Implementing Enhanced Policy Based Routing

This section explains the procedures for configuring Enhanced Policy Based Routing (ePBR) with ACLs, MPLS-TE, and BGP Flow spec.

Configuring ACLs with Enhanced Policy Based Routing

Enhanced Policy based routing (ePBR) is used to direct packets that arrive at an interface to a specified next-hop. ePBR is very useful in managing a large number of configured access lists more efficiently.

In ePBR, the router drops the traffic packets if the next hop configured in the PBR policy is not reachable. To avoid packet loss in such scenarios, you must configure multiple next hops for each access control entry.

Restrictions

- PBR is not supported on Pseudowire Headend (PHWE) subinterfaces.
- On Cisco ASR 9000 Series 3rd Generation Line Cards, compressed Access Control Lists (ACLs) are not supported when combined with Policy Based Routing (PBR). However, ACLs without compression can be used with PBR.

Configuration

Use the following sample configuration to configure ACLs with ePBR.

```
/* Configure an access list */
Router(config)# ipv4 access-list INBOUND-ACL
Router(config-ipv4-acl)# 10 permit ipv4 any host 1.1.1.10
Router(config-ipv4-acl)# 20 permit ipv4 any host 1.2.3.4
Router(config-ipv4-acl)# commit
Mon Nov  6 17:22:42.529 IST
Router(config-ipv4-acl)# exit

/* Configure a class map for the access list */
```

```
Router(config)# class-map type traffic match-any INBOUND-CLASS
Router(config-cmap)# match access-group ipv4 INBOUND-ACL
Router(config-cmap)# end-class-map
Router(config)# commit
Mon Nov  6 17:29:12.026 IST

/* Configure an ePBR policy map with the class map */
Router(config)# policy-map type pbr INBOUND-POLICY
Router(config-pmap)# class type traffic INBOUND-CLASS
Router(config-pmap-c)# redirect nexthop 192.168.10.1
Router(config-pmap-c)# exit
Router(config-pmap)# class type traffic class-default
Router(config-pmap-c)# transmit
Router(config-pmap-c)# commit
Mon Nov  6 17:25:33.858 IST
Router(config-pmap)# end-policy-map

/* Configure a GigE interface and apply the ePBR policy map to the interface */
Router(config)# interface GigabitEthernet 0/0/0/0
Router(config-if)# ipv4 address 10.10.10.1 255.255.255.0
Router(config-if)# service-policy type pbr input INBOUND-POLICY
Router(config-if)# commit
Mon Nov  6 17:31:23.645 IST
Router(config-if)# exit
```

Running Configuration

Validate the configuration by using the **show run** command.

```
Router(config)# show running-config
Mon Nov  6 17:31:59.015 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Mon Nov  6 17:31:23 2017 by UNKNOWN
!
ipv4 access-list INBOUND-ACL
 10 permit ipv4 any host 1.1.1.10
 20 permit ipv4 any host 1.2.3.4
!
!
class-map type traffic match-any INBOUND-CLASS
 match access-group ipv4 INBOUND-ACL
 end-class-map
!
!
policy-map type pbr INBOUND-POLICY
 class type traffic INBOUND-CLASS
  redirect ipv4 nexthop 192.168.10.1
 !
 class type traffic class-default
  transmit
 !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 service-policy type pbr input INBOUND-POLICY
 ipv4 address 10.10.10.1 255.255.255.0
!
```

Using ePBR for MPLS Packets on Subscriber Interfaces

The enhanced policy based routing (ePBR) match/redirect MPLS packets on subscriber interfaces feature enables the capability to match MPLS labeled packets and redirect those to an external server by re-writing the source and destination IP addresses of the packets. This feature is applicable when the DNS server (an external server) is hidden in the MPLS cloud.

The traffic that is entering the MPLS cloud will be matched for a specific destination address and based on it, the new destination will be set. When the packet returns from the DNS server, the source address is changed back to the original source address.

Use Case: Using ePBR for MPLS Packets on Subscriber Interfaces

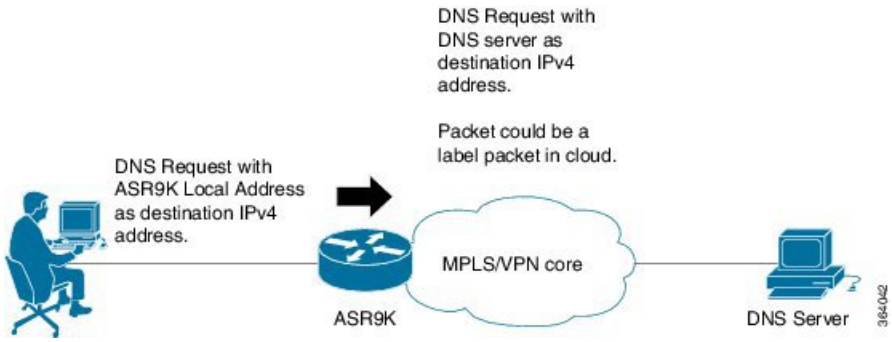
The ePBR match/redirect MPLS packets on subscriber Interfaces feature is applicable when a packet arrives at an interface with a destination address of a known server. This feature changes the known destination address to a required address that is hidden in the DNS cloud. For example, when the packet reaches a known interface with a specific IP address, say 10.0.0.1, it can to be redirected to a new IP address, say 172.16.0.1 , that is hidden in the cloud.

For subscriber to core DNS packets, the sequence for match and redirect is:

- Match the incoming packet for the known DNS server. This address could be a local address on the Cisco ASR 9000 Series Router, which the subscriber uses as DNS server address.
- Set the destination address to a new IP address to which the packet has to be redirected.

This figure explains the match and redirect sequence for subscriber to core DNS packets.

Figure 1: Subscriber to core DNS packets

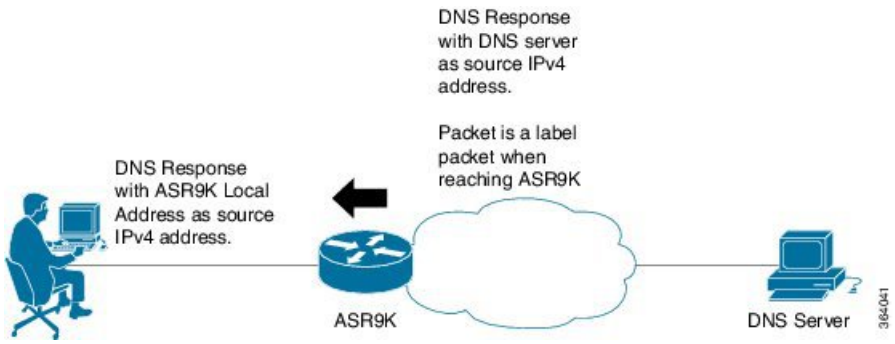


For core to subscriber DNS packets, the sequence for match and redirect is :

- Match the incoming labeled DNS packet's source IP address from the core.
- Set the source address to a local address, which the subscriber uses as DNS server address. The packet would be forwarded based on label + destination IP address, which is the subscriber address.

This figure explains the match and redirect sequence for core to subscriber DNS packets.

Figure 2: Core to subscriber DNS packets



Configuring ePBR-Based MPLS Redirection

These examples show how to configure ePBR-based MPLS match/redirect configuration.

Match configuration for IPv4 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_src_test
  set source-address ipv4 17.17.18.18
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_mpls_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_src_test
match mpls disposition access-group ipv4 ACL_MPLS_SRC
 end-class-map
!

show running-config ipv4 access-list ACL_MPLS_SRC
Wed Sep  3 02:53:40.918 UTC
ipv4 access-list ACL_MPLS_SRC
10 permit ipv4 30.1.1.1/24 112.112.0.1/24
!
```

Match configuration for IPv6 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_ipv6_src_test
  set source-address ipv4 10.10.10.10
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config class-map type traffic class_mpls_ipv6_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_ipv6_src_test
match mpls disposition access-group ipv6 ACL_MPLS_IPV6__SRC
 end-class-map
!
```

```
show running-config ipv6 access-list ACL_MPLS_IPV6_SRC
Wed Sep  3 02:53:40.918 UTC
Ipv6 access-list ACL_MPLS_IPV6_SRC
10 permit ipv6 any any
!
```

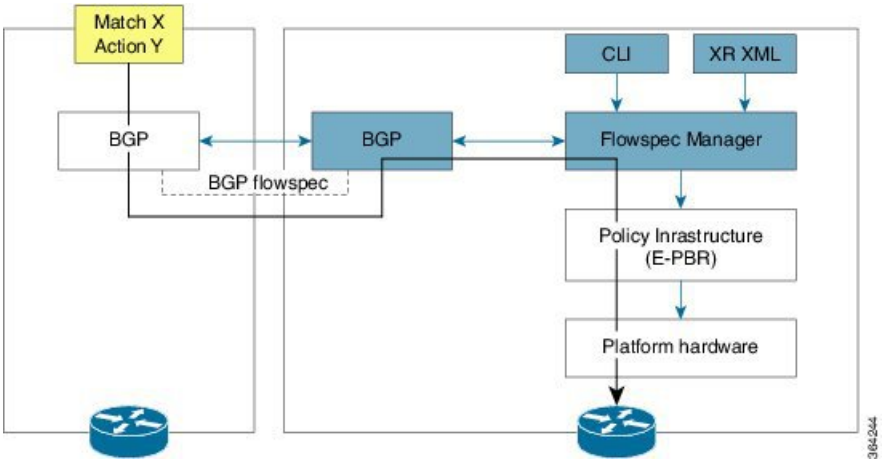
Set destination configuration:

```
show running-config policy-map type pbr pbr_prec_exp
Wed Sep  3 03:11:16.000 UTC
policy-map type pbr pbr_prec_exp
class type traffic class_prec_exp
  set destination-address ipv4 192.168.0.1
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_prec_e$
Wed Sep  3 03:11:30.339 UTC
class-map type traffic match-all class_prec_exp
match mpls experimental topmost 2
 match mpls disposition access-group ipv4 acl2
 end-class-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config ipv4 access-list acl2
Wed Sep  3 03:11:47.963 UTC
ipv4 access-list acl2
5 permit ipv4 host 10.10.10.10 any
10 permit ipv4 any any
!
```

BGP Flowspec Client-Server (Controller) Model and Configuration with ePBR

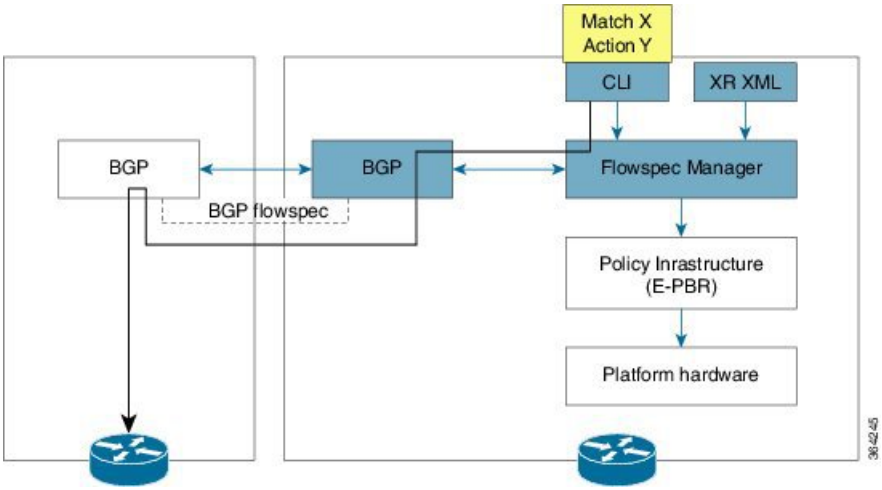
The BGP Flowspec model comprises of a Client and a Server (Controller). The Controller is responsible for sending or injecting the flowspec NRLI entry. The client (acting as a BGP speaker) receives that NRLI and programs the hardware forwarding to act on the instruction from the Controller. An illustration of this model is provided below.

BGP Flowspec Client



Here, the Controller on the left-hand side injects the flowspec NRLI, and the client on the right-hand side receives the information, sends it to the flowspec manager, configures the ePBR (Enhanced Policy-based Routing) infrastructure, which in turn programs the hardware from the underlaying platform in use.

BGP Flowspec Controller



The Controller is configured using CLI to provide that entry for NRLI injection.

BGP Flowspec Configuration

- **BGP-side**: You must enable the new address family for advertisement. This procedure is applicable for both the Client and the Controller. Enable BGP Flowspec, on page 7 explains the procedure.

  Client-side: No specific configuration, except availability of a flowspec-enabled peer.

- **Controller-side**: This includes the policy-map definition and the association to the ePBR configuration consists of two procedures: the class definition, and using that class in ePBR to define the action. The following topics explain the procedure:

  - Configure a Policy Map, on page 10
  - Configure a Class Map, on page 8
  - Link BGP Flowspec to ePBR Policies , on page 12

Configuring BGP Flowspec with ePBR

The following sections explain the procedures for configuring BGP flowspec with ePBR.

Use the following procedures to enable and configure the BGP flowspec feature:

- Enable BGP Flowspec, on page 7
- Configure a Class Map, on page 8
- Link BGP Flowspec to ePBR Policies , on page 12

Note To save configuration changes, you must commit changes when the system prompts you.

Enable BGP Flowspec

You must enable the address family for propagating the BGP flowspec policy on both the Client and Server using the following steps:

SUMMARY STEPS

1. **configure**
2. **router bgp** *as-number*
3. **address-family** { **ipv4** | **ipv6** | **vpnv4** | **vpnv6** } **flowspec**
4. **exit**
5. **neighbor** *ip-address*
6. **remote-as** *as-number*
7. **address-family** { **ipv4** | **ipv6** } **flowspec**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router bgp** *as-number* **Example:** `RP/0/RSP0/CPU0:router(config)# router bgp 100`	Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.
Step 3	**address-family** { **ipv4**	**ipv6**	**vpnv4**	**vpnv6** } **flowspec** **Example:** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 flowspec`	Specifies either the IPv4, IPv6, vpn4 or vpn6 address family and enters address family configuration submode, and initializes the global address family for flowspec policy mapping.

	Command or Action	Purpose
Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-bgp-af)# exit`	Returns the router to BGP configuration mode.
Step 5	**neighbor** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-bgp)#neighbor 1.1.1.1`	Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.
Step 6	**remote-as** *as-number* **Example:** `RP/0/RSP0/CPU0:router(config-bgp-nbr)#remote-as 100`	Assigns a remote autonomous system number to the neighbor.
Step 7	**address-family** { **ipv4** | **ipv6** } **flowspec** **Example:** `RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 flowspec`	Specifies an address family and enters address family configuration submode, and initializes the global address family for flowspec policy mapping.

Configuring an address family for flowspec policy mapping: Example

```
router bgp 100
 address-family ipv4 flowspec
 ! Initializes the global address family
 address-family ipv6 flowspec
 !
 neighbor 1.1.1.1
  remote-as 100
  address-family ipv4 flowspec
  ! Ties it to a neighbor configuration
  address-family ipv6 flowspec
  !
```

Configure a Class Map

In order to associate the ePBR configuration to BGP flowspec you must perform these sub-steps: define the class and use that class in ePBR to define the action. The steps to define the class include:

SUMMARY STEPS

1. **configure**
2. **class-map [type traffic] [match-all]** *class-map-name*
3. **match** *match-statement*
4. **end-class-map**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**class-map [type traffic] [match-all]** *class-map-name* **Example:** `RP/0/RSP0/CPU0:router(config)# class-map type traffic match all classc1`	Creates a class map to be used for matching packets to the class whose name you specify and enters the class map configuration mode. If you specify **match-any** , one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default. If you specify **match-all** , the traffic must match all the match criteria.
Step 3	**match** *match-statement* **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# match protocol ipv4 1 60`	Configures the match criteria for a class map on the basis of the statement specified. Any combination of tuples 1-13 match statements can be specified here. The tuple definition possibilities include: • Type 1: **match destination-address** {**ipv4** | **ipv6**} *address/mask length* • Type 2: **match source-address** {**ipv4** | **ipv6**} *address/mask length* • Type 3: **match protocol** {*protocol-value* | *min-value* *−max-value*} **Note** In case of IPv6, it will map to last next-header. • Type 4: Create two class-maps: one with source-port and another with destination-port: • **match source-port** {*source-port-value* | *min-value* *−max-value*} **Note** Only up to 5 port numbers are supported in a single match string. • **match destination-port** {*destination-port-value* | *min-value* *−max-value*} **Note** These are applicable only for TCP and UDP protocols.

	Command or Action	Purpose
		• Type 5: **match destination-port** {*destination-port-value* | [*min-value* – *max-value*]} • Type 6: **match source-port** {*source-port-value* | [*min-value* – *max-value*]} • Type 7: **match** {**ipv4** | **ipv6**} **icmp-code** {*value* | *min-value* –*max-value*} • Type 8: **match** {**ipv4** | **ipv6**} **icmp-type** {*value* | *min-value* –*max-value*} • Type 9: **match tcp-flag** *value* **bit-mask** *mask_value* • Type 10: **matchpacket length** {*packet-length-value* | *min-value* –*max-value*}} • Type 11: **match dscp** {*dscp-value* | *min-value* –*max-value*} • Type 12: **match fragment-type** {**dont-fragment** **is-fragment** **first-fragment** **last-fragment**} • Type 13: **match ipv6 flow-label ipv4 flow-label** {*value* | *min-value* –*max-value*} *BGP Flowspec Commands* in the *Routing Command Reference for Cisco ASR 9000 Series Routers* guide provides additional details on the various commands used for BGP flowspec configuration.
Step 4	**end-class-map** **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# end-class-map`	Ends the class map configuration and returns the router to global configuration mode.

What to do next

Associate the class defined in this procedure to a PBR policy as described in Configure a Policy Map, on page 10.

Configure a Policy Map

This procedure helps you define a policy map and associate it with traffic class you configured previously in Configure a Class Map, on page 8 .

SUMMARY STEPS

1. **configure**
2. **policy-map type pbr** *policy-map*
3. **class** *class-name*
4. **class type traffic** *class-name*
5. *action*
6. **exit**

7. **end-policy-map**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**policy-map type pbr** *policy-map* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type pbr policyp1`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters the policy map configuration mode.
Step 3	**class** *class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class class1`	Specifies the name of the class whose policy you want to create or change.
Step 4	**class type traffic** *class-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic classc1`	Associates a previously configured traffic class with the policy map, and enters control policy-map traffic class configuration mode.
Step 5	*action* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# set dscp 5`	Define extended community actions as per your requirement. The options include: • Traffic rate: **police rate** *rate* • Redirect VRF: **redirect** { **ipv4ipv6** }**extcommunity rt** *route_target_string* • Traffic Marking: **set** { **dscp** *rate* | **destination-address** {**ipv4** | **ipv6**} *8-bit value*} • Redirect IP NH: **redirect** { **ipv4ipv6** } **nexthop** *ipv4 addressipv6 address* { *ipv4 addressipv6 address*}
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# exit`	Returns the router to policy map configuration mode.

	Command or Action	Purpose
Step 7	**end-policy-map** **Example:** `RP/0/RSP0/CPU0:router(config-cmap)# end-policy-map`	Ends the policy map configuration and returns the router to global configuration mode.

What to do next

Perform VRF and flowspec policy mapping for distribution of flowspec rules using the procedure explained in Link BGP Flowspec to ePBR Policies , on page 12

Link BGP Flowspec to ePBR Policies

For BGP flowspec, an ePBR policy is applied on a per VRF basis, and this policy is applied on all the interfaces that are part of the VRF. If you have already configured a ePBR policy on an interface, it will not be overwritten by the BGP flowspec policy. If you remove the policy from an interface, ePBR infrastructure will automatically apply BGP flowspec policy on it, if one was active at the VRF level.

Note At a time only one ePBR policy can be active on an interface.

SUMMARY STEPS

1. **configure**
2. **flowspec**
3. **local-install interface-all**
4. **address-family ipv4**
5. **local-install interface-all**
6. **service-policy type pbr** *policy-name*
7. **exit**
8. **address-family ipv6**
9. **local-install interface-all**
10. **service-policy type pbr** *policy-name*
11. **vrf** *vrf-name*
12. **address-family ipv4**
13. **local-install interface-all**
14. **service-policy type pbr** *policy-name*
15. **exit**
16. **address-family ipv6**
17. **local-install interface-all**
18. **service-policy type pbr** *policy-name*
19. **commit**
20. **exit**
21. **show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**flowspec** **Example:** `RP/0/RSP0/CPU0:router(config)# flowspec`	Enters the flowspec configuration mode.
Step 3	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# address-family ipv4`	Specifies either an IPv4 address family and enters address family configuration submode.
Step 5	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 6	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv4 interface to be used as the service policy for that interface.
Step 7	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# exit`	Returns the router to flowspec configuration mode.
Step 8	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)#`	Specifies an IPv6 address family and enters address family configuration submode.

	Command or Action	Purpose
	`address-family ipv6`	
Step 9	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 10	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv6 interface to be used as the service policy for that interface.
Step 11	**vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec)# vrf vrf1`	Configures a VRF instance and enters VRF flowspec configuration submode.
Step 12	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf)# address-family ipv4`	Specifies an IPv4 address family and enters address family configuration submode.
Step 13	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 14	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv4 interface to be used as the service policy for that interface.
Step 15	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# exit`	Returns the router to VRF flowspec configuration submode.

	Command or Action	Purpose
Step 16	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf)# address-family ipv6`	Specifies either an IPv6 address family and enters address family configuration submode.
Step 17	**local-install interface-all** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# local-install interface-all`	(Optional) Installs the flowspec policy on all interfaces under the subaddress family.
Step 18	**service-policy type pbr** *policy-name* **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# service-policy type pbr policys1`	Attaches a policy map to an IPv6 interface to be used as the service policy for that interface.
Step 19	**commit**	
Step 20	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-flowspec-vrf-af)# exit`	Returns the router to flowspec configuration mode.
Step 21	**show flowspec** { **afi-all** | **client** | **ipv4** | **ipv6** | **summary** | **vrf** **Example:** `RP/0/RSP0/CPU0:routershow flowspec vrf vrf1 ipv4 summary`	(Optional) Displays flowspec policy applied on an interface.

Verify BGP Flowspec

Use these different **show** commands to verify your flowspec configuration. For instance, you can use the associated flowspec and BGP show commands to check whether flowspec rules are present in your table, how many rules are present, the action that has been taken on the traffic based on the flow specifications you have defined and so on.

SUMMARY STEPS

1. **show processes flowspec_mgr location all**
2. **show flowspec summary**

3. **show flowspec vrf** *vrf_name* | **all** { **afli-all** | **ipv4** | **ipv6** }
4. **show bgp ipv4 flowspec**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**show processes flowspec_mgr location all**
	Example:
	`# show processes flowspec_mgr location all`
	`node:  node0_3_CPU0`
	`Job Id: 10`
	`PID: 43643169`
	`Executable path:`
	`/disk0/iosxr-fwding-5.2.CSC33695-015.i/bin/flowspec_mgr`
	`Instance #: 1`
	`Version ID: 00.00.0000`
	`Respawn: ON`
	`Respawn count: 331`
	`Max. spawns per minute: 12`
	`Last started: Wed Apr  9 10:42:13 2014`
	`Started on config: cfg/gl/flowspec/`
	`Process group: central-services core: MAINMEM`
	`startup_path: /pkg/startup/flowspec_mgr.startup`
	`Ready: 1.113s`
	`Process cpu time: 0.225 user, 0.023 kernel, 0.248 total`
	`JID  TID CPU Stack pri state  TimeInState HR:MM:SS:MSEC  NAME`
	`1082  1  0  112K  10 Receive  2:50:23:0508 0:00:00:0241 flowspec_mgr`
	`1082  2  1  112K  10 Sigwaitinfo 2:52:42:0583 0:00:00:0000 flowspec_mgr`
		Specifies whether the flowspec process is running on your system or not. The flowspec manager is responsible for creating, distributing and installing the flowspec rules on the hardware.

Step 2	**show flowspec summary**
	Example:
	`# show flowspec summary`
	`FlowSpec Manager Summary:`
	`  Tables:  2`
	`  Flows:  1`
	`RP/0/3/CPU0:RA01_R4#`
		Provides a summary of the flowspec rules present on the entire node. In this example, the 2 table indicate that IPv4 and IPv6 has been enabled, and a single flow has been defined across the entire table.

Step 3	**show flowspec vrf** *vrf_name*	**all** { **afli-all**	**ipv4**	**ipv6** }
				Example:
				`# show flowspec vrf default ipv4 summary`
				`Flowspec VRF+AFI table summary:`
				`VRF: default`
				`  AFI: IPv4`
				`  Total Flows:  1`
					In order to obtain more granular information on the flowspec, you can filter the show commands based on a particular address-family or by a specific VRF name. In this example, 'vrf default' indicates that the flowspec has been defined on the default table. The 'IPv4 summary' shows the IPv4 flowspec rules present on that default table. As there are no IPv6s configured, the value shows 'zero' for ipv6 summary 'Table Flows' and 'Policies' parameters. 'VRF all' displays information across all the VRFs configured on

	Command or Action	Purpose
	Total Service Policies: 1 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf default ipv6 summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 RP/0/3/CPU0:RA01_R4# --- # show flowspec vrf all afi-all summary Flowspec VRF+AFI table summary: VRF: default AFI: IPv4 Total Flows: 1 Total Service Policies: 1 VRF: default AFI: IPv6 Total Flows: 0 Total Service Policies: 0 --- # show flowspec vrf default ipv4 Dest:110.1.1.0/24, Source:10.1.1.0/24,DPort:>=120&<=130, SPort:>=25&<=30,DSCP:=30 detail AFI: IPv4 Flow :Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30 Actions :Traffic-rate: 0 bps (bgp.1) Statistics (packets/bytes) Matched : 0/0 Transmitted : 0/0 Dropped : 0/0	the table and afli-all displays information for all address families (IPv4 and IPv6). The **detail** option displays the 'Matched', 'Transmitted, ' and 'Dropped' fields. These can be used to see if the flowspec rule you have defined is in action or not. If there is any traffic that takes this match condition, it indicates if any action has been taken (that is, how many packets were matched and whether these packets have been transmitted or dropped.
Step 4	**show bgp ipv4 flowspec** **Example:** # show bgp ipv4 flowspec Dest:110.1.1.0/24,Source:10.1.1.0/24, DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 BGP routing table entry for Dest:110.1.1.0/24, Source:10.1.1.0/24,Proto:=47,DPort:>=120&<=130,SPort:>=25&<=30,DSCP:=30/208 <snip> Paths: (1 available, best #1) Advertised to update-groups (with more than one peer): 0.3 Path #1: Received by speaker 0 Advertised to update-groups (with more than one peer): 0.3 Local 0.0.0.0 from 0.0.0.0 (3.3.3.3) Origin IGP, localpref 100, valid, redistributed, best, group-best Received Path ID 0, Local Path ID 1, version 42	Use this command to verify if a flowspec rule configured on the controller router is available on the BGP side. In this example, 'redistributed' indicates that the flowspec rule is not internally originated, but one that has been redistributed from the flowspec process to BGP. The extended community (BGP attribute used to send the match and action criteria to the peer routers) you have configured is also displayed here. In this example, the action defined is to rate limit the traffic.

	Command or Action	Purpose
	`Extended community: FLOWSPEC Traffic-rate:100,0`	

Supported Match and Set Operations—ABF, ePBR/Flowspec, and PBR

The following table illustrates the match/set criteria that is supported by ABF, ePBR/Flowspec, and PBR:

Table 1: Supported Match and Set Operations

match/set criteria	ABF	ePBR/Flowspec	PBR
source ip	match	match	match
destination ip	match	match	match
source protocol/port	match	match	match
destination protocol/port	match	match	match
nexthop ip	set	set	set
nexthop vrf	set	set	set
nexthop ip+vrf	set	NA	set
dscp	NA	match/set	NA
forward-class	NA	NA	set
police	NA	set	NA
access-group	NA	NA	match
flow-tag	NA	NA	match
fragment-type	NA	match	NA
packet length	NA	match	NA
ip protocol	match	match	match
tcp-flag	match	match	match
ipv4/ipv6 icmp-type	NA	match	NA
ipv4/ipv6 icmp-code	NA	match	NA
port	NA	match	NA
port-range	match	match	match

Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

Related Topic	Document Title
the Cisco ASR 9000 Series Router Transport Stack commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Transport Stack Commands in the IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*MPLS Label Distribution Protocol Commands in the MPLS Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router OSPF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*OSPF Commands in the Routing Command Reference for Cisco ASR 9000 Series Routers*
MPLS Label Distribution Protocol feature information	*Implementing MPLS Label Distribution Protocol in the MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
OSPF feature information	*Implementing OSPF in the Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

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