



Using Performance Routing to Control EIGRP Routes with mGRE DMVPN Hub-and-Spoke Support

The PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature introduces the ability to inject routes into the EIGRP routing table, which allows Performance Routing (PfR) to control prefixes and applications over EIGRP routes. This feature also adds support for multipoint Generic Routing Encapsulation (mGRE) Dynamic Multipoint Virtual Private Network (DMVPN) deployments that follow a hub-and-spoke network design.

- [Prerequisites for Using PfR to Control EIGRP Routes, on page 1](#)
- [Restrictions for Using PfR to Control EIGRP Routes, on page 1](#)
- [Information About Using PfR to Control EIGRP Routes, on page 2](#)
- [How to Configure PfR to Control EIGRP Routes, on page 4](#)
- [Configuration Examples for Using PfR to Control EIGRP Routes, on page 8](#)
- [Additional References, on page 9](#)
- [Feature Information for Using PfR to Control EIGRP Routes, on page 10](#)

Prerequisites for Using PfR to Control EIGRP Routes

This feature assumes that EIGRP is already configured in your network and that basic PfR functionality is also configured.

Restrictions for Using PfR to Control EIGRP Routes

- PfR does not support split tunneling.
- PfR supports hub-to-spoke links only. Spoke-to-spoke links are not supported. If you are deploying EIGRP in an mGRE DMVPN topology in your network, it must conform to a hub-and-spoke network design.
- PfR is supported on DMVPN Multipoint GRE (mGRE) deployments. Any multipoint interface deployment that has multiple next hops for the same destination IP address is not supported (for example, Ethernet).

Information About Using PfR to Control EIGRP Routes

PfR EIGRP Route Control

The PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature introduces PfR route control for EIGRP. When enabled, a parent route check is performed in the EIGRP database for controlling PfR prefixes and routes in addition to the existing BGP and static route databases.

PfR can only optimize paths for prefixes, which have an exact matching route or a less specific route (also called as parent route) in the routing protocols. The route being controlled by PfR can be an exact match of the parent route or can be a more specific one. For example, if PfR wants to control 10.1.1.0/24 but the EIGRP routing table has only 10.1.0.0/16 then the parent route is 10.1.0.0/16 and PfR will inject 10.1.1.0/24 in the EIGRP routing table.

If an exact matching parent route in the EIGRP routing table is found, PfR will attempt to install a route on an exit selected by the master controller by influencing the metric. If an exact match parent is not found, then PfR introduces a new route in the EIGRP table that matches the attributes of the parent. If the route installation in the EIGRP table is successful, PfR saves the EIGRP parent and registers for any updates to the parent route. If the parent route is removed, PfR will uncontrol any routes it has installed in the EIGRP table based on this parent route.

PfR monitors traffic performance for prefixes it is controlling either passively using NetFlow or actively using IP SLA probes. Performance statistics such as delay, loss, and reachability are gathered and compared against a set of policies configured for the prefixes. If the traffic performance does not conform to the policies, the prefix is said to be out-of-policy (OOP). PfR tries to find an alternate path when the prefix goes into the OOP state.

While both BGP and static route control are enabled by default, EIGRP route control must be configured. PfR always attempts to control a prefix using BGP first. If BGP route control fails, static route control is tried. When EIGRP route control is enabled, PfR will attempt to control a prefix using BGP first. If no parent route is found, PfR will try to use EIGRP route control. If EIGRP route controls fails, static route control is tried.

To find an alternate path for a prefix, PfR tries to send active probes from all the external interfaces on the border routers to a set of hosts in the destination prefix network. Before an active probe can be sent on an external interface, a parent route lookup is performed in routing protocol tables. When the PfR EIGRP mGRE DMVPN Hub-and-Spoke Support feature is enabled, PfR checks EIGRP routing tables, in addition to BGP and static routing tables, for a parent route, before sending active probes on external interfaces. Active probes are initiated on all the external interfaces that have a parent route in the EIGRP routing table. When the probe activity completes and the timer expires, statistics are sent from the border router to the master controller for policy decision and selection of an optimal exit.

When an exit is selected, a control prefix command is sent to the border router with the selected exit, specifying EIGRP as the protocol to install or modify the route. When the border router receives the command, it checks the EIGRP table to find a parent route. If a parent route is found, PfR will install or modify the route in the EIGRP table and will notify the master controller about the route control status.

If an EIGRP route is successfully installed and advertised into the domain, PfR continues to monitor traffic performance for this prefix and takes further action as mentioned above if the prefix goes OOP.

For more details about the PfR control mode and details about other PfR exit link selection control techniques including BGP, static routes, policy-based routing, and Protocol Independent Route Optimization (PIRO), see the Understanding Performance Routing module and the Performance Routing - Protocol Independent Route Optimization (PIRO) module.

PfR and mGRE Dynamic Multipoint VPN

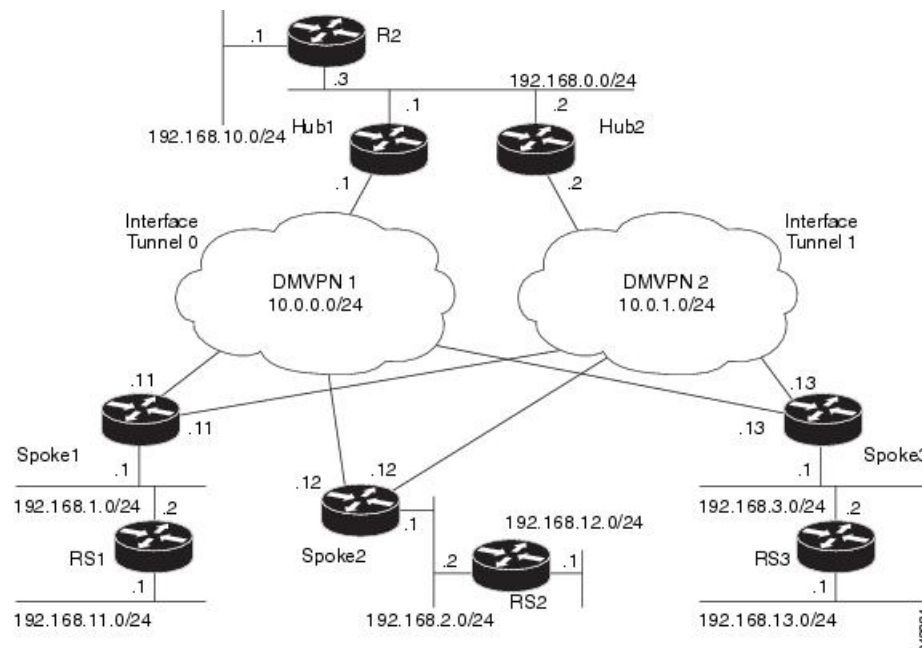
Performance Routing is supported on mGRE interfaces in Dynamic Multipoint VPN (DMVPN) topologies. DMVPN enables zero-touch deployment of IPsec encrypted VPN networks. Many DMVPN deployments use EIGRP networks, and support was added to PfR to allow DMVPN network deployments to use EIGRP route control within the DMVPN network. In the PfR EIGRP route control implementation, only hub-to-spoke network designs are supported.

In DMVPN topologies the mGRE interface works as a one-to-many interface and allows the dynamic creation of tunnels for each connected branch.

The figure below shows a typical dual DMVPN topology. The head office (R2) has one hub (hub1) that connects to the remote site spokes using one of the DMVPN networks (DMVPN 1 or DMVPN 2) or the MPLS-GETVPN network.

Remote site 1 (RS1) has spokes 1 and 2 that connect to the hub using the DMVPN1 and DMVPN2 networks. Remote site 2 (RS2) has spoke 3 and connects to the hub using DMVPN1 network only. This means that there is no redundancy at RS2 and any performance optimization is performed between the hub and RS2 only. Remote site 3 (RS3) has spoke 3 that connects to the hub using the DMVPN2 network and the MPLS-GETVPN network.

Figure 1: PfR Dual DMVPN Topology



When PfR is configured on the network, the system can perform these functions:

- Control and measure the performance of PfR traffic-classes on mGRE interfaces.
- Support load balancing for traffic over multipoint interfaces that are configured as PfR external interfaces. For example, in topologies with two DMVPN clouds PfR can be configured to load balance the traffic across the two tunnel interfaces to ensure that network performance is maintained.
- Reroute traffic from or to a multipoint interface for better performance. For example, PfR policies can be configured to select the best path to a spoke and the best path from the spoke to the hub.

- Provide a back-up connection if the primary connection fails. For example, in a topology with one MPLS-GETVPN and one DMVPN connection, the MPLS-GETVPN could act as a primary connection and PfR could be configured to use the DMVPN connection if the primary connection fails.



Note Before configuring a tunnel to PfR, configure a loopback interface (that is not attached to a VRF) with an IP address so that the internally created tunnel interface is enabled for IPv4 forwarding by unnumbering itself to this dummy loopback interface. You do not need to configure a loopback interface if the system has at least one interface that is not attached to a VRF and that is configured with an IPv4 address.

The DMVPN topology leverages protocols like multipoint GRE (mGRE) for hub-to-spoke functionality, and for spoke-to-spoke functionality it utilizes the Next Hop Resolution Protocol (NHRP). For more details about configuring mGRE DMVPN networks, see the "Dynamic Multipoint VPN" module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*. For general information about DMVPN, go to <http://www.cisco.com/go/dmvpn>.

How to Configure PfR to Control EIGRP Routes

Enabling PfR EIGRP Route Control and Setting a Community Value

Perform this task on the master controller to enable EIGRP route control. While both BGP and static route control are enabled by default, EIGRP route control must be enabled using a command-line interface (CLI) command, **mode route metric eigrp**. PfR always attempts to control a prefix using BGP first. If BGP route control fails, static route control is tried. When EIGRP route control is enabled, PfR will attempt to control a prefix using BGP first. If no parent route is found, PfR will try to use EIGRP route control. If EIGRP route control fails, static route control is tried.

This task can also set an extended community value for an injected EIGRP route to allow the routes to be uniquely identified. An EIGRP route may be injected by PfR to control the traffic defined by a traffic class when it goes out-of-policy (OOP). In this task, the PfR route control mode is configured globally with the **mode route control** command in PfR master controller configuration mode, and any injected EIGRP routes will be tagged with a value of 700.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pfr master**
4. **mode route control**
5. **mode route metric eigrp tag community**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	pfr master Example: Router(config)# pfr master	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	mode route control Example: Router(config-pfr-mc)# mode route control	Configures the PfR route control mode on a master controller. • The route and control keywords enable route control mode. In control mode, the master controller analyzes monitored traffic classes and implements changes based on policy parameters.
Step 5	mode route metric eigrp tag community Example: Router(config-pfr-mc)# mode route metric eigrp tag 7000	Enables EIGRP route control and sets an EIGRP tag and community number value for injected EIGRP routes. • Use the tag keyword to apply a tag to an EIGRP route under PfR control. The <i>community</i> argument is a number from 1 to 65535.
Step 6	end Example: Router(config-pfr-mc)# end	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Disabling PfR EIGRP Route Control



Note When this task is complete, PfR withdraws all the routes that are being controlled using the EIGRP protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. `pfr master`
4. `no mode route metric eigrp`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	pfr master Example: <pre>Router(config)# pfr master</pre>	Enters PfR master controller configuration mode to configure a router as a master controller and to configure global operations and policies.
Step 4	no mode route metric eigrp Example: <pre>Router(config-pfr-mc)# no mode route metric eigrp</pre>	Disables EIGRP route control and removes all the routes that are being controlled using the EIGRP protocol.
Step 5	end Example: <pre>Router(config-pfr-mc)# end</pre>	Exits PfR master controller configuration mode and returns to privileged EXEC mode.

Manually Verifying the PfR EIGRP-Controlled Routes

PfR automatically verifies route control changes in the network using NetFlow output. PfR monitors the NetFlow messages and uncontrols a traffic class if a message does not appear to verify the route control change. Perform the steps in this optional task if you want to manually verify that the traffic control implemented in the PfR control phase actually changes the traffic flow, and brings the OOP event to be in-policy.

All the steps in this task are optional and are not in any order. The information from these steps can verify that a specific prefix associated with a traffic class has been moved to another exit or entrance link interface, or that it is being controlled by PfR. The first two commands are entered at the master controller, the last two commands are entered at a border router.

Only partial command syntax for some of the **show** commands used in this task is displayed. For more details about PfR **show** commands, see the *Cisco IOS Performance Routing Command Reference*.

Before you begin

This task assumes that you have previously enabled EIGRP route control using PfR.

SUMMARY STEPS

1. **enable**
2. **show pfr master prefix *prefix* [detail]**
3. Move to a border router to enter the next step.
4. **enable**
5. **show pfr border routes eigrp [parent]**

DETAILED STEPS**Step 1 enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 show pfr master prefix *prefix* [detail]

This command is used to display the status of monitored prefixes. The output from this command includes information about the source border router, current exit interface, protocol, prefix delay, and egress and ingress interface bandwidth. In this example, the protocol displayed for the prefix 10.1.0.0/16 is EIGRP, which means that the parent route for the traffic class exists in the EIGRP routing table and EIGRP community values are used to control the prefix. Only syntax relevant to this task is shown in this step.

Example:

```
Router# show pfr master prefix 10.1.0.0
```

```
OER Prefix Statistics:
Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
P - Percentage below threshold, Jit - Jitter (ms),
MOS - Mean Opinion Score
Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
# - Prefix monitor mode is Special, & - Blackholed Prefix
% - Force Next-Hop, ^ - Prefix is denied
```

Prefix	State	Time	Curr BR	CurrI/F	Protocol	
	PasSDly	PasLDly	PasSun	PasLUn	PasSLos	PasLLos
	ActSDly	ActLDly	ActSun	ActLUn	EBw	IBw
	ActSJit	ActPMOS				
10.1.0.0/16	DEFAULT*	@69	10.1.1.1	Gil/22		EIGRP
	U	U	0	0	0	0
	U	U	0	0	22	8
	N	N				

Step 3 Move to a border router to enter the next step.

The next command is entered on a border router, not the master controller.

Example:

Step 4 enable

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 5 show pfr border routes eigrp [parent]

This command is entered on a border router. Use this command to display information about EIGRP routes controlled by PfR on a border router. In this example, the output shows that prefix 10.1.2.0/24 is being controlled by PfR. This command is used to show parent route lookup and route changes to existing parent routes when the parent route is identified from the EIGRP routing table.

Example:

```
Router# show pfr border routes eigrp

Flags: C - Controlled by oer, X - Path is excluded from control,
       E - The control is exact, N - The control is non-exact
Flags Network      Parent      Tag
CE   10.1.2.0/24   10.0.0.0/8  5000
```

In this example, the **parent** keyword is used and more details are shown about the parent route lookup.

Example:

```
Router# show pfr border routes eigrp parent

Network      Gateway      Intf      Flags
10.0.0.0/8   10.40.40.2   Gi0/0/2   1
Child Networks
Network      Flag
10.1.2.0/24  6
```

Troubleshooting Tips

If the **show** commands are not displaying output that verifies the EIGRP route control, use the **debug pfr border routes eigrp** command with the optional **detail** keyword for more information. Debugging must be enabled before entering the required commands, and the debug output depends on which commands are subsequently entered.

Configuration Examples for Using PfR to Control EIGRP Routes**Example Enabling PfR EIGRP Route Control and Setting a Community Value**

In the following configuration example, PfR route control is enabled first, and then the EIGRP route control is enabled and configured to set an extended community value of 700 to any injected EIGRP routes:

```
pfr master
```

```

mode route control
mode route metric eigrp tag 700
end

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration for Cisco IOS XE releases	“Configuring Basic Performance Routing” module
Information about configuration for the border router only functionality for Cisco IOS XE Releases 3.1 and 3.2	“Performance Routing Border Router Only Functionality” module
Concepts required to understand the Performance Routing operational phases for Cisco IOS XE releases	“Understanding Performance Routing” module
Advanced PfR configuration for Cisco IOS XE releases	“Configuring Advanced Performance Routing” module
IP SLAs overview	“Cisco IOS IP SLAs Overview” module
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-PFR-MIB • CISCO-PFR-TRAPS-MIB 	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for Using PfR to Control EIGRP Routes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Using PfR to Control EIGRP Routes

Feature Name	Releases	Feature Information
PfR EIGRP mGRE DMVPN Hub-and-Spoke Support	Cisco IOS XE Release 3.3S	<p>The PfR EIGRP feature introduces PfR route control capabilities based on EIGRP by performing a route parent check on the EIGRP database. This feature also adds support for mGRE Dynamic Multipoint VPN (DMVPN) deployments that follow a hub-and-spoke network design.</p> <p>The following commands were introduced or modified: debug pfr border routes, mode (PfR), show pfr border routes, and show pfr master prefix.</p>