Selective Address Tracking for Fast Session Deactivation

Perform this task to configure selective address tracking for fast session deactivation. The optional `route-map` keyword and `map-name` argument of the `neighbor fall-over` command are used to determine if a peering session with a BGP neighbor should be deactivated (reset) when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset.

**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.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router bgp autonomous-system-number`
4. `neighbor {ip-address|peer-group-name} remote-as autonomous-system-number`
5. `neighbor ip-address fall-over [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. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>router bgp autonomous-system-number</code></td>
<td>Enters router configuration mode for the specified routing process.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# router bgp 45000</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`neighbor {ip-address</td>
<td>peer-group-name} remote-as autonomous-system-number`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device(config-router)# neighbor 192.168.1.2 remote-as 40000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 5** | Applies a route map when a route to the BGP changes.  
*Example:*  
Device(config-router)# neighbor 192.168.1.2 remote-as 40000 fall-over route-map CHECK-NBR  
*In this example, the route map named CHECK-NBR is applied when the route to neighbor 192.168.1.2 changes.* |
| **Step 6** | Exits router configuration mode and enters global configuration mode.  
*Example:*  
Device(config-router)# exit |
| **Step 7** | Creates a prefix list for BGP next-hop route filtering.  
*Example:*  
Device(config)# ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28  
*Selective next-hop route filtering supports prefix length matching or source protocol matching on a per-address-family basis.*  
*The example creates a prefix list named FILTER28 that permits routes only if the mask length is greater than or equal to 28.* |
| **Step 8** | Configures a route map and enters route-map configuration mode.  
*Example:*  
Device(config)# route-map CHECK-NBR permit 10  
*In this example, a route map named CHECK-NBR is created. If there is an IP address match in the following match command, the IP address will be permitted.* |
| **Step 9** | Matches the IP addresses in the specified prefix list.  
*Example:*  
Device(config-route-map)# match ip address prefix-list FILTER28  
*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.* |
| **Step 10** | Exits configuration mode and returns to privileged EXEC mode.  
*Example:*  
Device(config-route-map)# end |

**Note:** Only the syntax applicable to this task is used in this example. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.
Configuration Examples for BGP Support for Next-Hop Address Tracking

Example: Enabling and Disabling BGP Next-Hop Address Tracking

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
```

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

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
```

Examples: Configuring BGP Selective Next-Hop Route Filtering

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
route-map CHECK-BGP25 deny 10
  match ip address prefix-list FILTER25
  exit
route-map CHECK-BGP25 deny 20
  match source-protocol bgp 1
```
Example: Configuring Fast Session Deactivation for a BGP Neighbor

In the following example, the BGP routing process is configured on device A and device B to monitor and use fast peering session deactivation for the neighbor session between the two devices. Although fast peering session deactivation is not required at both devices in the neighbor session, it will help the BGP networks in both autonomous systems to converge faster if the neighbor session is deactivated.

Device A

router bgp 40000
neighbor 192.168.1.1 remote-as 45000
neighbor 192.168.1.1 fall-over
end

Device B

router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.1.2 fall-over
end

Example: Configuring Selective Address Tracking for Fast Session Deactivation

The following example shows how to configure the BGP peering session to be reset if a route with a prefix of /28 or a more specific route to a peer destination is no longer available:

router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.1.2 fall-over route-map CHECK-NBR
exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
match ip address prefix-list FILTER28
end

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>BGP commands</td>
<td>Cisco IOS IP Routing: BGP Command Reference</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for BGP Support for Next-Hop Address Tracking

Table 1: Feature Information for BGP Support for Next-Hop Address Tracking

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Support for Next-Hop Address Tracking</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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. This feature was introduced on the Cisco ASR 1000 Series Routers. The following command was introduced in this feature: <code>bgp nexthop</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BGP Selective Address Tracking</td>
<td>12.2(31)SB 12.2(33)SRB</td>
<td>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. This feature was introduced on the Cisco ASR 1000 Series Routers. The following commands were modified by this feature: <code>bgp nexthop</code>, <code>neighbor fall-over</code>.</td>
</tr>
<tr>
<td>BGP Support for Fast Peering Session Deactivation</td>
<td>12.2(33)SRA 12.2(31)SB</td>
<td>The BGP Support for Fast Peering Session Deactivation feature introduced an event-driven notification system that allows a Border Gateway Protocol (BGP) process to monitor BGP peering sessions on a per-neighbor basis. This feature improves the response time of BGP to adjacency changes by allowing BGP to detect an adjacency change and deactivate the terminated session in between standard BGP scanning intervals. Enabling this feature improves overall BGP convergence. This feature was introduced on the Cisco ASR 1000 Series Routers. The following command was modified by this feature: <code>neighbor fall-over</code>.</td>
</tr>
</tbody>
</table>