



CHAPTER 4

Configuring Traffic Diversion

This chapter describes how to configure traffic diversion with the Cisco Guard (Guard).

Traffic diversion configuration is topology independent. The configuration procedures for Layer 2 and Layer 3 topologies are identical.

To save all configuration changes to the Guard memory, use the **write memory** command in router configuration mode.



Note

Information provided in this document regarding Cisco router configuration is for informational purposes only. Refer to the appropriate user guides for detailed information.

This chapter contains the following sections:

- [Understanding the BGP Diversion Method](#)
- [Understanding Traffic Forwarding Methods](#)
- [Long Diversion Method](#)

Understanding the BGP Diversion Method

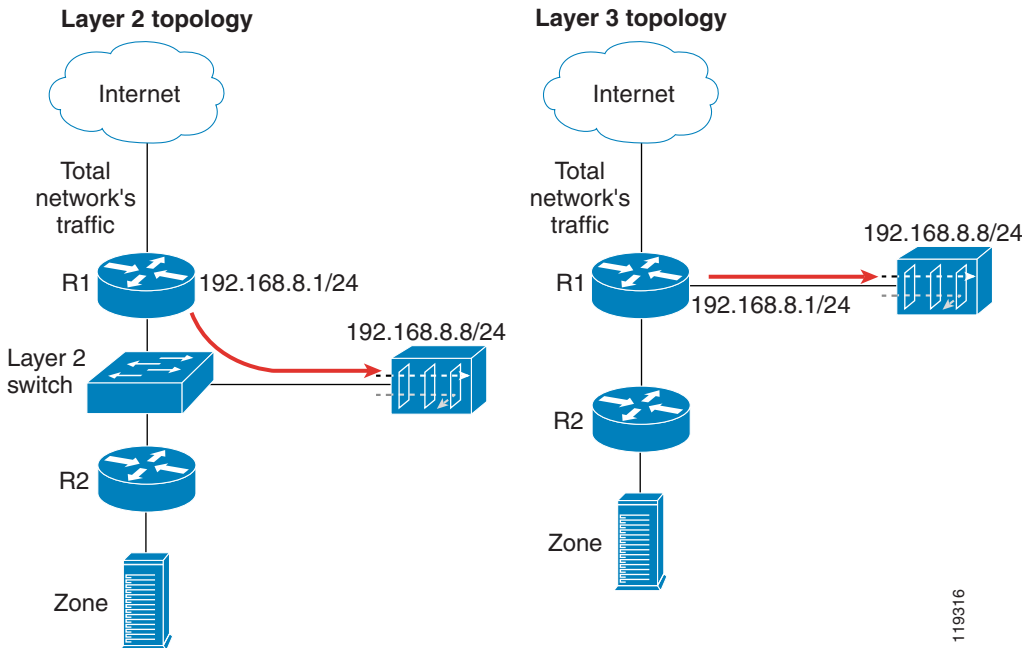
Following standard Border Gateway Protocol (BGP) routing definitions, routers select the routing path with the longest matching prefix (also known as the “most specific”). After establishing a BGP session with the router, the Guard sends a routing update where the Guard is listed as the best path for the protected zone. The network prefix that the Guard announces is longer than the one already listed in the router’s routing table, overriding the router's routing table definition. The prefix subnet is configured per zone subnet IP address. BGP is configured similarly in all networks.

To configure traffic diversion in Layer 2 and Layer 3 network topologies, perform the following:

1. Configure traffic diversion using BGP (see the “[Guard BGP Configuration](#)” section for more information).
2. Configure the appropriate traffic forwarding method (the “[Understanding Traffic Forwarding Methods](#)” section for more information).

[Figure 4-1](#) provides examples of Layer 2 and Layer 3 network topologies. In both network topologies, the Guard diverts the traffic from router R1.

Figure 4-1 BGP Configuration



After BGP diversion is established, the router's routing tables points to the Guard as the best route to the zone and the router forwards all traffic destined to the zone's IP address to the Guard.

This section contains the following topics:

- [BGP Configuration Guidelines](#)
- [Guard BGP Configuration](#)
- [Cisco Router BGP Configuration](#)

BGP Configuration Guidelines

This section provides general guidelines for BGP configuration on the Guard and on a divert-from router.



Note

The guidelines provided in this section apply to the BGP configuration on any router from which the Guard diverts the traffic. The sample BGP configurations in the following sections is presented using the syntax of the Cisco IOS software.



Note

The following examples are provided using common External Border Gateway Protocol (eBGP). You should consider the network configuration and determine whether eBGP or Internal Border Gateway Protocol (iBGP) should be implemented in your network.

Follow these guidelines when the Guard and adjacent routers operate using common eBGP:

1. Configure the Guard with an easily recognizable Autonomous System (AS) number.

The Guard sends routing information only when it diverts traffic. This route appears in the router's routing tables. Using a recognizable value allows you to easily identify the Guard in the router's routing tables.

2. To ensure that the Guard's routing information is not redistributed to other internal and external BGP neighboring devices, perform the following:
 - Configure the Guard to not send routing information and to drop incoming BGP routing information.
 - Set the Guard BGP community attribute values to **no-export** and **no-advertise**.

A match in the community attributes enables the Guard to filter BGP announcements on the router and enforce this policy.

3. Enter the **soft-reconfiguration inbound** command during the setup procedures. This command is useful for troubleshooting and allows you to restore a routing table without reconnecting to the neighboring device.

See the “[BGP Diverting Method](#)” section on page A-5 for more information about BGP.

Guard BGP Configuration

You can configure BGP on the Guard using the Zebra application (see <http://www.zebra.org> for more information about the Zebra application).

**Note**

We recommend that you configure a zone's diversion when the zone is in standby mode.

To enter diversion configuration on the Guard, perform the following steps:

Step 1

From the Configuration command group level, enter the following command:

```
admin@GUARD-conf# router
```

The following prompt appears, indicating that the system has entered the Zebra application in nonprivileged mode:

```
router>
```

**Tip**

At each command level of the Zebra application, press the question mark (?) key to display the list of commands available at this mode.

Step 2

Switch to the privileged mode by entering the following command:

```
router> enable
```

The following prompt appears, indicating that the system has entered the Zebra application privileged mode:

```
router#
```

**Note**

To quit the Zebra application, enter the **exit** command from the router command level. To exit from the current command group level to a higher group level, enter the **exit** command.

Step 3 Switch to terminal configuration mode by entering the following command:

```
router# config terminal
```

The following prompt appears, indicating that the system has entered the Zebra application configuration mode:

```
router(config)#
```

Step 4 Configure routing on the Guard using the commands shown in the following example. These commands observe the following conventions:

- Items in bold represent commands.
- Items in bold italic represent names. You may replace these names.
- Items in italics enclosed in angle brackets (< >) represent values that you must supply. Replace the terms in italics with the Guard and router (a divert-from router) values indicated. Do not include the angle brackets.



Note

You can use the prefix-list, route-map, or distribute-list method for filtering outgoing routing information about a router. The following example describes the distribute-list method. You can use the prefix-list or route-map filtering method types as long as the routing information is not sent to the Guard.

The following commands must be entered on the Guard:

```
router(config)# router bgp <Guard-AS-number>
router(config-router)# bgp router-id <Guard-IP-address>
router(config-router)# redistribute guard
router(config-router)# neighbor <Router-IP-address> remote-as <Router-AS-number>
router(config-router)# neighbor <Router-IP-address> description <description>
router(config-router)# neighbor <Router-IP-address> soft-reconfiguration inbound
router(config-router)# neighbor <Router-IP-address> distribute-list nothing-in in
router(config-router)# neighbor <Router-IP-address> route-map Guard-out out
router(config-router)# exit
router(config)# access-list nothing-in deny any
router(config)# route-map Guard-out permit 10
router(config-route-map)# set community no-export no-advertise
```

This section contains the following topics:

- [Guard BGP Configuration Example](#)
- [Displaying the Guard Router Configuration File](#)

Guard BGP Configuration Example

To display the Guard router configuration, enter the **show running-config** command from the router command level. In the following example, the router's AS number is 100, and the Guard's AS number is 64555.

The following partial sample output is displayed:

```
router# show running-config
... ..
router bgp 64555
  bgp router-id 192.168.8.8
  redistribute guard
  neighbor 192.168.8.1 remote-as 100
```

```

neighbor 192.168.8.1 description divert-from router
neighbor 192.168.8.1 soft-reconfiguration inbound
neighbor 192.168.8.1 distribute-list nothing-in in
neighbor 192.168.8.1 route-map Guard-out out
!
access-list nothing-in deny any
!
route-map Guard-out permit 10
set community 100:64555 no-export no-advertise
... ..

```

Displaying the Guard Router Configuration File

You can display the Guard router configuration file by entering the following command from the Global command group level:

```
show running-config router
```

The information that displays is the same information that displays when you enter the **show running-config** command from the router command level (see the “[Guard BGP Configuration Example](#)” section).

Cisco Router BGP Configuration

This section describes the router BGP configuration used when you configure a traffic diversion. The syntax in the commands is taken from the BGP configuration on a Cisco router.

These commands observe the following conventions:

- Items in bold represent commands.
- Items in bold italic represent names. You may replace these names.
- Items in italics enclosed in angle brackets (< >) represent values that you must supply. Replace the terms in italics with the Guard and router (a divert-from router) values indicated. Do not include the angle brackets.

The following configuration example shows the commands to use to configure BGP on a Cisco router:

```

R7200(config)# router bgp <Router-AS>
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor <Guard-IP-address> remote-as GuardAS
R7200(config-router)# neighbor <Guard-IP-address> description <description>
R7200(config-router)# neighbor <Guard-IP-address> soft-reconfiguration inbound
R7200(config-router)# neighbor <Guard-IP-address> distribute-list routesToGuard out
R7200(config-router)# neighbor <Guard-IP-address> route-map Guard-in in
R7200(config-router)# no synchronization
R7200(config-router)# exit
R7200(config)# ip bgp-community new-format
R7200(config)# ip community-list expanded <Guard-community-name> permit no-export no-advertise
R7200(config)# route-map Guard-in permit 10
R7200(config-route-map)# match community <Guard-community-name> exact match
R7200(config-route-map)# exit
R7200(config)# ip access-list standard routestoGuard
R7200(config-std-nacl)# deny any

```

The **no synchronization** command prevents the distribution of the Guard BGP routing updates into Interior Gateway Protocol (IGP).

Cisco Router BGP Configuration Example

To display the router configuration, enter the **show running-config** command from the router global command level. In the following example, the router's AS number is 100, and the Guard's AS number is 64555.

The following partial sample output is displayed:

```
R7200# show running-config
... ..
router bgp 100
  bgp log-neighbor-changes
  neighbor 192.168.8.8 remote-as 64555
  neighbor 192.168.8.8 description Guard
  neighbor 192.168.8.8 soft-reconfiguration inbound
  neighbor 192.168.8.8 distribute-list routesToGuard out
  neighbor 192.168.8.8 route-map Guard-in in
  no synchronization
  !
  ip bgp-community new-format
  ip community-list expanded Guard permit 100:64555 no-export no-advertise
  !
  route-map Guard-in permit 10
  match community Guard exact match
  ip access-list standard routesToGuard
  deny any
  ... ..
```

Understanding Traffic Forwarding Methods

This section provides details on traffic forwarding methods. Traffic forwarding methods are used to forward the cleaned traffic from the Guard to the next-hop router. See the [“Understanding the Traffic Forwarding Methods” section on page A-6](#) for more information.

The following terminology is used in this section:

- Divert-from router—Router from which the Guard diverts the destination zone traffic.
- Inject-to router—Router to which the Guard forwards the clean destination zone traffic.
- Next-hop router—Router that is the next hop to the zone according to the routing table on the divert-from router before the Guard activated traffic diversion.

This section contains the following topics:

- [Layer-2 Forwarding Method](#)
- [Policy-Based Routing Destination Forwarding Method](#)
- [VPN Routing Forwarding Destination Forwarding Method](#)
- [Policy-Based Routing VLAN Forwarding Method](#)
- [VPN Routing Forwarding VLAN Forwarding Method](#)
- [Tunnel Diversion Forwarding Method](#)

Layer-2 Forwarding Method

The Layer-2 Forwarding (L2F) method is used in a Layer 2 topology when all three devices—the Cisco Guard, the divert-from router, and the next-hop router—are located in one shared IP network (Figure 4-2).

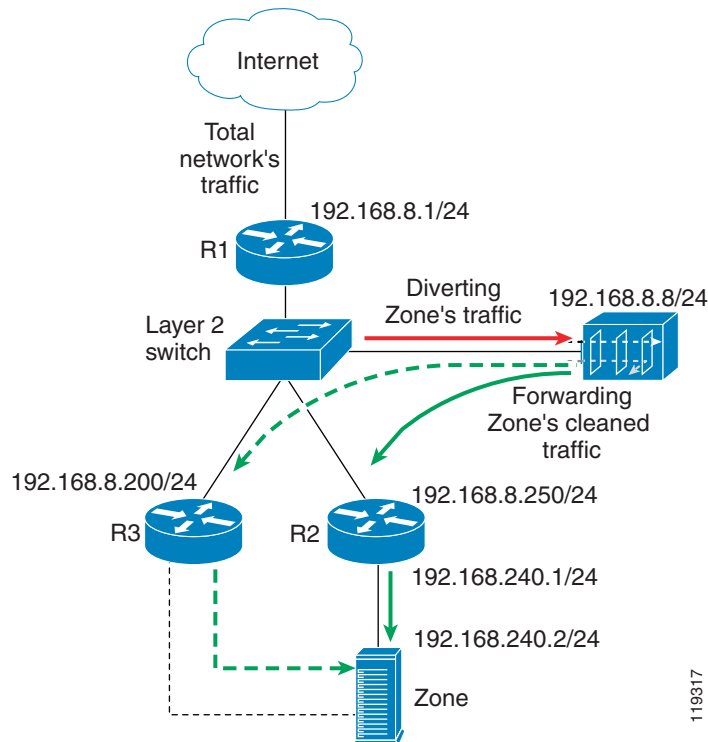
In a Layer 2 topology, a divert-from router and an inject-to router are two separate devices. The next-hop router and the inject-to router are the same device.

The Guard issues an ARP query to resolve the MAC address of the inject-to/next-hop router and then forwards the traffic. For this reason, no configuration on the routers is required when using the L2F method.

The zone may be connected as follows:

- Directly to a Layer 2 switch. In this case, connect the zone to the same IP subnet as the Guard and configure the zone's IP address as the inject-to router. The Guard forwards the traffic directly to the zone.
- Using an IP forwarding router. In this case, you must define the IP forwarding router as the Guard's next-hop router.

Figure 4-2 Layer-2 Forwarding Method



This section contains the following topics:

- [Guard L2F Configuration](#)
- [Router L2F Configuration](#)

Guard L2F Configuration

This section describes the Guard L2F configurations and contains the following topics:

- [Interface Statements](#)
- [BGP Statements](#)
- [Injection Configuration](#)

Interface Statements

You can configure the Guard's out-of-band interface as described in the [“Configuring a Physical Interface”](#) section.

The following example shows how to configure out-of-band interface giga1:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the [“Guard BGP Configuration”](#) section.

In the following example, the Guard's AS is 64555. The router's AS is 100 and the IP address is 192.168.8.1:

```
router bgp 64555
 redistribute guard
 neighbor 192.168.8.1 remote-as 100
 neighbor 192.168.8.1 description C7513
 neighbor 192.168.8.1 distribute-list nothing-in in
 neighbor 192.168.8.1 soft-reconfiguration inbound
 neighbor 192.168.8.1 route-map filt-out out
 !
 route-map filt-out permit 10
 set community no-advertise no-export 100:64555
 !
 access-list nothing-in deny any
```

Injection Configuration

You can configure traffic injection from the Guard to the zone by adding a static route to the zone or the next-hop router according to the network topology. You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) through the next-hop router (192.168.8.250):

```
router# configure terminal
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.250
```

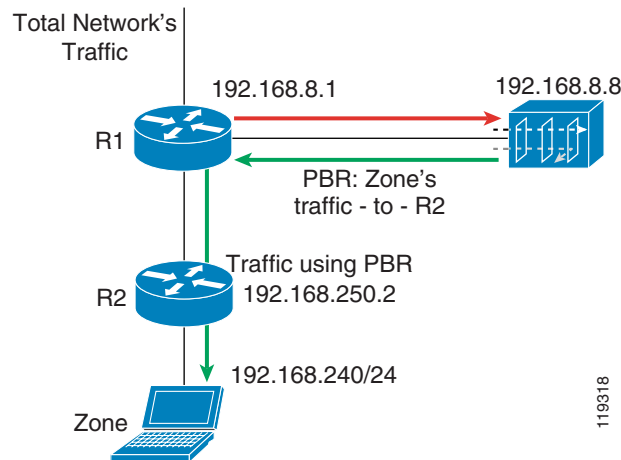
Router L2F Configuration

No configuration is required on the router.

Policy-Based Routing Destination Forwarding Method

Policy-Based Routing (PBR) destination is a static forwarding method that is deployed in Layer 3 network topologies, where the Guard forwards the filtered traffic to the same router from which the traffic was diverted (Figure 4-3).

Figure 4-3 PBR Destination Forwarding Method



To enable the Guard to divert the zone's traffic from the router, the Guard modifies the zone's route in the router's routing table and the Guard is listed as the best path to the zone.

An endless routing loop could occur if the router's routing table is not changed. Because the only entry for the traffic destined to the zone in the router's routing table is the Guard, filtered traffic from the Guard is sent back to the Guard.

To overcome routing loops, you can configure PBR destination on the inject-to router. PBR destination allows you to create rules that override the rules in the router's routing table and avoid endless routing loops. PBR destination enables you to add rules that are applied to the filtered traffic. These rules instruct the router to forward the filtered traffic to the zone, regardless of the routing table entries.

To configure the diversion in this network topology, you can configure the traffic diversion process using BGP (see the [“Guard BGP Configuration”](#) section for more information).

This section contains the following topics:

- [PBR Destination Configuration Guidelines](#)
- [Guard PBR Destination Configuration](#)
- [Cisco Router PBR Destination Configuration Examples](#)

PBR Destination Configuration Guidelines

The guidelines provided in this section apply to PBR destination configurations on any inject-to router.

To configure PBR destination on an inject-to router, follow these guidelines:

1. You must apply PBR destination on the router interface that is connected to the Guard.



Note You can apply PBR destination only to the traffic that comes from the Guard.

2. You must forward the traffic that is selected by PBR destination to the next-hop router. The next-hop router should have the following characteristics:
 - The next-hop router is connected directly to the divert-from router. In Layer 3 topology, the next-hop router and the inject-to router are the same device.
 - The divert-from router is not part of the next-hop router's route to the zone. (A configuration where the divert-from router is part of the next-hop router's route to the zone would result in a routing loop between the divert-from and the next-hop routers.)

PBR destination is applied using the **route-map** command and the **match** and **set** commands to define the conditions for policy routing packets. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. The user must enable PBR destination for the configured route map on a particular interface. All packets arriving on the specified interface that match the match clause are subject to PBR destination.

A PBR destination configuration consists of the following three parts:

- **Sequence**—Specifies the position that a new route map will have in the list of route maps already configured with the same name. Cisco routers process sequence numbers in ascending order.
You can define a separate route-map entry and sequence number for traffic that is to be forwarded to the zone and for all other traffic.
The sequence is configured using the **route-map** command. Using the **route-map** command puts the router into route-map configuration mode.
- **Matching statement**—Specifies the conditions under which policy routing occurs. You should specify the conditions under which an IP address is matched by using the **match** command. A match determines whether the next hop is modified.
- **Forwarding statement**—Specifies the routing actions to perform if the criteria enforced by the **match** commands are met. The **set ip next-hop route-map** configuration command indicates where to send packets that pass a match clause of a route map for policy routing.

Guard PBR Destination Configuration

The configuration in the following example refers to the network in [Figure 4-3](#).

- **BGP Statements**—You can enter the Guard router BGP configuration as described in the “[Guard BGP Configuration](#)” section.
- **Injection Configuration to the Next-Hop Router**—The next-hop router in the example is R2 (see [Figure 4-3](#)). To configure traffic injection from the Guard to the zone, add a static route to the inject-to router. You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24):

```
router# configure terminal
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.1
```

Cisco Router PBR Destination Configuration Examples

The following example shows the router PBR destination configuration used when configuring a diversion.

```
R7200(config)# interface FastEthernet 0/2
R7200(config-if)# description <Interface connected to the Guard>
R7200(config-if)# ip address <Router interface IP address> <Router interface IP mask>
R7200(config-if)# no ip directed-broadcast
```

```

R7200(config-if)# ip policy route-map <Guard-PBR-name>
R7200(config-if)# exit
R7200(config)# ip access-list extended <Zone-name>
R7200(config-ext-nacl)# permit ip any host <Zone IP address>
R7200(config-ext-nacl)# exit
R7200(config)# route-map <Guard-PBR-name> permit 10
R7200(config-route-map)# match ip address <Zone-name>
R7200(config-route-map)# set ip next-hop <next-hop router IP address>
R7200(config-route-map)# exit
R7200(config)# route-map <Guard-PBR-name> permit 100
R7200(config-route-map)# description let thru all other packets without modifying next-hop

```

This example shows a PBR destination traffic forwarding configuration for the sample network in [Figure 4-3](#). To display the router configuration, you enter the **show running-config** command.

The following partial example screen is displayed:

```

R7200# show running-config
... ..
interface FastEthernet0/2
description Interface connected to the Guard
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
 ip policy route-map GuardPbr
!
ip access-list extended zone-A
 permit ip any host 192.168.240.2
!
route-map GuardPbr permit 10
 match ip address zone-A
 set ip next-hop 192.168.250.2
!
route-map GuardPbr permit 100
description let thru all other packets without modifying next-hop

```

VPN Routing Forwarding Destination Forwarding Method

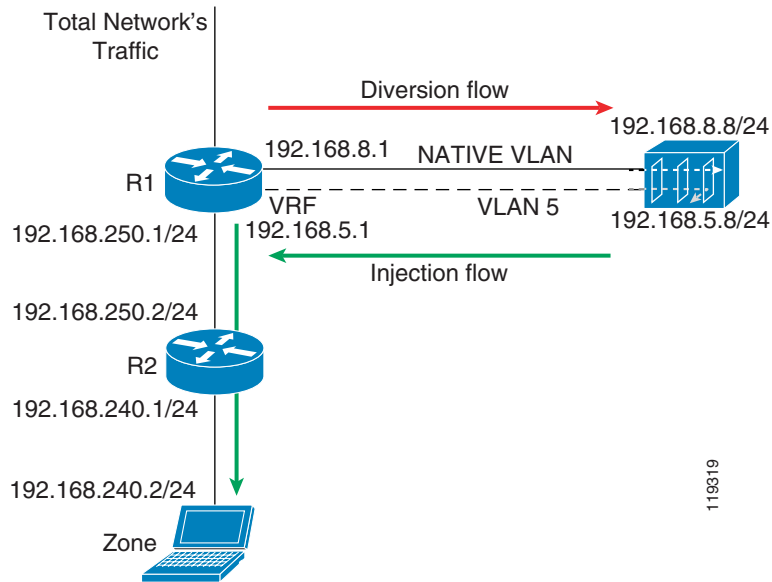
VPN Routing Forwarding Destination (VRF-DST) is a static forwarding method that is deployed in Layer 3 network topologies, where the Guard forwards the filtered traffic to the same router from which the traffic was diverted ([Figure 4-4](#)).

To enable the Guard to divert the zone's traffic from the router, the Guard modifies the zone's route in the router's routing table to make the Guard the best path to the zone.

An endless routing loop could occur if the router's routing table is not changed. Because the only entry for the traffic destined to the zone in the router's routing table is the Guard, the filtered traffic from the Guard is sent back to the Guard.

VRF-DST allows you to create another routing and forwarding table (called the VRF table) in addition to the main routing and forwarding tables. The additional routing table is configured to route traffic that is handled by the router's interface that faces the Guard.

Figure 4-4 VRF DST Forwarding Method



This section contains the following topics:

- [VRF-DST Configuration Guidelines](#)
- [Guard VRF-DST Configuration](#)

VRF-DST Configuration Guidelines

To configure VRF-DST on an inject-to-router, configure two separate interfaces on the router's physical interface facing the Guard as follows:

- **NATIVE VLAN interface**—This interface is used to divert traffic from the router to the Guard. Traffic on this VLAN is forwarded according to the global routing table. The Guard sends BGP announcements to divert the traffic to the Guard on this interface.
- **A Second VLAN interface**—This interface is used to divert the returned traffic from the Guard to the router. You configure a VRF table on this interface. The VRF table contains a static route to forward all zone traffic to a specified next-hop router.



Note

Use the VRF-DST method only when the next-hop router is static for each zone.

Guard VRF-DST Configuration

This section describes the Guard VRF-DST configuration. The configuration in the following examples refers to the network in [Figure 4-4](#).

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN Statements

The following example shows how to configure VLAN 5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the “[Guard BGP Configuration](#)” section.

Injection Configuration

The next-hop router in the example is R2 (see [Figure 4-3](#)). To configure traffic injection from the Guard to the zone, add a static route to the next-hop router.

You should configure the static route at the Guard’s router configuration level.

The following example shows how to configure a static route for the zone’s network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```



Note

VRF is supported from Cisco IOS Release 12.0(17) S/ST.

Creating a VRF Table

The following example shows how to create a VRF table on the inject-to router:

```
R7200(config)# ip vrf Guard-vrf
R7200(config)# rd 100:1
R7200(config)# route-target export 100:1
R7200(config)# route-target import 100:1
```

Interface Native VLAN Statements

The following example shows how to configure the Native VLAN on the divert-from router:

```
R7200(config)# interface fastEthernet1/0.1
R7200(config-if)# encapsulation dot1Q 1 native
R7200(config-if)# description << VLAN TO GUARD-DIVERSION >>
R7200(config-if)# ip address 192.168.8.1 255.255.255.0
R7200(config-if)# no ip directed-broadcast
```

Interface VLAN 5 Statements

The following example shows how to configure the VLAN 5 interface on the inject-to router:

```
R7200(config)# interface fastEthernet 1/0.5
R7200(config-if)# encapsulation dot1Q 5
R7200(config-if)# description << VLAN TO GUARD-INJECTION >>
R7200(config-if)# ip vrf forwarding Guard-vrf
R7200(config-if)# ip address 192.168.5.1 255.255.255.0
```

Interface to Zone Statements

The following example shows how to configure the router interface to the zone:

```
R7200(config)# interface fastEthernet 2/0
R7200(config-if)# description << LINK TO ZONE >>
R7200(config-if)# ip address 192.168.250.1 255.255.255.0
```

BGP Statements

Enter the router, R1, BGP configuration as described in the “Cisco Router BGP Configuration” section.

Static VRF-DST Statements

The following example shows how to configure static VRF on the inject-to router. The static VRF specifies the route to the zone. The parameter **global** indicates that the inject-to router's VRF table receives a copy of next-hop properties (outbound interface, MAC address) from global routing table.

```
R7200(config)# ip route vrf Guard-vrf 192.168.240.2 255.255.255.0 192.168.250.2 global
```

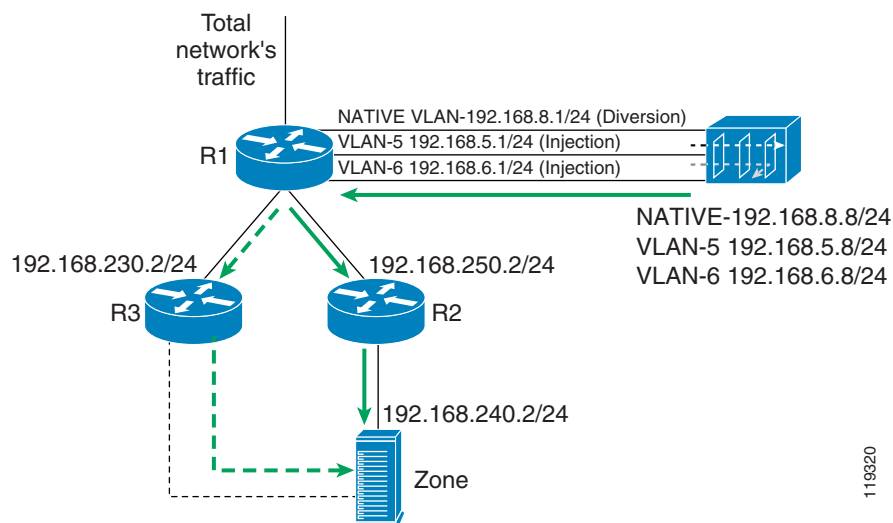
Policy-Based Routing VLAN Forwarding Method

You can use the Policy-Based Routing VLAN (PBR-VLAN) method when there is more than one possible next-hop router (Figure 4-5). You configure multiple VLAN (Virtual LAN, 802.1Q) trunks between the Guard and router R1 (the divert-from and inject-to router). Each VLAN in the trunk is associated with a different next-hop router. In addition, you configure PBR on each VLAN logical interface to forward the traffic on the VLAN to its corresponding next-hop router.

The Guard forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN. This action allows the Guard to change the next-hop router of a zone by changing the VLAN on which the packets are forwarded.

The native VLAN is used for traffic diversion. On this interface, the Guard sends the BGP announcements to the router.

Figure 4-5 PBR-VLAN Forwarding Method



This section contains the following topics:

- [Guard PBR-VLAN Configuration](#)
- [Cisco Router PBR-VLAN Configuration](#)

Guard PBR-VLAN Configuration

This section describes the Guard PBR-VLAN configuration. The following examples refer to the network in [Figure 4-5](#).

PBR-VLAN is applied on R1's interface facing the Guard. Zone traffic on VLAN-5 is forwarded to R2. Zone traffic on VLAN-6 is forwarded to R3.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN-5 Statements

The following example shows how to configure VLAN-5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

Interface VLAN-6 statements

The following example shows how to configure VLAN-6 on the in-band interface:

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.6# ip address 192.168.6.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the [“Guard BGP Configuration”](#) section.

Injection Configuration to R2

To configure traffic injection from the Guard to the zone, add a static route to the next-hop router R2.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

Injection Configuration to R3

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R3.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.6.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco Router PBR-VLAN Configuration

This section describes the Cisco router PBR-VLAN configurations.

Interface Native VLAN Statements

The following example shows how to configure the native VLAN for traffic diversion:

```
interface fastEthernet 1/0
description << NATIVE VLAN TO GUARD-DIVERSION >>
ip address 192.168.8.1 255.255.255.0
no ip directed-broadcast
```

VLAN-5 Creation

The following example shows how to create VLAN-5 on router R1:

```
interface fastEthernet 1/0.1
encapsulation dot1Q 5
description << VLAN-5 TO GUARD-INJECTION >>
ip address 192.168.5.1 255.255.255.0
ip policy route-map next-hop_R2
no ip directed-broadcast
```

VLAN-6 Creation

The following example shows how to create VLAN-6 on router R1:

```
interface fastEthernet 1/0.2
encapsulation dot1Q 6
description << VLAN-6 TO GUARD-INJECTION >>
ip address 192.168.6.1 255.255.255.0
ip policy route-map next-hop_R3
no ip directed-broadcast
```

Next-Hop Interface Configuration

The following example shows how to configure the interfaces to the next-hop routers:

```
interface fastEthernet 2/0
ip address 192.168.250.1 255.255.255.0
Description << LINK TO NEXT-HOP R2 >>
exit
interface fastEthernet 3/0
ip address 192.168.230.1 255.255.255.0
description << LINK TO NEXT-HOP R3 >>
```

BGP Statements

You can enter the router, R1, BGP configuration as described in the [“Cisco Router BGP Configuration”](#) section.

Route-Map Statements (PBR)

The following example shows how to configure PBR for the next-hop routers:

```
route-map next-hop_R2 permit 10
  set ip next-hop 192.168.250.2

route-map next-hop_R3 permit 10
  set ip next-hop 192.168.230.2
```

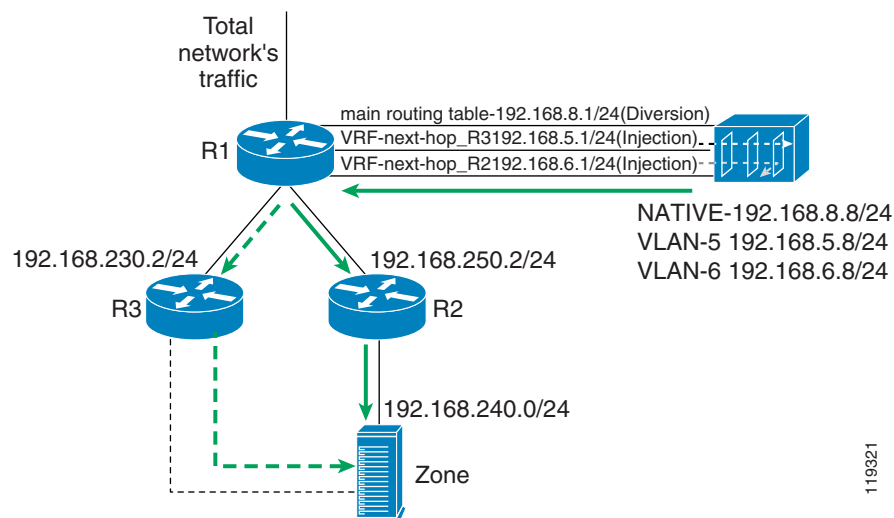
VPN Routing Forwarding VLAN Forwarding Method

The VPN Routing Forwarding VLAN (VRF-VLAN) method is similar to the PBR-VLAN method. A VRF table is associated with each VLAN on the inject-to router rather than a PBR table. Each VRF table directs the traffic on the VLAN to the corresponding next-hop router (Figure 4-6).

The Guard forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN. This action allows the Guard to change the next-hop router to the zone by changing the VLAN on which the packets are forwarded.

The native VLAN is used for traffic diversion. On this interface, the Guard sends the BGP announcements to the router.

Figure 4-6 VRF-VLAN Forwarding Method



This section contains the following topics:

- [Guard VRF-VLAN Configuration](#)
- [Cisco Router VRF-VLAN Configuration](#)

Guard VRF-VLAN Configuration

This section describes the Guard VRF-VLAN configuration. The following examples refer to the network in Figure 4-6.

VRF-VLAN is applied on R1's interface facing the Guard. Zone traffic on VLAN-5 is forwarded to R2. Zone traffic on VLAN-6 is forwarded to R3.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN-5 Statements

The following example shows how to configure VLAN-5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

Interface VLAN-6 Statements

The following example shows how to configure VLAN-6 on the in-band interface:

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.5# ip address 192.168.6.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the [“Guard BGP Configuration”](#) section.

Set the neighbor IP address to 192.168.8.1.

Injection Configuration to R2

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R2.

You should configure the static route at the Guard’s router configuration level.

The following example shows how to configure a static route for the zone’s network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

Injection Configuration to R3

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R3.

You should configure the static route at the Guard’s router configuration level.

The following example shows how to configure a static route for the zone’s network (192.168.240.0/24) via the VLAN interface on R1, 192.168.6.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco Router VRF-VLAN Configuration

This section describes the Cisco router VRF-VLAN configurations.

First VRF Table Production

The following example shows how to create the VRF table associated with router R2:

```
ip vrf next-hop_R2
```

```
rd 100:1
route-target export 100:1
route-target import 100:1
Second VRF Table Production
Create the VRF table associated with router R3:
ip vrf next-hop_R3
rd 100:1
route-target export 100:1
route-target import 100:1
```

Native VLAN Production

The following example shows how to configure the native VLAN on router R1:

```
interface fastEthernet 1/0
description <<NATIVE VLAN TO GUARD-DIVERSION>>
ip address 192.168.8.1 255.255.255.0
no ip directed-broadcast
```

VLAN-5 Creation

The following example shows how to create VLAN-5 on router R1:

```
interface fastEthernet 1/0.1
encapsulation dot1Q 5
description << VLAN-5 TO GUARD-INJECTION >>
ip address 192.168.5.1 255.255.255.0
ip vrf forwarding next-hop_R2
no ip directed-broadcast
```

VLAN-6 Creation

The following example shows how to create VLAN-6 on router R1 with the second VRF association:

```
interface fastEthernet 1/0.2
encapsulation dot1Q 6
description << VLAN-6 TO GUARD-INJECTION >>
ip address 192.168.6.1 255.255.255.0
ip vrf forwarding next-hop_R3
no ip directed-broadcast
```

Next-Hop Interfaces

The following example shows how to configure the interfaces to the next-hop routers:

```
interface fastEthernet 2/0
ip address 192.168.250.1 255.255.255.0
Description << LINK TO NEXT-HOP R2 >>
!
interface fastEthernet 3/0
ip address 192.168.230.1 255.255.255.0
description << LINK TO NEXT-HOP R3 >>
```

BGP Statements

You can enter the router, R1, BGP configuration as described in the [“Cisco Router BGP Configuration”](#) section.

Static VRF Routes

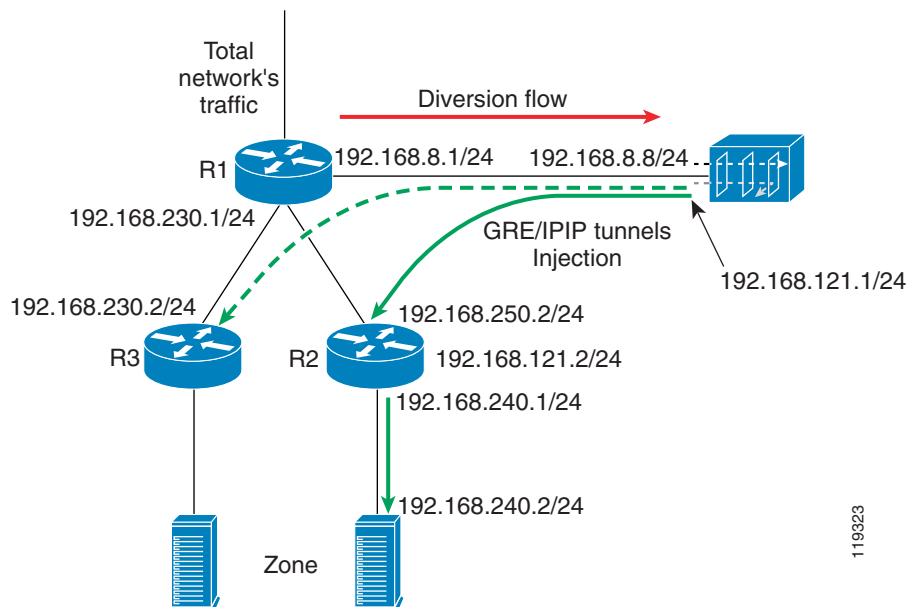
The following example shows how to configure static VRF on the inject-to router. The static VRF specifies the route to the zone. The parameter `global` indicates that the route to the next hop is learned from the global routing table.

```
R7200(config)# ip route vrf next-hop_R3 192.168.240.2 255.255.255.255 192.168.230.2 global
R7200(config)# ip route vrf next-hop_R2 192.168.240.2 255.255.255.255 192.168.250.2 global
```

Tunnel Diversion Forwarding Method

In the tunnel diversion method, a tunnel (GRE or IPIP) is created between the Guard and each of the next-hop routers (Figure 4-7). The Guard sends the traffic destined to the zone over the tunnel to the appropriate next-hop router. This action allows the Guard to change the next-hop router to a specified zone by changing the tunnel that the packets are forwarded on. Because the clean traffic from the Guard to the zone is encapsulated in the tunnel, the inject-to router performs a routing decision on the tunnel interface end point, not on the zone's address.

Figure 4-7 Tunnel Diversion Forwarding Method



This section contains the following topics:

- [Guard Tunnel Diversion Configuration](#)
- [Cisco Router Tunnel Diversion Configuration](#)

Guard Tunnel Diversion Configuration

This section describes the Guard tunnel diversion configuration. The following examples refer to the network in Figure 4-7.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Tunnel Interface Statements

The following example shows how to configure a Generic Routing Encapsulation (GRE) tunnel.

```
admin@GUARD-conf# interface gre1
admin@GUARD-conf-if-gre1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-gre1# tunnel source 192.168.8.8
admin@GUARD-conf-if-gre1# tunnel destination 192.168.250.2
```

The following example shows how to configure an IP in IP (IPIP) tunnel.

```
admin@GUARD-conf# interface ipip1
admin@GUARD-conf-if-ipip1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-ipip1# tunnel source 192.168.8.8
admin@GUARD-conf-if-ipip1# tunnel destination 192.168.250.2
```

BGP Statements

You can enter the Guard router BGP configuration as described in the “[Guard BGP Configuration](#)” section.

Set the neighbor IP address to 192.168.8.1.

Injection Configuration

The next-hop router in the example is R2. To configure traffic injection from the Guard to the zone, add a static route to the next-hop router.

You should configure the static route at the Guard’s router configuration level.

The following example shows how to configure a static route for the zone’s network (192.168.240.0/24) via the tunnel interface on R1, 192.168.121.2:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.121.2
```

Cisco Router Tunnel Diversion Configuration

Tunnel forwarding requires that you configure the router at the end of the tunnel (R2 in [Figure 4-7](#)). The diversion process requires that you configure the divert-from router (R1 in [Figure 4-7](#)).

R1 Diversion Configuration: BGP Statements

You can enter the router, R1, BGP configuration as described in the “[Cisco Router BGP Configuration](#)” section.

R2 Forwarding Configuration: Tunnel Interface on R2

The following example shows how to configure the tunnel on router R2:

```
interface tunnel 1
description << GRE tunnel to Guard >>
ip address 192.168.121.2 255.255.255.252
load-interval 30
```

```
tunnel source 192.168.250.2
tunnel destination 192.168.8.8
```

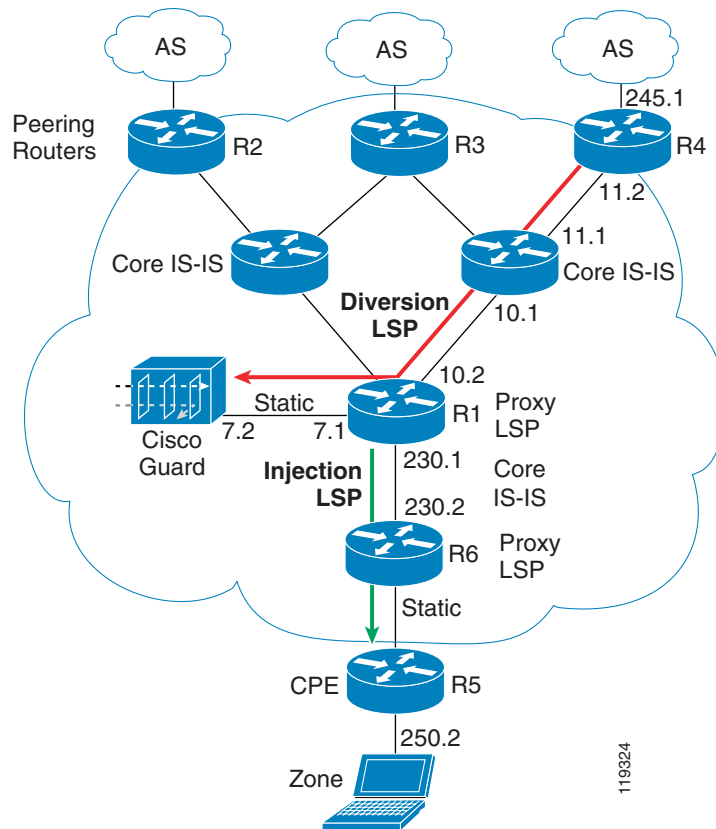
Long Diversion Method

Unlike standard diversion techniques where the Guard diverts traffic only from an adjacent directly connected router, the long diversion method diverts traffic from remotely located peering routers that may reside several hops away from the Guard.

Figure 4-8 includes the following network elements:

- Peering router (R4)
- Guard's adjacent router (R1)
- Zone's edge router (R6)
- Cisco Guard

Figure 4-8 Long Diversion Configuration



This section contains the following topics:

- [Packet Flow Example](#)
- [Long Diversion Configuration](#)

Packet Flow Example

The traffic flows to the zone's IP addresses (based on the loopback address that holds the Label Switched Path [LSP]).

Once an attack is identified, you activate the Guard to protect the attacked zone. The following steps automatically take place:

1. The Guard informs the peering routers (R2, R3, R4) about a new route to the zone. The next hop is defined as the Guard's loopback interface.
2. The zone's traffic is routed by the peering routers over the diversion LSP to the zone.
3. The Guard forwards the clean traffic to R1.
4. R1 performs an IP lookup and routes the packets, on the appropriate LSP, to the zone.

Long Diversion Configuration

The configuration in the following example refers to the network in [Figure 4-8](#).

Guard Long Diversion Configuration

This section describes the Guard long diversion configurations.

Guard CLI Loopback Configuration

The following example shows how to add a loopback interface to the Guard:

```
admin@GUARD# configure
admin@GUARD-conf# interface lo:2
admin@GUARD-conf-if-lo:2# ip address 1.1.1.1 255.255.255.255
admin@GUARD-conf-if-lo:2# no shutdown
admin@GUARD-conf-if-lo:2# exit
For changes to take effect you need to reload the software.
Type 'yes' to reload now, or any other key to reload manually later
yes
reloading...
```

Zebra CLI Loopback Configuration

The following example shows how to use the Zebra application to add a loopback interface to the routing configuration.



Note

For more information about the Zebra application, see <http://www.zebra.org>.

```
router(config)# router bgp 100
router(config-router)# redistribute Guard
router(config-router)# bgp router-id 192.168.8.16
router(config-router)# neighbor 192.168.8.1 remote-as 100
router(config-router)# neighbor 192.168.8.1 description << iBGP session to peering Router
>>
router(config-router)# neighbor 192.168.8.1 soft-reconfiguration inbound
router(config-router)# neighbor 192.168.8.1 route-map _new_next-hop out
router(config-router)# exit
router(config)# route-map _new_next-hop permit 10
router(config-route-map)# set ip next-hop 1.1.1.1
```

```
router(config)# ip route 0.0.0.0 0.0.0.0 192.168.7.1
```

Cisco Router Long Diversion Configuration

This section describes the Cisco router long diversion configuration.

Peering Router Configuration (R2, R3, and R4)

The sample configuration in this section applies to the peering routers: R2, R3, and R4 (see [Figure 4-8](#)). This section displays only the commands relevant to long diversion configuration.

The following example shows how to configure Multiprotocol Label Switching (MPLS) on the peering routers:

```
mpls ip
ip cef
```

The following example shows how to configure the loopback 0 interface. This interface will be used to build the LSP via Intermediate System-to-Intermediate System (IS-IS).

```
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
no ip directed-broadcast
load-interval 30
```

The following example shows how to configure the network connectivity interfaces:

```
interface fastEthernet 5/0
ip address 192.168.11.2 255.255.255.0
no ip directed-broadcast
load-interval 30
tag-switching ip (enable MPLS)
no cdp enable
```

The following example shows how to configure IS-IS:

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0003.00
```

The following example shows how to configure iBGP to the Guard:

```
router(config)# router bgp 100
R7200(config-router)# no synchronization
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor 192.168.8.16 remote-as 100
R7200(config-router)# neighbor 192.168.8.16 description << iBGP to the Guard >>
R7200(config-router)# neighbor 192.168.8.16 soft-reconfiguration inbound
```

Adjacent Router Configuration (R1)

The sample configuration in this section applies to the adjacent router R1 (see [Figure 4-8](#)). This section displays only the commands relevant to long diversion configuration.

The following example shows how to configure the loopback 0 interface. This interface will be used to build the LSP via IS-IS.

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
no ip directed-broadcast
```

The following example shows how to configure the network connectivity interfaces:

```
interface fastEthernet 5/0
 ip address 192.168.10.2 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 tag-switching ip (enable MPLS)
 no cdp enable
```

The following example shows how to configure the interface to the Guard.

**Note**

MPLS is not configured on this interface.

```
interface FastEthernet1/0
 ip address 192.168.7.1 255.255.255.0
 no ip directed-broadcast
```

The following example shows how to configure the interface to the Guard.

**Note**

MPLS is configured on this interface.

```
interface fastEthernet 0/1/1
 ip address 192.168.230.1 255.255.255.0
 tag-switching ip (enable MPLS)
 no cdp enable
```

The following example shows how to configure IS-IS:

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0002.00
```

The following example shows how to configure a static route on the egress proxy-LSR to the Guard loopback IP address (the IP address 1.1.1.1 is the loopback address configured on the Guard):

```
ip classless
 ip route 1.1.1.1 255.255.255.255 192.168.7.2
```

