

Configuring QoS Policy Propagation via Border Gateway Protocol

This chapter describes the tasks for configuring Policy Propagation via Border Gateway Protocol (BGP) on a router. For a complete description of the commands mentioned in this chapter, refer to the *Quality of Service Solutions Command Reference*; the commands are listed alphabetically within that guide. To locate documentation of specific commands, use the command reference, master index, or search online.

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

Policy Propagation via BGP Configuration Task List

The Policy Propagation via BGP feature allows you to classify packets by IP Precedence based on BGP community lists, BGP autonomous system paths, and access lists. After a packet has been classified, you can use other quality of service features such as committed access rate (CAR) and Weighted Random Early Detection (WRED) to specify and enforce policies to fit your business model.

Overview of Tasks

To configure Policy Propagation via BGP, perform the following basic tasks:

- Configure BGP and Cisco Express Forwarding (CEF) or Distributed CEF (DCEF).
- Define the policy.
- Apply the policy through BGP. To configure BGP, refer to the *Network Protocols Configuration Guide, Part 1*. To configure CEF and DCEF, refer to the *Cisco IOS Switching Services Configuration Guide*.
- Configure the BGP community list, BGP autonomous system path, or access list and enable the policy on an interface.
- Enable CAR or WRED to use the policy. To enable CAR, refer to the chapter “Configuring Committed Access Rate” in this guide. To configure WRED, refer to the chapter “Configuring Weighted Random Early Detection” in this guide.

This chapter describes how to configure Policy Propagation based on BGP community list, BGP autonomous system path, or access list. It assumes you have already configured BGP and CEF or DCEF. See the next section for the list of tasks covered in this chapter.

Configuration Task List

The tasks required to configure Policy Propagation via BGP and verify that the information is correct are described in the following sections in this chapter:

- Configure Policy Propagation Based on Community Lists
- Configure Policy Propagation Based on the AS Path Attribute
- Configure Policy Propagation Based on an Access List
- Monitor Policy Propagation via BGP

Note For the Policy Propagation via BGP feature to work, you must enable BGP and CEF/DCEF on the router. Subinterfaces on an ATM interface that have the **bgp-policy** command enabled must use CEF mode because DCEF is not supported. DCEF uses the Versatile Interface Processor (VIP) rather than the Route Switch Processor (RSP) to perform forwarding functions.

For examples of propagating policy using access lists, BGP community lists, and BGP autonomous system paths, see the section “Policy Propagation via BGP Configuration Examples” later in this chapter.

Configure Policy Propagation Based on Community Lists

This section describes how to configure Policy Propagation via BGP using community lists. The tasks listed in this section are required unless noted as optional. This section assumes you have already configured CEF/DCEF and BGP on your router.

To configure the router to propagate the IP Precedence based on the community lists, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	route-map <i>route-map-name</i> [permit deny [<i>sequence-number</i>]]	Define a route map to control redistribution and enter route-map configuration mode.
2	match community-list <i>community-list-number</i> [exact]	Match a BGP community list.
3	set ip precedence [<i>number</i> <i>name</i>]	Set the IP Precedence field when the community list matches. You can specify either a precedence number or name.
4	router bgp <i>autonomous-system</i>	Enter router configuration mode.
5	table-map <i>route-map-name</i>	Modify the metric and tag values when the IP routing table is updated with BGP learned routes.
6	ip community-list <i>community-list-number</i> { permit deny } <i>community-number</i>	Create a community list for BGP and control access to it.
7	interface <i>interface-type interface-number</i>	Specify the interfaces (or subinterface) and enter interface configuration mode.
8	bgp-policy { source destination } ip-prec-map	Classify packets using IP Precedence.
9	ip bgp-community new-format	(Optional) Configure a new community format so that the community number is displayed in the short form.
10	end	Exit configuration mode.

Configure Policy Propagation Based on the AS Path Attribute

This section describes how to configure Policy Propagation via BGP based on the autonomous system (AS) path. The tasks listed in this section are required unless noted as optional. This section assumes you have already configured CEF/DCEF and BGP on your router.

To configure the router to propagate the IP Precedence based on the autonomous system path attribute, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	route-map <i>route-map-name</i> [permit deny [<i>sequence-number</i>]]	Define a route map to control redistribution and enter route-map configuration mode.
2	match as-path <i>path-list-number</i>	Match a BGP autonomous system path access list.
3	set ip precedence [<i>number</i> <i>name</i>]	Set the IP Precedence field when the autonomous system path matches. Specify either a precedence number or name.
4	router bgp <i>autonomous-system</i>	Enter router configuration mode.
5	table-map <i>route-map-name</i>	Modify the metric and tag values when the IP routing table is updated with BGP learned routes.
6	ip as-path access-list <i>access-list-number</i> { permit deny } <i>as-regular-expression</i>	Define an autonomous system path access list.
7	interface <i>interface-type interface-number</i>	Specify the interfaces (or subinterface) and enter interface configuration mode.
8	bgp-policy { source destination } ip-prec-map	Classify packets using IP Precedence.
9	end	Exit configuration mode.

Configure Policy Propagation Based on an Access List

This section describes how to configure Policy Propagation via BGP based on an access list. The tasks listed in this section are required unless noted as optional. This section assumes you have already configured CEF/DCEF and BGP on your router.

To configure the router to propagate the IP Precedence based on an access list, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	route-map <i>route-map-name</i> [permit deny [<i>sequence-number</i>]]	Define a route map to control redistribution and enter route-map configuration mode.
2	match ip address <i>access-list-number</i>	Match an access list.
3	set ip precedence [<i>number</i> <i>name</i>]	Set the IP Precedence field when the autonomous system path matches.
4	router bgp <i>autonomous-system</i>	Enter router configuration mode.
5	table-map <i>route-map-name</i>	Modify the metric and tag values when the IP routing table is updated with BGP learned routes.
6	access-list <i>access-list-number</i> { permit deny } <i>source</i>	Define an access list.
7	interface <i>interface-type interface-number</i>	Specify the interfaces (or subinterface) and enter interface configuration mode.

Step	Command	Purpose
8	bgp-policy {source destination} ip-prec-map	Classify packets using IP Precedence.
9	end	Exit configuration mode.

Monitor Policy Propagation via BGP

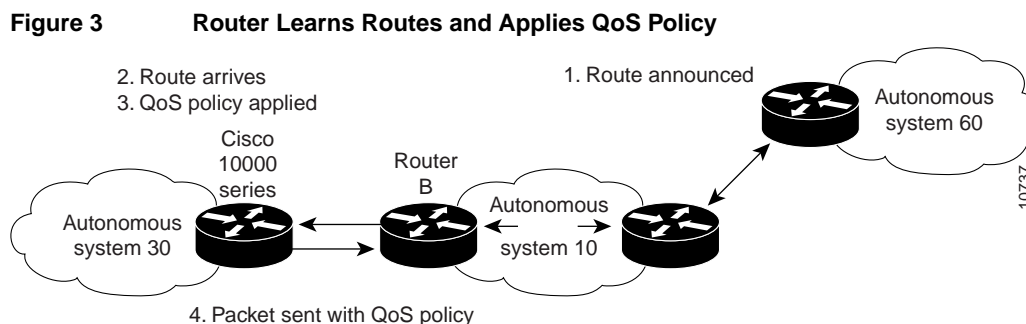
To monitor the Policy Propagation via BGP configuration, use any of the following commands in EXEC mode. The commands listed in this section are optional.

Command	Purpose
show ip bgp	Show entries in the BGP routing table, to verify the correct community is set on the prefixes.
show ip bgp community-list community-list-number	Show routes permitted by the BGP community list, to verify that the correct prefixes are selected.
show ip cef network	Show entries in the FIB table based on the IP address, to verify that CEF has the correct precedence value for the prefix.
show ip interface	Show information about the interface.
show ip route prefix	Show the current status of the routing table, to verify that the correct precedence values are set on the prefixes.

Policy Propagation via BGP Configuration Examples

The following example shows how to create route maps to match access lists, BGP community lists, and BGP Autonomous System paths, and apply IP Precedence to routes learned from neighbors.

In the following example, Router A (Cisco 10000 Series) learns routes from AS 10 and AS 60. QoS policy is applied to all packets that match the defined route maps. Any packets from Router A (Cisco 10000 Series) to AS 10 or AS 60 are sent the appropriate QoS policy.



Router A's (Cisco 10000 Series) Configuration

```
interface serial 5/0/0/1:0
ip address 200.28.38.2 255.255.255.0
bgp-policy destination ip-prec-map
no ip mroute-cache
no cdp enable
frame-relay interface-dlci 20 IETF

router bgp 30
  table-map precedence-map
  neighbor 20.20.20.1 remote-as 10
  neighbor 20.20.20.1 send-community
  neighbor 20.20.20.1 route-map precedence-map out
  !
ip bgp-community new-format
!
! Match community 1 and set the IP Precedence to priority
route-map precedence-map permit 10
  match community 1
  set ip precedence priority
!
! Match community 2 and set the IP Precedence to immediate
route-map precedence-map permit 20
  match community 2
  set ip precedence immediate
!
! Match community 3 and set the IP Precedence to flash
route-map precedence-map permit 30
  match community 3
  set ip precedence flash
!
! Match community 4 and set the IP Precedence to flash-override
route-map precedence-map permit 40
  match community 4
  set ip precedence flash-override
!
! Match community 5 and set the IP Precedence to critical
route-map precedence-map permit 50
  match community 5
  set ip precedence critical
!
! Match community 6 and set the IP Precedence to internet
route-map precedence-map permit 60
  match community 6
  set ip precedence internet
!
! Match community 7 and set the IP Precedence to network
route-map precedence-map permit 70
  match community 7
  set ip precedence network
!
! Match ip address access list 69 or match AS path 1
! and set the IP Precedence to critical
route-map precedence-map permit 75
  match ip address 69
  match as-path 1
  set ip precedence critical
!
! For everything else, set the IP Precedence to routine
route-map precedence-map permit 80
  set ip precedence routine
!
! Define the community lists
ip community-list 1 permit 60:1
```

```
ip community-list 2 permit 60:2
ip community-list 3 permit 60:3
ip community-list 4 permit 60:4
ip community-list 5 permit 60:5
ip community-list 6 permit 60:6
ip community-list 7 permit 60:7
!
! Define the AS path
ip as-path access-list 1 permit ^10_60
!
! Define the access list
access-list 69 permit 69.0.0.0
```

Router B's Configuration

```
router bgp 10
 neighbor 30.30.30.1 remote-as 30
 neighbor 30.30.30.1 send-community
 neighbor 30.30.30.1 route-map send_community out
!
ip bgp-community new-format
!
! Match prefix 10 and set community to 60:1
route-map send_community permit 10
 match ip address 10
 set community 60:1
!
! Match prefix 20 and set community to 60:2
route-map send_community permit 20
 match ip address 20
 set community 60:2
!
! Match prefix 30 and set community to 60:3
route-map send_community permit 30
 match ip address 30
 set community 60:3
!
! Match prefix 40 and set community to 60:4
route-map send_community permit 40
 match ip address 40
 set community 60:4
!
! Match prefix 50 and set community to 60:5
route-map send_community permit 50
 match ip address 50
 set community 60:5
!
! Match prefix 60 and set community to 60:6
route-map send_community permit 60
 match ip address 60
 set community 60:6
!
! Match prefix 70 and set community to 60:7
route-map send_community permit 70
 match ip address 70
 set community 60:7
!
! For all others, set community to 60:8
route-map send_community permit 80
 set community 60:8
!
! Define the access lists
access-list 10 permit 61.0.0.0
access-list 20 permit 62.0.0.0
```

```
access-list 30 permit 63.0.0.0
access-list 40 permit 64.0.0.0
access-list 50 permit 65.0.0.0
access-list 60 permit 66.0.0.0
access-list 70 permit 67.0.0.0
```

