



CHAPTER 11

Configuring Advanced BGP

This chapter describes how to configure advanced features of the Border Gateway Protocol (BGP) on the Cisco NX-OS device.

This chapter includes the following sections:

- [Information About Advanced BGP, page 11-1](#)
- [Licensing Requirements for Advanced BGP, page 11-12](#)
- [Prerequisites for Advanced BGP, page 11-12](#)
- [Guidelines and Limitations for Advanced BGP, page 11-13](#)
- [Default Settings, page 11-14](#)
- [Configuring Advanced BGP, page 11-14](#)
- [Verifying the Advanced BGP Configuration, page 11-43](#)
- [Related Topics, page 11-45](#)
- [Additional References, page 11-46](#)
- [Feature History for BGP, page 11-46](#)

Information About Advanced BGP

BGP is an interdomain routing protocol that provides loop-free routing between organizations or autonomous systems. Cisco NX-OS supports BGP version 4. BGP version 4 includes multiprotocol extensions that allow BGP to carry routing information for IP multicast routes and multiple Layer 3 protocol address families. BGP uses TCP as a reliable transport protocol to create TCP sessions with other BGP-enabled devices called BGP peers. When connecting to an external organization, the router creates external BGP (eBGP) peering sessions. BGP peers within the same organization exchange routing information through internal BGP (iBGP) peering sessions.

This section includes the following topics:

- [Peer Templates, page 11-2](#)
- [Authentication, page 11-2](#)
- [Route Policies and Resetting BGP Sessions, page 11-3](#)
- [eBGP, page 11-3](#)
- [iBGP, page 11-3](#)

Send document comments to nexus7k-docfeedback@cisco.com.

- [Capabilities Negotiation, page 11-6](#)
- [Route Dampening, page 11-6](#)
- [Load Sharing and Multipath, page 11-7](#)
- [Route Aggregation, page 11-7](#)
- [BGP Conditional Advertisement, page 11-8](#)
- [BGP Next-Hop Address Tracking, page 11-8](#)
- [Route Redistribution, page 11-9](#)
- [BFD, page 11-9](#)
- [Tuning BGP, page 11-10](#)
- [Multiprotocol BGP, page 11-10](#)
- [Graceful Restart and High Availability, page 11-10](#)
- [ISSU, page 11-12](#)
- [Virtualization Support, page 11-12](#)

Peer Templates

BGP peer templates allow you to create blocks of common configuration that you can reuse across similar BGP peers. Each block allows you to define a set of attributes that a peer then inherits. You can choose to override some of the inherited attributes as well, making it a very flexible scheme for simplifying the repetitive nature of BGP configurations.

Cisco NX-OS implements three types of peer templates:

- The peer-session template defines BGP peer session attributes, such as the transport details, remote autonomous system number of the peer, and session timers. A peer-session template can also inherit attributes from another peer-session template (with locally defined attributes that override the attributes from an inherited peer-session).
- A peer-policy template defines the address-family dependent policy aspects for a peer including the inbound and outbound policy, filter-lists, and prefix-lists. A peer-policy template can inherit from a set of peer-policy templates. Cisco NX-OS evaluates these peer-policy templates in the order specified by the preference value in the inherit configuration. The lowest number is preferred over higher numbers.
- The peer template can inherit the peer-session and peer-policy templates to allow for simplified peer definitions. It is not mandatory to use a peer template but it can simplify the BGP configuration by providing reusable blocks of configuration.

Authentication

You can configure authentication for a BGP neighbor session. This authentication method adds an MD5 authentication digest to each TCP segment sent to the neighbor to protect BGP against unauthorized messages and TCP security attacks.



Note

The MD5 password must be identical between BGP peers.

Send document comments to nexus7k-docfeedback@cisco.com.

Route Policies and Resetting BGP Sessions

You can associate a route policy to a BGP peer. Route policies use route maps to control or modify the routes that BGP recognizes. You can configure a route policy for inbound or outbound route updates. The route policies can match on different criteria, such as a prefix or AS_path attribute, and selectively accept or deny the routes. Route policies can also modify the path attributes. See [Chapter 17, “Configuring Policy-Based Routing,”](#) for more information on route policies.

When you change a route policy applied to a BGP peer, you must reset the BGP sessions for that peer. Cisco NX-OS supports the following three mechanisms to reset BGP peering sessions:

- **Hard reset**—A hard reset tears down the specified peering sessions, including the TCP connection, and deletes routes coming from the specified peer. This option interrupts packet flow through the BGP network. Hard reset is disabled by default.
- **Soft reconfiguration inbound**—A soft reconfiguration inbound triggers routing updates for the specified peer without resetting the session. You can use this option if you change an inbound route policy. Soft reconfiguration inbound saves a copy of all routes received from the peer before processing the routes through the inbound route policy. If you change the inbound route policy, Cisco NX-OS passes these stored routes through the modified inbound route policy to update the route table without tearing down existing peering sessions. Soft reconfiguration inbound can use significant memory resources to store the unfiltered BGP routes. Soft reconfiguration inbound is disabled by default.
- **Route Refresh**—A route refresh updates the inbound routing tables dynamically by sending route refresh requests to supporting peers when you change an inbound route policy. The remote BGP peer responds with a new copy of its routes that the local BGP speaker processes with the modified route policy. Cisco NX-OS automatically sends an outbound route refresh of prefixes to the peer.
- BGP peers advertise the route refresh capability as part of the BGP capability negotiation when establishing the BGP peer session. Route refresh is the preferred option and enabled by default.



Note

BGP also uses route maps for route redistribution, route aggregation, route dampening, and other features. See [Chapter 16, “Configuring Route Policy Manager,”](#) for more information on route maps.

eBGP

External BGP (eBGP) allows you to connect BGP peers from different autonomous systems to exchange routing updates. Connecting to external networks enables traffic from your network to be forwarded to other networks and across the Internet.

You should use loopback interfaces for establishing eBGP peering sessions because loopback interfaces are less susceptible to interface flapping. An interface flap occurs when the interface is administratively brought up or down because of a failure or maintenance issue. See the [“Configuring eBGP” section on page 11-26](#) for information on multihop, fast external failovers, and limiting the size of the AS-path attribute.

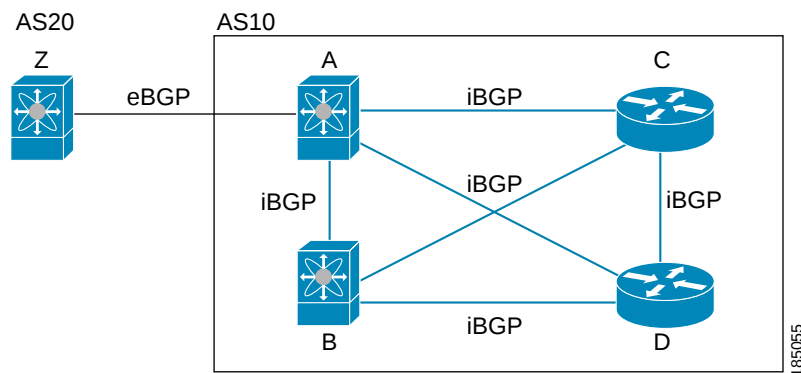
iBGP

Internal BGP (iBGP) allows you to connect BGP peers within the same autonomous system. You can use iBGP for multihomed BGP networks (networks that have more than one connection to the same external autonomous system).

Send document comments to nexus7k-docfeedback@cisco.com.

Figure 11-1 shows an iBGP network within a larger BGP network.

Figure 11-1 iBGP Network



iBGP networks are fully meshed. Each iBGP peer has a direct connection to all other iBGP peers to prevent network loops.

For single-hop iBGP peers with update-source configured under neighbor configuration mode, the peer supports fast external fall-over.



Note

You should configure a separate interior gateway protocol in the iBGP network.

This section includes the following topics:

- [AS Confederations, page 11-4](#)
- [Route Reflector, page 11-5](#)

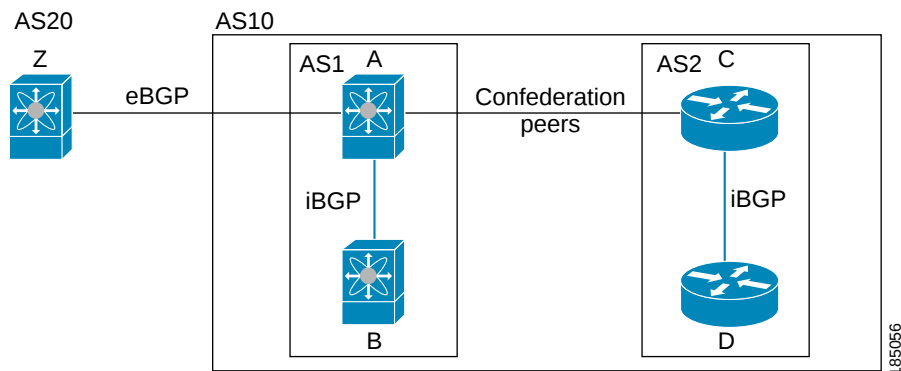
AS Confederations

A fully meshed iBGP network becomes complex as the number of iBGP peers grows. You can reduce the iBGP mesh by dividing the autonomous system into multiple subautonomous systems and grouping them into a single confederation. A confederation is a group of iBGP peers that use the same autonomous system number to communicate to external networks. Each subautonomous system is fully meshed within itself and has a few connections to other subautonomous systems in the same confederation.

Send document comments to nexus7k-docfeedback@cisco.com.

Figure 11-2 shows the BGP network from Figure 11-1, split into two subautonomous systems and one confederation.

Figure 11-2 AS Confederation



In this example, AS10 is split into two subautonomous systems, AS1 and AS2. Each subautonomous system is fully meshed, but there is only one link between the subautonomous systems. By using AS confederations, you can reduce the number of links compared to the fully meshed autonomous system in Figure 11-1.

Route Reflector

You can alternately reduce the iBGP mesh by using a route reflector configuration where route reflectors pass learned routes to neighbors so that all iBGP peers do not need to be fully meshed.

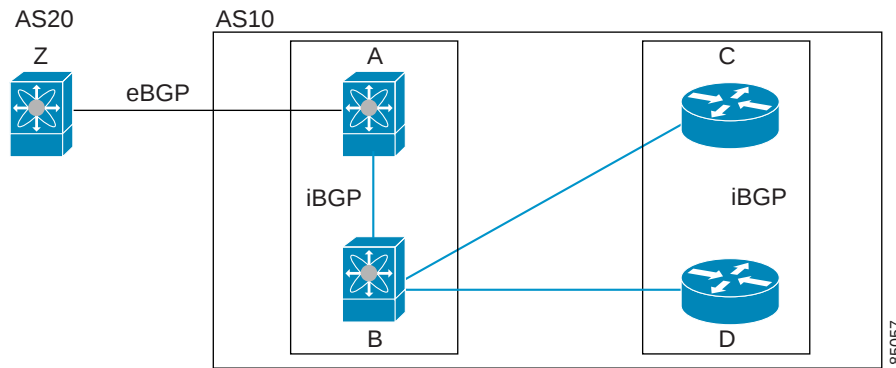
Figure 11-1 shows a simple iBGP configuration with four meshed iBGP speakers (routers A, B, C, and D). Without route reflectors, when router A receives a route from an external neighbor, it advertises the route to all three iBGP neighbors.

When you configure an iBGP peer to be a route reflector, it becomes responsible for passing iBGP learned routes to a set of iBGP neighbors.

In Figure 11-3, router B is the route reflector. When the route reflector receives routes advertised from router A, it advertises (reflects) the routes to routers C and D. Router A no longer has to advertise to both routers C and D.

Send document comments to nexus7k-docfeedback@cisco.com.

Figure 11-3 Route Reflector



The route reflector and its client peers form a cluster. You do not have to configure all iBGP peers to act as client peers of the route reflector. You must configure any nonclient peer as fully meshed to guarantee that complete BGP updates reach all peers.

Capabilities Negotiation

A BGP speaker can learn about BGP extensions that are supported by a peer by using the capabilities negotiation feature. Capabilities negotiation allows BGP to use only the set of features supported by both BGP peers on a link.

If a BGP peer does not support capabilities negotiation, Cisco NX-OS attempts a new session to the peer without capabilities negotiation if you have configured the address family as IPv4. Any other multiprotocol configuration (such as IPv6) requires capabilities negotiation.

Route Dampening

Route dampening is a BGP feature that minimizes the propagation of flapping routes across an internetwork. A route flaps when it alternates between the available and unavailable states in rapid succession.

For example, consider a network with three BGP autonomous systems: AS1, AS2, and AS3. Suppose that a route in AS1 flaps (it becomes unavailable). Without route dampening, AS1 sends a withdraw message to AS2. AS2 propagates the withdrawal message to AS3. When the flapping route reappears, AS1 sends an advertisement message to AS2, which sends the advertisement to AS3. If the route repeatedly becomes unavailable, and then available, AS1 sends many withdrawal and advertisement messages that propagate through the other autonomous systems.

Route dampening can minimize flapping. Suppose that the route flaps. AS2 (in which route dampening is enabled) assigns the route a penalty of 1000. AS2 continues to advertise the status of the route to neighbors. Each time that the route flaps, AS2 adds to the penalty value. When the route flaps so often that the penalty exceeds a configurable suppression limit, AS2 stops advertising the route, regardless of how many times that it flaps. The route is now dampened.

The penalty placed on the route decays until the reuse limit is reached. At that time, AS2 advertises the route again. When the reuse limit is at 50 percent, AS2 removes the dampening information for the route.

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

The router does not apply a penalty to a resetting BGP peer when route dampening is enabled, even though the peer reset withdraws the route.

Load Sharing and Multipath

BGP can install multiple equal-cost eBGP or iBGP paths into the routing table to reach the same destination prefix. Traffic to the destination prefix is then shared across all the installed paths.

The BGP best-path algorithm considers the paths as equal-cost paths if the following attributes are identical:

- Weight
- Local preference
- AS_path
- Origin code
- Multi-exit discriminator (MED)
- IGP cost to the BGP next hop

BGP selects only one of these multiple paths as the best path and advertises the path to the BGP peers.

**Note**

Paths that are received from different AS confederations are considered as equal-cost paths if the external AS_path values and the other attributes are identical.

**Note**

When you configure a route reflector for iBGP multipath, and the route reflector advertises the selected best path to its peers, the next hop for the path is not modified.

Route Aggregation

You can configure aggregate addresses. Route aggregation simplifies route tables by replacing a number of more specific addresses with an address that represents all the specific addresses. For example, you can replace these three more specific addresses, 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 with one aggregate address, 10.1.0.0/16.

Aggregate prefixes are present in the BGP route table so that fewer routes are advertised.

**Note**

Cisco NX-OS does not support automatic route aggregation.

Route aggregation can lead to forwarding loops. To avoid this problem, when BGP generates an advertisement for an aggregate address, it automatically installs a summary discard route for that aggregate address in the local routing table. BGP sets the administrative distance of the summary discard to 220 and sets the route type to discard. BGP does not use discard routes for next-hop resolution.

Send document comments to nexus7k-docfeedback@cisco.com.

BGP Conditional Advertisement

BGP conditional advertisement allows you to configure BGP to advertise or withdraw a route based on whether or not a prefix exists in the BGP table. This feature is useful, for example, in multihomed networks, in which you want BGP to advertise some prefixes to one of the providers only if information from the other provider is not present.

Consider an example network with three BGP autonomous systems: AS1, AS2, and AS3, where AS1 and AS3 connect to the Internet and to AS2. Without conditional advertisement, AS2 propagates all routes to both AS1 and AS3. With conditional advertisement, you can configure AS2 to advertise certain routes to AS3 only if routes from AS1 do not exist (if for example, the link to AS1 fails).

BGP conditional advertisement adds an exist or not-exist test to each route that matches the configured route map. See the [“Configuring BGP Conditional Advertisement” section on page 11-32](#) for more information.

BGP Next-Hop Address Tracking

BGP monitors the next-hop address of installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. BGP next-hop address tracking speeds up this next-hop reachability test by triggering the verification process when routes change in the Routing Information Base (RIB) that may affect BGP next-hop reachability.

BGP receives notifications from the RIB when the next-hop information changes (event-driven notifications). BGP is notified when any of the following events occurs:

- The next hop becomes unreachable.
- The next hop becomes reachable.
- The fully recursed Interior Gateway Protocol (IGP) metric to the next hop changes.
- The first hop IP address or first hop interface changes.
- The next hop becomes connected.
- The next hop becomes unconnected.
- The next hop becomes a local address.
- The next hop becomes a nonlocal address.



Note

Reachability and recursed metric events trigger a best-path recalculation.

Event notifications from the RIB are classified as critical and noncritical. Notifications for critical and noncritical events are sent in separate batches. However, a noncritical event is sent with the critical events if the noncritical event is pending and there is a request to read the critical events.

- Critical events are related to next-hop reachability, such as the loss of next hops resulting in a switchover to a different path. A change in the IGP metric for a next hop resulting in a switchover to a different path can also be considered a critical event.
- Non-critical events are related to next hops being added without affecting the best path or changing the IGP metric to a single next hop.

See the [“Configuring BGP Next-Hop Address Tracking” section on page 11-24](#) for more information.

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

Critical and non-critical events can be configured individually on a per address family basis. For more information on address families, see the “Configuring MPLS Layer 3 VPNs” chapter in the *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*.

Route Redistribution

You can configure BGP to redistribute static routes or routes from other protocols. You must configure a route map with the redistribution to control which routes are passed into BGP. A route map allows you to filter routes based on attributes such as the destination, origination protocol, route type, route tag, and so on. See [Chapter 16, “Configuring Route Policy Manager,”](#) for more information.

Prior to Cisco NX-OS Release 5.2(1), when you redistribute BGP to IGP, iBGP is redistributed as well. To override this behavior, you must insert an additional deny statement into the route map. Beginning with Cisco NX-OS Release 5.2(1), redistribution varies as follows:

- In a non-MPLS VPN scenario, iBGP is not redistributed to IGP by default.
- In an MPLS VPN scenario (route distinguisher configured under a VRF), iBGP is redistributed to IGP by default.

You can use route maps to override the default behavior in both scenarios, but be careful when doing so as incorrect use of route maps can result in network loops. The following examples show how to use route maps to change the default behavior.

You can change the default behavior for scenario 1 by modifying the route map as follows:

```
route-map foo permit 10
  match route-type internal
router ospf 1
  redistribute bgp 100 route-map foo
```

Similarly, you can change the default behavior for scenario 2 by modifying the route map as follows:

```
route-map foo deny 10
  match route-type internal
router ospf 1
  vrf bar
    redistribute bgp 100 route-map foo
```

BFD

This feature supports bidirectional forwarding detection (BFD) for IPv4 only. BFD is a detection protocol designed to provide fast forwarding-path failure detection times. BFD provides subsecond failure detection between two adjacent devices and can be less CPU-intensive than protocol hello messages because some of the BFD load can be distributed onto the data plane on supported modules.

BFD for BGP is supported on eBGP peers and iBGP single-hop peers. Configure the update-source option in neighbor configuration mode for iBGP single-hop peers using BFD.

**Note**

BFD is not supported on other iBGP peers or for multihop eBGP peers.

See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*, for more information.

Send document comments to nexus7k-docfeedback@cisco.com.

Tuning BGP

You can modify the default behavior of BGP through BGP timers and by adjusting the best-path algorithm.

This section includes the following topics:

- [BGP Timers, page 11-10](#)
- [Tuning the Best-Path Algorithm, page 11-10](#)

BGP Timers

BGP uses different types of timers for neighbor session and global protocol events. Each established session has a minimum of two timers for sending periodic keepalive messages and for timing out sessions when peer keepalives do not arrive within the expected time. In addition, there are other timers for handling specific features. Typically, you configure these timers in seconds. The timers include a random adjustment so that the same timers on different BGP peers trigger at different times.

Tuning the Best-Path Algorithm

You can modify the default behavior of the best-path algorithm through optional configuration parameters, including changing how the algorithm handles the multi-exit discriminator (MED) attribute and the router ID.

Multiprotocol BGP

BGP on Cisco NX-OS supports multiple address families. Multiprotocol BGP (MP-BGP) carries different sets of routes depending on the address family. For example, BGP can carry one set of routes for IPv4 unicast routing, one set of routes for IPv4 multicast routing, and one set of routes for IPv6 multicast routing. You can use MP-BGP for reverse-path forwarding (RPF) checks in IP multicast networks.

**Note**

Because Multicast BGP does not propagate multicast state information, you need a multicast protocol, such as Protocol Independent Multicast (PIM).

Use the router address-family and neighbor address-family configuration modes to support multiprotocol BGP configurations. MP-BGP maintains separate RIBs for each configured address family, such as a unicast RIB and a multicast RIB for BGP.

A multiprotocol BGP network is backward compatible but BGP peers that do not support multiprotocol extensions cannot forward routing information, such as address family identifier information, that the multiprotocol extensions carry.

Graceful Restart and High Availability

Cisco NX-OS supports nonstop forwarding and graceful restart for BGP.

Send document comments to nexus7k-docfeedback@cisco.com.

You can use nonstop forwarding (NSF) for BGP to forward data packets along known routes in the Forward Information Base (FIB) while the BGP routing protocol information is being restored following a failover. With NSF, BGP peers do not experience routing flaps. During a failover, the data traffic is forwarded through intelligent modules while the standby supervisor becomes active.

If a Cisco NX-OS router experiences a cold reboot, the network does not forward traffic to the router and removes the router from the network topology. In this scenario, BGP experiences a nongraceful restart and removes all routes. When Cisco NX-OS applies the startup configuration, BGP reestablishes peering sessions and relearns the routes.

A Cisco NX-OS router that has dual supervisors can experience a stateful supervisor switchover. During the switchover, BGP uses nonstop forwarding to forward traffic based on the information in the FIB, and the system is not removed from the network topology. A router whose neighbor is restarting is referred to as a “helper.” After the switchover, a graceful restart operation begins. When it is in progress, both routers reestablish their neighbor relationship and exchange their BGP routes. The helper continues to forward prefixes pointing to the restarting peer, and the restarting router continues to forward traffic to peers even though those neighbor relationships are restarting. When the restarting router has all route updates from all BGP peers that are graceful restart capable, the graceful restart is complete, and BGP informs the neighbors that it is operational again.

For single-hop iBGP peers with update-source configured under neighbor configuration mode, the peer supports fast external fall-over.

Low Memory Handling

BGP reacts to low memory for the following conditions:

- Minor alert—BGP does not establish any new eBGP peers. BGP continues to establish new iBGP peers and confederate peers. Established peers remain, but reset peers are not re-established.
- Severe alert—BGP shuts down select established eBGP peers every two minutes until the memory alert becomes minor. For each eBGP peer, BGP calculates the ratio of total number of paths received to the number of paths selected as best paths. The peers with the highest ratio are selected to be shut down to reduce memory usage. You must clear a shutdown eBGP peer before you can bring the eBGP peer back up to avoid oscillation.



Note You can exempt important eBGP peers from this selection process.

- Critical alert—BGP gracefully shuts down all the established peers. You must clear a shutdown BGP peer before you can bring the BGP peer back up.

See the [“Tuning BGP” section on page 11-37](#) for more information on how to exempt a BGP peer from a shutdown due to a low memory condition.

Send document comments to nexus7k-docfeedback@cisco.com.

ISSU

Cisco NX-OS supports in-service software upgrades (ISSU). ISSU allows you to upgrade software without impacting forwarding.

The following conditions are required to support ISSU:

- Graceful restart must be enabled (default)
- Keepalive and hold timers must not be smaller than their default values

If either of these requirements is not met, Cisco NX-OS issues a warning. You can proceed with the upgrade or downgrade, but service might be disrupted.



Note

Cisco NX-OS cannot guarantee ISSU for non-default timer values if the negotiated hold time between BGP peers is less than the system switchover time.

Virtualization Support

Cisco NX-OS supports multiple instances of BGP that run on the same system. BGP supports virtual routing and forwarding (VRF) instances that exist within virtual device contexts (VDCs). You can configure one BGP instance in a VDC, but you can have multiple VDCs on the system.

By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF. See the *Cisco NX-OS Virtual Device Context Configuration Guide* and [Chapter 14, “Configuring Layer 3 Virtualization.”](#)

Licensing Requirements for Advanced BGP

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	BGP requires an Enterprise Services license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the <i>Cisco NX-OS Licensing Guide</i> .

Prerequisites for Advanced BGP

Advanced BGP has the following prerequisites:

- You must enable BGP (see the [“Enabling BGP”](#) section on page 10-11).
- You should have a valid router ID configured on the system.
- You must have an AS number, either assigned by a Regional Internet Registry (RIR) or locally administered.
- You must have reachability (such as an interior gateway protocol [IGP], a static route, or a direct connection) to the peer that you are trying to make a neighbor relationship with.
- You must explicitly configure an address family under a neighbor for the BGP session establishment.

Send document comments to nexus7k-docfeedback@cisco.com.

Guidelines and Limitations for Advanced BGP

Advanced BGP has the following configuration guidelines and limitations:

- The dynamic AS number prefix peer configuration overrides the individual AS number configuration inherited from a BGP template.
- If you configure a dynamic AS number for prefix peers in an AS confederation, BGP establishes sessions with only the AS numbers in the local confederation.
- BGP sessions created through a dynamic AS number prefix peer ignore any configured eBGP multihop time-to-live (TTL) value or a disabled check for directly connected peers.
- Configure a router ID for BGP to avoid automatic router ID changes and session flaps.
- Use the maximum-prefix configuration option per peer to restrict the number of routes received and system resources used.
- Configure the update source to establish a session with eBGP multihop sessions.
- Specify a BGP route map if you configure a redistribution.
- Configure the BGP router ID within a VRF.
- If you decrease the keepalive and hold timer values, the network might experience session flaps.
- If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*).
- When you redistribute BGP to IGP, iBGP is redistributed as well. To override this behavior, you must insert an additional deny statement into the route map.
- Cisco NX-OS does not support multi-hop BFD. BFD for BGP has the following limitations:
 - BFD is supported only for BGP IPv4.
 - BFD is supported only for eBGP peers and iBGP single-hop peers.
 - To enable BFD for iBGP single-hop peers, you must configure the update-source option on the physical interface.
 - BFD is not supported for multi-hop iBGP peers and multi-hop eBGP peers.
- For single-hop iBGP peers with update-source configured under neighbor configuration mode, the peer supports fast external fall-over.
- The following guidelines and limitations apply to the **remove-private-as** command:
 - It applies only to eBGP peers.
 - It can be configured only in neighbor configuration mode and not in neighbor-address-family mode.
 - If the AS-path includes both private and public AS numbers, the private AS numbers are not removed.
 - If the AS-path contains the AS number of the eBGP neighbor, the private AS numbers are not removed.
 - Private AS numbers are removed only if all AS numbers in that AS-path belong to a private AS number range. Private AS numbers are not removed if a peer's AS number or a non-private AS number is found in the AS-path segment.

Send document comments to nexus7k-docfeedback@cisco.com.

Default Settings

Table 11-1 lists the default settings for BGP parameters.

Table 11-1 *Default BGP Parameters*

Parameters	Default
BGP feature	Disabled
Keep alive interval	60 seconds
Hold timer	180 seconds
Dynamic capability	Enabled

Configuring Advanced BGP

This section includes the following topics:

- [Configuring BGP Session Templates, page 11-15](#)
- [Configuring BGP Peer-Policy Templates, page 11-17](#)
- [Configuring BGP Peer Templates, page 11-19](#)
- [Configuring Prefix Peering, page 11-22](#)
- [Configuring BGP Authentication, page 11-23](#)
- [Resetting a BGP Session, page 11-23](#)
- [Modifying the Next-Hop Address, page 11-24](#)
- [Configuring BGP Next-Hop Address Tracking, page 11-24](#)
- [Configuring Next-Hop Filtering, page 11-25](#)
- [Disabling Capabilities Negotiation, page 11-25](#)
- [Configuring eBGP, page 11-26](#)
- [Configuring AS Confederations, page 11-28](#)
- [Configuring Route Reflector, page 11-28](#)
- [Configuring Route Dampening, page 11-30](#)
- [Configuring Load Sharing and ECMP, page 11-31](#)
- [Configuring Maximum Prefixes, page 11-31](#)
- [Configuring Dynamic Capability, page 11-31](#)
- [Configuring Aggregate Addresses, page 11-32](#)
- [Configuring BGP Conditional Advertisement, page 11-32](#)
- [Configuring Route Redistribution, page 11-35](#)
- [Configuring Multiprotocol BGP, page 11-36](#)
- [Tuning BGP, page 11-37](#)
- [Configuring a Graceful Restart, page 11-40](#)
- [Configuring Virtualization, page 11-42](#)

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring BGP Session Templates

You can use BGP session templates to simplify the BGP configuration for multiple BGP peers with similar configuration needs. BGP templates allow you to reuse common configuration blocks. You configure BGP templates first and then apply these templates to BGP peers.

With BGP session templates, you can configure session attributes such as inheritance, passwords, timers, and security.

A peer-session template can inherit from one other peer-session template. You can configure the second template to inherit from a third template. The first template also inherits this third template. This indirect inheritance can continue for up to seven peer-session templates.

Any attributes configured for the neighbor take priority over any attributes inherited by that neighbor from a BGP template.

BEFORE YOU BEGIN

You must enable BGP (see the “[Enabling BGP](#)” section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

**Note**

When editing a template, you can use the **no** form of a command at either the peer or template level to explicitly override a setting in a template. You must use the **default** form of the command to reset that attribute to the default state.

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer-session** *template-name*
4. (Optional) **password number** *password*
5. (Optional) **timers** *keepalive hold*
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **inherit peer-session** *template-name*
9. (Optional) **description** *text*
10. (Optional) **show bgp peer-session** *template-name*
11. (Optional) **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp autonomous-system-number Example: switch(config)# router bgp 65536 switch(config-router)#	Enables BGP and assigns the autonomous system number to the local BGP speaker.
Step 3	template peer-session template-name Example: switch(config-router)# template peer-session BaseSession switch(config-router-stmp)#	Enters peer-session template configuration mode.
Step 4	password number password Example: switch(config-router-stmp)# password 0 test	(Optional) Adds the clear text password <i>test</i> to the neighbor. The password is stored and displayed in type 3 encrypted form (3DES).
Step 5	timers keepalive hold Example: switch(config-router-stmp)# timers 30 90	(Optional) Adds the BGP keepalive and holdtimer values to the peer-session template. The default keepalive interval is 60. The default hold time is 180.
Step 6	exit Example: switch(config-router-stmp)# exit switch(config-router)#	Exits peer-session template configuration mode.
Step 7	neighbor ip-address remote-as as-number Example: switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	Places the router in the neighbor configuration mode for BGP routing and configures the neighbor IP address.
Step 8	inherit peer-session template-name Example: switch(config-router-neighbor)# inherit peer-session BaseSession switch(config-router-neighbor)	Applies a peer-session template to the peer.
Step 9	description text Example: switch(config-router-neighbor)# description Peer Router A switch(config-router-neighbor)	(Optional) Adds a description for the neighbor.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 10	show bgp peer-session <i>template-name</i> Example: switch(config-router-neighbor)# show bgp peer-session BaseSession	(Optional) Displays the peer-policy template.
Step 11	copy running-config startup-config Example: switch(config-router-neighbor)# copy running-config startup-config	(Optional) Saves this configuration change.

Use the **show bgp neighbor** command to see the template applied. See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*, for details on all commands available in the template.

This example shows how to configure a BGP peer-session template and apply it to a BGP peer:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BaseSession
switch(config-router-stmp)# timers 30 90
switch(config-router-stmp)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# description Peer Router A
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# copy running-config startup-config
```

Configuring BGP Peer-Policy Templates

You can configure a peer-policy template to define attributes for a particular address family. You assign a preference to each peer-policy template and these templates are inherited in the order specified, for up to five peer-policy templates in a neighbor address family.

Cisco NX-OS evaluates multiple peer policies for an address family using the preference value. The lowest preference value is evaluated first. Any attributes configured for the neighbor take priority over any attributes inherited by that neighbor from a BGP template.

Peer-policy templates can configure address family-specific attributes such as AS-path filter lists, prefix lists, route reflection, and soft reconfiguration.

BEFORE YOU BEGIN

You must enable BGP (see the [“Enabling BGP”](#) section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).



Note

When editing a template, you can use the **no** form of a command at either the peer or template level to explicitly override a setting in a template. You must use the default form of the command to reset that attribute to the default state.

Send document comments to nexus7k-docfeedback@cisco.com.

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer-policy** *template-name*
4. (Optional) **advertise-active-only**
5. (Optional) **maximum-prefix** *number*
6. **exit**
7. **neighbor** *ip-address* **remote-as** *as-number*
8. **address-family** {*ipv4* | *ipv6* | *vpn4* | *vpn6*} {**multicast** | **unicast**}
9. **inherit peer-policy** *template-name* *preference*
10. (Optional) **show bgp peer-policy** *template-name*
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp <i>autonomous-system-number</i> Example: switch(config)# router bgp 65536 switch(config-router)#	Enables BGP and assigns the autonomous system number to the local BGP speaker.
Step 3	template peer-policy <i>template-name</i> Example: switch(config-router)# template peer-policy BasePolicy switch(config-router-ptmp)#	Creates a peer-policy template.
Step 4	advertise-active-only Example: switch(config-router-ptmp)# advertise-active-only	(Optional) Advertises only active routes to the peer.
Step 5	maximum-prefix <i>number</i> Example: switch(config-router-ptmp)# maximum-prefix 20	(Optional) Sets the maximum number of prefixes allowed from this peer.
Step 6	exit Example: switch(config-router-ptmp)# exit switch(config-router)#	Exits peer-policy template configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 7	neighbor <i>ip-address</i> remote-as <i>as-number</i> Example: switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address.
Step 8	address-family { <i>ipv4</i> <i>ipv6</i> <i>vpnv4</i> <i>vpnv6</i> } { <i>multicast</i> <i>unicast</i> } Example: switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	Enters global address family configuration mode for the IPv4 address family.
Step 9	inherit peer-policy <i>template-name</i> <i>preference</i> Example: switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1	Applies a peer-policy template to the peer address family configuration and assigns the preference value for this peer policy.
Step 10	show bgp peer-policy <i>template-name</i> Example: switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy	(Optional) Displays the peer-policy template.
Step 11	copy running-config startup-config Example: switch(config-router-neighbor-af)# copy running-config startup-config	(Optional) Saves this configuration change.

Use the **show bgp neighbor** command to see the template applied. See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*, for details on all commands available in the template.

This example shows how to configure a BGP peer-session template and apply it to a BGP peer:

This example shows how to configure a BGP peer-policy template and apply it to a BGP peer:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BasePolicy
switch(config-router-ptmp)# maximum-prefix 20
switch(config-router-ptmp)# exit
switch(config-router)# neighbor 192.168.1.1 remote-as 65536
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy
switch(config-router-neighbor-af)# copy running-config startup-config
```

Configuring BGP Peer Templates

You can configure BGP peer templates to combine session and policy attributes in one reusable configuration block. Peer templates can also inherit peer-session or peer-policy templates. Any attributes configured for the neighbor take priority over any attributes inherited by that neighbor from a BGP template. You configure only one peer template for a neighbor, but that peer template can inherit peer-session and peer-policy templates.

Send document comments to nexus7k-docfeedback@cisco.com.

Peer templates support session and address family attributes, such as eBGP multihop time-to-live, maximum prefix, next-hop self, and timers.

BEFORE YOU BEGIN

You must enable BGP (see the “[Enabling BGP](#)” section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).



Note

When editing a template, you can use the **no** form of a command at either the peer or template level to explicitly override a setting in a template. You must use the default form of the command to reset that attribute to the default state.

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **template peer** *template-name*
4. **inherit peer-session** *template-name*
5. **address-family** {**ipv4** | **ipv6** | **vpn4** | **vpn6**} {**multicast** | **unicast**}
6. **inherit peer** *template-name*
7. **exit**
8. **timers** *keepalive hold*
9. **exit**
10. **neighbor** *ip-address* **remote-as** *as-number*
11. **inherit peer** *template-name*
12. **timers** *keepalive hold*
13. (Optional) **show bgp peer-template** *template-name*
14. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp <i>autonomous-system-number</i> Example: switch(config)# router bgp 65536	Enters BGP mode and assigns the autonomous system number to the local BGP speaker.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 3	template peer <i>template-name</i> Example: <pre>switch(config-router)# template peer BasePeer switch(config-router-neighbor)#</pre>	Enters peer template configuration mode.
Step 4	inherit peer-session <i>template-name</i> Example: <pre>switch(config-router-neighbor)# inherit peer-session BaseSession</pre>	(Optional) Inherits a peer-session template in the peer template.
Step 5	address-family { <i>ipv4</i> <i>ipv6</i> <i>vpnv4</i> <i>vpnv6</i> } { <i>multicast</i> <i>unicast</i> } Example: <pre>switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#</pre>	(Optional) Configures the global address family configuration mode for the IPv4 address family.
Step 6	inherit peer <i>template-name</i> Example: <pre>switch(config-router-neighbor-af)# inherit peer BasePolicy</pre>	(Optional) Applies a peer template to the neighbor address family configuration.
Step 7	exit Example: <pre>switch(config-router-neighbor-af)# exit switch(config-router-neighbor)#</pre>	Exits BGP neighbor address family configuration mode.
Step 8	timers <i>keepalive hold</i> Example: <pre>switch(config-router-neighbor)# timers 45 100</pre>	(Optional) Adds the BGP timer values to the peer. These values override the timer values in the peer-session template, BaseSession.
Step 9	exit Example: <pre>switch(config-router-neighbor)# exit switch(config-router)#</pre>	Exits BGP peer template configuration mode.
Step 10	neighbor <i>ip-address</i> remote-as <i>as-number</i> Example: <pre>switch(config-router)# neighbor 192.168.1.2 remote-as 65536 switch(config-router-neighbor)#</pre>	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address.
Step 11	inherit peer <i>template-name</i> Example: <pre>switch(config-router-neighbor)# inherit peer BasePeer</pre>	Inherits the peer template.
Step 12	timers <i>keepalive hold</i> Example: <pre>switch(config-router-neighbor)# timers 60 120</pre>	(Optional) Adds the BGP timer values to this neighbor. These values override the timer values in the peer template and the peer-session template.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 13	show bgp peer-template <i>template-name</i> Example: switch(config-router-neighbor-af)# show bgp peer-template BasePeer	(Optional) Displays the peer template.
Step 14	copy running-config startup-config Example: switch(config-router-neighbor-af)# copy running-config startup-config	(Optional) Saves this configuration change.

Use the **show bgp neighbor** command to see the template applied. See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x*, for details on all commands available in the template.

This example shows how to configure a BGP peer template and apply it to a BGP peer:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer BasePeer
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

Configuring Prefix Peering

BGP supports the definition of a set of peers using a prefix for both IPv4 and IPv6. This feature allows you to not have to add each neighbor to the configuration.

When defining a prefix peering, you must specify the remote AS number with the prefix. BGP accepts any peer that connects from that prefix and autonomous system if the prefix peering does not exceed the configured maximum peers allowed.

When a BGP peer that is part of a prefix peering disconnects, Cisco NX-OS holds its peer structures for a defined prefix peer timeout value. An established peer can reset and reconnect without danger of being blocked because other peers have consumed all slots for that prefix peering.

To configure the BGP prefix peering timeout value, use the following command in router configuration mode:

Command	Purpose
timers prefix-peer-timeout <i>value</i> Example: switch(config-router-neighbor)# timers prefix-peer-timeout 120	Configures the timeout value for prefix peering. The range is from 0 to 1200 seconds. The default value is 30.

Send document comments to nexus7k-docfeedback@cisco.com.

To configure the maximum number of peers, use the following command in neighbor configuration mode:

Command	Purpose
maximum-peers <i>value</i> Example: switch(config-router-neighbor)# maximum-peers 120	Configures the maximum number of peers for this prefix peering. The range is from 1 to 1000.

This example shows how to configure a prefix peering that accepts up to 10 peers:

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 65536
switch(config-router-neighbor)# maximum-peers 10
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

Use the **show ip bgp neighbor** command to show the details of the configuration for that prefix peering with a list of the currently accepted instances and the counts of active, maximum concurrent, and total accepted peers.

Configuring BGP Authentication

You can configure BGP to authenticate route updates from peers using MD5 digests.

To configure BGP to use MD5 authentication, use the following command in neighbor configuration mode:

Command	Purpose
password [0 3 7] <i>string</i> Example: switch(config-router-neighbor)# password BGPPassword	Configures an MD5 password for BGP neighbor sessions.

Resetting a BGP Session

If you modify a route policy for BGP, you must reset the associated BGP peer sessions. If the BGP peers do not support route refresh, you can configure a soft reconfiguration for inbound policy changes. Cisco NX-OS automatically attempts a soft reset for the session.

To configure soft reconfiguration inbound, use the following command in neighbor address-family configuration mode:

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
soft-reconfiguration inbound Example: switch(config-router-neighbor-af)# soft-reconfiguration inbound	Enables soft reconfiguration to store the inbound BGP route updates. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.

To reset a BGP neighbor session, use the following command in any mode:

Command	Purpose
clear bgp {ipv4 ipv6 vpvv4 vpvv6} {unicast multicast} ip-address soft {in out} Example: switch# clear bgp ip unicast 192.0.2.1 soft in	Resets the BGP session without tearing down the TCP session.

Modifying the Next-Hop Address

You can modify the next-hop address used in a route advertisement in the following ways:

- Disable next-hop calculation and use the local BGP speaker address as the next-hop address.
- Set the next-hop address as a third-party address. Use this feature in situations where the original next-hop address is on the same subnet as the peer that the route is being sent to. Using this feature saves an extra hop during forwarding.

To modify the next-hop address, use the following commands in address-family configuration mode:

Command	Purpose
next-hop-self Example: switch(config-router-neighbor-af)# next-hop-self	Uses the local BGP speaker address as the next-hop address in route updates. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
next-hop-third-party Example: switch(config-router-neighbor-af)# next-hop-third-party	Sets the next-hop address as a third-party address. Use this command for single-hop EBGp peers that do not have next-hop-self configured

Configuring BGP Next-Hop Address Tracking

BGP next-hop address tracking is enabled by default and cannot be disabled.

You can modify the delay interval between RIB checks to increase the performance of BGP next-hop tracking.

To modify the BGP next-hop address tracking, use the following commands in address-family configuration mode:

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
nexthop trigger-delay {critical non-critical} <i>milliseconds</i> Example: switch(config-router-af)# nexthop trigger-delay critical 5000	Specifies the next-hop address tracking delay timer for critical next-hop reachability routes and for noncritical routes. The range is from 1 to 4294967295 milliseconds. The critical timer default is 3000. The noncritical timer default is 10000.

Configuring Next-Hop Filtering

BGP next-hop filtering allows you to specify that when a next-hop address is checked with the RIB, the underlying route for that next-hop address is passed through the route map. If the route map rejects the route, the next-hop address is treated as unreachable.

BGP marks all next hops that are rejected by the route policy as invalid and does not calculate the best path for the routes that use the invalid next-hop address.

To configure BGP next-hop filtering, use the following command in address-family configuration mode:

Command	Purpose
nexthop route-map <i>name</i> Example: switch(config-router-af)# nexthop route-map nextHopLimits	Specifies a route map to match the BGP next-hop route to. The name can be any case-sensitive, alphanumeric string up to 63 characters.

Disabling Capabilities Negotiation

You can disable capabilities negotiations to interoperate with older BGP peers that do not support capabilities negotiation.

To disable capabilities negotiation, use the following command in neighbor configuration mode:

Command	Purpose
dont-capability-negotiate Example: switch(config-router-neighbor)# dont-capability-negotiate	Disables capabilities negotiation. You must manually reset the BGP sessions after configuring this command.

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring eBGP

This section includes the following topics:

- [Disabling eBGP Single-Hop Checking, page 11-26](#)
- [Configuring eBGP Multihop, page 11-26](#)
- [Disabling a Fast External Fallover, page 11-26](#)
- [Limiting the AS-path Attribute, page 11-27](#)
- [Configuring Local AS Support, page 11-27](#)

Disabling eBGP Single-Hop Checking

You can configure eBGP to disable checking whether a single-hop eBGP peer is directly connected to the local router. Use this option for configuring a single-hop loopback eBGP session between directly connected switches.

To disable checking whether or not a single-hop eBGP peer is directly connected, use the following command in neighbor configuration mode:

Command	Purpose
disable-connected-check	Disables checking whether or not a single-hop eBGP peer is directly connected. You must manually reset the BGP sessions after using this command.
Example: switch(config-router-neighbor)# disable-connected-check	

Configuring eBGP Multihop

You can configure the eBGP time-to-live (TTL) value to support eBGP multihop. In some situations, an eBGP peer is not directly connected to another eBGP peer and requires multiple hops to reach the remote eBGP peer. You can configure the eBGP TTL value for a neighbor session to allow these multihop sessions.

To configure eBGP multihop, use the following command in neighbor configuration mode:

Command	Purpose
ebgp-multihop <i>ttl-value</i>	Configures the eBGP TTL value for eBGP multihop. The range is from 2 to 255. You must manually reset the BGP sessions after using this command.
Example: switch(config-router-neighbor)# ebgp-multihop 5	

Disabling a Fast External Fallover

By default, the Cisco Nexus 7000 Series device supports fast external fallover for neighbors in all VRFs and address-families (IPv4 or IPv6). Typically, when a BGP router loses connectivity to a directly connected eBGP peer, BGP triggers a fast external fallover by resetting the eBGP session to the peer. You can disable this fast external fallover to limit the instability caused by link flaps.

Send document comments to nexus7k-docfeedback@cisco.com.

To disable fast external fallover, use the following command in router configuration mode:

Command	Purpose
no fast-external-fallover	Disables a fast external fallover for eBGP peers. This command is enabled by default.
Example: switch(config-router)# no fast-external-fallover	

Limiting the AS-path Attribute

You can configure eBGP to discard routes that have excessive AS numbers in the AS-path attribute.

To discard routes that have excessive AS numbers in the AS-path attribute, use the following command in router configuration mode:

Command	Purpose
maxas-limit <i>number</i>	Discards eBGP routes that have a number of AS-path segments that exceed the specified limit. The range is from 1 to 2000.
Example: switch(config-router)# maxas-limit 50	

Configuring Local AS Support

The local-AS feature allows a router to appear to be a member of a second autonomous system (AS), in addition to its real AS. Local AS allows two ISPs to merge without modifying peering arrangements. Routers in the merged ISP become members of the new autonomous system but continue to use their old AS numbers for their customers.

This feature can only be used for true eBGP peers. You cannot use this feature for two peers that are members of different confederation sub-autonomous systems.

To configure eBGP local AS support, use the following command in neighbor configuration mode:

Command	Purpose
local-as <i>number</i> [no-prepend [replace-as [dual-as]]]	Configures eBGP to prepend the local AS <i>number</i> to the AS_PATH attribute. The AS <i>number</i> can be a 16-bit integer or a 32-bit integer in the form of a higher 16-bit decimal number and a lower 16-bit decimal number in xx.xx format.
Example: switch(config-router-neighbor)# local-as 1.1	

This example shows how to configure local AS support on a VRF:

```
switch(config)# router bgp 1
switch(config-router)# vrf test
switch(config-router-vrf)# local-as 1
switch(config-router-vrf)# show running-config bgp
```

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring AS Confederations

To configure an AS confederation, you must specify a confederation identifier. To the outside world, the group of autonomous systems within the AS confederation look like a single autonomous system with the confederation identifier as the autonomous system number.

To configure a BGP confederation identifier, use the following command in router configuration mode:

Command	Purpose
<code>confederation identifier as-number</code>	Configures a confederation identifier for an AS confederation. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Example: <pre>switch(config-router)# confederation identifier 4000</pre>	

To configure the autonomous systems that belong to the AS confederation, use the following command in router configuration mode:

Command	Purpose
<code>bgp confederation peers as-number [as-number2...]</code>	Specifies a list of autonomous systems that belong to the confederation. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Example: <pre>switch(config-router)# bgp confederation peers 5 33 44</pre>	

Configuring Route Reflector

You can configure iBGP peers as route reflector clients to the local BGP speaker, which acts as the route reflector. Together, a route reflector and its clients form a cluster. A cluster of clients usually has a single route reflector. In such instances, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure in the network, you can configure a cluster with more than one route reflector. You must configure all route reflectors in the cluster with the same 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

BEFORE YOU BEGIN

You must enable BGP (see the [“Enabling BGP”](#) section on page 10-11).

Ensure that you are in the correct VDC (or use the `switchto vdc` command).

SUMMARY STEPS

1. **configure terminal**
2. **router bgp as-number**
3. **cluster-id cluster-id**
4. **address-family {ipv4 | ipv6 | vpnv4 | vpnv6} {unicast | multicast}**
5. (Optional) **client-to-client reflection**
6. **exit**

Send document comments to nexus7k-docfeedback@cisco.com.

7. **neighbor** *ip-address* **remote-as** *as-number*
8. **address-family** {*ipv4* | *ipv6* | *vpnv4* | *vpnv6*} {**unicast** | **multicast**}
9. **route-reflector-client**
10. (Optional) **show** **bgp** {*ipv4* | *ipv6* | *vpnv4* | *vpnv6*} {**unicast** | **multicast**} **neighbors**
11. (Optional) **copy** **running-config** **startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp <i>as-number</i> Example: switch(config)# router bgp 65536 switch(config-router)#	Enters BGP mode and assigns the autonomous system number to the local BGP speaker.
Step 3	cluster-id <i>cluster-id</i> Example: switch(config-router)# cluster-id 192.0.2.1	Configures the local router as one of the route reflectors that serve the cluster. You specify a cluster ID to identify the cluster. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
Step 4	address-family { <i>ipv4</i> <i>ipv6</i> <i>vpnv4</i> <i>vpnv6</i> } { unicast multicast } Example: switch(config-router)# address-family ipv4 unicast switch(config-router-af)#	Enters router address family configuration mode for the specified address family.
Step 5	client-to-client reflection Example: switch(config-router-af)# client-to-client reflection	(Optional) Configures client-to-client route reflection. This feature is enabled by default. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
Step 6	exit Example: switch(config-router-neighbor)# exit switch(config-router)#	Exits router address configuration mode.
Step 7	neighbor <i>ip-address</i> remote-as <i>as-number</i> Example: switch(config-router)# neighbor 192.0.2.10 remote-as 65536 switch(config-router-neighbor)#	Configures the IP address and AS number for a remote BGP peer.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 8	address-family { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } Example: switch(config-router-neighbor)# address-family ipv4 unicast switch(config-router-neighbor-af)#	Enters neighbor address family configuration mode for the unicast IPv4 address family.
Step 9	route-reflector-client Example: switch(config-router-neighbor-af)# route-reflector-client	Configures the device as a BGP route reflector and configures the neighbor as its client. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Step 10	show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } neighbors Example: switch(config-router-neighbor-af)# show bgp ip unicast neighbors	(Optional) Displays the BGP peers.
Step 11	copy running-config startup-config Example: switch(config-router-neighbor-af)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to configure the router as a route reflector and add one neighbor as a client:

```
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.10 remote-as 65536
switch(config-router-neighbor)# address-family ip unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# copy running-config startup-config
```

Configuring Route Dampening

You can configure route dampening to minimize route flaps propagating through your iBGP network.

To configure route dampening, use the following command in address-family or VRF address family configuration mode:

Command	Purpose
dampening [{ half-life reuse-limit suppress-limit max-suppress-time route-map <i>map-name</i> }] Example: switch(config-router-af)# dampening route-map bgpDamp	Disables capabilities negotiation. The parameter values are as follows: half-life—The range is from 1 to 45. reuse-limit—The range is from 1 to 20000. suppress-limit—The range is from 1 to 20000. max-suppress-time—The range is from 1 to 255.

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring Load Sharing and ECMP

You can configure the maximum number of paths that BGP adds to the route table for equal-cost multipath load balancing.

To configure the maximum number of paths, use the following command in router address-family configuration mode:

Command	Purpose
<code>maximum-paths [ibgp] maxpaths</code>	Configures the maximum number of equal-cost paths for load sharing. The range is from 1 to 16. The default is 1.

Configuring Maximum Prefixes

You can configure the maximum number of prefixes that BGP can receive from a BGP peer. If the number of prefixes exceeds this value, you can optionally configure BGP to generate a warning message or tear down the BGP session to the peer.

To configure the maximum allowed prefixes for a BGP peer, use the following command in neighbor address-family configuration mode:

Command	Purpose
<code>maximum-prefix maximum [threshold] [restart time warning-only]</code> Example: switch(config-router-neighbor-af)# maximum-prefix 12	Configures the maximum number of prefixes from a peer. The parameter ranges are as follows: <i>maximum</i>—The range is from 1 to 300000. <i>Threshold</i>—The range is from 1 to 100 percent. The default is 75 percent. <i>time</i>—The range is from 1 to 65535 minutes. This command triggers an automatic notification and session reset for the BGP neighbor sessions if the prefix limit is exceeded.

Configuring Dynamic Capability

You can configure dynamic capability for a BGP peer.

To configure dynamic capability, use the following command in neighbor configuration mode:

Command	Purpose
<code>dynamic-capability</code> Example: switch(config-router-neighbor)# dynamic-capability	Enables dynamic capability. This command triggers an automatic notification and session reset for the BGP neighbor sessions.

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring Aggregate Addresses

You can configure aggregate address entries in the BGP route table.

To configure an aggregate address, use the following command in router address-family configuration mode:

Command	Purpose
<pre>aggregate-address ip-prefix/length [as-set] [summary-only] [advertise-map map-name] [attribute-map map-name] [suppress-map map-name]</pre> Example: <pre>switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set</pre>	Creates an aggregate address. The path advertised for this route is an autonomous system set that consists of all elements contained in all paths that are being summarized: • The as-set keyword generates autonomous system set path information and community information from contributing paths. • The summary-only keyword filters all more specific routes from updates. • The advertise-map keyword and argument specify the route map used to select attribute information from selected routes. • The attribute-map keyword and argument specify the route map used to select attribute information from the aggregate. • The suppress-map keyword and argument conditionally filter more specific routes.

Configuring BGP Conditional Advertisement

You can configure BGP conditional advertisement to limit the routes that BGP propagates. You define the following two route maps:

- **Advertise map**—Specifies the conditions that the route must match before BGP considers the conditional advertisement. This route map can contain any appropriate match statements.
- **Exist map or nonexistent map**—Defines the prefix that must exist in the BGP table before BGP propagates a route that matches the advertise map. The nonexistent map defines the prefix that must not exist in the BGP table before BGP propagates a route that matches the advertise map. BGP processes only the permit statements in the prefix list match statements in these route maps.

If the route does not pass the condition, BGP withdraws the route if it exists in the BGP table.

BEFORE YOU BEGIN

You must enable BGP (see the “[Enabling BGP](#)” section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **router bgp as-number**

Send document comments to nexus7k-docfeedback@cisco.com.

3. **neighbor** *ipaddress remote-as as-number*
4. **address-family** {*ipv4 | ipv6 | vpnv4 | vpnv6*} {**unicast** | **multicast**}
5. **advertise-map** *adv-map* {**exist-map** *exist-rmap* | **non-exist-map** *nonexist-rmap*}
6. (Optional) **show ip bgp neighbor**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp <i>as-number</i> Example: switch(config)# router bgp 65536 switch(config-router)#	Enters BGP mode and assigns the autonomous system number to the local BGP speaker.
Step 3	neighbor <i>ip-address remote-as as-number</i> Example: switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address.
Step 4	address-family { <i>ipv4 ipv6 vpnv4 vpnv6</i> } { unicast multicast } Example: switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	Enters address family configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 5	<pre>advertise-map adv-map {exist-map exist-rmap non-exist-map nonexist-rmap}</pre> Example: <pre>switch(config-router-neighbor-af)# advertise-map advertise exist-map exist</pre>	Configures BGP to conditionally advertise routes based on the two configured route maps: <i>adv-map</i>—Specifies a route map with match statements that the route must pass before BGP passes the route to the next route map. The <i>adv-map</i> is a case-sensitive, alphanumeric string up to 63 characters. <i>exist-rmap</i>—Specifies a route map with match statements for a prefix list. A prefix in the BGP table must match a prefix in the prefix list before BGP advertises the route. The <i>exist-rmap</i> is a case-sensitive, alphanumeric string up to 63 characters. <i>nonexist-rmap</i>—Specifies a route map with match statements for a prefix list. A prefix in the BGP table must not match a prefix in the prefix list before BGP advertises the route. The <i>nonexist-rmap</i> is a case-sensitive, alphanumeric string up to 63 characters.
Step 6	<pre>show ip bgp neighbor</pre> Example: <pre>switch(config-router-neighbor-af)# show ip bgp neighbor</pre>	(Optional) Displays information about BGP and the configured conditional advertisement route maps.
Step 7	<pre>copy running-config startup-config</pre> Example: <pre>switch(config-router-neighbor-af)# copy running-config startup-config</pre>	(Optional) Saves this configuration change.

This example shows how to configure BGP conditional advertisement:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
```

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring Route Redistribution

You can configure BGP to accept routing information from another routing protocol and redistribute that information through the BGP network. Optionally, you can assign a default metric for redistributed routes.

BEFORE YOU BEGIN

You must enable BGP (see the [“Enabling BGP”](#) section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *as-number*
3. **address-family** {*ipv4* | *ipv6* | *vpnv4* | *vpnv6*} {*unicast* | *multicast*}
4. **redistribute** {*direct* | {*eigrp* | *isis* | *ospf* | *ospfv3* | *rip*} *instance-tag* | *static*} **route-map** *map-name*
5. (Optional) **default-metric** *value*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp <i>as-number</i> Example: switch(config)# router bgp 65536 switch(config-router)#	Enters BGP mode and assigns the autonomous system number to the local BGP speaker.
Step 3	address-family { <i>ipv4</i> <i>ipv6</i> <i>vpnv4</i> <i>vpnv6</i> } { <i>unicast</i> <i>multicast</i> }	Enters address family configuration mode.
Step 4	redistribute { <i>direct</i> { <i>eigrp</i> <i>isis</i> <i>ospf</i> <i>ospfv3</i> <i>rip</i> } <i>instance-tag</i> <i>static</i> } route-map <i>map-name</i> Example: switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap	Redistributes routes from other protocols into BGP. See the “Configuring Route Maps” section on page 16-13 for more information about route maps.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 5	default-metric <i>value</i> Example: switch(config-router-af)# default-metric 33	(Optional) Generates a default metric into BGP.
Step 6	copy running-config startup-config Example: switch(config-router-af)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to redistribute EIGRP into BGP:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute eigrp 201 route-map Eigrpmap
switch(config-router-af)# copy running-config startup-config
```

Configuring Multiprotocol BGP

You can configure MP-BGP to support multiple address families, including IPv4 and IPv6 unicast and multicast routes.

BEFORE YOU BEGIN

You must enable BGP (see the [“Enabling BGP” section on page 10-11](#)).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *as-number*
3. **neighbor** *ip-address* **remote-as** *as-number*
4. **address-family** {**ipv4** | **ipv6** | **vpnv4** | **vpnv6**} {**unicast** | **multicast**}
5. (Optional) **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp as-number Example: switch(config)# router bgp 65536 switch(config-router)#	Enters BGP mode and assigns the autonomous system number to the local BGP speaker.
Step 3	neighbor ip-address remote-as as-number Example: switch(config-router)# neighbor 192.168.1.2 remote-as 65537 switch(config-router-neighbor)#	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address.
Step 4	address-family {ipv4 ipv6 vpnv4 vpnv6} {unicast multicast} Example: switch(config-router-neighbor)# address-family ipv4 multicast switch(config-router-neighbor-af)#	Enters address family configuration mode.
Step 5	copy running-config startup-config Example: switch(config-router-neighbor-af)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to enable advertising and receiving IPv4 and IPv6 routes for multicast RPF for a neighbor:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8::1
switch(config-if)# router bgp 65536
switch(config-router)# neighbor 192.168.1.2 remote-as 35537
switch(config-router-neighbor)# address-family ipv4 multicast
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# address-family ipv6 multicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

Tuning BGP

You can tune BGP characteristics through a series of optional parameters.

To tune BGB, use the following optional commands in router configuration mode:

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
bestpath [always-compare-med compare-routerid med { missing-as-worst non-deterministic }] Example: <pre>switch(config-router)# bestpath always-compare-med</pre>	Modifies the best-path algorithm. The optional parameters are as follows: • always-compare-med—Compares MED on paths from different autonomous systems. • compare-routerid—Compares the router IDs for identical eBGP paths. • med missing-as-worst—Treats a missing MED as the highest MED. • med non-deterministic—Does not always pick the best MED path from among the paths from the same autonomous system.
enforce-first-as Example: <pre>switch(config-router)# enforce-first-as</pre>	Enforces the neighbor autonomous system to be the first AS number listed in the AS_path attribute for eBGP.
log-neighbor-changes Example: <pre>switch(config-router)# log-neighbor-changes</pre>	Generates a system message when a neighbor changes state.
router-id <i>id</i> Example: <pre>switch(config-router)# router-id 209.165.20.1</pre>	Manually configures the router ID for this BGP speaker.
timers [bestpath-delay <i>delay</i> bgp keepalive <i>holdtime</i> prefix-peer-timeout <i>timeout</i>] Example: <pre>switch(config-router)# timers bgp 90 270</pre>	Sets the BGP timer values. The optional parameters are as follows: • delay—Initial best-path timeout value after a restart. The range is from 0 to 3600 seconds. The default value is 300. • keepalive—BGP session keepalive time. The range is from 0 to 3600 seconds. The default value is 60. • holdtime—BGP session hold time. The range is from 0 to 3600 seconds. The default value is 180. • timeout—Prefix peer timeout value. The range is from 0 to 1200 seconds. The default value is 30. You must manually reset the BGP sessions after configuring this command.

Send document comments to nexus7k-docfeedback@cisco.com.

To tune BGP, use the following optional command in router address-family configuration mode:

Command	Purpose
distance <i>ebgp-distance ibgp-distance local-distance</i> Example: <pre>switch(config-router-af)# distance 20 100 200</pre>	Sets the administrative distance for BGP. The range is from 1 to 255. The defaults are as follows: <i>ebgp-distance</i>—20. <i>ibgp-distance</i>—200. <i>local-distance</i>—220. Local-distance is the administrative distance used for aggregate discard routes when they are installed in the RIB.

To tune BGP, use the following optional commands in neighbor configuration mode:

Command	Purpose
description <i>string</i> Example: <pre>switch(config-router-neighbor)# description main site</pre>	Sets a descriptive string for this BGP peer. The string can be up to 80 alphanumeric characters.
low-memory exempt Example: <pre>switch(config-router-neighbor)# low-memory exempt</pre>	Exempts this BGP neighbor from a possible shutdown due to a low memory condition.
transport connection-mode passive Example: <pre>switch(config-router-neighbor)# transport connection-mode passive</pre>	Allows a passive connection setup only. This BGP speaker does not initiate a TCP connection to a BGP peer. You must manually reset the BGP sessions after configuring this command.
remove-private-as Example: <pre>switch(config-router-neighbor)# remove-private-as</pre>	Removes private AS numbers from outbound route updates to an eBGP peer. This command triggers an automatic soft clear or refresh of BGP neighbor sessions. Note See the “Guidelines and Limitations for Advanced BGP” section for more information on this command.
update-source <i>interface-type number</i> Example: <pre>switch(config-router-neighbor)# update-source ethernet 2/1</pre>	Configures the BGP speaker to use the source IP address of the configured interface for BGP sessions to the peer. This command triggers an automatic notification and session reset for the BGP neighbor sessions. Single-hop iBGP peers support fast external failover when update-source is configured.

To tune BGP, use the following optional commands in neighbor address-family configuration mode:

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
suppress-inactive Example: switch(config-router-neighbor-af) # suppress-inactive	Advertises the best (active) routes only to the BGP peer. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
default-originate [route-map <i>map-name</i>] Example: switch(config-router-neighbor-af) # default-originate	Generates a default route to the BGP peer.
filter-list <i>list-name</i> {in out} Example: switch(config-router-neighbor-af) # filter-list BGPFilter in	Applies an AS_path filter list to this BGP peer for inbound or outbound route updates. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
prefix-list <i>list-name</i> {in out} Example: switch(config-router-neighbor-af) # prefix-list PrefixFilter in	Applies a prefix list to this BGP peer for inbound or outbound route updates. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
send-community Example: switch(config-router-neighbor-af) # send-community	Sends the community attribute to this BGP peer. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.
send-community extended Example: switch(config-router-neighbor-af) # send-community extended	Sends the extended community attribute to this BGP peer. This command triggers an automatic soft clear or refresh of BGP neighbor sessions.

Configuring a Graceful Restart

You can configure a graceful restart and enable the graceful restart helper feature for BGP.

BEFORE YOU BEGIN

You must enable BGP (see the [“Enabling BGP” section on page 10-11](#)).

Create the VDCs and VRFs.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **router bgp** *as-number*
3. **graceful-restart**
4. **graceful-restart** [restart-time *time* | stalepath-time *time*]
5. **graceful-restart-helper**
6. (Optional) **show running-config bgp**

Send document comments to nexus7k-docfeedback@cisco.com.

7. (Optional) copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	router bgp as-number Example: switch(config)# router bgp 65536 switch(config-router)#	Creates a new BGP process with the configured autonomous system number.
Step 3	graceful-restart Example: switch(config-router)# graceful-restart	Enables a graceful restart and the graceful restart helper functionality. This command is enabled by default. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Step 4	graceful-restart [restart-time time stalepath-time time] Example: switch(config-router)# graceful-restart restart-time 300	Configures the graceful restart timers. The optional parameters are as follows: restart-time—Maximum time for a restart sent to the BGP peer. The range is from 1 to 3600 seconds. The default is 120. stalepath-time—Maximum time that BGP keeps the stale routes from the restarting BGP peer. The range is from 1 to 3600 seconds. The default is 300. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Step 5	graceful-restart-helper Example: switch(config-router)# graceful-restart-helper	Enables the graceful restart helper functionality. Use this command if you have disabled graceful restart but you still want to enable graceful restart helper functionality. This command triggers an automatic notification and session reset for the BGP neighbor sessions.
Step 6	show running-config bgp Example: switch(config-router)# show running-config bgp	(Optional) Displays the BGP configuration.
Step 7	copy running-config startup-config Example: switch(config-router)# copy running-config startup-config	(Optional) Saves this configuration change.

Send document comments to nexus7k-docfeedback@cisco.com.

This example shows how to enable a graceful restart:

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# graceful-restart
switch(config-router)# copy running-config startup-config
```

Configuring Virtualization

You can configure one BGP process in each VDC. You can create multiple VRFs within each VDC and use the same BGP process in each VRF.

BEFORE YOU BEGIN

You must enable BGP (see the “[Enabling BGP](#)” section on page 10-11).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **exit**
4. **router bgp** *as-number*
5. **vrf** *vrf-name*
6. **neighbor** *ip-address* **remote-as** *as-number*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	vrf context <i>vrf-name</i> Example: switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#	Creates a new VRF and enters VRF configuration mode.
Step 3	exit Example: switch(config-vrf)# exit switch(config)#	Exits VRF configuration mode.
Step 4	router bgp <i>as-number</i> Example: switch(config)# router bgp 65536 switch(config-router)#	Creates a new BGP process with the configured autonomous system number.

Send document comments to nexus7k-docfeedback@cisco.com.

	Command	Purpose
Step 5	vrf <i>vrf-name</i> Example: switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	Enters the router VRF configuration mode and associates this BGP instance with a VRF.
Step 6	neighbor <i>ip-address</i> remote-as <i>as-number</i> Example: switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536 switch(config-router--vrf-neighbor)#	Configures the IP address and AS number for a remote BGP peer.
Step 7	copy running-config startup-config Example: switch(config-router-vrf-neighbor)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to create a VRF and configure the router ID in the VRF:

```
switch# configure terminal
switch(config)# vrf context NewVRF
switch(config-vrf)# exit
switch(config)# router bgp 65536
switch(config-router)# vrf NewVRF
switch(config-router-vrf)# neighbor 209.165.201.1 remote-as 65536
switch(config-router-vrf-neighbor)# copy running-config startup-config
```

Verifying the Advanced BGP Configuration

To display the BGP configuration, perform one of the following tasks:

Command	Purpose
show bgp all [summary] [vrf <i>vrf-name</i>]	Displays the BGP information for all address families.
show bgp convergence [vrf <i>vrf-name</i>]	Displays the BGP information for all address families.
show bgp { ipv4 ipv6 vpn4 vpn6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] community { regex <i>expression</i> [community] [no-advertise] [no-export] [no-export-subconfed] } [vrf <i>vrf-name</i>]	Displays the BGP routes that match a BGP community.
show bgp [vrf <i>vrf-name</i>] { ipv4 ipv6 vpn4 vpn6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] community-list <i>list-name</i> [vrf <i>vrf-name</i>]	Displays the BGP routes that match a BGP community list.

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] extcommunity { regex <i>expression</i> generic [non-transitive transitive] <i>aa4:nn</i> [exact-match] } [vrf <i>vrf-name</i>]	Displays the BGP routes that match a BGP extended community.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] extcommunity-list <i>list-name</i> [exact-match] } [vrf <i>vrf-name</i>]	Displays the BGP routes that match a BGP extended community list.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] { dampening dampened-paths [regex <i>expression</i>] } [vrf <i>vrf-name</i>]	Displays the information for BGP route dampening. Use the clear bgp dampening command to clear the route flap dampening information.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] history-paths [regex <i>expression</i>] [vrf <i>vrf-name</i>]	Displays the BGP route history paths.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] filter-list <i>list-name</i> [vrf <i>vrf-name</i>]	Displays the information for the BGP filter list.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] neighbors [<i>ip-address</i> <i>ipv6-prefix</i>] [vrf <i>vrf-name</i>]	Displays the information for BGP peers. Use the clear bgp neighbors command to clear these neighbors.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] { nexthop nexthop-database } [vrf <i>vrf-name</i>]	Displays the information for the BGP route next hop.
show bgp paths	Displays the BGP path information.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] policy <i>name</i> [vrf <i>vrf-name</i>]	Displays the BGP policy information. Use the clear bgp policy command to clear the policy information.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] prefix-list <i>list-name</i> [vrf <i>vrf-name</i>]	Displays the BGP routes that match the prefix list.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] received-paths [vrf <i>vrf-name</i>]	Displays the BGP paths stored for soft reconfiguration.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] regex <i>expression</i> [vrf <i>vrf-name</i>]	Displays the BGP routes that match the AS_path regular expression.
show bgp { ipv4 ipv6 vpnv4 vpnv6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] route-map <i>map-name</i> [vrf <i>vrf-name</i>]	Displays the BGP routes that match the route map.
show bgp peer-policy <i>name</i> [vrf <i>vrf-name</i>]	Displays the information about BGP peer policies.

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
show bgp peer-session <i>name</i> [vrf <i>vrf-name</i>]	Displays the information about BGP peer sessions.
show bgp peer-template <i>name</i> [vrf <i>vrf-name</i>]	Displays the information about BGP peer templates. Use the clear bgp peer-template command to clear all neighbors in a peer template.
show bgp process	Displays the BGP process information.
show { ipv4 ipv6 vpn4 vpn6 } bgp options	Displays the BGP status and configuration information. This command has multiple options. See the <i>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x</i> , for more information.
show { ipv4 ipv6 vpn4 vpn6 } mbgp options	Displays the BGP status and configuration information. This command has multiple options. See the <i>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x</i> , for more information.
show running-configuration bgp	Displays the current running BGP configuration.

Monitoring BGP Statistics

To display BGP statistics, use the following commands:

Command	Purpose
show bgp { ipv4 ipv6 vpn4 vpn6 } { unicast multicast } [<i>ip-address</i> <i>ipv6-prefix</i>] flap-statistics [vrf <i>vrf-name</i>]	Displays the BGP route flap statistics. Use the clear bgp flap-statistics command to clear these statistics.
show bgp sessions [vrf <i>vrf-name</i>]	Displays the BGP sessions for all peers. Use the clear bgp sessions command to clear these statistics.
show bgp sessions [vrf <i>vrf-name</i>]	Displays the BGP sessions for all peers. Use the clear bgp sessions command to clear these statistics.
show bgp statistics	Displays the BGP statistics.

Related Topics

The following topics can give more information on BGP:

- [Chapter 10, “Configuring Basic BGP,”](#)
- [Chapter 16, “Configuring Route Policy Manager,”](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Additional References

For additional information related to implementing BGP, see the following sections:

- [Related Documents, page 11-46](#)
- [RFCs, page 11-46](#)
- [MIBs, page 11-46](#)

Related Documents

Related Topic	Document Title
BGP CLI commands	<i>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x</i>
VDCs and VRFs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x</i>

RFCs

RFC	Title
RFC 2918	Route Refresh Capability for BGP-4

MIBs

MIBs	MIBs Link
BGP4-MIB	To locate and download MIBs, go to the following URL:
CISCO-BGP4-MIB	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for BGP

[Table 11-2](#) lists the release history for this feature.

Table 11-2 Feature History for BGP

Feature Name	Releases	Feature Information
VPN address families	5.2(1)	Added support for VPN address families.
BFD	5.0(2)	Added support for BFD. See the <i>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x</i> , for more information.
ISSU	4.2(3)	Lowered the BGP minimum hold-time check to eight seconds.
Next-hop addressing	4.2(1)	Added support for the BGP next-hop address tracking and filtering.

Send document comments to nexus7k-docfeedback@cisco.com.

Table 11-2 *Feature History for BGP (continued)*

Feature Name	Releases	Feature Information
4-Byte AS numbers	4.2(1)	Added support for 4-byte AS numbers in plaintext notation.
Conditional advertisement	4.2(1)	Added support for conditionally advertising BGP routes based on the existence of other routes in the BGP table.
Dynamic AS number for prefix peers	4.1(2)	Added support for a range of AS numbers for the BGP prefix peer configuration.
BGP	4.0(1)	This feature was introduced.

Send document comments to nexus7k-docfeedback@cisco.com.