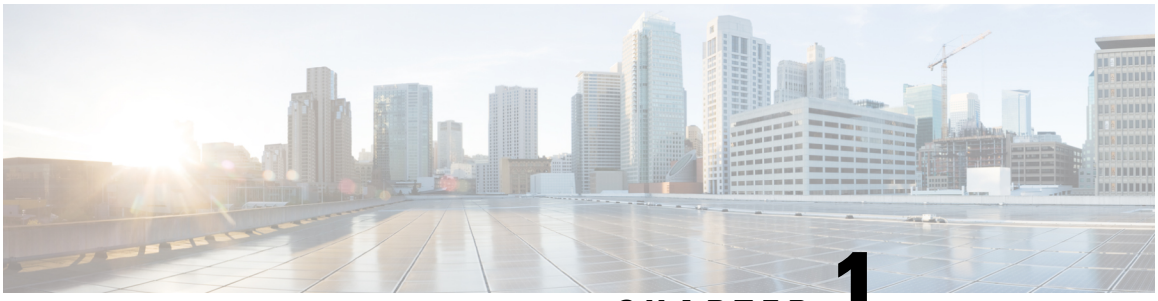
# Performance Routing Version 3 Configuration Guide, Cisco IOS XE Fuji 16.8.x

**First Published:** 2018-03-30

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS



CHAPTER 1

# Read Me First

### Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

### Feature Information

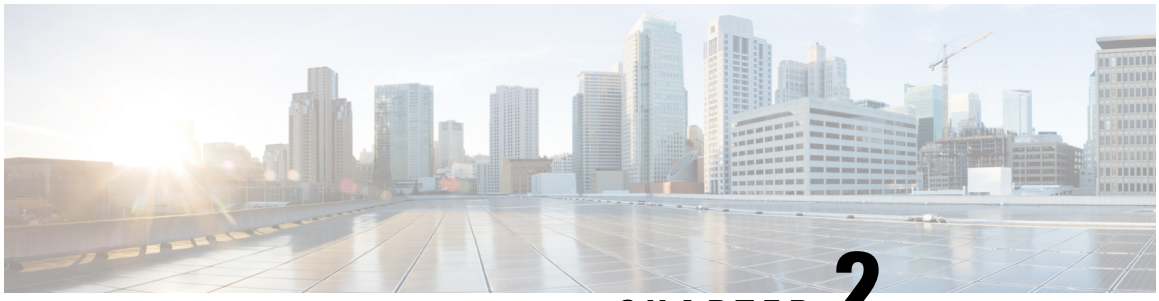
Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

### Related References

- Cisco IOS Command References, All Releases

### Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.



CHAPTER 2

# About this Guide



## Audience

The *Performance Routing Version 3 Configuration Guide* is for network managers and administrators. This guide provides an overview on Performance Routing v3 and describes how to configure performance routing v3 on Cisco devices.

## Document Organization

This document is organized into the following chapters:

| Chapter | Description |
|---|---|
| Overview of Performance Routing v3 | Describes the design and different device roles in PfRv3. |
| Configuring Performance Routing v3 | Describes the configuration, verification, and monitoring operations for different components of PfRv3. |
| Performance Routing v3 Transit Site Support | Describes PfRv3 transit site support, and provides information on how to configure and verify PfRv3 transit sites configurations. |
| Performance Routing v3 Zero SLA Support | Describes PfRv3 Zero SLA support, and provides information on how to configure and verify PfRv3 Zero SLA configurations. |
| Troubleshooting | Describes the common troubleshooting scenarios along with the workaround. |
| PfRv3 Remote Prefix Tracking | Describes the PfRv3 remote site prefixes, prefix tracking, and how to display site prefixes. |

| Chapter | Description |
|---|---|
| Command Reference | Lists the various commands required to configure, verify, and debug PfRv3 configurations. |

# Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier font` | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier font`** | Bold Courier font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |

| Convention | Description |
|---|---|
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### Reader Alert Conventions

This document uses the following conventions for reader alerts:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip** Means *the following information will help you solve a problem.*

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver** Means *the described action saves time.* You can save time by performing the action described in the paragraph.

**Warning** **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

# New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Performance Routing v3 Configuration Guide*.

The following table summarizes the new and changed features for the *Cisco Performance Routing v3 Configuration Guide* and where they are documented.

***Table 1: New and Changed Features***

| Feature Name | Releases | Feature Information | Where Documented |
|---|---|---|---|
| Performance Routing v3 | 15.5(1)T<br>Cisco IOS XE 3.13S | PfRv3 is an intelligent-path control mechanism for improving application delivery and WAN efficiency. PfRv3 protects critical application and increases bandwidth utilization and serves as an integral part of the overall Cisco Intelligent WAN (IWAN) solution. | |
| Performance Routing v3 Zero SLA Support | 15.5(1)T<br>Cisco IOS XE 3.14S | The PfRv3 zero SLA support feature enables users to reduce probing frequency on various ISP links. | |
| Performance Routing v3 Transit Site Support | 15.5(2)T<br>Cisco IOS XE 3.15S | The PfRv3 transit site support feature enables enterprise organizations to configure multiple data centers at the hub site. | |

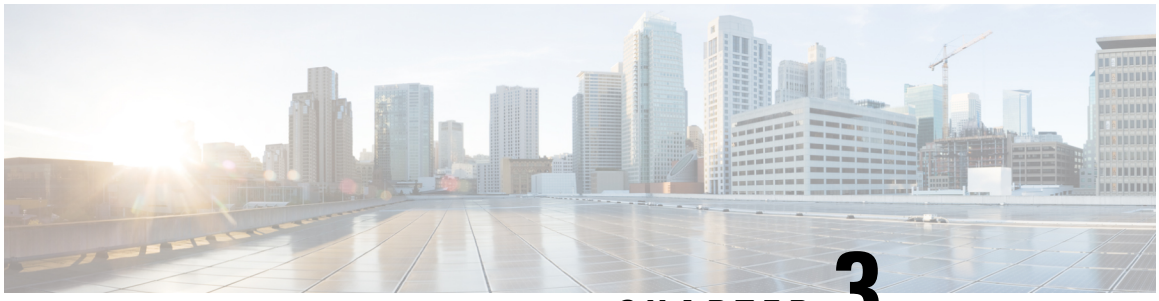
# Additional References for PfRv3

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco PfRv3 commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples | Cisco IOS Performance Routing Command Reference |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br><br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br><br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html<br><br>http://www.cisco.com/support |



CHAPTER 3

# Performance Routing Version 3



# Performance Routing Version 3

Performance Routing Version 3 (PfRv3) is the evolution of Performance Routing (PfR). PfRv3 is an intelligent-path control mechanism for improving application delivery and WAN efficiency. It protects critical applications, increases bandwidth utilization, and serves as an integral part of the Cisco Intelligent WAN (IWAN) solution. PfRv3 uses differentiated services code points (DSCP) and application-based policy framework to provide a multi-site aware bandwidth and path control optimization.

## Feature Information for PfRv3

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 2: Feature Information for Configuring PfRv3*

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 | | Performance Routing v3 (PfRv3) is the evolution of Performance Routing.<br>PfRv3 is an intelligent-path control mechanism for improving application delivery and WAN efficiency. It protects critical applications, increases bandwidth utilization, and serves as an integral part of the Cisco Intelligent WAN (IWAN) solution.<br>The following commands were modified by this feature: **domain default**, **vrf default**, **master**, **source-interface**, **site-prefixes**, **password**, **monitor-interval**, **route-control**, **load-balance**, **enterprise-prefix**, **advanced**, **minimum-mask-length**, **mitigation-mode**, **threshold-variance**, **smart-probes**, **collector**, **class**, **match**, **priority**, **path-preference**, **border**, **domain-path**. |

# Hardware and Software Support

Cisco Performance Routing Version 3 (PfRv3) supports the following Cisco platforms and software releases:

| Device | Cisco IOS Software Release | Hub/Remote Site |
|---|---|---|
| Cisco ISR 4000 Series Routers | Cisco IOS XE 3.13 or later | Hub site or remote site |
| Cisco ASR 1000 Series Routers | Cisco IOS XE 3.13 or later | Hub site |
| Cisco CSR 1000v Series Routers | Cisco IOS XE 3.14 or later | Hub site (master controller)<br>Branch site (master controller and border router) |
| Cisco ISR-G2 Series Routers | Cisco IOS 15.5(1)T1 or later<br>Cisco IOS 15.4(3)M1 or later | Remote site |

# Restrictions for Configuring Performance Routing v3

- Asymmetric routing is not supported for application-based policy.
- A new session cannot be established with application-based policy during blackout failure until route converges to backup path. For application-based flows, application ID is not recognized by Network Based Application Recognition (NBAR2) until session gets established and packet exchanges directly. You can configure Differentiated Services Code Point (DSCP) based policy for fast failover with blackout failure.
- PfRv3 does not support High Availability (HA) for both master and border routers. ESP switch over can trigger temporary unreachable event for one to two seconds.
- IPv6 is not supported.
- Network Address Translation (NAT) is not supported.
- Remarking DSCP for traffic flows on WAN interface is not supported.
- On a HUB Master Controller (MC), when a class is configured for matching application within a PFRv3 domain, the list of NBAR application names are limited if there is no active Border Router (BR).

**Note** Use at atleast one active BR for the MC to display all possible NBAR application names based on the protocol pack installed in BR.

**Note** PfRv2 is not supported on Cisco IOS 15.6(3)M and Cisco IOS 15.7(3)M or later releases. Cisco IOS XE 16.3.1 has PfRv2 CLIs, but the functionality is not supported.

# Information About PfRv3

## Performance Routing v3 Overview

Performance Routing Version 3 (PfRv3) is a one-touch provisioning and multi-site coordination solution that simplifies network provisioning. It enables intelligence of Cisco devices to improve application performance and availability. PfRv3 is an application-based policy driven framework that provides a multi-site aware bandwidth and path control optimization for WAN and cloud-based applications.

PfRv3 monitors network performance and selects best path for each application based on criteria such as reachability, delay, jitter, and loss. It evenly distributes traffic and maintains equivalent link utilization levels and load balances traffic.

It is tightly integrated with existing AVC components such as Performance Monitoring, Quality of Service (QoS), and NBAR2. PfRv3 is useful for enterprise and managed service providers looking for ways to increase their WAN reliability and availability while saving cost.

## Benefits of PfRv3

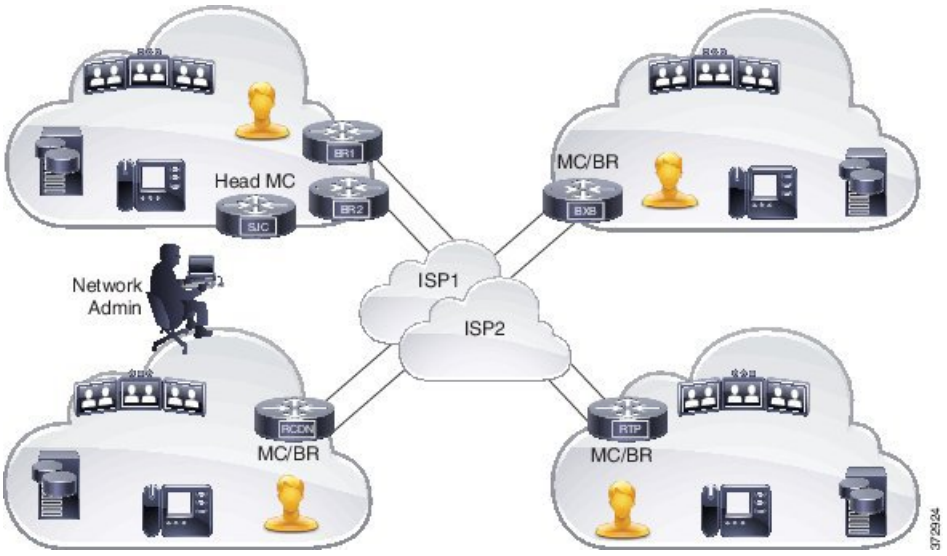
Performance Routing Version 3 provides the following benefits:

- Centralized provisioning — Policies are defined on the hub-master controller and then distributed to all branches. Hence, per-site provisioning is not required in PfRv3.
- Simple provisioning — PfRv3 has simplified policies with pre-existing templates that a user can choose from.
- Enterprise domain — All sites belong to an enterprise domain and are connected with peering.
- Application and DSCP-based policies — Policies are provisioned based on applications. PfRv3 provides application visibility such as bandwidth, performance, and correlation to Quality of Service (QoS) queues by using Unified Monitoring.
- Automatic discovery — PfRv3 site are discovered using peering. Each site peers with the hub site. The WAN interfaces are automatically discovered on the branch sites.
- Scalable passive monitoring — PfRv3 uses Unified Monitor to monitor traffic going into WAN links and traffic coming from the WAN links. It monitors performance metrics based on per DSCP instead of per flow or per prefix basis.
- Smart probing — PfRv3 uses probing mechanism that generates traffic only when there in no traffic. It generates real-time transport protocol traffic, which allows measuring jitter and packet loss using performance monitors.
- Scaling — Smart probing and enhanced passive metrics helps to attain scale up to 2000 branches.
- VRF awareness — Different policies can be configured for different VRFs.

## PfRv3 Design Overview

An enterprise organization has a hub and branch site. The hub site consists of master controller and border router.

***Figure 1: PfRv3 Design Topology***




- In a network, all the policies are created on the hub-master controller. Policies dictate the desired treatment for a set of specified differentiated service code points (DSCPs) or application IDs (such as telepresence, WebEx, and so on) in the network. The policies are percolated to all the master controllers on the network

via Service Advertisement Framework (SAF). The policies can be modified by the hub-master controller and the modified policies are sent over the SAF framework so that all the nodes in the network are in sync with the hub-master controller. The hub-master controller collects information about flows handled by border routers. This information is exported to the master controller periodically using the performance monitoring instances (PMI) exporter. A domain can be configured on the central location (Hub) and branches. PfRv3 allows only one domain configuration. Virtual Routing and Forwarding (VRF) and roles are defined on a domain.

- PfRv3 is enabled on the WAN interface of the hub-border routers. The border routers give the flow information to the branch-master controller.
- Every branch has a local-master controller. The master controller can be either co-located with a branch router or a separate router. You must configure both local master and branch border on the same domain. Border devices establishes connection with local-master controller only if both are in the same domain. In a scenario where master and border configurations are on different domain, peering rejects all messages from different peers. Border devices are automatically shut down for five minutes. The connection is established only when the domain conflict is resolved.

  Based on the flow information provided by the hub-border router, the branch-master (local-master) controller applies appropriate controls on the branch router per flow. It ascertains if a flow is operating within the policy limits or out-of-policy. The master-controller to branch-border communication is done via a TCP connection. This connection is used for tasks such as sending configuration and control information from master controller to branch router and flow information from branch router to master controller.
- The branch router is the enforcer, which classifies and measures metrics and sends them to the local-master controller. It is also responsible for path enforcement.

## PfRv3 Configuration Components

PfRv3 comprises of the following configuration components:

- Device setup and role — Identifies devices in the network where PfRv3 should be configured and in what role.
- Policy configurations — Identifies the traffic in the network and determines what policies to apply.

## Device Setup and Role

There are four different roles a device can play in PfRv3 configuration:

- Hub-master controller — The master controller at the hub site, which can be either a data center or a head quarter. All policies are configured on hub-master controller. It acts as master controller for the site and makes optimization decision.
- Hub-border router — The border controller at the hub site. PfRv3 is enabled on the WAN interfaces of the hub-border routers. You can configure more than one WAN interface on the same device. You can have multiple hub border devices. On the hub-border router, PfRv3 must be configured with the address of the local hub-master controller, path names, and path-ids of the external interfaces. You can use the global routing table (default VRF) or define specific VRFs for the hub-border routers.
- Branch-master controller — The branch-master controller is the master controller at the branch site. There is no policy configuration on this device. It receives policy from the hub-master controller. This device acts as master controller for the branch site and makes optimization decision.

- Branch- border router — The border device at the branch-site. There is no configuration other than enabling of PfRv3 border-master controller on the device. The WAN interface that terminates on the device is detected automatically.

## Domain Policies

Domain policies are defined only on the hub-master controller and then sent over peering infrastructure to all the branch-master controllers. Policies can be defined per application or per differentiated service code point (DSCP). You cannot mix and match DSCP and application-based policies in the same class group. Traffic that does not match any of the classification and match statements falls into a default group, which is load balanced (no performance measurement is done).

**Note** You can either select an existing template for a policy or customize your policies for a domain type.

The following table lists the existing templates for domain type policy:

| Pre-defined Template | Threshold Definition |
|---|---|
| Voice | Priority 1 one-way-delay threshold 150 threshold 150 (msec)<br>Priority 2 packet-loss-rate threshold 1 (%)<br>Priority 2 byte-loss-rate threshold 1 (%)<br>Priority 3 jitter 30 (msec) |
| Real-time-video | Priority 1 packet-loss-rate threshold 1 (%)<br>Priority 1 byte-loss-rate threshold 1 (%)<br>Priority 2 one-way-delay threshold 150 (msec)<br>Priority 3 jitter 20 (msec) |
| Low-latency-data | Priority 1 one-way-delay threshold 100 (msec))<br>Priority 2 byte-loss-rate threshold 5 (%)<br>Priority 2 packet-loss-rate threshold 5 (%) |
| Bulk-data | Priority 1 one-way-delay threshold 300 (msec)<br>Priority 2 byte-loss-rate threshold 5 (%)<br>Priority 2 packet-loss-rate threshold 5 (%) |
| Best-effort | Priority 1 one-way-delay threshold 500 (msec)<br>Priority 2 byte-loss-rate threshold 10 (%)<br>Priority 2 packet-loss-rate threshold 10 (%) |
| Scavenger | Priority 1 one-way-delay threshold 500 (msec)<br>Priority 2 byte-loss-rate threshold 50 (%)<br>Priority 2 packet-loss-rate threshold 50 (%) |

| Pre-defined Template | Threshold Definition |
|---|---|
| Custom | Defines customized user-defined policy values |

## PfRv3 and Link Group Configuration

PfRv3 allows you to configure the following option for link grouping:

- Allows up to five primary path preferences and four fallback path preferences
- Allows a fallback blackhole configuration
- Allows a fallback routing configuration

During Policy Decision Point (PDP), the exits are first sorted on the available bandwidth and then a second sort algorithm places all primary path preferences in the front of the list followed by fallback preferences. If you have a configuration of primary Internet Service Provider (ISP) 1 and ISP2 and ISP3 as fallback, during policy decision, ISP1 is selected as the primary channel and if ISP2 is equally good it is selected as the fallback. ISP3 is considered only if ISP2 is bad in bandwidth availability.

Routing configuration means that when the traffic is uncontrolled, the routing table takes the responsibility of pushing the flow out of the box.

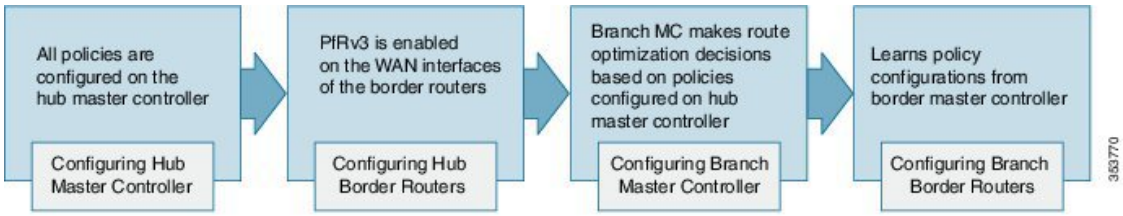
# Configuring Performance Routing Version 3

# Configuring PfRv3

There are four different roles a device can play in the PfRv3 configuration:

- Hub Master Controller
- Hub Border Router
- Branch Master Controller
- Branch Border Router

***Figure 2: PfRv3 Workflow***




## Configuring Hub Master Controller

The hub-master controller is located at the hub site in the Intelligent WAN (IWAN) topology and all policies are configured on the hub-master controller. For more information on hub-master controller, refer to the topic Hub Master Controller. For information on hardware and software supported on hub-master controller, refer to the topic Hardware and Software Requirements.

You can use the global routing table (default VRF) or define specific VRFs for the hub-master controller.

**Note** If default VRF (Global Routing Table) is used, then specific VRF definitions can be omitted.

**Note** The following configuration task is supported on both Cisco IOS Release 15.4 MT and Cisco IOS XE Release 3.13.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address-mask*
5. **exit**
6. **domain** {*domain-name* | **default**}
7. **vrf** {*vrf-name* | **default**}
8. **master** {**hub** | **branch** | **transit**}
9. **source-interface loopback** *interface-number*
10. **enterprise-prefix prefix-list** *site-list*
11. **site-prefixes prefix-list** *site -list*
12. **exit**
13. **ip prefix-list** *ip-list* **seq** *sequence-number* **permit** *ip-prefix-network* **le** *le-length*
14. **end**
15. (Optional) **show domain** *domain-name* **master status**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)# ip address 10.8.3.3 255.255.255.255` | Configures an IP address for an interface on the hub-master controller. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode.<br>**Note** You can either configure a default domain or define a specific domain for the master controller configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration. |
| **Step 7** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain.<br>**Note** You can configure specific VRF definition also for the hub-master controller configuration. |
| **Step 8** | **master** {**hub** \| **branch** \| **transit**}<br>**Example:**<br>`Device(config-domain-vrf)# master hub` | Enters master controller configuration mode and configures the master as a hub. When the master hub is configured, EIGRP SAF auto-configuration is enabled by default and requests from remote sites are sent to the hub-master controller. |
| **Step 9** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-mc)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller.<br>**Note** The source-interface loopback also serves as a site ID of a particular site (hub or branch) on the master controller. |
| **Step 10** | **enterprise-prefix prefix-list** *site-list*<br>**Example:**<br>`Device(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE` | Configures an enterprise prefix-list with static site targets.<br>**Note** The **enterprise-prefix prefix-list** command defines the boundary for all the internal enterprise prefixes. A prefix that is not from the prefix-list is considered as internet prefix and is routed over internet-bound links. |
| **Step 11** | **site-prefixes prefix-list** *site -list*<br>**Example:** | Configures the prefix-list containing list of site prefixes. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-domain-vrf-mc)# site-prefixes prefix-list Data_Center_1` | **Note** The **site-prefix prefix-list** defines static site-prefix for the local site and disables automatic site-prefix learning on the border router. The static-site prefix list is only required for hub and transit sites. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-domain-vrf-mc)# exit` | Exits from master controller configuration mode and returns to domain configuration mode.<br>**Note** Exit from domain configuration mode and enter in global configuration mode using the **exit** command. |
| **Step 13** | **ip prefix-list** *ip-list* **seq** *sequence-number* **permit** *ip-prefix-network* **le** *le-length*<br>**Example:**<br>`Device(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24`<br>`Device(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24` | Configures the IP prefix list to filter traffic based on the IP network defined in the configuration. |
| **Step 14** | **end**<br>**Example:**<br>`Device(config)# end` | Exits configuration mode and returns to privileged EXEC mode. |
| **Step 15** | (Optional) **show domain** *domain-name* **master status**<br>**Example:**<br>`Device# show domain one master status` | Use this show command to display the status of a master controller. |

### What to do next

Configuring Domain Policies

Configuring Hub Border Routers

Configuring Branch Routers

Verifying PfRv3 Configuration

Configuring Channel-based Metrics Measurement

## Configuring Hub Border Router

The border routers on the central site register to the central master controller with their external interface and the path names configured on the external interface. You can use the global routing table (default VRF) or define specific VRFs for hub-border routers.

**Note** On the hub-border router, you must configure PfRv3 with the following:

- The source interface of the border router
- The IP address of the hub-master controller
- The path name on external interfaces

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address-mask*
5. **exit**
6. **domain** {*domain-name* | **default**}
7. **vrf** {*vrf-name* | **default**}
8. **border**
9. **source-interface loopback** *interface-number*
10. **master** [*ip-address* | **local**]
11. **exit**
12. **exit**
13. **exit**
14. **interface** *tunnel-name*
15. **ip address** *ip-address mask*
16. **domain** *domain-name* **path** *path-name*
17. **end**
18. (Optional) **show domain** *domain-name* **border status**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface loopback** *interface-number*<br>**Example:** | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# interface Loopback0` | |
| **Step 4** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)# ip address 10.8.1.1 255.255.255.255` | Configures an IP address for an interface on the hub-border router (Border Router 1). |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain one` | Enters domain configuration mode. |
| **Step 7** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures Virtual Routing and Forwarding (VRF) for the default domain.<br>**Note** You can also configure specific VRF definition for hub-border configuration. |
| **Step 8** | **border**<br>**Example:**<br>`Device(config-domain-vrf)# border` | Enters border configuration mode. |
| **Step 9** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-br)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller. |
| **Step 10** | **master** [*ip-address* \| **local**]<br>**Example:**<br>`Device(config-domain-vrf-br)# master 10.8.3.3` | Configures the IP address of the hub-master controller. You can also configure the local domain master controller as the master. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-domain-vrf-br)# exit` | Exits border configuration mode and enters VRF configuration mode. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-domain-vrf)# exit` | Exits VRF configuration mode and enters domain configuration mode. |
| **Step 13** | **exit**<br>**Example:** | Exits domain configuration mode and enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-domain)# exit` | |
| **Step 14** | **interface** *tunnel-name*<br>**Example:**<br>`Device(config)# interface Tunnel100` | Enters interface configuration mode. |
| **Step 15** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.100.84 255.255.255.0` | Configures an IP address for the tunnel interface. |
| **Step 16** | **domain** *domain-name* **path** *path-name*<br>**Example:**<br>`Device(config-if)# domain one path MPLS` | Configures the Internet Service Provider (ISP). There are two types of external interfaces, enterprise link such as DMVPN tunnel interface and internet-bound interface. Internet-bound external interface is configured only on the hub site for the internet edge deployment and cannot be discovered by any branch site.<br>We recommend using front VRF on the tunnel interface for enterprise links over internet ISP links.<br>**Note** You can configure multiple ISPs. If you are defining specific domain name for example, domain_cisco, you must specify the same domain name for configuring ISP paths. |
| **Step 17** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |
| **Step 18** | (Optional) **show domain** *domain-name* **border status**<br>**Example:**<br>`Device# show domain one border status` | Use this show command to display the status of a border router. |

### What to do next

Configuring Branch Master Controller

Configuring Branch Border Router

Verifying PfRv3 Configuration

## Configuring Domain Policies

**Note** You can define policies based on either per application or per differentiated services code point (DSCP) but, you cannot mix and match DSCP and application-based policies in the same class group. You can use predefined policies from the template or create custom policies.

### Before you begin

Configure a device as hub-master controller at the hub site. To know more about how to configure a hub-master controller, see Configuring Hub Master Controller, on page 15 section.

## SUMMARY STEPS

1. **domain** {*domain-name* | **default**}
2. **vrf** {*vrf-name* | **default**}
3. **master** [**hub** | **branch** | **transit**]
4. **monitor-interval** *seconds* **dscp ef**
5. **load-balance**
6. **class** *class-name* **sequence** *sequence-number*
7. **match {application | dscp}** *services-value* **policy**
8. **path-preference** *path-name* **fallback** *path-name*
9. **priority** *priority-number* [**jitter** | **loss** | **one-way-delay**] **threshold** *threshold-value*
10. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode.<br>**Note** You can either configure a default domain or define a specific domain for the border configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration. |
| **Step 2** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain.<br>**Note** You can configure specific VRF definition also for the hub-master controller configuration. |
| **Step 3** | **master** [**hub** \| **branch** \| **transit**]<br>**Example:**<br>`Device(config-domain-vrf)# master hub` | Enters master controller configuration mode and configures the master as a hub. When the master hub is configured, EIGRP SAF auto-configuration is enabled by default and requests from remote sites are sent to the hub master controller. |
| **Step 4** | **monitor-interval** *seconds* **dscp ef**<br>**Example:**<br>`Device(config-domain-vrf-mc)# monitor-interval 2 dscp ef` | Configures interval time that defines monitoring interval on ingress monitors.<br>**Note** For critical applications monitor interval is set to 2 seconds. Default value is 30 seconds. You can lower the monitor interval for critical applications to achieve a fast fail over to the secondary path. This is known as quick monitor. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **load-balance**<br>**Example:**<br>`Device(config-domain-vrf-mc)# load-balance` | Configures load balancing.<br>**Note** When load balancing is enabled, all the traffic that falls in the default class is load balanced. When load balancing is disabled, PfRv3 deletes this default class and traffic is not load balanced and is routed based on the routing table information. |
| **Step 6** | **class** *class-name* **sequence** *sequence-number*<br>**Example:**<br>`Device(config-domain-vrf-mc)# class VOICE sequence 10` | Enters policy class configuration mode.<br>**Note** Class-name value must be in all capitals. |
| **Step 7** | **match {application \| dscp}** *services-value* **policy**<br>**Example:**<br>`Device(config-domain-vrf-mc-class)# match dscp ef policy voice` | Configures policy on per DSCP basis. You can select a DSCP value from 0 to 63. You can select the following policy types:<br>• **best-effort**<br>• **bulk-data**<br>• **custom**<br>• **low-latency-data**<br>• **real-time-video**<br>• **scavenger**<br>• **voice**<br>In this example, the domain policy type is configured for voice. |
| **Step 8** | **path-preference** *path-name* **fallback** *path-name*<br>**Example:**<br>`Device(config-domain-vrf-mc-class)# path-preference MPLS fallback INET` | Configures the path preference for applications.<br>**Note** You can configure up to five primary path preferences and four fallback preferences. Group policies sharing the same purpose can be defined under the same class path preference. You cannot configure different path preference under the same class. |
| **Step 9** | **priority** *priority-number* [**jitter** \| **loss** \| **one-way-delay**] **threshold** *threshold-value*<br>**Example:**<br>`Device(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10`<br>`Device(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600` | Enters class type configuration mode. Configures the user-defined threshold value for loss, jitter, and one-way-delay for the policy type. Threshold values are defined in usec.<br>**Note** You can configure class type priorities only for a custom policy. You can configure multiple priorities for custom policies. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 200` | |
| **Step 10** | **end**<br>**Example:**<br>`Device(config)# end` | Exits configuration mode and returns to privileged EXEC mode. |

### What to do next

Verifying PfRv3 Configurations

## Configuring Branch Master Controller

You must configure the IP address of the hub-master controller for setting up the branch-master controller. You can use the global routing table (default VRF) or define specific VRFs for the branch-master controller.

**Note** If default VRF (Global Routing Table) is used, then VRF definition can be omitted.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address-mask*
5. **domain** {*domain-name* | **default**}
6. **vrf** {*vrf-name* | **default**}
7. **master branch**
8. **source-interface loopback** *interface-number*
9. **hub** *ip-address*
10. **end**
11. (Optional) **show domain** *domain-name* **master status**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)# ip address 10.2.10.10 255.255.255.255` | Configures an IP address for an interface on the branch-master controller. |
| **Step 5** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode.<br>**Note** You can either configure a default domain or define a specific domain for master controller configuration. If you are defining the specific domain, for example "domain_cisco", you must configure the same domain for all devices for PfRv3 configuration. |
| **Step 6** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures Virtual Routing and Forwarding (VRF) for the default domain.<br>**Note** You can also configure specific VRF definition for branch border configuration. |
| **Step 7** | **master branch**<br>**Example:**<br>`Device(config-domain-vrf)# master branch` | Configures the device as master branch. |
| **Step 8** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-mc)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller. |
| **Step 9** | **hub** *ip-address*<br>**Example:**<br>`Device(config-domain-vrf-mc)# hub 10.8.3.3` | Specifies the IP address of the hub master controller. |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-domain-vrf-mc)# end` | Exits master controller domain configuration mode and returns to privileged EXEC mode. |
| **Step 11** | (Optional) **show domain** *domain-name* **master status**<br>**Example:**<br>`Device# show domain one master status` | Use this show command to display the status of a master controller. |

### What to do next

Configuring Branch Border Router

Verifying Border Router

## Configuring Branch Border Router

A border router on a branch site must register to the local master controller. You need not provision any external interfaces for border routers on branch. Interfaces are learnt during the discovery process together with the path names (colors). You can use the global routing table (default VRF) or define specific VRFs for border routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **domain** {*domain-name* | **default**}
4. **vrf** {*vrf-name* | **default**}
5. **border**
6. **source-interface loopback** *interface-number*
7. **master** *ip-address*
8. **end**
9. (Optional) **show domain** *domain-name* **border status**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode. |
| **Step 4** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures Virtual Routing and Forwarding (VRF) for the default domain.<br>**Note** You can also configure specific VRF definition for the branch-border configuration. |
| **Step 5** | **border**<br>**Example:** | Enters border configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-domain-vrf)# border` | |
| **Step 6** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-br)# source-interface Loopback0` | Configures the loopback address used as a source for peering with other sites or the master controller. |
| **Step 7** | **master** *ip-address*<br>**Example:**<br>`Device(config-domain-vrf-br)# master 10.1.1.1` | Specifies the IP address of the branch-master controller. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-domain-vrf-br)# end` | Exits border configuration mode and returns to privileged EXEC mode. |
| **Step 9** | (Optional) **show domain** *domain-name* **border status**<br>**Example:**<br>`Device# show domain one border status` | Use this show command to display the status of a border router. |

### What to do next

Verifying PfRv3 Configurations

## Configuring Branch Master Controller and Border Router

A branch device can be configured to perform the role of a master controller and a border router. The branch-master controller or border router peers with the hub-master controller and receives all policy updates from it.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address-mask*
5. **exit**
6. **domain** {*domain-name* | **default**}
7. **vrf** {*vrf-name* | **default**}
8. **border**
9. **source-interface loopback** *interface-number*
10. **master local**
11. **master branch**
12. **source-interface loopback** *interface-number*
13. **hub** *ip-address*
14. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)# ip address 10.2.12.12 255.255.255.255` | Configures an IP address for an interface on the branch master controller. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode. |
| **Step 7** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures Virtual Routing and Forwarding (VRF) for the default domain. |
| **Step 8** | **border**<br>**Example:**<br>`Device(config-domain-vrf)# border` | Enters border configuration mode. |
| **Step 9** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-br)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller. |
| **Step 10** | **master local**<br>**Example:** | Configures the local IP address of the device as branch-master controller. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-domain-vrf-br)# master local` | |
| **Step 11** | **master branch**<br>**Example:**<br>`Device(config-domain-vrf-mc)# master branch` | Configures the master type of the device as a branch. |
| **Step 12** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-mc)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller. |
| **Step 13** | **hub** *ip-address*<br>**Example:**<br>`Device(config-domain-vrf-mc)# hub 10.8.3.3` | Configures the IP address of the hub-master controller. |
| **Step 14** | **end**<br>**Example:**<br>`Device(config-domain-vrf-mc)# end` | Exits the configuration mode and returns to privileged EXEC mode. |

### What to do next

Verifying PfRv3 Configuration

# Verifying PfRv3 Configuration

## Verifying Hub Master Controller Configurations

Use the following show commands in any order to verify the status of the hub-master controller.

### SUMMARY STEPS

1. **show domain** *domain-name* **master policy**
2. **show domain** *domain-name* **master status**
3. **show domain** *domain-name* **master exits**
4. **show domain** *domain-name* **master peering**
5. **show derived-config | section eigrp**
6. **show domain** *domain-name* **master discovered-sites**

### DETAILED STEPS

**Step 1** **show domain** *domain-name* **master policy**

This command displays the policy information configured on the hub master controller.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- Policy publishing status to remote sites

- Policy threshold per class based on either DSCP or application
- Class default is enabled

**Example:**

```
HubMC# show domain one master policy

No Policy publish pending
------------------------------------------------------------------------------------------------------------------------
class VOICE sequence 10
  path-preference MPLS fallback INET
  class type: Dscp Based
    match dscp ef policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class VIDEO sequence 20
  path-preference INET fallback MPLS
  class type: Dscp Based
    match dscp af41 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1
    match dscp cs4 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class CRITICAL sequence 30
  path-preference MPLS fallback INET
  class type: Dscp Based
    match dscp af31 policy custom
      priority 2 packet-loss-rate threshold 10.0 percent
      priority 1 one-way-delay threshold 600 msec
      priority 2 byte-loss-rate threshold 10.0 percent
      Number of Traffic classes using this policy: 1

class default
  match dscp all
    Number of Traffic classes using this policy: 3
------------------------------------------------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 3: show domain master policy Field Descriptions***

| Field | Description |
|---|---|
| No policy publish pending | Specifies if the policy publishing is pending to remote sites. |

| Field | Description |
|---|---|
| class | Name of the class type. In this example, the following classes are listed:<br>• VOICE<br>• VIDEO<br>• CRITICAL |
| path-preference | Specifies the path preferred for the class type. |
| match | Specifies the DSCP value to match for a policy type. |
| priority | Specifies the detailed policy threshold per class, based on the DSCP or application. |

**Step 2** **show domain** *domain-name* **master status**

This command displays the status of the hub-master controller.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- Operational status is Up
- Configured status is Up
- External interfaces with appropriate path names are defined
- Load balancing is enabled
- Default channels for load-sharing are enabled and configured

**Example:**

```
HubMC# show domain one master status

------------------------------------------------------------------------------------------------------------------------
*** Domain MC Status ***

Master VRF: Global

Instance Type: Hub
Instance id: 0
Operational status: Up
Configured status: Up
Loopback IP Address: 10.8.3.3
Load Balancing:
 Admin Status: Enabled
 Operational Status: Up
 Enterprise top level prefixes configured: 1
 Max Calculated Utilization Variance: 1%
 Last load balance attempt: 00:27:23 ago
 Last Reason: Variance less than 20%
 Total unbalanced bandwidth:
       External links: 0 Kbps Internet links: 0 Kpbs
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
```

```
Minimum Mask Length: 28
Sampling: off

Borders:
  IP address: 10.8.2.2
  Connection status: CONNECTED (Last Updated 1d11h ago )
  Interfaces configured:
    Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
        Number of default Channels: 3

  Tunnel if: Tunnel0

  IP address: 10.8.1.1
  Connection status: CONNECTED (Last Updated 1d11h ago )
  Interfaces configured:
    Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
        Number of default Channels: 3

  Tunnel if: Tunnel0
------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 4: show domain master status Field Descriptions***

| Field | Description |
|---|---|
| Instance Type | Displays the instance type of the device. In this output, the device is configured as a hub. |
| Operational Status | Displays the operational status of the hub. |
| Configured Status | Displays the configuration status of the hub. |
| Load Balancing | Displays the load balancing status. If load balancing is enabled, the master controller will load balance the default-class traffic among all the external interfaces. |
| Borders | Displays the information of border routers connected to the hub master controller. |
| Number of default Channels | Displays the number of channels configured. |

**Step 3** **show domain** *domain-name* **master exits**

This command displays the summary of the external interfaces configured at the hub site.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- External interface capacity
- Egress utilization
- Number of traffic classes per DSCP on external interface
- Range of Egress utilization

**Example:**

```
HubMC# show domain one master exits

------------------------------------------------------------------------------------------------------------------

*** Domain MC Status ***

BR address: 10.8.2.2 | Name: Tunnel200 | type: external | Path: INET |
    Egress capacity: 50000 Kbps | Egress BW: 17514 Kbps | Ideal:17948 Kbps | under:
434 Kbps | Egress Utilization: 35 %
    DSCP: cs4[32]-Number of Traffic Classes[1]
    DSCP: af41[34]-Number of Traffic Classes[1]
    DSCP: cs5[40]-Number of Traffic Classes[1]

BR address: 10.8.1.1 | Name: Tunnel100 | type: external | Path: MPLS |
   Egress capacity: 100000 Kbps | Egress BW: 36331 Kbps | Ideal:35896 Kbps | over:
435 Kbps | Egress Utilization: 36 %
   DSCP: cs1[8]-Number of Traffic Classes[1]
   DSCP: af11[10]-Number of Traffic Classes[1]
   DSCP: af31[26]-Number of Traffic Classes[1]
   DSCP: ef[46]-Number of Traffic Classes[1]

------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 5: show domain master exits Field Descriptions***

| Field | Description |
|---|---|
| BR address | IP address of border routers configured at the hub site. |
| type | Type of interface. Internal or external. In this example, the type is external. |
| Path | Name of the path. |
| Egress capacity | Egress capacity of the interface. |
| DSCP | Number of traffic classed configured per DSCP on external interfaces. |

**Step 4** **show domain** *domain-name* **master peering**

This command displays the peering information of the hub-master controller.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- Peering state status
- Cent-policy status
- PMI status
- Globals service status

**Example:**

```
HubMC# show domain one master peering
```

```
------------------------------------------------------------------------------------------------------------------

*** Domain MC Status ***

Peering state: Enabled
Origin: Loopback0(10.8.3.3)
Peering type: Listener

Subscribed service:
   cent-policy (2) :
   site-prefix (1) :
      Last Notification Info: 00:23:15 ago, Size: 160, Compressed size: 144, Status: No Error, Count:
 3
   service-provider (4) :
   globals (5) :
      Last Notification Info: 00:03:09 ago, Size: 325, Compressed size: 218, Status: No Error, Count:
 6
   pmi (3) :

Published service:
   site-prefix (1) :
      Last Publish Info: 00:03:10 ago, Size: 209, Compressed size: 138, Status: No Error
   cent-policy (2) :
      Last Publish Info: 00:02:58 ago, Size: 2244, Compressed size: 468, Status: No Error
   pmi (3) :
      Last Publish Info: 02:03:12 ago, Size: 2088, Compressed size: 458, Status: No Error
   globals (5) :
      Last Publish Info: 00:03:09 ago, Size: 325, Compressed size: 198, Status: No Error

------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 6: show domain master peering Field Descriptions***

| Field | Description |
|---|---|
| Peering state | Status of peering. |
| Subscribed services | Lists the status of services subscribed to. |
| Published services | Services published by the hub-master controller to the remote sites. |

**Step 5** **show derived-config | section eigrp**

This command displays if EIGRP SAF is automatically configured.

Check the following fields in the output to ensure that the hub-master controller is configured accurately:

- EIGRP SAF configuration is auto enabled
- EIGRP SAF peering status between hub and branch sites

**Example:**

```
HubMC# show derived-config | section eigrp

------------------------------------------------------------------------------------------------------------------

router eigrp #AUTOCFG# (API-generated auto-configuration, not user configurable)
```

```
 !
 service-family ipv4 autonomous-system 59501
  !
  sf-interface Loopback0
   hello-interval 120
   hold-time 600
  exit-sf-interface
  !
  topology base
  exit-sf-topology
  remote-neighbors source Loopback0 unicast-listen
 exit-service-family
-------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 6** **show domain** *domain-name* **master discovered-sites**

This command displays the sites that are remotely connected to the hub site.

**Example:**

```
HubMC# show domain one master discovered-sites

------------------------------------------------------------------------------------------------------------------------

*** Domain MC DISCOVERED sites ***

   Number of sites: 3
 *Traffic classes [Performance based][Load-balance based]

Site ID: 255.255.255.255
  DSCP :default[0]-Number of traffic classes[0][0]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[0][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[0][0]

Site ID: 10.2.10.10
  DSCP :default[0]-Number of traffic classes[1][1]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[1][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[1][0]

Site ID: 10.2.11.11
  DSCP :default[0]-Number of traffic classes[0][0]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[0][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[0][0]

------------------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

# Verifying Hub Border Router Configurations

Use the following show commands in any order to verify the status of the hub border routers.

## SUMMARY STEPS

1. **show domain** *domain-name* **border status**
2. **show domain** *domain-name* **border peering**
3. **show platform software pfrv3 rp active smart-probe**
4. **show platform software pfrv3 fp active smart-probe**
5. **show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail**

## DETAILED STEPS

### Step 1 **show domain** *domain-name* **border status**

This command displays the status of the border routers configured at the hub site.

Check the following fields in the output to ensure that the hub-border routers are configured accurately:

- Border status is UP
- External interfaces are listed with the right path names
- Minimum requirement is met

**Example:**

```
HubBR# show domain one border status


------------------------------------------------------------------------------------------------------------------

      ****Border Status****

Instance Status: UP
Present status last updated: 02:07:43 ago
Loopback: Configured Loopback0 UP (10.8.2.2)
Master: 10.8.3.3
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:07:42
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
     Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
     Name: Tunnel200 Interface Index: 154 SNMP Index: 10 SP:INET Status: UP

Auto Tunnel information:

     Name:Tunnel0 if_index: 15
     Borders reachable via this tunnel: 10.8.2.2

------------------------------------------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

*Table 7: **show domain border status** Field Descriptions*

| Field | Description |
|---|---|
| Instance Status | Displays the instance status. |
| Master | IP address of the master controller. |
| Minimum Requirement | Displays the minimum requirement status of the border router. |
| External Wan interfaces | Displays the information of external interfaces configured on border router. |
| Auto Tunnel information | Displays the information of auto-tunnel configuration. |

**Step 2** **show domain** *domain-name* **border peering**

This command displays the border router peering status.

Check the following fields in the output to ensure that the hub-border router is configured accurately:

- Peering status
- PMI status
- Site-perfix status
- Globals service status

**Example:**

```
HubBR# show domain one border peering

------------------------------------------------------------------------------------------------------------

Peering state: Enabled
Origin: Loopback0(10.8.2.2)
Peering type: Peer(With 10.8.3.3)
Subscribed service:
     pmi (3) :
      Last Notification Info: 02:09:49 ago, Size: 2088, Compressed size: 478, Status:
No Error, Count: 1
     site-prefix (1) :
      Last Notification Info: 00:06:19 ago, Size: 128, Compressed size: 134, Status:
No Error, Count: 6
     globals (5) :
      Last Notification Info: 00:09:48 ago, Size: 325, Compressed size: 218, Status:
No Error, Count: 9

Published service:

------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

*Table 8: **show domain border peering** Field Descriptions*

| Field | Description |
|---|---|
| Peering state | Status of peering. |
| Peering type | Type of peering. In this example, the border router is peering with master-hub controller. |
| Subscribed service | Lists the status of services subscribed to. In this example, the following services are subscribed:<br>• pmi<br>• site-prefix<br>• globals |
| Published services | Services published by the hub-border routers to the remote sites. |

**Step 3** **show platform software pfrv3 rp active smart-probe**

**Note** To verify the status of a hub-border router on Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform software pfrv3 rp active smart-probe** command.

This command displays the PfRv3 smart probe status on a Cisco ASR 1000 Series Aggregation Services Router configured at the hub site.

**Example:**

```
HubBR# show platform software pfrv3 rp active smart-probe

------------------------------------------------------------------------------------------------------------------------

PfRv3 smart probe parameters :

Total number of PfRv3 smart probe: 1

Parameters :
  vrf id = 0
  Probe src = 10.8.3.3
  Src port = 18000, Dst port = 19000
  Unreach time = 1000, Probe period = 500
  Discovery = false
  Dscp bitmap = 0xffffffffffffffff
  interval = 10000
  Discovery_probe = true
  minimum prefix length = 28

------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 4** **show platform software pfrv3 fp active smart-probe**

**Note** To verify the smart probe status of a embedded-service- processor on Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform software pfrv3 fp active smart-probe** command.

This command displays the PfRv3 smart probe status on a Cisco ASR 1000 Series Aggregation Services Router configured at the hub site.

**Example:**

```
HubBR# show platform software pfrv3 fp active smart-probe

------------------------------------------------------------------------------------------------------------------------

PfRv3 smart probe parameters :

Total number of PfRv3 smart probe: 1

Parameters :
  vrf id = 0
  Probe src = 10.8.3.3
  Src port = 18000, Dst port = 19000
  Unreach time = 1000, Probe period = 500
  Discovery = false
  Dscp bitmap = 0xffffffffffffffff
  interval = 10000
  Discovery_probe = true
  minimum prefix length = 28

------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 5** **show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail**

**Note** To verify the platform hardware information for PfR v3 on Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail** command.

This command displays the platform hardware information on a Cisco ASR 1000 Series Aggregation Services Router configured at the hub site.

**Example:**

```
HubBR# show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail

------------------------------------------------------------------------------------------------------------------------

PfRv3 QFP CLIENT GLOBAL INFO

Number of Instances: 1

Instance
 hash val: 5
 tbl id: 0
 symmetry: Off
 discovery: Off
 discovery_probe: On
 probe info:
   probe src: 10.8.3.3, src port: 18000, dst port: 19000
   unreach time: 1000, probe period: 500
   dscp bitmap: 0xffffffffffffffff, interval: 10000
   mml: 28
 exmem info:
   PPE addr: 0xe80b7830
```

```
------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

## Verifying Branch Master Controller Configurations

Use the following show commands in any order to verify the status of the branch-master controller.

### SUMMARY STEPS

1. **show domain** *domain-name* **master status**
2. **show domain** *domain-name* **master policy**

### DETAILED STEPS

**Step 1** **show domain** *domain-name* **master status**

This command displays the status information of the branch-master controller.

Check the following fields in the output to ensure that the branch-master controller is configured accurately:

- External interfaces are listed with correct path names
- Minimum requirements are met
- Path names are correct

**Example:**

```
BRMC# show domain one master status

------------------------------------------------------------------------------------------------------------------------

   *** Domain MC Status ***

   Master VRF: Global

    Instance Type: Branch
    Instance id:   0
    Operational status: Up
    Configured status: Up
    Loopback IP Address: 10.2.10.10
    Load Balancing:
     Operational Status: Up
     Max Calculated Utilization Variance: 21%
     Last load balance attempt: 00:00:07 ago
     Last Reason: No channels yet for load balancing
    Total unbalanced bandwidth:
            External links: 5327 Kbps Internet links: 0 Kpbs
    Route Control: Enabled
    Mitigation mode Aggressive: Disabled
    Policy threshold variance: 20
    Minimum Mask Length: 28
    Sampling: off
    Minimum Requirement: Met
```

```
    Borders:
      IP address: 10.2.10.10
      Connection status: CONNECTED (Last Updated 02:03:22 ago )
      Interfaces configured:
         Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
             Number of default Channels: 0

         Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
             Number of default Channels: 0

         Tunnel if: Tunnel0
```

---

The following table describes the significant fields shown in the command output.

***Table 9: show domain master status Field Descriptions***

| Field | Description |
|---|---|
| Instance Type | Displays the instance type of the device. In this output, the device is configured as a branch. |
| Operational Status | Displays the operational status of the branch-master controller. |
| Configured Status | Displays the configuration status of the branch-master controller. |
| Load Balancing | Displays the load balancing status. If load balancing is enabled on the hub-master controller, the branch master controller receives load balanced traffic. |
| Borders | Displays the information of border routers connected to the branch-master controller, and external interfaces connected to path names. |

**Step 2** **show domain** *domain-name* **master policy**

This command displays the policy information received from the hub-master controller.

**Example:**

```
BRMC# show domain one master policy
```

```
---------------------------------------------------------------------------------------------------------------
class VOICE sequence 10
  path-preference MPLS fallback INET
  class type: Dscp Based
    match dscp ef policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class VIDEO sequence 20
  path-preference INET fallback MPLS
```

```
  class type: Dscp Based
    match dscp af41 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1
    match dscp cs4 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class CRITICAL sequence 30
  path-preference MPLS fallback INET
  class type: Dscp Based
    match dscp af31 policy custom
      priority 2 packet-loss-rate threshold 10.0 percent
      priority 1 one-way-delay threshold 600 msec
      priority 2 byte-loss-rate threshold 10.0 percent
      Number of Traffic classes using this policy: 1

class default
   match dscp all
------------------------------------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 10: show domain master policy Field Descriptions***

| Field | Description |
|---|---|
| class | Name of the class type. In this example, the following classes are listed:<br>• VOICE<br>• VIDEO<br>• CRITICAL |
| path-preference | Specifies the path preferred for the class type. |
| match | Specifies the DSCP value to match for a policy type. |
| priority | Specifies the detailed policy threshold per class, based on the DSCP or application. |

## Verifying Branch Border Configurations

Use the following show commands in any order to verify the status of the branch-border router.

### SUMMARY STEPS

1. **show domain** *domain-name* **border status**

2. **show eigrp service-family ipv4 neighbors detail**
3. **show domain** *domain-name* **master peering**
4. **show domain** *domain-name* **border pmi**
5. **show flow monitor type performance-monitor**

## DETAILED STEPS

**Step 1** **show domain** *domain-name* **border status**

This command displays the status information of the branch-border routers.

Check the following fields in the output to ensure that the branch-border routers are configured accurately:

- Border status is UP
- External interfaces are listed with the right path names
- Minimum requirement is met

**Example:**

```
BR# show domain one border status

------------------------------------------------------------------------------------------------------------------

*** Border Status ***

Instance Status: UP
Present status last updated: 02:11:47 ago
Loopback: Configured Loopback0 UP (10.2.10.10)
Master: 10.2.10.10
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:11:41
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
     Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
     Name: Tunnel200 Interface Index: 15 SNMP Index: 10 SP:INET Status: UP

Auto Tunnel information:

  Name:Tunnel0 if_index: 19
  Borders reachable via this tunnel:

------------------------------------------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

*Table 11: **show domain border status** Field Descriptions*

| Field | Description |
|---|---|
| Instance Status | Displays the instance status of the device. |

| Field | Description |
|---|---|
| Master | Displays the IP address of the local-master controller. |
| Connection Status with Master | Displays the connection status with master controller.<br>• UP - Indicates that the connection is successful and the policy information is communicated from the master controller to the border router. |
| External Wan Interfaces | Displays the information about external WAN tunnel interfaces connected to the branch-master controller. |

**Step 2** **show eigrp service-family ipv4 neighbors detail**

This command displays the SAF peering information of the local master controller.

**Example:**

```
BR# show eigrp service-family ipv4 neighbors detail

------------------------------------------------------------------------------------------------------------------------

EIGRP-SFv4 VR(#AUTOCFG#) Service-Family Neighbors for AS(59501)
H    Address                 Interface             Hold Uptime  SRTT  RTO  Q   Seq
                                                   (sec)         (ms)      Cnt Num
0    10.8.3.3                Lo0                   497 02:12:18   5   100  0   31
    Remote Static neighbor (static multihop)
    Version 17.0/4.0, Retrans: 0, Retries: 0, Prefixes: 6
    Topology-ids from peer - 0
Max Nbrs: 65535, Current Nbrs: 0

------------------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 3** **show domain** *domain-name* **master peering**

This command displays the peering information of the branch-master controller.

Check the following fields in the output to ensure that the branch-border routers are configured accurately:

- Peering status
- PMI status
- Site-perfix status
- Globals service status

**Example:**

```
BR# show domain one master peering

------------------------------------------------------------------------------------------------------------------------

Peering state: Enabled
Origin:        Loopback0(10.2.10.10)
Peering type:    Listener, Peer(With 10.8.3.3)
```

```
Subscribed service:
     cent-policy (2) :
       Last Notification Info: 00:24:15 ago, Size: 2244, Compressed size: 488, Status:
No Error, Count: 5
     site-prefix (1) :
       Last Notification Info: 00:24:15 ago, Size: 128, Compressed size: 134, Status:
No Error, Count: 35
     service-provider (4) :
     globals (5) :
       Last Notification Info: 00:24:15 ago, Size: 325, Compressed size: 218, Status:
No Error, Count: 19

Published service:
     site-prefix (1) :
       Last Publish Info: 00:49:11 ago, Size: 160, Compressed size: 124, Status: No
Error
     globals (5) :
       Last Publish Info: 10:29:09 ago, Size: 325, Compressed size: 198, Status: No
Error

------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the command output.

***Table 12: show domain master peering Field Descriptions***

| Field | Description |
|---|---|
| Peering state | Status of peering. |
| Subscribed services | Displays the subscribed services list. |
| Published services | Displays the services published by the branch-master controller to the branch-border routers. |

**Step 4** **show domain** *domain-name* **border pmi**

This command displays the performance monitor information applied on the external interfaces.

Check the following fields in the output to ensure that the branch-border router is configured accurately and performance monitors are correctly applied on external interfaces :

- Ingress policy activation
- Egress policy activation
- PMI status

**Example:**

```
BR# show domain one border pmi

****Pfrv3 PMI INFORMATION****

Ingress policy Pfrv3-Policy-Ingress-0-4:
Ingress policy activated on:
  Tunnel200 Tunnel100

[SNIP]

------------------------------------------------------------------------
```

```
Egress policy Pfrv3-Policy-Egress-0-3:
Egress policy activated on:
  Tunnel200 Tunnel100
------------------------------------------------------------------------
PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-1]
   Trigger Nbar:No
------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-2]
```

The fields shown above are self-explanatory.

**Step 5** **show flow monitor type performance-monitor**

This command displays the flow monitor information for passive-performance monitoring on the egress interface of WAN. The flow monitors are automatically generated.

Check the following fields in the output to ensure that the branch-border router is configured accurately:

- Cache type
- Flow monitor interval time
- Export spreading status

**Example:**

```
BR# show flow monitor type performance-monitor

Flow Monitor type performance-monitor MON-Egress-aggregate-0-48-9:
       Description :User defined
       Flow Record :CENT-FLOWREC-Egress-aggregate-0-11
     Flow Exporter :CENT_FLOW_EXP-2
        Cache type :synchronized
           entries :4000
          interval :30 (seconds)
      history size :0 (intervals)
           timeout :1 (intervals)
   export spreading:TRUE
 Interface applied :2

Flow Monitor type performance-monitor MON-Egress-prefix-learn-0-48-10:
       Description :User defined
       Flow Record :CENT-FLOWREC-Egress-prefix-learn-0-12
     Flow Exporter :CENT_FLOW_EXP-2
        Cache type :synchronized
           entries :700
          interval :30 (seconds)
      history size :0 (intervals)
           timeout :1 (intervals)
   export spreading:FALSE
 Interface applied :2

Flow Monitor type performance-monitor MON-Ingress-per-DSCP-0-48-11:
      Description :User defined
      Flow Record :CENT-FLOWREC-Ingress-per-DSCP-0-13
    Flow Exporter :not configured
       Cache type :synchronized
          entries :2000
         interval :30 (seconds)
     history size :0 (intervals)
          timeout :1 (intervals)
  export spreading:FALSE
```

```
Interface applied :2
```

The fields shown above are self-explanatory.

# Monitoring PfRv3

## Monitoring Site Prefix

Site prefixes are internal prefixes for each site. The site prefix database resides on both the master controller and the border routers. Site prefixes are learned from monitoring traffic moving in the egress direction on the WAN interface.

- The site prefix database at hub site learns the site prefixes and their origins from both local egress flow and advertisements from remote peers.
- The site prefix database at border router learns the site prefixes and their origins only from remote peer's advertisements.

**Note** By default, master controller and border routers age out all the site prefixes at a frequency of 24 hours.

### SUMMARY STEPS

1. **show domain** *domain-name* **master site-prefix**
2. **show domain** *domain-name* **border site-prefix**
3. **show domain** *domain-name* **border pmi | begin prefix-learn**

### DETAILED STEPS

**Step 1** **show domain** *domain-name* **master site-prefix**

This command displays the site- prefix status information of the hub master controller.

**Example:**

```
HubMC# show domain one master site-prefix

        Change will be published between 5-60 seconds
        Next Publish 00:54:41 later
        Prefix DB Origin: 10.8.3.3
        Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id             Site-prefix           Last Updated         Flag
-------------------------------------------------------------------------------------------------------
10.2.10.10         10.1.10.0/24           00:42:07  ago          S,
10.2.10.10         10.2.10.10/32          00:42:07  ago          S,
10.2.11.11         10.2.11.11/32          00:18:25  ago          S,
10.8.3.3           10.8.3.3/32            1d05h     ago          L,
10.8.3.3           10.8.0.0/16            1d05h     ago          C,
255.255.255.255    *10.0.0.0/8            1d05h     ago          T,
```

```
-------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 2** **show domain** *domain-name* **border site-prefix**

This command displays the site- prefix status information of the hub-border router.

**Example:**

```
HubBR# show domain one border site-prefix

         Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id           Site-prefix         Last Updated       Flag
-------------------------------------------------------------------------------------------------
10.2.10.10        10.1.10.0/24        00:59:12 ago        S,
10.2.11.11        10.1.11.0/24        01:14:42 ago        S,
10.2.10.10        10.2.10.10/32       01:08:04 ago        S,
10.2.11.11        10.2.11.11/32       01:22:01 ago        S,
10.8.3.3          10.8.3.3/32         01:30:22 ago        S,
10.8.3.3          10.8.0.0/16         01:30:22 ago        S,C,
255.255.255.255  *10.0.0.0/8          01:30:22 ago        S,T,
-------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 3** **show domain** *domain-name* **border pmi | begin prefix-learn**

This command displays the automatically learned site- prefix status information of the hub-border router.

**Example:**

```
HubBR# show domain one border pmi | begin prefix-learn

-------------------------------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-29]
    monitor-interval:30
    minimum-mask-length:28
    key-list:
      ipv4 source prefix
      ipv4 source mask
      routing vrf input
    Non-key-list:
      counter bytes long
      counter packets long
      timestamp absolute monitoring-interval start
   DSCP-list:N/A
   Class:CENT-Class-Egress-ANY-0-51

   Exporter-list:
     10.2.10.10
-------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

# Monitoring Traffic Classes

PfRv3 manages aggregation of flows called traffic classes. A traffic class is an aggregation of flow going to the same destination prefix, with the same DSCP and application name (if application-based policies are used).

Traffic classes are divided in the following groups:

- Performance traffic classes — This is the traffic class where the performance metrics is defined for the policy type.
- Non-performance traffic classes — This is the default traffic class and does not have any performance metrics associated with it.

The master-hub controller learns the traffic classes by monitoring the traffic moving in egress direction on WAN interface.

## SUMMARY STEPS

1. **show domain** *domain-name* **master traffic-classes summary**
2. **show domain** *domain-name* **master traffic-classes**
3. **show domain** *domain-name* **master traffic-classes policy** *policy-name*

## DETAILED STEPS

### Step 1 **show domain** *domain-name* **master traffic-classes summary**

This command displays the summary information of all the traffic classes.

**Example:**

```
HubMC# show domain one master traffic-classes summary

------------------------------------------------------------------------------------------------------------
APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
SP - SERVICE PROVIDER, PC = PRIMARY CHANNEL ID,
BC - BACKUP CHANNEL ID, BR - BORDER, EXIT - WAN INTERFACE
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN


Dst-Site-Pfx    Dst-Site-Id   APP     DSCP   TC-ID    APP-ID  State  SP
PC/BC      BR/EXIT
10.1.10.0/24    10.2.10.10    N/A     af11   193      N/A     CN     MPLS
59/60 10.8.2.2/Tunnel100
10.1.10.0/24    10.2.10.10    N/A     cs1    192      N/A     CN     MPLS
57/58 10.8.2.2/Tunnel100
10.1.10.0/24    10.2.10.10    N/A     cs5    191      N/A     CN     MPLS
55/NA 10.8.2.2/Tunnel100
10.1.10.0/24 10.2.10.10       N/A     ef     190      N/A     CN     MPLS
52/NA 10.8.2.2/Tunnel100
10.1.10.0/24    10.2.10.10    N/A     af41   195      N/A     CN     INET
64/63 10.8.1.1/Tunnel200
10.1.10.0/24    10.2.10.10    N/A     cs4    189      N/A     CN     INET
54/53 10.8.1.1/Tunnel200
10.1.10.0/24    10.2.10.10    N/A     af31   194      N/A     CN     MPLS
61/62 10.8.2.2/Tunnel100
 Total Traffic Classes: 7 Site: 7 Internet: 0

------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 2** **show domain** *domain-name* **master traffic-classes**

This command displays the status information of the traffic class for the hub-master controller.

**Example:**

```
HubMC# show domain one master traffic-classes

------------------------------------------------------------------------------------------------
Dst-Site-Prefix: 10.1.10.0/24         DSCP: af11 [10] Traffic class id:193
 TC Learned:                 00:22:13 ago
 Present State:              CONTROLLED
 Current Performance Status: not monitored (default class)
 Current Service Provider:   MPLS since 00:12:10
 Previous Service Provider:  INET for 298 sec
 BW Used:                    9195 Kbps
 Present WAN interface:      Tunnel100 in Border 10.8.2.2
 Present Channel (primary):  59
 Backup Channel:             60
 Destination Site ID:        10.2.10.10
 Class-Sequence in use:      default
 Class Name:                 default
 BW Updated:                 00:00:14 ago
 Reason for Route Change:    Load Balance
------------------------------------------------------------------------------------------------

Dst-Site-Prefix: 10.1.10.0/24        DSCP: cs1 [8] Traffic class id:192
 TC Learned:                00:22:14 ago
 Present State:             CONTROLLED
 Current Performance Status:not monitored (default class)
 Current Service Provider:  MPLS since 00:12:40
 Previous Service Provider: INET for 184 sec
 BW Used:                   9251 Kbps
 Present WAN interface:     Tunnel100 in Border 10.8.2.2
 Present Channel (primary): 57
 Backup Channel:            58
 Destination Site ID:       10.2.10.10
 Class-Sequence in use:     default
 Class Name:                default
 BW Updated: 00:00:12       ago
 Reason for Route Change:   Load Balance
.
.
.
------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 3** **show domain** *domain-name* **master traffic-classes policy** *policy-name*

This command displays the occurrence of performance issues in a policy traffic class.

**Example:**

```
HubMC# show domain one master traffic-classes policy VIDEO

------------------------------------------------------------------------------------------------
Dst-Site-Prefix: 10.1.10.0/24       DSCP: cs4 [32]      Traffic class id:200
 TC Learned:                 00:06:00 ago
 Present State:              CONTROLLED
 Current Performance Status: in-policy
```

```
 Current Service Provider:   MPLS since 00:00:30 (hold until 59 sec)
 Previous Service Provider:  INET for 117 sec
 (A fallback provider. Primary provider will be re-evaluated 00:02:30 later)
 BW Used:                    309 Kbps
 Present WAN interface:      Tunnel100 in Border 10.8.2.2
 Present Channel (primary):  76
 Backup Channel:             73
 Destination Site ID:        10.2.10.10
 Class-Sequence in use:      20
 Class Name:                 VIDEO using policy User-defined
   priority 2 packet-loss-rate threshold 5.0 percent
   priority 1 one-way-delay threshold 150 msec
   priority 2 byte-loss-rate threshold 5.0 percent
 BW Updated:                 00:00:03 ago
 Reason for Route Change:    Delay
.
.
.
-------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

### Cisco IOS XE Platform Commands

To view traffic-classes on Cisco IOS XE platform, use the following show commands in any order:

### SUMMARY STEPS

1. **show platform software pfrv3 rp active route-control traffic-class**
2. **show platform software pfrv3 fp active route-control traffic-class**
3. **show platform hardware qfp active feature pfrv3 client route-control traffic-class detail**
4. **show platform software interface rp active name** *interface-name*
5. **show platform software interface fp active name** *interface-name*
6. **show platform hardware qfp active interface if-name** *interface-name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show platform software pfrv3 rp active route-control traffic-class** | This command displays the traffic class information for a platform. |
| **Step 2** | **show platform software pfrv3 fp active route-control traffic-class** | This command displays the traffic class information for a platform. |
| **Step 3** | **show platform hardware qfp active feature pfrv3 client route-control traffic-class detail** | This command displays the hardware information for the configured policy. |
| **Step 4** | **show platform software interface rp active name** *interface-name* | This command displays the ingress interface information for PfRv3. |
| **Step 5** | **show platform software interface fp active name** *interface-name* | This command displays the ingress interface information for PfRv3. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show platform hardware qfp active interface if-name** *interface-name* | This command displays the interface information in a data plane path for PfRv3. |

## Monitoring Channels

A channel is a unique combination of destination site-Id, path name, and DSCP value. A channel is created when there is a new DSCP value, or an interface, or a site is added to the network. Performance is measured per channel on remote site and feedback is sent to the source site in case of performance failure.

### SUMMARY STEPS

1. **show domain** *domain-name* **master channels dscp ef**
2. **show domain** *domain-name* **master channels link-name** *path-name*
3. **show domain** *domain-name* **border channels**
4. **show domain** *domain-name* **border exporter statistics**
5. **show domain** *domain-name* **border channels parent-route**
6. **show domain** *domain-name* **border parent-route**

### DETAILED STEPS

**Step 1** **show domain** *domain-name* **master channels dscp ef**

This command displays channel information from the hub site. You can view the information of an active and backup channel using this command.

**Example:**

```
HubMC# show domain one master channels dscp ef

Legend: * (Value obtained from Network delay:)

Channel Id: 89   Dst Site-Id: 10.2.10.10 Link Name: MPLS DSCP: ef [46] TCs: 1
  Channel Created: 00:01:15 ago
  Provisional State: Initiated and open
  Operational state: Available
  Interface Id: 14
  Estimated Channel Egress Bandwidth: 5380 Kbps
  Immitigable Events Summary:
  Total Performance Count: 0, Total BW Count: 0
  TCA Statitics:
     Received 0 ; Processed 0 ; Unreach_rcvd:0

------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 2** **show domain** *domain-name* **master channels link-name** *path-name*

This command displays channel status information and the unreachable threshold crossing alerts (TCA) and on demand export (ODE) on a hub-master controller.

**Example:**

```
HubMC# show domain one master channels link-name INET

       Legend: * (Value obtained from Network delay:)

Channel Id: 25 Dst Site-Id: 10.2.10.10 Link Name: INET DSCP: default [0] TCs: 0
  Channel Created: 13:39:27 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Interface Id: 13
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated : 00:00:01 ago
    Packet Count : 0
    Byte Count : 0
    One Way Delay : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean : N/A
    Unreachable : TRUE
  ODE Stats Bucket Number: 2
   Last Updated : 00:00:57 ago
    Packet Count : 0
    Byte Count : 0
    One Way Delay : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean : N/A
    Unreachable : TRUE
   TCA Statitics:
     Received:4 ; Processed:1 ; Unreach_rcvd:4
  Latest TCA Bucket
    Last Updated : 00:00:01 ago
.
.
.
------------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 3** **show domain** *domain-name* **border channels**

This command displays channel information from the hub-border site.

**Example:**

```
HubBR# show domain one border channels

Border Smart Probe Stats:
-------------------------------------------------------------------------------------------------

Channel id: 21
 Channel dscp: 0
 Channel site: 255.255.255.255
 Channel interface: Tunnel200
 Channel operation state: Initiated_n_open
 Channel RX state: reachable
 Channel TX state: reachable
 Channel next hop: 0.0.0.0
 Channel recv_probes: 0
 Channel send_probes: 0
 Channel recv_packets: 0
```

```
 Channel send_packets: 0
 Channel recv_bytes: 0
 Channel send_bytes 0
 Last Probe Received: N/A
 Last Probe Sent: N/A
.
.
.
------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 4** **show domain** *domain-name* **border exporter statistics**

This command displays the border site exporter statistics information.

**Example:**

```
HubBR# show domain one border exporter statistics

show on-demand exporter(default vrf)

On-demand exporter
Border: 10.2.10.10
 Process ID: SEND=176, RECV=523

 Interface: Tunnel200 (index=15, service provider=INET)
  Bandwidth: Ingress=23464 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =7609 Kbit/sec, Capacity=50000 Kbit/sec

Total sent BW packets:               0
Total sent BW templates:             0, Last sent: not yet sent

 Interface: Tunnel100 (index=14, service provider=MPLS)
  Bandwidth: Ingress=30285 Kbit/sec, Capacity=50000 Kbit/sec
             Egress =3757 Kbit/sec, Capacity=50000 Kbit/sec

Total sent BW packets:               0
Total sent BW templates:             0, Last sent: not yet sent

Global Stats:
  Table ID lookup count: 0
  Table ID Channel found count: 0
  Table ID Next hop found count: 0
------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 5** **show domain** *domain-name* **border channels parent-route**

This command displays the parent route information of a border channel.

**Note** PRv3 determines parent route preference in the following order: NHRP cache (when spoke-to-spoke direct tunnels are established), BGP, EIGRP, static routes, and RIB. A less specific prefix match from a higher preferred protocol will be selected over a more specific prefix from a less preferred protocol source. For example, prefix 10.0.0.0/8 is available through BGP and a more specific path is available through EIGRP. IWAN will not follow the longest prefix match available through EIGRP but will select 10.0.0.0/8 from BGP.

**Example:**

```
HubBR# show domain one border channels parent route

Channel id: 21, Dscp: defa [0], Site-Id: 255.255.255.255, Path: INET, Interface: Tunnel200
 Nexthop: 0.0.0.0
 Protocol: None

Channel id: 23, Dscp: defa [0], Site-Id: 10.2.11.11, Path: INET, Interface: Tunnel200
 Nexthop: 10.0.200.11
 Protocol: BGP

Channel id: 25, Dscp: defa [0], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
 Nexthop: 10.0.200.10
 Protocol: BGP

Channel id: 88, Dscp: cs4 [20], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
 Nexthop: 10.0.200.10
 Protocol: BGP

Channel id: 91, Dscp: ef [2E], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
 Nexthop: 10.0.200.10
 Protocol: BGP

Channel id: 92, Dscp: af11 [A], Site-Id: 10.2.10.10, Path: INET, Interface: Tunnel200
 Nexthop: 10.0.200.10
 Protocol: BGP
------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

**Step 6** **show domain** *domain-name* **border parent-route**

This command displays the parent route information of a channel.

**Example:**

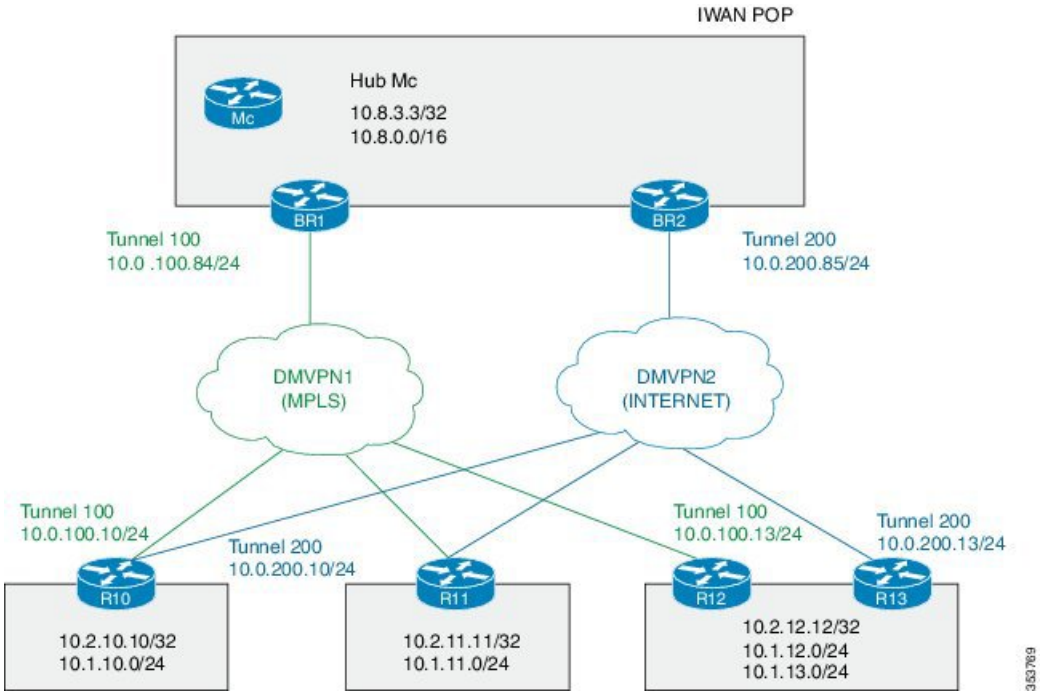
```
HubBR# show domain one border parent route

Border Parent Route Details:
Prot: BGP, Network: 10.2.10.10/32, Gateway: 10.0.200.10, Interface: Tunnel200, Ref count: 8
Prot: BGP, Network: 10.2.11.11/32, Gateway: 10.0.200.11, Interface: Tunnel200, Ref count: 1
------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

# Example: Configuring Performance Routing Version 3

Let us consider a use case scenario, where the service provider of a large enterprise network wants to optimize the WAN reliability and bandwidth of its network infrastructure based on applications between the head quarter site and branch sites. The service provider wants the network to intelligently choose a path that meets the performance requirement of its video-based applications over non-critical applications.

*Figure 3: PfRv3 Topology*




In this example, the following routers are used:

- Hub Master Controller — Cisco ASR 1002-X router configured with bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps and has a quad-core 2.13 GHz processor (with three memory options 4-GB, 8-GB, and 16-GB)
- Hub Border Routers — Cisco ASR 1002 Series Router configured with an Embedded Services Processor 5 (ESP5)
- Branch Routers — Cisco 4451X Integrated Services Router.

## Example: Configuring Hub Master Controller

### Configure the interfaces on hub master controller

```
HubMC> enable
HubMC# configure terminal
HubMC(config)# interface Loopback0
HubMC(config-if)# ip address 10.8.3.3 255.255.255.255
HubMC(config-if)# exit
```

### Configure the device as hub-master controller

```
HubMC(config)# domain one
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE
HubMC(config-domain-vrf-mc)# site-prefixes prefix-list DATA_CENTER_1
HubMC(config-domain-vrf-mc)# exit
```

### Configure IP prefix-lists

```
HubMC(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24
HubMC(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24
```

## Example: Configuring Domain Policies on Hub Master Controller

```
HubMC(config)# domain one
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# monitor-interval 2 dscp ef
HubMC(config-domain-vrf-mc)# load-balance
HubMC(config-domain-vrf-mc)# class VOICE sequence 10
HubMC(config-domain-vrf-mc-class)# match dscp ef policy voice
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc)# class VIDEO sequence 20
HubMC(config-domain-vrf-mc-class)# match dscp af41 policy real-time-video
HubMC(config-domain-vrf-mc-class)# match dscp cs4 policy real-time-video
HubMC(config-domain-vrf-mc-class)# path-preference INET fallback MPLS
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc)# class CRITICAL sequence 30
HubMC(config-domain-vrf-mc-class)# match dscp af31 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600
HubMC(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 600
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
```

## Example: Configuring Hub Border Routers

### Configure the interfaces on hub border router (BR1)

```
BR1> enable
BR1# configure terminal
BR1(config)# interface Loopback0
BR1(config-if)# ip address 10.8.1.1 255.255.255.255
BR1(config-if)exit
```

### Configure the device as border router (BR1)

```
BR1(config)# domain one
BR1(config-domain)# vrf default
BR1(config-domain-vrf)# border
BR1(config-domain-vrf-br)# source-interface Loopback0
BR1(config-domain-vrf-br)# master 10.8.3.3
BR1(config-domain-vrf-br)# exit
```

### Configure tunnel from BR1 to DMVPN1 (MPLS)Link

```
BR1(config)# interface Tunnel100
BR1(config-if)# bandwidth 100000
BR1(config-if)# ip address 10.0.100.84 255.255.255.0
BR1(config-if)# no ip redirects
BR1(config-if)# ip mtu 1400
```

```
BR1(config-if)# ip nhrp authentication cisco
BR1(config-if)# ip nhrp map multicast dynamic
BR1(config-if)# ip nhrp network-id 1
BR1(config-if)# ip nhrp holdtime 600
BR1(config-if)# ip tcp adjust-mss 1360
BR1(config-if)# load-interval 30
BR1(config-if)# tunnel source GigabitEthernet3
BR1(config-if)# tunnel mode gre multipoint
BR1(config-if)# tunnel key 100
BR1(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
BR1(config-if)# domain one path MPLS
```

### Configure the interfaces on hub border router (BR2)

```
BR2> enable
BR2# configure terminal
BR2(config)# interface Loopback0
BR2(config-if)# ip address 10.8.2.2 255.255.255.255
BR2(config-if)# exit
```

### Configure the device as border router (BR2)

```
BR2(config)# domain one
BR2(config-domain)# vrf default
BR2(config-domain-vrf)# border
BR2(config-domain-vrf-br)# source-interface Loopback0
BR2(config-domain-vrf-br)# master 10.8.3.3
BR2(config-domain-vrf-br)# exit
```

### Configure tunnel from BR2 to DMVPN2 (INTERNET)Link

```
BR2(config)# interface Tunnel200
BR2(config-if)# bandwidth 50000
BR2(config-if)# ip address 10.0.200.85 255.255.255.0
BR2(config-if)# no ip redirects
BR2(config-if)# ip mtu 1400
BR2(config-if)# ip nhrp authentication cisco
BR2(config-if)# ip nhrp map multicast dynamic
BR2(config-if)# ip nhrp network-id 2
BR2(config-if)# ip nhrp holdtime 600
BR2(config-if)# ip tcp adjust-mss 1360
BR2(config-if)# load-interval 30
BR2(config-if)# delay 1000
BR2(config-if)# tunnel source GigabitEthernet3
BR2(config-if)# tunnel mode gre multipoint
BR2(config-if)# tunnel key 200
BR2(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
BR2(config-if)# domain one path INET
```

## Example: Configuring Branch Routers (Single CPE)

### Configure the interfaces (R10)

```
R10> enable
R10# configure terminal
R10(config)# interface Loopback0
R10(config-if)# ip address 10.2.10.10 255.255.255.255
R10(config-if)exit
```

### Configure the device as branch master controller (R10)

```
R10(config)# domain one
R10(config-domain)# vrf default
R10(config-domain-vrf)# border
R10(config-domain-vrf-br)# source-interface Loopback0
R10(config-domain-vrf-br)# master local
R10(config-domain-vrf-br)# exit
R10(config-domain-vrf)# master branch
R10(config-domain-vrf-mc)# source-interface Loopback0
R10(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R10

```
R10(config)# interface Tunnel100
R10(config-if)# bandwidth 100000
R10(config-if)# ip address 10.0.100.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map 10.0.100.84 172.16.84.4
R10(config-if)# ip nhrp map multicast 172.16.84.4
R10(config-if)# ip nhrp network-id 1
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.100.84
R10(config-if)# ip nhrp registration timeout 60
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# tunnel source GigabitEthernet2
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 100
R10(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
```

### Configure another tunnel path from R10

```
R10(config)# interface Tunnel200
R10(config-if)# bandwidth 50000
R10(config-if)# ip address 10.0.200.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R10(config-if)# ip nhrp multicast 172.16.85.5
R10(config-if)# ip nhrp network-id 2
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.200.85
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# tunnel source GigabitEthernet3
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 200
R10(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
```

### Configure the interfaces (R11)

```
R11> enable
R11# configure terminal
R11(config)# interface Loopback0
R11(config-if)# ip address 10.2.11.11 255.255.255.255
R11(config-if)# exit
```

### Configure the device as branch master controller (R11)

```
R11(config)# domain one
R11(config-domain)# vrf default
R11(config-domain-vrf)# border
R11(config-domain-vrf-br)# source-interface Loopback0
R11(config-domain-vrf-br)# master local
R11(config-domain-vrf-br)# exit
R11(config-domain-vrf)# master branch
R11(config-domain-vrf-mc)# source-interface Loopback0
R11(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R11

```
R11(config)# interface Tunnel100
R11(config-if)# bandwidth 100000
R11(config-if)# ip address 10.0.100.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map 10.0.100.84 172.16.84.4
R11(config-if)# ip nhrp map multicast 172.16.84.4
R11(config-if)# ip nhrp network-id 1
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nhs 10.0.100.84
R11(config-if)# ip nhrp registration timeout 60
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# tunnel source GigabitEthernet2
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 100
R11(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
```

### Configure another tunnel path from R11

```
R11(config)# interface Tunnel200
R11(config-if)# bandwidth 50000
R11(config-if)# ip address 10.0.200.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R11(config-if)# ip nhrp multicast 172.16.85.5
R11(config-if)# ip nhrp network-id 2
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nhs 10.0.200.85
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# tunnel source GigabitEthernet3
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 200
R11(config-if)# tunnel vrf INET2
R11(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
```

## Example: Configuring Branch Routers (Dual CPE)

### Configure the interfaces (R12)

```
R12> enable
R12# configure terminal
R12(config)# interface Loopback0
R12(config-if)# ip address 10.2.12.12 255.255.255.255
R12(config-if)# exit
```

### Configure the device as branch master controller (R12)

```
R12(config)# domain one
R12(config-domain)# vrf default
R12(config-domain-vrf)# border
R12(config-domain-vrf-br)# source-interface Loopback0
R12(config-domain-vrf-br)# master local
R12(config-domain-vrf-br)# exit
R12(config-domain-vrf)# master branch
R12(config-domain-vrf-mc)# source-interface Loopback0
R12(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R12

```
R12(config)# interface Tunnel100
R12(config-if)# bandwidth 100000
R12(config-if)# ip address 10.0.100.13 255.255.255.0
R12(config-if)# no ip redirects
R12(config-if)# ip mtu 1400
R12(config-if)# ip nhrp authentication cisco
R12(config-if)# ip nhrp map 10.0.100.84 172.16.84.4
R12(config-if)# ip nhrp map multicast 172.16.84.4
R12(config-if)# ip nhrp network-id 1
R12(config-if)# ip nhrp holdtime 600
R12(config-if)# ip nhrp nhs 10.0.100.84
R12(config-if)# ip nhrp registration timeout 60
R12(config-if)# ip tcp adjust-mss 1360
R12(config-if)# load-interval 30
R12(config-if)# delay 1000
R12(config-if)# tunnel source GigabitEthernet3
R12(config-if)# tunnel mode gre multipoint
R12(config-if)# tunnel key 100
R12(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
```

### Configure the interfaces (R13)

```
R13> enable
R13# configure terminal
R13(config)# interface Loopback0
R13(config-if)# ip address 10.2.13.13 255.255.255.255
R13(config-if)# exit
```

### Configure the device as a border router with R12 as the master controller (R13)

```
R13(config)# domain one
R13(config-domain)# vrf default
R13(config-domain-vrf)# border
R13(config-domain-vrf-br)# source-interface Loopback0
R13(config-domain-vrf-br)# master 10.2.12.12
```

### Configure the tunnel interface and tunnel path from R13

```
R13(config)# interface Tunnel200
R13(config-if)# bandwidth 50000
```

```
R13(config-if)# ip address 10.0.200.13 255.255.255.0
R13(config-if)# no ip redirects
R13(config-if)# ip mtu 1400
R13(config-if)# ip nhrp authentication cisco
R13(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R13(config-if)# ip nhrp multicast 172.16.85.5
R13(config-if)# ip nhrp network-id 2
R13(config-if)# ip nhrp holdtime 600
R13(config-if)# ip nhrp nhs 10.0.200.85
R13(config-if)# ip tcp adjust-mss 1360
R13(config-if)# load-interval 30
R13(config-if)# delay 1000
R13(config-if)# tunnel source GigabitEthernet6
R13(config-if)# tunnel mode gre multipoint
R13(config-if)# tunnel key 200
R13(config-if)# tunnel vrf INET2
R13(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
```

### Verifying PfRv3 Configuration

To verify the PfRv3 configuration, use the following show commands in any order:

**show domain** *domain-name* **master status**

```
HubMC# show domain one master status

------------------------------------------------------------------------------------------------------------------
*** Domain MC Status ***

Master VRF: Global

Instance Type: Hub
Instance id: 0
Operational status: Up
Configured status: Up
Loopback IP Address: 10.8.3.3
Load Balancing:
 Admin Status: Enabled
 Operational Status: Up
 Enterprise top level prefixes configured: 1
 Max Calculated Utilization Variance: 1%
 Last load balance attempt: 00:27:23 ago
 Last Reason: Variance less than 20%
 Total unbalanced bandwidth:
       External links: 0 Kbps Internet links: 0 Kpbs
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
Minimum Mask Length: 28
Sampling: off

Borders:
  IP address: 10.8.2.2
  Connection status: CONNECTED (Last Updated 1d11h ago )
  Interfaces configured:
    Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
        Number of default Channels: 3

  Tunnel if: Tunnel0

  IP address: 10.8.1.1
  Connection status: CONNECTED (Last Updated 1d11h ago )
  Interfaces configured:
```

```
    Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
        Number of default Channels: 3

  Tunnel if: Tunnel0
--------------------------------------------------------------------------------
```

### show domain *domain-name* master discovered-sites

```
HubMC# show domain one master discovered-sites

------------------------------------------------------------------------------------------------------------------------

*** Domain MC DISCOVERED sites ***

Number of sites: 3

*Traffic classes [Performance based][Load-balance based]

Site ID: 255.255.255.255
  DSCP :default[0]-Number of traffic classes[0][0]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[0][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[0][0]

Site ID: 10.2.10.10
  DSCP :default[0]-Number of traffic classes[1][1]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[1][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[1][0]

Site ID: 10.2.11.11
  DSCP :default[0]-Number of traffic classes[0][0]
  DSCP :af31[26]-Number of traffic classes[0][0]
  DSCP :cs4[32]-Number of traffic classes[0][0]
  DSCP :af41[34]-Number of traffic classes[0][0]
  DSCP :cs5[40]-Number of traffic classes[0][0]
  DSCP :ef[46]-Number of traffic classes[0][0]

------------------------------------------------------------------------------------------------------------------------
```

### show domain *domain-name* border status

```
HubBR# show domain one border status


------------------------------------------------------------------------------------------------------------------------
****Border Status****

Instance Status: UP
Present status last updated: 02:07:43 ago
Loopback: Configured Loopback0 UP (10.8.2.2)
Master: 10.8.3.3
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:07:42
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
```

```
Minimum Requirement: Met
External Wan interfaces:
    Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP

Auto Tunnel information:
    Name:Tunnel0 if_index: 15
    Borders reachable via this tunnel: 10.8.2.2

------------------------------------------------------------------------------------------------------
```

### show platform software pfrv3 rp active smart-probe

```
HubBR# show platform software pfrv3 rp active smart-probe

------------------------------------------------------------------------------------------------------

PfRv3 smart probe parameters :

Total number of PfRv3 smart probe: 1

Parameters :
  vrf id = 0
  Probe src = 10.8.3.3
  Src port = 18000, Dst port = 19000
  Unreach time = 1000, Probe period = 500
  Discovery = false
  Dscp bitmap = 0xffffffffffffffff
  interval = 10000
  Discovery_probe = true
  minimum prefix length = 28

------------------------------------------------------------------------------
```

### show derived-config | section eigrp

```
HubMC# show derived-config | section eigrp

------------------------------------------------------------------------------------------------------

router eigrp #AUTOCFG# (API-generated auto-configuration, not user configurable)
 !
 service-family ipv4 autonomous-system 59501
  !
  sf-interface Loopback0
   hello-interval 120
   hold-time 600
  exit-sf-interface
  !
  topology base
  exit-sf-topology
  remote-neighbors source Loopback0 unicast-listen
 exit-service-family
------------------------------------------------------------------------------
```

### show domain *domain-name* master policy

```
HubMC# show domain one master policy

No Policy publish pending
------------------------------------------------------------------------------------------------------
class VOICE sequence 10
  path-preference MPLS fallback INET
```

```
  class type: Dscp Based
    match dscp ef policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class VIDEO sequence 20
  path-preference INET fallback MPLS
  class type: Dscp Based
    match dscp af41 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1
    match dscp cs4 policy custom
      priority 2 packet-loss-rate threshold 5.0 percent
      priority 1 one-way-delay threshold 150 msec
      priority 2 byte-loss-rate threshold 5.0 percent
      Number of Traffic classes using this policy: 1

class CRITICAL sequence 30
  path-preference MPLS fallback INET
  class type: Dscp Based
    match dscp af31 policy custom
      priority 2 packet-loss-rate threshold 10.0 percent
      priority 1 one-way-delay threshold 600 msec
      priority 2 byte-loss-rate threshold 10.0 percent
      Number of Traffic classes using this policy: 1

class default
  match dscp all
    Number of Traffic classes using this policy: 3
------------------------------------------------------------------------------------------------------
```

### show domain *domain-name* border pmi

```
BR# show domain one border pmi

****Pfrv3 PMI INFORMATION****
Ingress policy Pfrv3-Policy-Ingress-0-4:
Ingress policy activated on:
Tunnel200 Tunnel100
[SNIP]
------------------------------------------------------------------------
Egress policy Pfrv3-Policy-Egress-0-3:
Egress policy activated on:
Tunnel200 Tunnel100
------------------------------------------------------------------------
PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-1]
Trigger Nbar:No
------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-2]
With application based policy:
```

### show ip access-lists dynamic

```
BR# show ip access-lists dynamic

Extended IP access list mma-dvmc-acl#3
10 deny ip any 224.0.0.0 15.255.255.255
20 deny ip any any dscp cs6
```

```
30 permit tcp any any
40 permit udp any neq 18000 any neq 19000
50 permit icmp any any
```

### show domain *domain-name* master site-prefix

```
HubMC# show domain one master site-prefix

Change will be published between 5-60 seconds
Next Publish 00:54:41 later
Prefix DB Origin: 10.8.3.3
Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id          Site-prefix          Last Updated           Flag
-----------------------------------------------------------------------------------------------
10.2.10.10       10.1.10.0/24          00:42:07 ago           S,
10.2.10.10       10.2.10.10/32         00:42:07 ago           S,
10.2.11.11       10.2.11.11/32         00:18:25 ago           S,
10.8.3.3         10.8.3.3/32           1d05h    ago           L,
10.8.3.3         10.8.0.0/16           1d05h    ago           C,
255.255.255.255  *10.0.0.0/8           1d05h    ago           T,
-----------------------------------------------------------------------------------------------
```

### show domain *domain-name* border site-prefix

```
HubBR# show domain one border site-prefix

Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;

Site-id             Site-prefix         Last Updated     Flag
-----------------------------------------------------------------------------------------------
10.2.10.10          10.1.10.0/24        00:59:12 ago       S,
10.2.11.11          10.1.11.0/24        01:14:42 ago       S,
10.2.10.10          10.2.10.10/32       01:08:04 ago       S,
10.2.11.11          10.2.11.11/32       01:22:01 ago       S,
10.8.3.3            10.8.3.3/32         01:30:22 ago       S,
10.8.3.3            10.8.0.0/16         01:30:22 ago       S,C,
255.255.255.255     *10.0.0.0/8         01:30:22 ago       S,T,
-----------------------------------------------------------------------------------------------
```

### show domain *domain-name* master traffic-classess summary

```
HubMC# show domain one master traffic-classes summary

-----------------------------------------------------------------------------------------------
APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
SP - SERVICE PROVIDER, PC = PRIMARY CHANNEL ID,
BC - BACKUP CHANNEL ID, BR - BORDER, EXIT - WAN INTERFACE
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN

Dst-Site-Pfx   Dst-Site-Id   APP   DSCP   TC-ID   APP-ID   State    SP
PC/BC     BR/EXIT
10.1.10.0/24   10.2.10.10    N/A   af11   193     N/A      CN       MPLS
59/60 10.8.2.2/Tunnel100
10.1.10.0/24   10.2.10.10    N/A   cs1    192     N/A      CN       MPLS
57/58 10.8.2.2/Tunnel100
10.1.10.0/24   10.2.10.10    N/A   cs5    191     N/A      CN       MPLS
55/NA 10.8.2.2/Tunnel100
10.1.10.0/24   10.2.10.10    N/A   ef     190     N/A      CN       MPLS
52/NA 10.8.2.2/Tunnel100
10.1.10.0/24   10.2.10.10    N/A   af41   195     N/A      CN       INET
64/63 10.8.1.1/Tunnel200
10.1.10.0/24   10.2.10.10    N/A   cs4    189     N/A      CN       INET
54/53 10.8.1.1/Tunnel200
10.1.10.0/24   10.2.10.10    N/A   af31   194     N/A      CN       MPLS
61/62 10.8.2.2/Tunnel100
```

```
 Total Traffic Classes: 7 Site: 7 Internet: 0
------------------------------------------------------------------------------------------
```

### show domain *domain-name* master traffic-classess policy

```
HubMC# show domain one master traffic-classes policy VIDEO

------------------------------------------------------------------------------------------
Dst-Site-Prefix:  10.1.10.0/24    DSCP: cs4 [32]    Traffic class id:200
   TC Learned:                   00:06:00 ago
   Present State:                CONTROLLED
   Current Performance Status:   in-policy
   Current Service Provider:     MPLS since 00:00:30 (hold until 59 sec)
   Previous Service Provider:    INET for 117 sec
  (A fallback provider. Primary provider will be re-evaluated 00:02:30 later)
   BW Used:                      309 Kbps
   Present WAN interface:        Tunnel100 in Border 10.8.2.2
   Present Channel (primary):    76
   Backup Channel:               73
   Destination Site ID:          10.2.10.10
   Class-Sequence in use:        20
   Class Name:                   VIDEO using policy User-defined
     priority 2 packet-loss-rate threshold 5.0 percent
     priority 1 one-way-delay threshold 150 msec
     priority 2 byte-loss-rate threshold 5.0 percent
   BW Updated: 00:00:03 ago
   Reason for Route Change: Delay
.
.
.
------------------------------------------------------------------------------------------
```

### show running-config

```
HubMC# show running-config

------------------------------------------------------------------------------------------

Building configuration...
Current configuration : 5137 bytes
!
! Last configuration change at 02:37:06 CST Mon Nov 3 2014
! NVRAM config last updated at 02:35:51 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubMC
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
no logging console
!
no aaa new-model
```

```
clock timezone CST 8 0
!
!
!
no ip domain lookup
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
master hub
source-interface Loopback0
site-prefixes prefix-list DC1_PREFIX
monitor-interval 2 dscp cs5
monitor-interval 2 dscp ef
load-balance
enterprise-prefix prefix-list ENTERPRISE_PREFIX
class VOICE sequence 10
match dscp ef policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
path-preference MPLS fallback INET
class VIDEO sequence 20
match dscp af41 policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
match dscp cs4 policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
path-preference INET fallback MPLS
class CRITICAL sequence 30
match dscp af31 policy custom
priority 2 loss threshold 10
priority 1 one-way-delay threshold 600
path-preference MPLS fallback INET
!
!
license udi pid CSR1000V sn 90KU0SDCWNB
license boot level ax
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
!
!
!
!
!
```

```
!
interface Loopback0
ip address 10.8.3.3 255.255.255.255
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.208 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
no ip address
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet2.100
encapsulation dot1Q 100
ip address 10.8.101.1 255.255.255.0
!
interface GigabitEthernet2.101
encapsulation dot1Q 101
ip address 10.8.102.1 255.255.255.0
!
interface GigabitEthernet2.102
encapsulation dot1Q 102
ip address 10.8.103.1 255.255.255.0
!
interface GigabitEthernet2.103
encapsulation dot1Q 103
ip address 10.8.104.1 255.255.255.0
!
interface GigabitEthernet3
description --INTERNAL--
ip address 10.8.24.2 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet4
description --INTERNAL--
ip address 10.8.25.2 255.255.255.0
speed 1000
no negotiation auto
!
!
router eigrp 100
network 10.8.3.3 0.0.0.0
network 10.8.24.0 0.0.0.255
network 10.8.25.0 0.0.0.255
redistribute connected
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1_PREFIX seq 10 permit 10.8.0.0/16
!
ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
no service-routing capabilities-manager
```

```
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login
!
ntp logging
ntp source Loopback0
ntp master 3
!
end
```

---

### show running-config

```
HubBR1# show running-config
```

---

```
Building configuration...
Current configuration : 5312 bytes
!
! Last configuration change at 02:31:02 CST Mon Nov 3 2014
! NVRAM config last updated at 02:31:02 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubBR1
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET1
rd 65512:1
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
```

```
!
!
!
!
no ip domain lookup
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
border
source-interface Loopback0
master 10.8.3.3
!
!
license udi pid CSR1000V sn 952V3LWQECD
license boot level ax
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp performance
crypto isakmp profile ISAKMP-INET1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0
!
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET1
!
```

```
!
!
!
!
!
!
!
!
interface Loopback0
ip address 10.8.1.1 255.255.255.255
!
interface Tunnel100
bandwidth 100000
ip address 10.0.100.84 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
load-interval 30
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel key 100
tunnel protection ipsec profile DMVPN-PROFILE1
domain one path MPLS
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.210 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description --INTERNAL--
ip address 10.8.24.4 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet3
description --MPLS--
ip address 172.16.84.4 255.255.255.0
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet4
no ip address
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet5
ip address 101.1.4.1 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet6
no ip address
speed 1000
no negotiation auto
!
!
```

```
router eigrp 100
network 10.8.2.2 0.0.0.0
network 10.8.24.0 0.0.0.255
redistribute bgp 10 metric 100000 1 255 255 1500
distance eigrp 90 210
!
router ospf 100
router-id 10.8.1.1
network 172.16.84.4 0.0.0.0 area 0
!
router bgp 10
bgp router-id 10.8.1.1
bgp log-neighbor-changes
bgp listen range 10.0.100.0/24 peer-group MPLS-SPOKES
neighbor MPLS-SPOKES peer-group
neighbor MPLS-SPOKES remote-as 10
neighbor MPLS-SPOKES timers 20 60
!
address-family ipv4
bgp redistribute-internal
network 10.8.1.1 mask 255.255.255.255
network 10.8.3.3 mask 255.255.255.255
network 10.8.101.0 mask 255.255.255.0
network 10.8.102.0 mask 255.255.255.0
network 10.8.103.0 mask 255.255.255.0
network 10.8.104.0 mask 255.255.255.0
aggregate-address 10.8.0.0 255.255.0.0 summary-only
neighbor MPLS-SPOKES activate
neighbor MPLS-SPOKES send-community
neighbor MPLS-SPOKES default-originate
neighbor MPLS-SPOKES route-map MPLS-DC1-IN in
neighbor MPLS-SPOKES route-map MPLS-DC1-OUT out
distance bgp 20 109 109
exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-DMVPN permit 10:100
ip community-list standard INET-DMVPN permit 10:200
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1-LOCAL-ROUTES seq 10 permit 0.0.0.0/0
ip prefix-list DC1-LOCAL-ROUTES seq 20 permit 10.8.0.0/16 le 32
no service-routing capabilities-manager
!
route-map MPLS-DC1-IN deny 10
match ip address prefix-list DC1-LOCAL-ROUTES
!
route-map MPLS-DC1-IN permit 20
set community 10:100
!
route-map TO-PEER permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set ip next-hop self
set community no-advertise
!
route-map site_prefixes permit 10
```

```
match ip address prefix-list site_prefixes
!
route-map MPLS-DC1-OUT permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set community 10:100
!
route-map MPLS-DC1-OUT permit 20
description readvertise routes learned from MPLS DMVPN cloud
match community MPLS-DMVPN
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

---

### show running-config

```
HubBR2# show running-config
```

---

```
Current configuration : 5254 bytes
!
! Last configuration change at 02:30:54 CST Mon Nov 3 2014
! NVRAM config last updated at 02:25:26 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname HubBR2
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
rd 65512:2
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
```

```
exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
no ip domain lookup
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
border
source-interface Loopback0
master 10.8.3.3
!
!
license udi pid CSR1000V sn 94EFH1HPLI9
license boot level ax
spanning-tree extend system-id
!
!
redundancy
99
mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING2 vrf INET2
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp performance
crypto isakmp profile ISAKMP-INET2
keyring DMVPN-KEYRING2
match identity address 0.0.0.0 INET2
!
```

```
crypto ipsec security-association replay disable
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE2
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
!
!
interface Loopback0
ip address 10.8.2.2 255.255.255.255
!
interface Tunnel200
bandwidth 50000
ip address 10.0.200.85 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 2
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
load-interval 30
delay 1000
tunnel source GigabitEthernet4
tunnel mode gre multipoint
tunnel key 200
100
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
domain one path INET
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.209 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description --INTERNAL--
ip address 10.8.25.5 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet3
ip address 101.1.4.2 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet4
description --INET--
vrf forwarding INET2
ip address 172.16.85.5 255.255.255.0
load-interval 30
speed 1000
```

```
no negotiation auto
!
!
router eigrp 100
network 10.8.1.1 0.0.0.0
network 10.8.25.0 0.0.0.255
redistribute bgp 10 metric 100000 1 255 255 1500
distance eigrp 90 210
!
router ospf 100 vrf INET2
router-id 10.8.2.2
network 172.16.85.5 0.0.0.0 area 0
!
router bgp 10
bgp router-id 10.8.2.2
bgp log-neighbor-changes
bgp listen range 10.0.200.0/24 peer-group INET-SPOKES
neighbor INET-SPOKES peer-group
neighbor INET-SPOKES remote-as 10
neighbor INET-SPOKES timers 20 60
!
address-family ipv4
bgp redistribute-internal
network 10.8.2.2 mask 255.255.255.255
network 10.8.3.3 mask 255.255.255.255
network 10.8.101.0 mask 255.255.255.0
network 10.8.102.0 mask 255.255.255.0
network 10.8.103.0 mask 255.255.255.0
network 10.8.104.0 mask 255.255.255.0
aggregate-address 10.8.0.0 255.255.0.0 summary-only
neighbor INET-SPOKES activate
neighbor INET-SPOKES send-community
neighbor INET-SPOKES default-originate
neighbor INET-SPOKES route-map INET-DC1-IN in
neighbor INET-SPOKES route-map INET-DC1-OUT out
distance bgp 20 109 109
exit-address-family
!
!
101
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-DMVPN permit 10:100
ip community-list standard INET-DMVPN permit 10:200
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list DC1-LOCAL-ROUTES seq 10 permit 0.0.0.0/0
ip prefix-list DC1-LOCAL-ROUTES seq 20 permit 10.8.0.0/16 le 32
no service-routing capabilities-manager
!
route-map INET-DC1-IN deny 10
match ip address prefix-list DC1-LOCAL-ROUTES
!
route-map INET-DC1-IN permit 20
set community 10:200
!
route-map TO-PEER permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
```

```
set ip next-hop self
set community no-advertise
!
route-map site_prefixes permit 10
match ip address prefix-list site_prefixes
!
route-map INET-DC1-OUT permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set community 10:200
!
route-map INET-DC1-OUT permit 20
description readvertise routes learned from INTERNET DMVPN cloud
match community INET-DMVPN
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

---

### show running-config

```
BR10# show running-config
```

---

```
Building configuration...
Current configuration : 8517 bytes
!
! Last configuration change at 02:29:54 CST Mon Nov 3 2014
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial
!
hostname Branch10
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
rd 65512:2
!
address-family ipv4
```

```
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
border
source-interface Loopback0
master local
master branch
source-interface Loopback0
hub 10.8.3.3
!
!
license udi pid CSR1000V sn 92WYKUIJKRO
license boot level ax
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
```

```
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
!
crypto keyring DMVPN-KEYRING1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring DMVPN-KEYRING2 vrf INET2
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 40 5
crypto isakmp profile ISAKMP-INET1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0
crypto isakmp profile ISAKMP-INET2
keyring DMVPN-KEYRING2
match identity address 0.0.0.0 INET2
!
crypto ipsec security-association idle-time 60
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET1
!
crypto ipsec profile DMVPN-PROFILE2
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
!
interface Loopback0
ip address 10.2.10.10 255.255.255.255
!
interface Tunnel100
bandwidth 100000
ip address 10.0.100.10 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map 10.0.100.84 172.16.84.4
ip nhrp map multicast 172.16.84.4
ip nhrp network-id 1
ip nhrp holdtime 600
ip nhrp nhs 10.0.100.84
ip nhrp registration timeout 60
ip nhrp shortcut
```

```
ip tcp adjust-mss 1360
load-interval 30
delay 1000
tunnel source GigabitEthernet2
tunnel mode gre multipoint
tunnel key 100
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
bandwidth 50000
ip address 10.0.200.10 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map 10.0.200.85 172.16.85.5
ip nhrp map multicast 172.16.85.5
ip nhrp network-id 2
ip nhrp holdtime 600
ip nhrp nhs 10.0.200.85
ip nhrp registration timeout 60
ip nhrp shortcut
ip tcp adjust-mss 1360
load-interval 30
delay 1000
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel key 200
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.212 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description --MPLS--
ip address 172.16.101.10 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet3
description --INET--
vrf forwarding INET2
ip address 172.16.102.10 255.255.255.0
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet4
no ip address
speed 1000
no negotiation auto
!
interface GigabitEthernet5
no ip address
speed 1000
no negotiation auto
!
interface GigabitEthernet5.100
encapsulation dot1Q 100
ip address 10.1.10.1 255.255.255.0
!
router ospf 200 vrf INET2
```

```
network 172.16.102.10 0.0.0.0 area 0
!
router ospf 100
router-id 10.2.10.10
network 101.7.7.2 0.0.0.0 area 0
network 172.16.101.10 0.0.0.0 area 0
!
router bgp 10
bgp router-id 10.2.10.10
bgp log-neighbor-changes
neighbor MPLS-HUB peer-group
neighbor MPLS-HUB remote-as 10
neighbor MPLS-HUB timers 20 60
neighbor INET-HUB peer-group
neighbor INET-HUB remote-as 10
neighbor INET-HUB timers 20 60
neighbor 10.0.100.84 peer-group MPLS-HUB
neighbor 10.0.200.85 peer-group INET-HUB
!
address-family ipv4
network 10.1.10.0 mask 255.255.255.0
network 10.2.10.10 mask 255.255.255.255
neighbor MPLS-HUB send-community
neighbor MPLS-HUB route-map MPLS-SPOKE-IN in
neighbor MPLS-HUB route-map MPLS-SPOKE-OUT out
neighbor INET-HUB send-community
neighbor INET-HUB route-map INET-SPOKE-IN in
neighbor INET-HUB route-map INET-SPOKE-OUT out
neighbor 10.0.100.84 activate
neighbor 10.0.100.84 soft-reconfiguration inbound
neighbor 10.0.200.85 activate
neighbor 10.0.200.85 soft-reconfiguration inbound
exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-HUB1 permit 10:100
ip community-list standard MPLS-HUB2 permit 10:101
ip community-list standard INET-HUB1 permit 10:200
ip community-list standard INET-HUB2 permit 10:201
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
ip access-list extended RC
permit tcp host 10.1.10.2 any
ip access-list extended SMP
permit udp any eq 18000 any eq 19000
!
!
ip prefix-list INET-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list INET-DMVPN seq 10 permit 10.8.0.0/16
!
ip prefix-list MPLS-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list MPLS-DMVPN seq 10 permit 10.8.0.0/16
no service-routing capabilities-manager
!
route-map MPLS-SPOKE-OUT deny 10
match ip address prefix-list INET-DMVPN
!
```

```
route-map MPLS-SPOKE-OUT permit 20
!
route-map INET-SPOKE-OUT deny 10
match ip address prefix-list MPLS-DMVPN
!
route-map INET-SPOKE-OUT permit 20
!
route-map MPLS-SPOKE-IN permit 5
match ip address prefix-list MPLS-DMVPN
set local-preference 201
!
route-map MPLS-SPOKE-IN permit 10
match community MPLS-HUB1
set local-preference 201
!
route-map MPLS-SPOKE-IN permit 20
match community MPLS-HUB2
set local-preference 200
!
route-map INET-SPOKE-IN permit 5
match ip address prefix-list MPLS-DMVPN
set local-preference 151
!
route-map INET-SPOKE-IN permit 30
match community INET-HUB1
set local-preference 151
!
route-map INET-SPOKE-IN permit 40
match community INET-HUB2
set local-preference 150
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

---

### show running-config

```
BR11# show running-config
```

---

```
Building configuration...
Current configuration : 6929 bytes
!
! Last configuration change at 02:30:33 CST Mon Nov 3 2014
! NVRAM config last updated at 02:30:34 CST Mon Nov 3 2014
!
```

```
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial
!
hostname Branch11
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
rd 65512:2
!
address-family ipv4
exit-address-family
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
border
source-interface Loopback0
master local
```

```
master branch
source-interface Loopback0
hub 10.8.3.3
!
!
license udi pid CSR1000V sn 9YRYPG7XWOA
license boot level ax
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring DMVPN-KEYRING2 vrf INET2
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 40 5
crypto isakmp profile ISAKMP-INET1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0
crypto isakmp profile ISAKMP-INET2
keyring DMVPN-KEYRING2
match identity address 0.0.0.0 INET2
!
crypto ipsec security-association idle-time 60
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET1
!
crypto ipsec profile DMVPN-PROFILE2
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET2
!
!
!
!
!
!
!
```

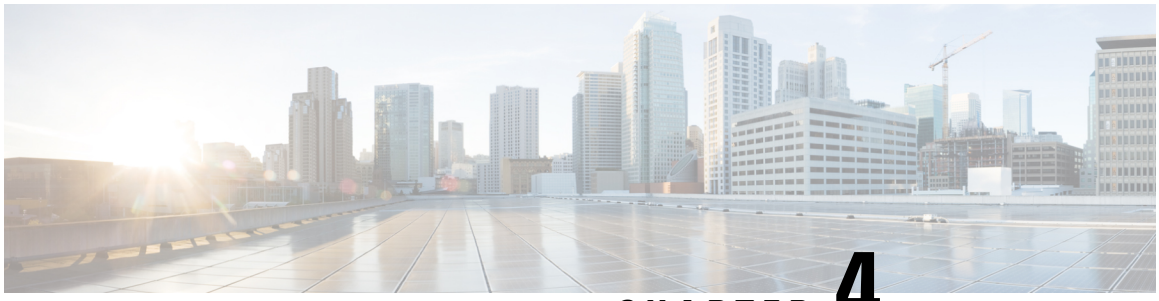
```
!
!
interface Loopback0
ip address 10.2.11.11 255.255.255.255
!
interface Tunnel100
bandwidth 100000
ip address 10.0.100.11 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map 10.0.100.84 172.16.84.4
ip nhrp map multicast 172.16.84.4
ip nhrp network-id 1
ip nhrp holdtime 600
ip nhrp nhs 10.0.100.84
ip nhrp registration timeout 60
ip nhrp shortcut
ip tcp adjust-mss 1360
load-interval 30
delay 1000
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel key 100
tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
bandwidth 50000
ip address 10.0.200.11 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map 10.0.200.85 172.16.85.5
ip nhrp map multicast 172.16.85.5
ip nhrp network-id 2
ip nhrp holdtime 600
ip nhrp nhs 10.0.200.85
ip nhrp registration timeout 60
ip nhrp shortcut
ip tcp adjust-mss 1360
load-interval 30
delay 1000
tunnel source GigabitEthernet6
tunnel mode gre multipoint
tunnel key 200
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.213 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet3
description --MPLS--
ip address 172.16.111.11 255.255.255.0
load-interval 30
negotiation auto
!
```

```
interface GigabitEthernet4
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet5
no ip address
negotiation auto
!
interface GigabitEthernet5.200
encapsulation dot1Q 200
ip address 10.1.11.1 255.255.255.0
!
interface GigabitEthernet6
description --INET--
vrf forwarding INET2
ip address 172.16.112.11 255.255.255.0
negotiation auto
!
router ospf 200 vrf INET2
network 172.16.112.11 0.0.0.0 area 0
!
router ospf 100
router-id 10.2.11.11
network 101.7.8.2 0.0.0.0 area 0
network 172.16.111.11 0.0.0.0 area 0
!
router bgp 10
bgp router-id 10.2.11.11
bgp log-neighbor-changes
neighbor MPLS-HUB peer-group
neighbor MPLS-HUB remote-as 10
neighbor MPLS-HUB timers 20 60
neighbor INET-HUB peer-group
neighbor INET-HUB remote-as 10
neighbor INET-HUB timers 20 60
neighbor 10.0.100.84 peer-group MPLS-HUB
neighbor 10.0.200.85 peer-group INET-HUB
!
address-family ipv4
network 10.1.11.0 mask 255.255.255.0
network 10.2.11.11 mask 255.255.255.255
neighbor MPLS-HUB send-community
neighbor MPLS-HUB route-map MPLS-SPOKE-IN in
neighbor MPLS-HUB route-map MPLS-SPOKE-OUT out
neighbor INET-HUB send-community
neighbor INET-HUB route-map INET-SPOKE-IN in
neighbor INET-HUB route-map INET-SPOKE-OUT out
neighbor 10.0.100.84 activate
neighbor 10.0.100.84 soft-reconfiguration inbound
neighbor 10.0.200.85 activate
neighbor 10.0.200.85 soft-reconfiguration inbound
exit-address-family
!
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
ip community-list standard MPLS-HUB1 permit 10:100
ip community-list standard MPLS-HUB2 permit 10:101
ip community-list standard INET-HUB1 permit 10:200
ip community-list standard INET-HUB2 permit 10:201
```

```
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!
ip prefix-list INET-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list INET-DMVPN seq 10 permit 10.8.0.0/16
!
ip prefix-list MPLS-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list MPLS-DMVPN seq 10 permit 10.8.0.0/16
no service-routing capabilities-manager
!
route-map MPLS-SPOKE-OUT deny 10
match ip address prefix-list INET-DMVPN
!
route-map MPLS-SPOKE-OUT permit 20
!
route-map INET-SPOKE-OUT deny 10
match ip address prefix-list MPLS-DMVPN
!
route-map INET-SPOKE-OUT permit 20
!
route-map MPLS-SPOKE-IN permit 5
match ip address prefix-list MPLS-DMVPN
set local-preference 201
!
route-map MPLS-SPOKE-IN permit 10
match community MPLS-HUB1
set local-preference 201
!
route-map MPLS-SPOKE-IN permit 20
match community MPLS-HUB2
set local-preference 200
!
route-map site_prefixes permit 10
match ip address prefix-list site_prefixes
!
route-map INET-SPOKE-IN permit 5
match ip address prefix-list MPLS-DMVPN
set local-preference 151
!
route-map INET-SPOKE-IN permit 30
match community INET-HUB1
set local-preference 151
!
route-map INET-SPOKE-IN permit 40
match community INET-HUB2
set local-preference 150
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
```

```
no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
```

---



CHAPTER 4

# PfRv3 Transit Site Support

Starting with Cisco IOS XE Release 3.15S and Cisco IOS Release 15.5(2)T release, Performance Routing version 3 (PfRv3) supports multiple data centers at the hub site. The multi-data center or the transit site support feature enables service providers to scale their network infrastructure, and load-balance the traffic when required.



# Feature Information for PfRv3 Transit Site Support

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 13: Feature Information for PfRv3 Transit Site Support***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Transit Site Support | 15.5(2)T<br><br>Cisco IOS XE Release 3.15S | The PfRv3 Transit Site Support feature enables service providers to configure multiple-data centers at the hub site.<br><br>The following commands were modified by this feature: **master** (domain VRF configuration), **domain** (interface configuration). |

# Prerequisites for PfRv3 Transit Site Support

- Upgrade all branch sites, hub, and transit sites with latest Cisco IOS image to enable transit site support feature.

# Restrictions for PfRv3 Transit Site Support

- Multiple next hops are supported only on hub or transit hub.
- Basic tunnel function is not supported between an old Cisco IOS release version and a new version, if transit site support is enabled.
- Hub sites must be connected by a Layer 3 routed link, which provides primary routing between the hub sites. Routing between hub sites over the DMVPN network is not supported

# Information About PfRv3 Transit Site Support

## Information About Transit Site Support

The multi-data center or the transit site support feature enables service providers to scale their network infrastructure, and load-balance the traffic when required. The multi-data center support enables all the hub sites to be connected with all the branch sites in an enterprise network. For example, in a use case scenario, an organization with two data centers and a single branch site, the branch site can communicate with the master-hub controller through the two next-hops (hub-branch routers) located at the hub site. If one hub-border router is down, then the branch site can still communicate through the second hub-border router. To differentiate the traffic from different hub-border routers, a path-id is configured on each interface of every channel. The branch router determines the inbound traffic based on the path-id of hub-branch routers. A path-id is a unique 32-bit number for a path between two sites.

## PfRv3 Transit Site Use Case Scenarios

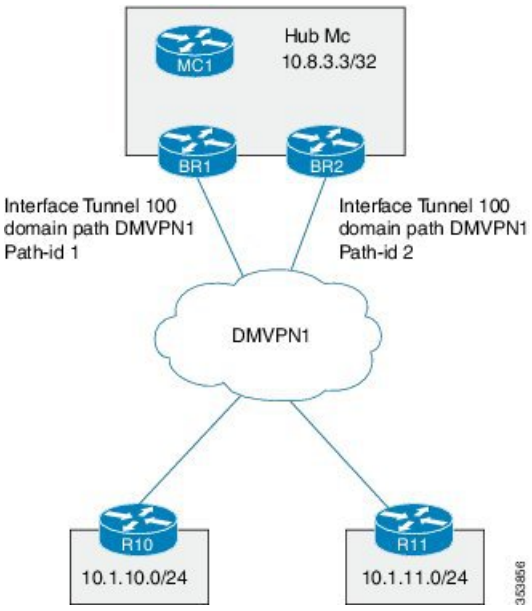
The transit site support feature supports the following use case scenarios:

- Single data center with multiple borders
- Dual data center with multiple borders
- Dual data center with same prefix

### Single Data Center with Multiple Borders

In the following illustration, spoke A (R10) is connected to two (BR1 and BR2) DMVPN hubs in a single Dynamic Multipoint VPN (DMVPN) domain. There are two paths and two next-hops to the hub site from the spoke A. To differentiate traffic from different ISP paths, a path-id is added on each domain path. Use the **domain** *domain-name* **path** *path-name* **path-id** command to configure the path-ids.

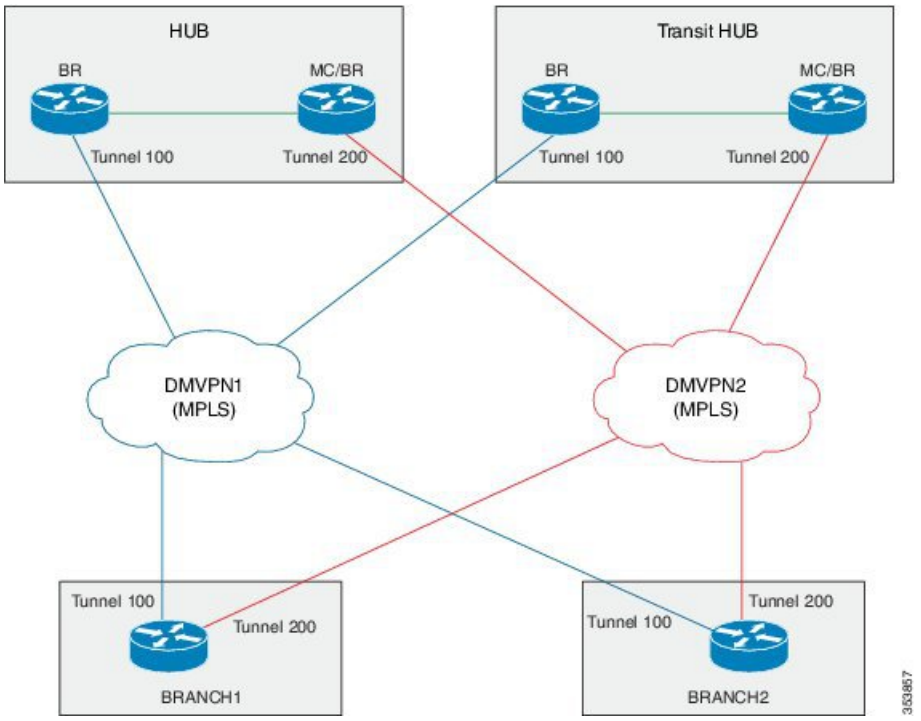
*Figure 4: Single Data Center with Multiple Borders*




### Dual Data Center with Multiple Borders

In the following illustration, the two data centers are connected to all the branch sites. You can use both the data centers in active mode and use separate prefixes for both the data centers. To differentiate the traffic originating from different data centers, a transit-id is assigned to each data center. The valid range for a transit-id is from 1 to 62. By default, 0 is assigned to the master hub. Use the **master transit** command to configure the transit-id.

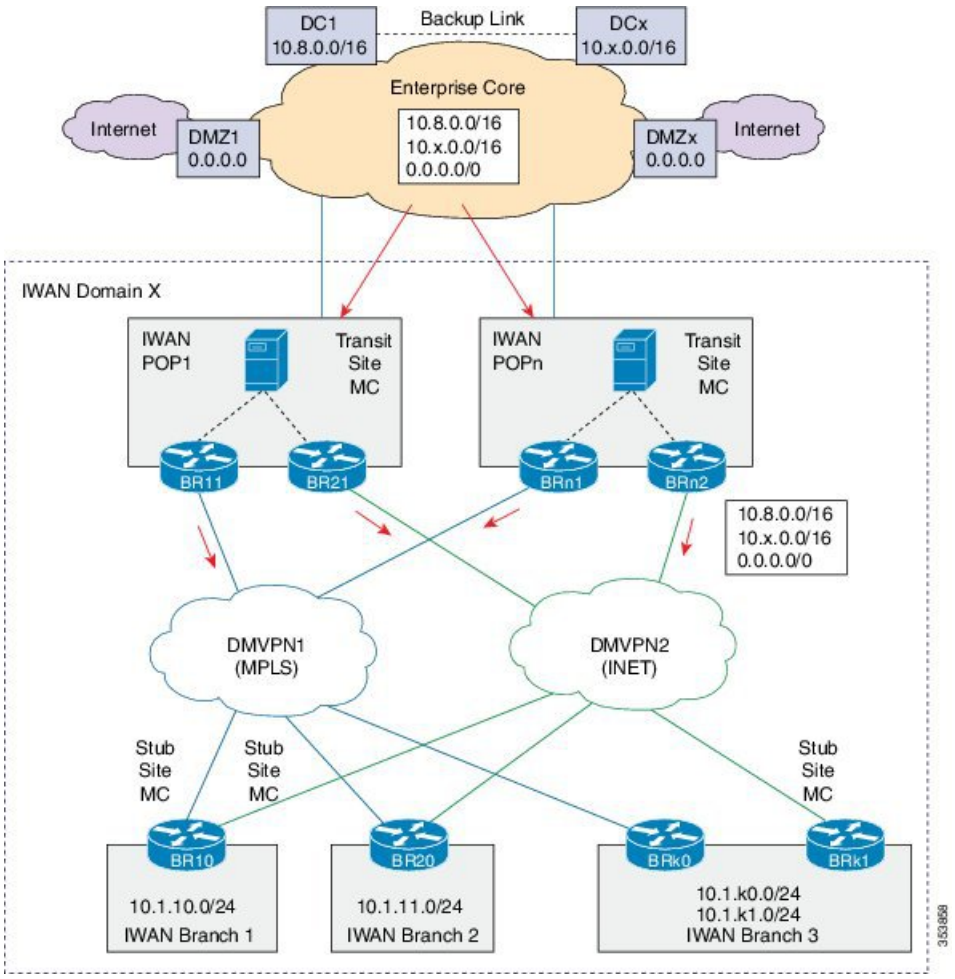
*Figure 5: Dual Data Center with Multiple Borders*




### Dual Data Center with Same Prefix

In the following illustration, two data centers are connected to all the branch sites. However, in this scenario both the data centers are active and load-balance the traffic. If one data center is down, then traffic is routed through the other data center. Both the data centers share the same prefix.

*Figure 6: Dual Data Center with Same Prefix*




# How to Configure Transit Site Support

## Configuring Transit Hub

### Before you begin

Configure the primary hub before configuring the transit hub.

**Note** In the current release, transit hub support is available only on Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers.

**Note** All policies are configured on the primary hub-master controller.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **exit**
5. **domain** {*domain-name* | **default**}
6. **vrf** {*vrf-name* | **default**}
7. **master transit** *pop-id*
8. **source-interface loopback** *interface-number*
9. **site-prefixes prefix-list** *site -list*
10. **hub** *ip-address*
11. **exit**
12. **end**
13. (Optional) **show domain** *domain-name* **master status**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Enters interface configuration mode. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 5** | **domain** {*domain-name* | **default**}<br>**Example:** | Enters domain configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# domain default` | **Note** You can either configure a default domain or define a specific domain for the transit hub configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration. |
| **Step 6** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain. |
| **Step 7** | **master transit** *pop-id*<br>**Example:**<br>`Device(config-domain-vrf)# master transit 1` | Enters master-controller configuration mode and configures the master as a transit hub. The valid range for a pop-id is from 1 to 62. |
| **Step 8** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-mc)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller.<br>**Note** The source-interface loopback also serves as a site ID of a particular site (hub or branch) on the master controller. |
| **Step 9** | **site-prefixes prefix-list** *site -list*<br>**Example:**<br>`Device(config-domain-vrf-mc)# site-prefixes prefix-list Data_Center_1` | Configures the prefix-list containing list of site prefixes.<br>**Note** You must configure the static-site prefix list for a hub and transit sites. |
| **Step 10** | **hub** *ip-address*<br>**Example:**<br>`Device(config-domain-vrf-mc)# hub 10.8.3.3` | Configures the hub for the transit site. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-domain-vrf-mc)# exit` | Exits from master controller configuration mode and returns to domain configuration mode.<br>**Note** Exit from domain configuration mode and enter in global configuration mode using the **exit** command. |
| **Step 12** | **end**<br>**Example:**<br>`Device(config)# end` | Exits configuration mode and returns to privileged EXEC mode. |
| **Step 13** | (Optional) **show domain** *domain-name* **master status**<br>**Example:**<br>`Device# show domain one master status` | Use this show command to display the status of a master controller. |

# Configuring Transit Site Border Routers

**Note** In Cisco IOS XE Release 3.15S and Cisco IOS Release 15.5(2)T release, the transit site support is available only on Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers.

In a transit site support scenario, you must configure hub-border routers with the following:

- The source interface of the border router
- The IP address of the hub-master controller
- The domain path name on external interfaces
- The domain path ID for each external interface

To configure multiple hub-border routers to the same ISP path, perform the following task on each hub-border router.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address-mask*
5. **exit**
6. **domain** {*domain-name* | **default**}
7. **vrf** {*vrf-name* | **default**}
8. **border**
9. **source-interface loopback** *interface-number*
10. **master** *ip-address*
11. **exit**
12. **exit**
13. **exit**
14. **interface** *tunnel-name*
15. **ip address** *ip-address mask*
16. **description** *description-line*
17. **domain** *domain-name* **path** *path-name* **path-id** *path-id*
18. **end**
19. (Optional) **show domain** *domain-name* **border status**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device> enable` | |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address-mask*<br>**Example:**<br>`Device(config-if)# ip address 10.9.4.4 255.255.255.255` | Configures an IP address for an interface on the hub-border router (Border Router 1). |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **domain** {*domain-name* \| **default**}<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode. |
| **Step 7** | **vrf** {*vrf-name* \| **default**}<br>**Example:**<br>`Device(config-domain)# vrf default` | Configures Virtual Routing and Forwarding (VRF) for the default domain.<br>**Note** You can configure specific VRF definition for the hub-border configuration. |
| **Step 8** | **border**<br>**Example:**<br>`Device(config-domain-vrf)# border` | Enters border configuration mode and configures the device as border. |
| **Step 9** | **source-interface loopback** *interface-number*<br>**Example:**<br>`Device(config-domain-vrf-br)# source-interface Loopback0` | Configures the loopback used as a source for peering with other sites or master controller. |
| **Step 10** | **master** *ip-address*<br>**Example:**<br>`Device(config-domain-vrf-br)# master 10.9.3.3` | Configures the IP address of the hub-master controller. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-domain-vrf-br)# exit` | Exits border configuration mode and enters VRF configuration mode. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-domain-vrf)# exit` | Exits VRF configuration mode and enters domain configuration mode. |
| **Step 13** | **exit**<br>**Example:**<br>`Device(config-domain)# exit` | Exits domain configuration mode and enters global configuration mode. |
| **Step 14** | **interface** *tunnel-name*<br>**Example:**<br>`Device(config)# interface Tunnel100` | Enters interface configuration mode. |
| **Step 15** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.100.84 255.255.255.0` | Configures an IP address for the tunnel interface. |
| **Step 16** | **description** *description-line*<br>**Example:**<br>`Device1(config-if)# description primary path`<br>`Device2(config-if)# description secondary path` | Configures a description to associate with an ISP path. |
| **Step 17** | **domain** *domain-name* **path** *path-name* **path-id** *path-id*<br>**Example:**<br>`Device(config-if)# domain default path MPLS path-id 1` | Configures the Internet Service Provider (ISP) associated with the domain and the path. There are two types of external interfaces, enterprise link such as DMVPN tunnel interface and internet -bound interface. Multiple next hop is supported only on DMVPN tunnel interfaces. The path-id is a unique identifier for each path in a domain. Valid values for a path-id are from 1 to 62.<br>We recommend using front VRF on the tunnel interface for enterprise links.<br>**Note** You can configure multiple ISPs. If you are defining specific domain name for example, domain_cisco, you must specify the same domain name for configuring ISP paths.<br>You must assign a unique path-id for all the paths that are connected from hub-border routers to the same ISP domain. |
| **Step 18** | **end**<br>**Example:** | Exits interface configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)# end` | |
| **Step 19** | (Optional) **show domain** *domain-name* **border status**<br>**Example:**<br>`Device# show domain default border status` | Use this show command to display the status of a border router. |

### What to do next

Verifying PfRv3 Transit Site Support

# Verifying PfRv3 Transit Site Support

The **show** commands can be entered in any order.

### Before you begin

Configure multiple DMVPN paths from hub-border routers or from transit-hub border routers.

## SUMMARY STEPS

1. **show domain** *domain-name* **master channels**
2. **show domain** *domain-name* **border channel**
3. **show domain** *domain-name* **master site-prefix**
4. **show domain** *domain-name* **border site-prefix**
5. **show domain** *domain-name* **master channels dst-site-id** *destination-site-id*

## DETAILED STEPS

**Step 1** **show domain** *domain-name* **master channels**

Displays channel information of the hub-master controller.

**Example:**

```
HubMC# show domain default master channels

------------------------------------------------------------------------------------------------
Channel Id: 8  Dst Site-Id: 10.2.11.11  Link Name: MPLS  DSCP: default [0] pfr-label: 0:0 | 2:30
[0x21E] TCs: 0
  Channel Created: 03:19:14 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Channel to hub: FALSE
  Interface Id: 11
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:21 ago
    Packet Count  : 0
    Byte Count    : 0
```

```
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:52 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
   TCA Statistics:
      Received:355 ; Processed:354 ; Unreach_rcvd:355
  Latest TCA Bucket
   Last Updated  : 00:00:21 ago
    Local unreachable TCA received(Check for stale TCA 00:00:09 later)
.
.
.
------------------------------------------------------------------------------------------
```

**Step 2** **show domain** *domain-name* **border channel**

Displays the information of border router channels at the hub site.

**Example:**

```
HubBR# show domain default border channels

------------------------------------------------------------------------------------------
Border Smart Probe Stats:

 Smart probe parameters:
   Source address used in the Probe: 10.2.10.10
   Unreach time: 1000 ms
   Probe source port: 18000
   Probe destination port: 19000
   Interface Discovery: ON
   Probe freq for channels with traffic :10 secs
   Discovery Probes: OFF
   Number of transit probes consumed :29
   Number of transit probes re-routed: 0
   DSCP's using this: [0] [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17]
 [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37]
 [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57]
 [58] [59] [60] [61] [62] [63] [64]
   All the other DSCPs use the default interval: 10 secs

Channel id: 20
  Channel create time: 06:42:54 ago
  Site id : 10.2.11.11
  DSCP : default[0]
  Service provider : MPLS
  Pfr-Label : 0:0 | 0:0 [0x0]
  exit path-id: 0
  Exit path-id sent on wire: 0
  Number of Probes sent : 77407
  Number of Probes received : 75949
  Last Probe sent : 00:00:00 ago
  Last Probe received : 00:00:00 ago
  Channel state : Initiated and open
  Channel next_hop : 10.0.100.11
```

```
  RX Reachability : Reachable
  TX Reachability : Reachable
  Channel is sampling 0 flows
  Channel remote end point: 10.0.100.11
  Channel to hub: FALSE
  Version: 3
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Probe freq with traffic : 1 in 10000 ms

.
.
.
------------------------------------------------------------------------------------------------
```

**Step 3** **show domain** *domain-name* **master site-prefix**

Displays the details of site-prefixes configured to the master hub.

**Example:**

```
HubMC# show domain default master site-prefix

------------------------------------------------------------------------------------------------
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 11:28:29.421 CET Tue Mar 17 2015

  Change will be published between 5-60 seconds
  Next Publish 00:33:03 later
  Prefix DB Origin: 10.9.3.3
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-shared

Site-id              Site-prefix          Last Updated         DC Bitmap  Flag
------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         01:25:15 ago         0x0         S
10.2.11.11            10.1.11.0/24         01:25:19 ago         0x0         S
10.2.10.10            10.2.10.10/32        01:25:15 ago         0x0         S
10.2.11.11            10.2.11.11/32        01:25:19 ago         0x0         S
10.2.12.12            10.2.12.12/32        01:28:54 ago         0x0         S
10.8.3.3              10.8.3.3/32          01:28:47 ago         0x1         S
10.9.3.3              10.8.0.0/16          01:28:47 ago         0x5         C,M
10.8.3.3              10.8.0.0/16          01:28:47 ago         0x5         C,M
10.9.3.3              10.9.3.3/32          03:29:04 ago         0x4         L
10.9.3.3              10.9.0.0/16          01:28:47 ago         0x5         C,M
10.8.3.3              10.9.0.0/16          01:28:47 ago         0x5         C,M
255.255.255.255      *10.0.0.0/8           01:28:47 ago         0x1         S,T

------------------------------------------------------------------------------------------------
```

**Step 4** **show domain** *domain-name* **border site-prefix**

Displays the details of site-prefixes configured on the border.

**Example:**

```
HubBR# show domain default border site-prefix

------------------------------------------------------------------------------------------------

Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-shared

Site-id              Site-prefix          Last Updated         DC Bitmap  Flag
------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         00:36:58 ago         0x0         S
10.2.11.11            10.1.11.0/24         00:37:02 ago         0x0         S
```

```
10.2.10.10            10.2.10.10/32        00:36:58 ago         0x0         S
10.2.11.11            10.2.11.11/32        00:37:02 ago         0x0         S
10.2.12.12            10.2.12.12/32        00:40:37 ago         0x0         S
10.8.3.3              10.8.3.3/32          00:40:29 ago         0x1         S
10.9.3.3              10.8.0.0/16          00:38:40 ago         0x5         S,C,M
10.8.3.3              10.8.0.0/16          00:38:40 ago         0x5         S,C,M
10.9.3.3              10.9.3.3/32          00:38:40 ago         0x4         S
10.9.3.3              10.9.0.0/16          00:38:40 ago         0x5         S,C,M
10.8.3.3              10.9.0.0/16          00:38:40 ago         0x5         S,C,M
255.255.255.255      *10.0.0.0/8           00:40:29 ago         0x1         S,T
------------------------------------------------------------------------------------------
```

**Step 5** **show domain** *domain-name* **master channels dst-site-id** *destination-site-id*

Displays the details of destination site-ids configured with hub-master controller.

**Note** Use this command on a spoke or a branch device to view the details of the destination site-ids.

**Example:**

```
BR# show domain default master channels dst-site-id 10.8.3.3

------------------------------------------------------------------------------------------

Legend: * (Value obtained from Network delay:)

Channel Id: 27  Dst Site-Id: 10.8.3.3  Link Name: INET  DSCP: default [0] pfr-label: 0:20 | 0:0
[0x140000] TCs: 0
  Channel Created: 01:16:34 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: TRUE
  Interface Id: 12
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Estimated Channel Egress Bandwidth: 5 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  Site Prefix List
    10.8.3.3/32 (Active)
    10.8.0.0/16 (Active)
    10.9.0.0/16 (Standby)
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:24 ago
    Packet Count  : 562
Byte Count    : 47208
    One Way Delay : 71 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 619 usec
    Unreachable   : FALSE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:54 ago
    Packet Count  : 558
    Byte Count    : 46872
    One Way Delay : 55 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 556 usec
    Unreachable   : FALSE
   TCA Statistics:
      Received:133 ; Processed:133 ; Unreach_rcvd:0
  Latest TCA Bucket
   Last Updated  : 00:00:24 ago
```

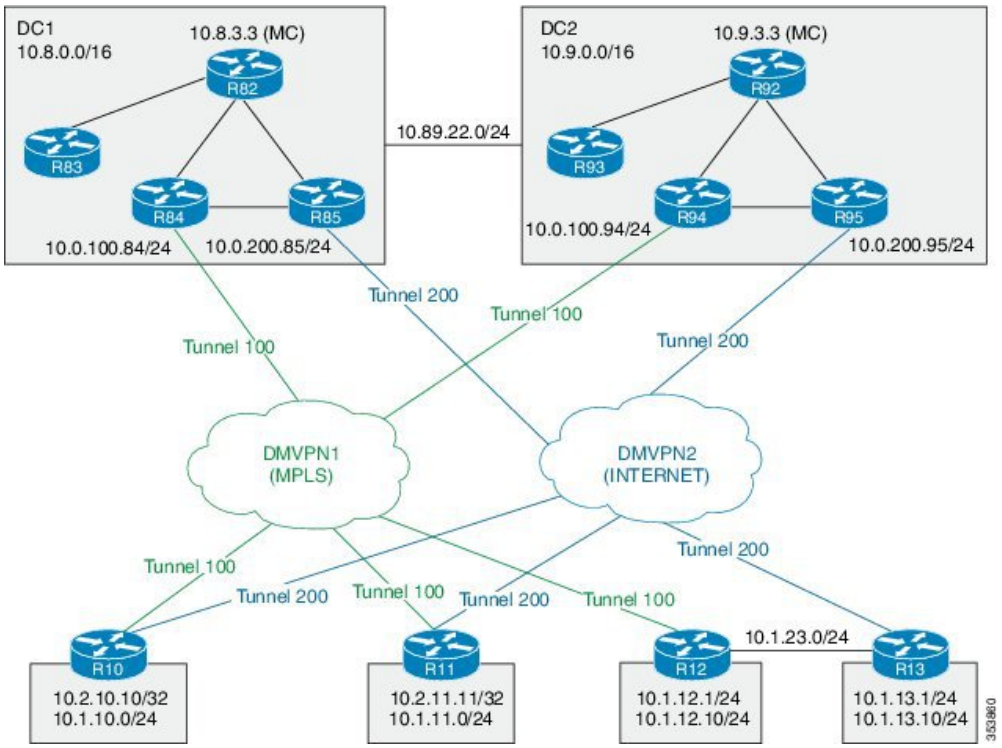
```
    One Way Delay : 71 msec*
    Loss Rate Pkts: NA
    Loss Rate Byte: NA
    Jitter Mean   : NA
    Unreachability: FALSE
.
.
.
----------------------------------------------------------------------------------------------
```

# Configuration Examples for PfRv3 Transit Site Support

## Example: Configuring Transit Site Support

In this use case scenario, an enterprise organization has two data centers with multiple-border routers connected to the same ISP domain. The branch-border routers can reach the hub-master controller through multiple next-hops.

***Figure 7: PfRv3 Transit Hub Topology***




In this example, the following routers are used:

- Hub Master Controller — Cisco ASR 1002-X router configured with an embedded services processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps.

- Hub Border Routers — Cisco ASR 1000 Series Embedded Services Processor 2
- Branch Routers — Cisco 4451X Integrated Services Router.

### Example: Configuring Data Center 1 (DC1) Devices

#### Configure the interfaces on master hub controller (R82)

```
HubMC> enable
HubMC# configure terminal
HubMC(config)# interface Loopback0
HubMC(config-if)# ip address 10.8.3.3 255.255.255.255
HubMC(config-if)# exit
```

#### Configure the device as hub-master controller

```
HubMC(config)# domain default
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE_PREFIX
HubMC(config-domain-vrf-mc)# site-prefixes prefix-list DC1_PREFIX
HubMC(config-domain-vrf-mc)# exit
```

#### Configure IP prefix-lists

```
HubMC(config)# ip prefix-list DC1_PREFIX seq 10 permit 10.8.0.0/16
HubMC(config)# ip prefix-list DC1_PREFIX seq 10 permit 10.9.0.0/16
HubMC(config)# ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
```

#### Configure domain policies on hub master controller

```
HubMC(config)# domain default
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# site-prefixes prefix-list DC1_PREFIX
HubMC(config-domain-vrf-mc)# load-balance
HubMC(config-domain-vrf-mc)# enterprise-prefix  prefix-list ENTERPRISE_PREFIX

HubMC(config-domain-vrf-mc)# class VOICE sequence 10
HubMC(config-domain-vrf-mc-class)# match dscp ef policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 5
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay  threshold 150
HubMC(config-domain-vrf-mc-class-type)# exit
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
HubMC(config-domain-vrf-mc-class)# exit

HubMC(config-domain-vrf-mc)# class VIDEO sequence 20
HubMC(config-domain-vrf-mc-class)# match dscp af41 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 5
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay  threshold 150
HubMC(config-domain-vrf-mc-class-type)# exit
HubMC(config-domain-vrf-mc-class)# match dscp cs4 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 5
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay  threshold 150
HubMC(config-domain-vrf-mc-class-type)# exit
HubMC(config-domain-vrf-mc-class)# path-preference INET fallback MPLS
HubMC(config-domain-vrf-mc-class)# exit


HubMC(config-domain-vrf-mc)# class CRITICAL sequence 30
```

```
HubMC(config-domain-vrf-mc-class)# match dscp af31 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600
HubMC(config-domain-vrf-mc-class-type)# exit
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
HubMC(config-domain-vrf-mc)# class DEFAULT sequence 100
HubMC(config-domain-vrf-mc-class)# match dscp default policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 5
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 50
HubMC(config-domain-vrf-mc-class-type)# priority 3 jitter threshold 200000
HubMC(config-domain-vrf-mc-class-type)# exit
```

### Configure hub border routers on DC1 (R84)

```
BR84> enable
BR84# configure terminal
BR84(config)# interface Loopback0
BR84(config-if)# ip address 10.8.4.4 255.255.255.255
BR84(config-if)exit
```

### Configure the device as border router (BR84)

```
BR84(config)# domain default
BR84(config-domain)# vrf default
BR84(config-domain-vrf)# border
BR84(config-domain-vrf-br)# source-interface Loopback0
BR84(config-domain-vrf-br)# master 10.8.3.3
BR84(config-domain-vrf-br)# exit
```

### Configure tunnel from BR84 to DMVPN1 (MPLS)Link

```
BR84(config)# interface Tunnel100
BR84(config-if)# bandwidth 100000
BR84(config-if)# ip address 10.0.100.84 255.255.255.0
BR84(config-if)# no ip redirects
BR84(config-if)# ip mtu 1400
BR84(config-if)# ip nhrp authentication cisco
BR84(config-if)# ip nhrp map multicast dynamic
BR84(config-if)# ip nhrp network-id 1
BR84(config-if)# ip nhrp holdtime 60
BR84(config-if)# ip nhrp redirect
BR84(config-if)# ip tcp adjust-mss 1360
BR84(config-if)# load-interval 30
BR84(config-if)# delay 1000
BR84(config-if)# tunnel source Ethernet0/1
BR84(config-if)# tunnel mode gre multipoint
BR84(config-if)# tunnel key 100
BR84(config-if)# tunnel vrf IWAN-TRANSPORT-1
BR84(config-if)# domain path MPLS path-id 10
```

### Configure hub border routers on DC1 (R85)

```
BR85> enable
BR85# configure terminal
BR85(config)# interface Loopback0
BR85(config-if)# ip address 10.8.5.5 255.255.255.255
BR85(config-if)exit
```

### Configure the device as border router (BR85)

```
BR85(config)# domain default
BR85(config-domain)# vrf default
BR85(config-domain-vrf)# border
BR85(config-domain-vrf-br)# source-interface Loopback0
```

```
BR85(config-domain-vrf-br)# master 10.8.3.3
BR85(config-domain-vrf-br)# exit
```

### Configure tunnel from BR84 to DMVPN2 (INET)Link

```
BR85(config)# interface Tunnel200
BR85(config-if)# bandwidth 5000
BR85(config-if)# ip address 10.0.200.85 255.255.255.0
BR85(config-if)# no ip redirects
BR85(config-if)# ip mtu 1400
BR85(config-if)# ip nhrp authentication cisco
BR85(config-if)# ip nhrp map multicast dynamic
BR85(config-if)# ip nhrp network-id 2
BR85(config-if)# ip nhrp holdtime 60
BR85(config-if)# ip nhrp redirect
BR85(config-if)# ip tcp adjust-mss 1360
BR85(config-if)# load-interval 30
BR85(config-if)# delay 1000
BR85(config-if)# tunnel source Ethernet0/1
BR85(config-if)# tunnel mode gre multipoint
BR85(config-if)# tunnel key 200
BR85(config-if)# tunnel vrf IWAN-TRANSPORT-2
BR85(config-if)# domain path INET path-id 20
```

## Example: Configuring Data Center 2 (DC2) Devices

### Configure the interfaces on master hub controller (R92)

```
HubMC> enable
HubMC# configure terminal
HubMC(config)# interface Loopback0
HubMC(config-if)# ip address 10.9.3.3 255.255.255.255
HubMC(config-if)# exit
```

### Configure the device as transit-hub master controller

```
HubMC(config)# domain default
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master transit 2
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# site-prefixes prefix-list DC2_PREFIX
HubMC(config-domain-vrf-mc)# hub 10.8.3.3
HubMC(config-domain-vrf-mc)# exit
```

### Configure IP prefix-lists

```
HubMC(config)# ip prefix-list DC2_PREFIX seq 10 permit 10.9.0.0/16
HubMC(config)# ip prefix-list DC2_PREFIX seq 20 permit 10.8.0.0/16
HubMC(config)# ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
```

### Configure hub border routers on DC2 (R94)

```
BR94> enable
BR94# configure terminal
BR94(config)# interface Loopback0
BR94(config-if)# ip address 10.9.4.4 255.255.255.255
BR94(config-if)exit
```

### Configure the device as border router (BR94)

```
BR94(config)# domain default
BR94(config-domain)# vrf default
BR94(config-domain-vrf)# border
BR94(config-domain-vrf-br)# source-interface Loopback0
```

```
BR94(config-domain-vrf-br)# master 10.9.3.3
BR94(config-domain-vrf-br)# exit
```

### Configure tunnel from BR94 to DMVPN1 (MPLS)Link

```
BR94(config)# interface Tunnel100
BR94(config-if)# bandwidth 1000
BR94(config-if)# ip address 10.0.100.94 255.255.255.0
BR94(config-if)# no ip redirects
BR94(config-if)# ip mtu 1400
BR94(config-if)# ip nhrp authentication cisco
BR94(config-if)# ip nhrp map multicast dynamic
BR94(config-if)# ip nhrp network-id 1
BR94(config-if)# ip nhrp holdtime 60
BR94(config-if)# ip nhrp redirect
BR94(config-if)# ip tcp adjust-mss 1360
BR94(config-if)# load-interval 30
BR94(config-if)# delay 1000
BR94(config-if)# tunnel source Ethernet0/1
BR94(config-if)# tunnel mode gre multipoint
BR94(config-if)# tunnel key 100
BR94(config-if)# tunnel vrf IWAN-TRANSPORT-1
BR94(config-if)# domain path MPLS path-id 30
```

### Configure hub border routers on DC2 (R95)

```
BR95> enable
BR95# configure terminal
BR95(config)# interface Loopback0
BR95(config-if)# ip address 10.9.5.5 255.255.255.255
BR95(config-if)exit
```

### Configure the device as border router (BR95)

```
BR95(config)# domain default
BR95(config-domain)# vrf default
BR95(config-domain-vrf)# border
BR95(config-domain-vrf-br)# source-interface Loopback0
BR95(config-domain-vrf-br)# master 10.9.3.3
BR95(config-domain-vrf-br)# exit
```

### Configure tunnel from BR95 to DMVPN2 (INET)Link

```
BR95(config)# interface Tunnel200
BR95(config-if)# bandwidth 1000
BR95(config-if)# ip address 10.0.200.95 255.255.255.0
BR95(config-if)# no ip redirects
BR95(config-if)# ip mtu 1400
BR95(config-if)# ip nhrp authentication cisco
BR95(config-if)# ip nhrp map multicast dynamic
BR95(config-if)# ip nhrp network-id 2
BR95(config-if)# ip nhrp holdtime 60
BR95(config-if)# ip nhrp redirect
BR95(config-if)# ip tcp adjust-mss 1360
BR95(config-if)# load-interval 30
BR95(config-if)# delay 1000
BR95(config-if)# tunnel source Ethernet0/1
BR95(config-if)# tunnel mode gre multipoint
BR95(config-if)# tunnel key 200
BR95(config-if)# tunnel vrf IWAN-TRANSPORT-2
BR95(config-if)# domain path INET path-id 40
```

## Example: Configuring Branch Routers

### Configure the interfaces (R10)

```
R10> enable
R10# configure terminal
R10(config)# interface Loopback0
R10(config-if)# ip address 10.2.10.10 255.255.255.255
R10(config-if)# exit
```

### Configure the device as branch-master controller (R10)

```
R10(config)# domain default
R10(config-domain)# vrf default
R10(config-domain-vrf)# border
R10(config-domain-vrf-br)# source-interface Loopback0
R10(config-domain-vrf-br)# master local
R10(config-domain-vrf-br)# exit
R10(config-domain-vrf)# master branch
R10(config-domain-vrf-mc)# source-interface Loopback0
R10(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R10

```
R10(config)# interface Tunnel100
R10(config-if)# bandwidth 400
R10(config-if)# ip address 10.0.100.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map multicast dynamic
R10(config-if)# ip nhrp network-id 1
R10(config-if)# ip nhrp holdtime 60
R10(config-if)# ip nhrp nhs 10.0.100.84 nbma 172.16.84.4 multicast
R10(config-if)# ip nhrp nhs 10.0.100.94 nbma 172.16.94.4 multicast
R10(config-if)# ip nhrp registration no-unique
R10(config-if)# ip nhrp registration timeout 60
R10(config-if)# ip nhrp shortcut
R10(config-if)# ip nhrp redirect
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# no nhrp route-watch
R10(config-if)# if-state nhrp
R10(config-if)# tunnel source Ethernet0/1
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 100
R10(config-if)# tunnel vrf IWAN-TRANSPORT-1

R10(config)# interface Tunnel200
R10(config-if)# bandwidth 5000
R10(config-if)# ip address 10.0.200.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map multicast dynamic
R10(config-if)# ip nhrp network-id 2
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.200.85 nbma 172.16.85.5 multicast
R10(config-if)# ip nhrp nhs 10.0.200.95 nbma 172.16.95.5 multicast
R10(config-if)# ip nhrp registration no-unique
R10(config-if)# ip nhrp registration timeout 60
```

```
R10(config-if)# ip nhrp shortcut
R10(config-if)# ip nhrp redirect
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# no nhrp route-watch
R10(config-if)# if-state nhrp
R10(config-if)# tunnel source Ethernet0/2
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 200
R10(config-if)# tunnel vrf IWAN-TRANSPORT-2
```

### Configure the interfaces (R11)

```
R11> enable
R11# configure terminal
R11(config)# interface Loopback0
R11(config-if)# ip address 10.2.11.11 255.255.255.255
R11(config-if)# exit
```

### Configure the device as branch master controller (R11)

```
R11(config)# domain default
R11(config-domain)# vrf default
R11(config-domain-vrf)# border
R11(config-domain-vrf-br)# source-interface Loopback0
R11(config-domain-vrf-br)# master local
R11(config-domain-vrf-br)# exit
R11(config-domain-vrf)# master branch
R11(config-domain-vrf-mc)# source-interface Loopback0
R11(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R11

```
R11(config)# interface Tunnel100
R11(config-if)# bandwidth 2000
R11(config-if)# ip address 10.0.100.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map multicast dynamic
R11(config-if)# ip nhrp network-id 1
R11(config-if)# ip nhrp holdtime 60
R11(config-if)# ip nhrp nhs 10.0.100.84 nbma 172.16.84.4 multicast
R11(config-if)# ip nhrp nhs 10.0.100.94 nbma 172.16.94.4 multicast
R11(config-if)# ip nhrp registration no-unique
R11(config-if)# ip nhrp registration timeout 60
R11(config-if)# ip nhrp shortcut
R11(config-if)# ip nhrp redirect
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# no nhrp route-watch
R11(config-if)# if-state nhrp
R11(config-if)# tunnel source Ethernet0/1
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 100
R11(config-if)# tunnel vrf IWAN-TRANSPORT-1

R11(config)# interface Tunnel200
R11(config-if)# bandwidth 5000
R11(config-if)# ip address 10.0.200.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
```

```
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map multicast dynamic
R11(config-if)# ip nhrp network-id 2
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nhs 10.0.200.85 nbma 172.16.85.5 multicast
R11(config-if)# ip nhrp nhs 10.0.200.95 nbma 172.16.95.5 multicast
R11(config-if)# ip nhrp registration no-unique
R11(config-if)# ip nhrp registration timeout 60
R11(config-if)# ip nhrp shortcut
R11(config-if)# ip nhrp redirect
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# no nhrp route-watch
R11(config-if)# if-state nhrp
R11(config-if)# tunnel source Ethernet0/2
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 200
R11(config-if)# tunnel vrf IWAN-TRANSPORT-2
```

### Configure the interfaces (R12)

```
R12> enable
R12# configure terminal
R12(config)# interface Loopback0
R12(config-if)# ip address 10.2.12.12 255.255.255.255
R12(config-if)# exit
```

### Configure the device as branch-master controller (R12)

```
R12(config)# domain default
R12(config-domain)# vrf default
R12(config-domain-vrf)# border
R12(config-domain-vrf-br)# source-interface Loopback0
R12(config-domain-vrf-br)# master local
R12(config-domain-vrf-br)# exit
R12(config-domain-vrf)# master branch
R12(config-domain-vrf-mc)# source-interface Loopback0
R12(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R12

```
R12(config)# interface Tunnel100
R12(config-if)# bandwidth 400
R12(config-if)# ip address 10.0.100.12 255.255.255.0
R12(config-if)# no ip redirects
R12(config-if)# ip mtu 1400
R12(config-if)# ip nhrp authentication cisco
R12(config-if)# ip nhrp map multicast dynamic
R12(config-if)# ip nhrp network-id 1
R12(config-if)# ip nhrp holdtime 600
R12(config-if)# ip nhrp nhs 10.0.100.84 nbma 172.16.84.4 multicast
R12(config-if)# ip nhrp nhs 10.0.100.94 nbma 172.16.94.4 multicast
R12(config-if)# ip nhrp registration no-unique
R12(config-if)# ip nhrp registration timeout 60
R12(config-if)# ip nhrp shortcut
R12(config-if)# ip tcp adjust-mss 1360
R12(config-if)# load-interval 30
R12(config-if)# delay 1000
R12(config-if)# no nhrp route-watch
R12(config-if)# if-state nhrp
R12(config-if)# tunnel source Ethernet0/1
R12(config-if)# tunnel mode gre multipoint
```

```
R12(config-if)# tunnel key 100
R12(config-if)# tunnel vrf IWAN-TRANSPORT-1
```

### Configure the interfaces (R13)

```
R13> enable
R13# configure terminal
R13(config)# interface Loopback0
R13(config-if)# ip address 10.2.13.13 255.255.255.255
R13(config-if)# exit
```

### Configure the device as a border router with R12 as the master controller (R13)

```
R13(config)# domain default
R13(config-domain)# vrf default
R13(config-domain-vrf)# border
R13(config-domain-vrf-br)# source-interface Loopback0
R13(config-domain-vrf-br)# master 10.2.12.12
R13(config-domain-vrf-br)# exit
```

### Configure the tunnel interface and tunnel path from R13

```
R13(config)# interface Tunnel200
R13(config-if)# bandwidth 400
R13(config-if)# ip address 10.0.200.13 255.255.255.0
R13(config-if)# no ip redirects
R13(config-if)# ip mtu 1400
R13(config-if)# ip nhrp authentication cisco
R13(config-if)# ip nhrp network-id 2
R13(config-if)# ip nhrp holdtime 600
R13(config-if)# ip nhrp nhs 10.0.200.85 nbma 172.16.85.5 multicast
R13(config-if)# ip nhrp nhs 10.0.100.95 nbma 172.16.95.5 multicast
R13(config-if)# ip nhrp registration no-unique
R13(config-if)# ip nhrp registration timeout 60
R13(config-if)# ip nhrp shortcut
R13(config-if)# ip tcp adjust-mss 1360
R13(config-if)# load-interval 30
R13(config-if)# delay 1000
R13(config-if)# if-state nhrp
R13(config-if)# tunnel source Ethernet0/2
R13(config-if)# tunnel mode gre multipoint
R13(config-if)# tunnel key 200
R13(config-if)# tunnel vrf IWAN-TRANSPORT-2
```

## Verifying PfRv3 Transit Site Configuration

To verify the PfRv3 transit site configuration, use the following show commands in any order:

```
HubMC2# show domain default master status

------------------------------------------------------------------------------------------------
*** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Transit
  POP ID:      2
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 10.9.3.3
  Load Balancing:
   Operational Status: Up
   Max Calculated Utilization Variance: 0%
```

```
   Last load balance attempt: 03:07:30 ago
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kbps
  Route Control: Enabled
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length: 28
  Minimum Requirement: Met

  Borders:
    IP address: 10.9.5.5
    Version: 2
    Connection status: CONNECTED (Last Updated 03:25:38 ago )
    Interfaces configured:
Name: Tunnel200 | type: external | Service Provider: INET path-id:40 | Status: UP | Zero-SLA:
 NO
          Number of default Channels: 0


    Tunnel if: Tunnel0

    IP address: 10.9.4.4
    Version: 2
    Connection status: CONNECTED (Last Updated 03:25:37 ago )
    Interfaces configured:
      Name: Tunnel100 | type: external | Service Provider: MPLS path-id:30 | Status: DOWN
    Tunnel if: Tunnel0

------------------------------------------------------------------------------------------

HubMC2# show domain default master channels

------------------------------------------------------------------------------------------
Channel Id: 8  Dst Site-Id: 10.2.11.11  Link Name: MPLS  DSCP: default [0] pfr-label: 0:0
| 2:30 [0x21E] TCs: 0
  Channel Created: 03:19:14 ago
  Provisional State: Initiated and open
  Operational state: Available but unreachable
  Channel to hub: FALSE
  Interface Id: 11
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:21 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:52 ago
    Packet Count  : 0
    Byte Count    : 0
    One Way Delay  : N/A
    Loss Rate Pkts : N/A
    Loss Rate Bytes: N/A
    Jitter Mean    : N/A
    Unreachable   : TRUE
```

```
   TCA Statistics:
      Received:355 ; Processed:354 ; Unreach_rcvd:355
  Latest TCA Bucket
   Last Updated  : 00:00:21 ago
    Local unreachable TCA received(Check for stale TCA 00:00:09 later)
.
.
.
------------------------------------------------------------------------------------------------

HubMC2#  show domain default master site-capability device-capb path-id

------------------------------------------------------------------------------------------------

Site pop id : 1
Site mc type : Transit
Border Address : 10.9.4.4
Service provider: MPLS path-id: 30 if_index: 11
Border Address : 10.9.5.5
Service provider: INET path-id: 40 if_index: 11

------------------------------------------------------------------------------------------------



HubMC2# show domain default master site-prefix

------------------------------------------------------------------------------------------------
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 11:28:29.421 CET Tue Mar 17 2015

  Change will be published between 5-60 seconds
  Next Publish 00:33:03 later
  Prefix DB Origin: 10.9.3.3
  Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-shared

Site-id              Site-prefix          Last Updated         DC Bitmap  Flag
------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         01:25:15 ago         0x0         S
10.2.11.11            10.1.11.0/24         01:25:19 ago         0x0         S
10.2.10.10            10.2.10.10/32        01:25:15 ago         0x0         S
10.2.11.11            10.2.11.11/32        01:25:19 ago         0x0         S
10.2.12.12            10.2.12.12/32        01:28:54 ago         0x0         S
10.8.3.3              10.8.3.3/32          01:28:47 ago         0x1         S
10.9.3.3              10.8.0.0/16          01:28:47 ago         0x5         C,M
10.8.3.3              10.8.0.0/16          01:28:47 ago         0x5         C,M
10.9.3.3              10.9.3.3/32          03:29:04 ago         0x4         L
10.9.3.3              10.9.0.0/16          01:28:47 ago         0x5         C,M
10.8.3.3              10.9.0.0/16          01:28:47 ago         0x5         C,M
255.255.255.255      *10.0.0.0/8           01:28:47 ago         0x1         S,T

------------------------------------------------------------------------------------------------

HubMC2# show domain default master policy

------------------------------------------------------------------------------------------------

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 11:31:10.977 CET Tue Mar 17 2015

  class VOICE sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp ef policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
```

```
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent

  class VIDEO sequence 20
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp af41 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent
      match dscp cs4 policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 150 msec
        priority 2 byte-loss-rate threshold 5.0 percent

  class CRITICAL sequence 30
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp af31 policy custom
        priority 2 packet-loss-rate threshold 10.0 percent
        priority 1 one-way-delay threshold 600 msec
        priority 2 byte-loss-rate threshold 10.0 percent
        Number of Traffic classes using this policy: 1

class DEFAULT0 sequence 100
    class type: Dscp Based
      match dscp default policy custom
        priority 2 packet-loss-rate threshold 5.0 percent
        priority 1 one-way-delay threshold 50 msec
        priority 3 jitter threshold 200000 usec
        priority 2 byte-loss-rate threshold 5.0 percent
        Number of Traffic classes using this policy: 1

  class default
      match dscp all

------------------------------------------------------------------------------------------------

HubMC2# show domain default master discovered

------------------------------------------------------------------------------------------------
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 14:31:58.410 CET Tue Mar 17 2015


  *** Domain MC DISCOVERED sites ***

  Number of sites:  5
 *Traffic classes [Performance based][Load-balance based]

 Site ID: 255.255.255.255
  Site Discovered:06:32:33 ago
    Off-limits: Disabled
    DSCP :default[0]-Number of traffic classes[0][0]
    DSCP :af31[26]-Number of traffic classes[0][0]

 Site ID: 10.8.3.3
  Site Discovered:06:30:37 ago
    Off-limits: Disabled
    DSCP :default[0]-Number of traffic classes[0][0]
    DSCP :af31[26]-Number of traffic classes[0][0]

 Site ID: 10.2.10.10
  Site Discovered:06:30:37 ago
    Off-limits: Disabled
```

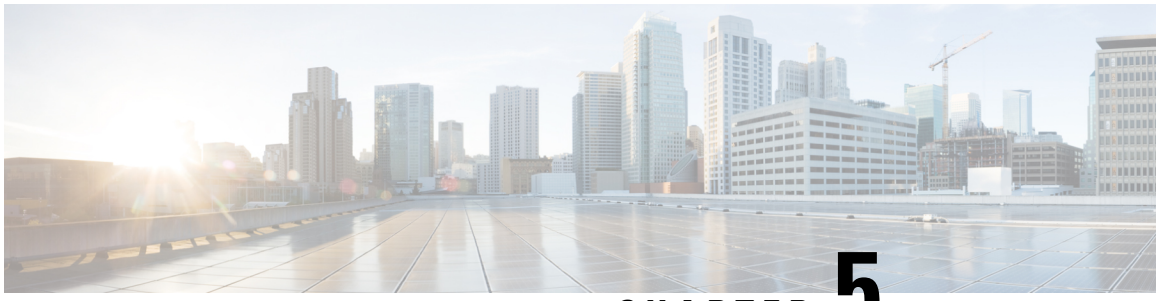
```
    DSCP :default[0]-Number of traffic classes[1][0]
    DSCP :af31[26]-Number of traffic classes[1][0]

Site ID: 10.2.11.11
  Site Discovered:06:30:34 ago
    Off-limits: Disabled
    DSCP :default[0]-Number of traffic classes[0][0]
    DSCP :af31[26]-Number of traffic classes[0][0]

 Site ID: 10.2.12.12
  Site Discovered:06:30:37 ago
    Off-limits: Disabled
    DSCP :default[0]-Number of traffic classes[0][0]
    DSCP :af31[26]-Number of traffic classes[0][0]
------------------------------------------------------------------------------------------------

BR94# show domain default border status

------------------------------------------------------------------------------------------------

**** Border Status ****

Instance Status: UP
Present status last updated: 06:39:21 ago
Loopback: Configured Loopback0 UP (10.9.4.4)
Master: 10.9.3.3
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 06:39:15
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
     Name: Tunnel100 Interface Index: 11 SNMP Index: 8 SP: MPLS path-id: 30 Status: DOWN
Zero-SLA: NO

Auto Tunnel information:

   Name:Tunnel0 if_index: 12
   Borders reachable via this tunnel:  10.9.5.5

------------------------------------------------------------------------------------------------

BR94# show domain default border site-prefix

------------------------------------------------------------------------------------------------

Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured; M-shared

Site-id              Site-prefix          Last Updated         DC Bitmap  Flag
------------------------------------------------------------------------------
10.2.10.10            10.1.10.0/24         00:36:58 ago         0x0         S
10.2.11.11            10.1.11.0/24         00:37:02 ago         0x0         S
10.2.10.10            10.2.10.10/32        00:36:58 ago         0x0         S
10.2.11.11            10.2.11.11/32        00:37:02 ago         0x0         S
10.2.12.12            10.2.12.12/32        00:40:37 ago         0x0         S
10.8.3.3              10.8.3.3/32          00:40:29 ago         0x1         S
10.9.3.3              10.8.0.0/16          00:38:40 ago         0x5         S,C,M
10.8.3.3              10.8.0.0/16          00:38:40 ago         0x5         S,C,M
10.9.3.3              10.9.3.3/32          00:38:40 ago         0x4         S
10.9.3.3              10.9.0.0/16          00:38:40 ago         0x5         S,C,M
10.8.3.3              10.9.0.0/16          00:38:40 ago         0x5         S,C,M
```

```
255.255.255.255      *10.0.0.0/8           00:40:29 ago         0x1         S,T
-------------------------------------------------------------------------------------------------

R10# show domain default master channels dst-site-id 10.8.3.3

-------------------------------------------------------------------------------------------------

Legend: * (Value obtained from Network delay:)

Channel Id: 27  Dst Site-Id: 10.8.3.3  Link Name: INET  DSCP: default [0] pfr-label: 0:20
| 0:0 [0x140000] TCs: 0
  Channel Created: 01:16:34 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: TRUE
  Interface Id: 12
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Estimated Channel Egress Bandwidth: 5 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  Site Prefix List
    10.8.3.3/32 (Active)
    10.8.0.0/16 (Active)
    10.9.0.0/16 (Standby)
  ODE Stats Bucket Number: 1
   Last Updated  : 00:00:24 ago
    Packet Count  : 562
Byte Count    : 47208
    One Way Delay : 71 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 619 usec
    Unreachable   : FALSE
  ODE Stats Bucket Number: 2
   Last Updated  : 00:00:54 ago
    Packet Count  : 558
    Byte Count    : 46872
    One Way Delay : 55 msec*
    Loss Rate Pkts: 0.0 %
    Loss Rate Byte: 0.0 %
    Jitter Mean   : 556 usec
    Unreachable   : FALSE
   TCA Statistics:
      Received:133 ; Processed:133 ; Unreach_rcvd:0
  Latest TCA Bucket
   Last Updated  : 00:00:24 ago
    One Way Delay : 71 msec*
    Loss Rate Pkts: NA
    Loss Rate Byte: NA
    Jitter Mean   : NA
    Unreachability: FALSE
.
.
.
-------------------------------------------------------------------------------------------------

R10# show domain default border status

-------------------------------------------------------------------------------------------------

Tue Mar 24 04:52:50.379

**** Border Status ****
```

```
Instance Status: UP
Present status last updated: 3d14h ago
Loopback: Configured Loopback0 UP (10.2.10.10)
Master: 10.2.10.10
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 3d14h
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
Name: Tunnel100 Interface Index: 14 SNMP Index: 8 SP: MPLS Status: UP Zero-SLA: NO Path-id
 List: 0:10, 1:30
Name: Tunnel200 Interface Index: 15 SNMP Index: 9 SP: INET Status: UP Zero-SLA: NO Path-id
 List: 0:20, 1:40

Auto Tunnel information:

Name:Tunnel0 if_index: 13
Borders reachable via this tunnel:

-------------------------------------------------------------------------------------------------

R10# show domain default master status

-------------------------------------------------------------------------------------------------

*** Domain MC Status ***

Master VRF: Global

Instance Type: Branch
Instance id: 0
Operational status: Up
Configured status: Up
Loopback IP Address: 10.2.10.10
Load Balancing:
Operational Status: Up
Max Calculated Utilization Variance: 1%
Last load balance attempt: never
Last Reason: Variance less than 20%
Total unbalanced bandwidth:
External links: 0 Kbps Internet links: 0 Kbps
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
Minimum Mask Length: 28
Minimum Requirement: Met

Borders:
IP address: 10.2.10.10
Version: 2
Connection status: CONNECTED (Last Updated 3d14h ago )
Interfaces configured:
Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP | Zero-SLA: NO
Number of default Channels: 0

Path-id list: 0:10 1:30

Name: Tunnel200 | type: external | Service Provider: INET | Status: UP | Zero-SLA: NO
Number of default Channels: 0
```

```
Path-id list: 0:20 1:40

Tunnel if: Tunnel0

------------------------------------------------------------------------------------------------

R10# show domain default master site-capability 10.9.3.3 path-id

------------------------------------------------------------------------------------------------

Site id : 10.9.3.3
Site pop id : 1
Site mc type : Transit
Border Address : 10.9.4.4
Service provider: MPLS path-id: 30 if_index: 11
Border Address : 10.9.5.5
Service provider: INET path-id: 40 if_index: 11

------------------------------------------------------------------------------------------------

R10# show domain default master site-capability 10.8.3.3 path-id

------------------------------------------------------------------------------------------------

Site id : 10.8.3.3
Site pop id : 0
Site mc type : Hub
Border Address : 10.8.5.5
Service provider: INET path-id: 20 if_index: 11
Border Address : 10.8.4.4
Service provider: MPLS path-id: 10 if_index: 11

------------------------------------------------------------------------------------------------

R10#  show domain default border channels service-provider INET

------------------------------------------------------------------------------------------------

Tue Mar 24 04:53:39.968

Border Smart Probe Stats:

Smart probe parameters:
Source address used in the Probe: 10.2.10.10
Unreach time: 1000 ms
Probe source port: 18000
Probe destination port: 19000
Interface Discovery: ON
Probe freq for channels with traffic :10 secs
Discovery Probes: OFF
Number of transit probes consumed :0
Number of transit probes re-routed: 0
DSCP's using this: [0] [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15]
[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33]
[34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51]
[52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64]
All the other DSCPs use the default interval: 10 secs


Channel id: 6
Channel create time: 3d14h ago
Site id : 10.8.3.3
DSCP : default[0]
Service provider : INET
Pfr-Label : 0:20 | 0:0 [0x140000]
```

```
exit path-id: 0
Exit path-id sent on wire: 0
Number of Probes sent : 5657983
Number of Probes received : 5823008
Last Probe sent : 00:00:00 ago
Last Probe received : 00:00:00 ago
Channel state : Discovered and open
Channel next_hop : 10.0.200.85
RX Reachability : Reachable
TX Reachability : Reachable
Channel is sampling 0 flows
Channel remote end point: 10.0.200.85
Channel to hub: TRUE
Version: 3
Supports Zero-SLA: Yes
Muted by Zero-SLA: No
Probe freq with traffic : 1 in 10000 ms
.
.
.

------------------------------------------------------------------------------------------------

R10#  show ip nhrp nhs
------------------------------------------------------------------------------------------------

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel100:
10.0.100.84 RE NBMA Address: 172.16.84.4 priority = 0 cluster = 0
10.0.100.94 RE NBMA Address: 172.16.94.4 priority = 0 cluster = 0

Tunnel200:
10.0.200.85 RE NBMA Address: 172.16.85.5 priority = 0 cluster = 0
10.0.200.95 RE NBMA Address: 172.16.95.5 priority = 0 cluster = 0


------------------------------------------------------------------------------------------------
```



CHAPTER 5

# PfRv3 Zero SLA Support

The Performance Routing v3 (PfRv3) Zero SLA Support feature enables users to reduce probing frequency on various ISP links, such as 3G, 4G, and LTE. When the Zero SLA (0-SLA) feature is configured on an ISP link, only the channel with the DSCP (Differentiated Services Code Point) value 0 is probed. For all other DSCPs, channels are created only if there is traffic, but no probing is performed.



# Feature Information for PfRv3 Zero SLA Support

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 14: Feature Information for PfRv3 Zero SLA Support***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Path of Last Resort Support | 15.5(3)M | The PfRv3 Path of Last Resort is a route used by the device when a service provider cannot be reached or the exits are out of bandwidth.<br><br>The following commands were modified or added by this feature: **domain path isp-name**, **show domain default vrf border**, **show domain default vrf master**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| Performance Routing v3 Zero SLA Support | 15.5(1)T<br>Cisco IOS XE Release 3.14S | The Performance Routing v3 Zero SLA Support enables users to reduce probing frequency on various ISP links.<br>The following command was modified by this feature:**domain** (interface configuration). |

# Prerequisites for PfRv3 Zero SLA Support

- Upgrade hub-border routers with the latest Cisco IOS image to configure the Zero SLA feature.

# Restrictions for PfRv3 Zero SLA Support

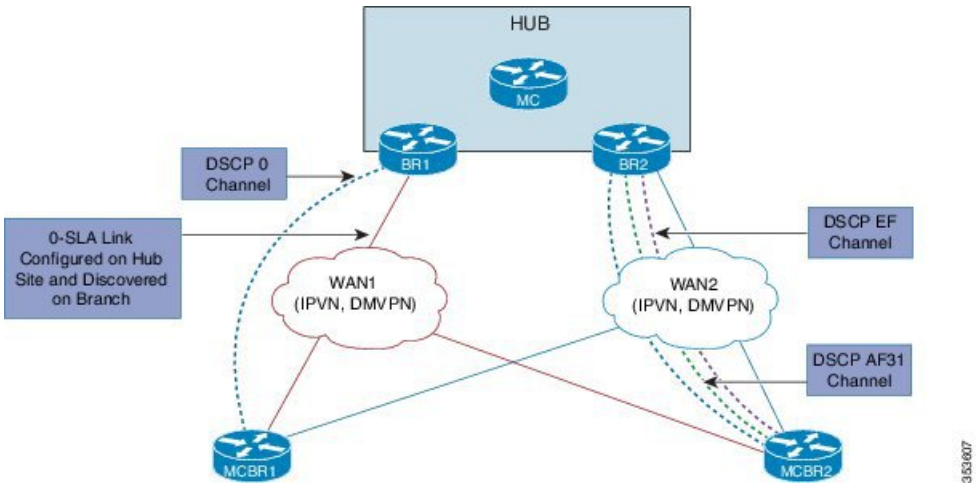
- Fast-monitor interval and brown out features are not supported with Zero SLA configurations.

# Information About PfRv3 Zero SLA Support

## Information About Zero SLA

The Zero SLA (0-SLA) feature enables users to reduce probing frequency in their network infrastructure. Reduction in probing process helps in reducing cost especially when ISPs charge based on traffic, and helps in optimizing network performance when ISPs provide limited bandwidth. When this feature is configured, probe is sent only on the DSCP-0 channel. For all other DSCPs, channels are created if there is traffic, but no probing is performed. The reachability of other channels is learnt from the DSCP-0 channel that is available at the same branch site.

*Figure 8: Probing on Zero SLA*




In the above illustration, the branch and hub sites are connected with red and blue ISP links. On the red ISP link, Zero SLA is configured at the hub site. Traffic exists on DSCP-0, DSCP AF31, and DSCP-EF channels on both ISP links, but on the red link probing is sent only on the DSCP-0 channel. A probe sent during the WAN discovery signals if a link is a Zero SLA link or a normal link.

# Information About Path of Last Resort

A Path of Last Resort is a route used by the device when a service provider cannot be reached or the exits are out of bandwidth. This feature is supported for 3G and 4G metered links. When the service provider is not available, the traffic is routed to the path of last resort if you have specified the **path of last resort** keyword in the **domain path** command. When the exits are up with optimum bandwidth, the links are transitioned back. The following are the different supported modes:

- Standby mode—No traffic classes are routed over the path of last resort service provider.
- Active mode—Traffic classes are routed over the path of last resort service provider.
- Disabled mode—The path of last resort is not enabled for the interface.

The path of last resort routes are muted when it is in standby mode. The smart probe frequency is reduced to 1 packet every 10 seconds from 20 packets per second.

# Compatibility Matrix for Zero SLA Support

In Performance Routing v3, capability negation happens through service advertisement framework (SAF) messages. When the PfR v3 domain comes up, it registers itself to the SAF to publish the compatibility and support for different release versions.

Use the **show domain default master site-capability** command to view the release version and the capability negation between hub and branch sites.

The following table shows the devices with various Cisco IOS/XE release versions and its support for Zero SLA within a single branch.

| Master Controller | Border Router | Compatibility Between Release Versions | Zero SLA Support |
|---|---|---|---|
| Cisco IOS XE Release 3.14 or later<br>Cisco IOS Release 15.5(1)T or later | Cisco IOS XE Release 3.14 or later<br>Cisco IOS Release 15.5(1)T or later | Yes | If the master controller and border routers have the same Cisco IOS release versions, the Zero SLA feature is enabled. |
| Cisco IOS XE Release 3.14 or later<br>Cisco IOS Release 15.5(1)T or later | Cisco IOS XE Release 3.13 or earlier<br>Cisco IOS Release 15.4T or earlier | Yes | If the master controller has the latest Cisco IOS release and the border router has the earlier release version, the Zero SLA feature is disabled. |
| Cisco IOS XE Release 3.13<br>Cisco IOS Release 15.4T | Cisco IOS XE Release 3.13<br>Cisco IOS Release 15.4T | Yes | Zero SLA is not supported on Cisco IOS XE Release 3.13. |
| Cisco IOS XE Release 3.13<br>Cisco IOS Release 15.4T | Cisco IOS XE Release 3.14 or later<br>Cisco IOS Release 15.5(1)T or later | No | The release versions are not compatible and hence, Zero SLA cannot be enabled. |

**Note**

- If you are configuring PfRv3 on a site, it is mandatory that the hub master and the hub border routers in a site are on the same version of the Cisco IOS XE software.
- In a site, the branch master controller and the associated borders in the branch should also have the same version of the Cisco IOS XE software. But, it is not mandatory for the software version on the hub master or the hub border to match the software version on the branch master controller and its borders.
- Ensure that the Cisco IOS XE software version installed on the hub master, hub border router, branch master controller and borders support Zero SLA.

# How to Configure PfRv3 Zero SLA Support

## Configuring PfRv3 Zero SLA Support

Configure the Zero SLA (0-SLA) feature on the border router at the hub site.

### Before you begin

Configure PfRv3 topology on the hub and branch site. For more information on configuring PfRv3, see the "How to Configure PfRv3" topic in the *Performance Routing v3 Configuration Guide*.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **bandwidth** *bandwidth-value*
5. **ip address** *ip-address mask*
6. **domain path** *isp-name* [**internet-bound** | **path-id** | **path-last-resort** | **zero-sla**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface tunnel** *tunnel-number*<br>**Example:**<br>`Device(config)# interface tunnel 100` | Enters interface configuration mode. |
| **Step 4** | **bandwidth** *bandwidth-value*<br>**Example:**<br>`Device(config-if)# bandwidth 10000000` | Configures inherited and received bandwidth values for the tunnel interface. The bandwidth value is in kilobits and the valid values are 1 to 10000000. |
| **Step 5** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.32.1.1 255.0.0.0` | Configures an IP address of the border router at the hub site. |
| **Step 6** | **domain path** *isp-name* [**internet-bound** \| **path-id** \| **path-last-resort** \| **zero-sla**]<br>**Example:**<br>`Device(config-if)# domain path ISP1 zero-sla` | Specifies a service provider for the interface.<br>• **internet-bound**—Configures an internet bound interface.<br>• **path-id**—Configures service provider's path-id for the interface.<br>• **path-last-resort**—Configures the interface to be a path of a last resort.<br>• **zero-sla**—Configures Zero SLA for the interface.<br>**Note** You can configure multiple Internet Service Providers (ISPs). If you are defining a specific domain name for an ISP (for example, domain_abc), you must specify the same domain name while configuring the ISP paths. |

# Verifying PfRv3 Zero SLA Support

The **show** commands can be entered in any order.

### Before you begin

Configure Zero SLA on the hub-border router.

### SUMMARY STEPS

1. **show domain default master status**
2. **show domain default master channel**
3. **show domain default border status**
4. **show domain default border channel**
5. **show domain default master site-capability**
6. **show domain default vrf** *vrf-name* **master status**
7. **show domain default vrf** *vrf-name* **border status**
8. **show domain default vrf** *vrf-name* **master channels**
9. **show domain default vrf** *vrf-name* **border channels**
10. **show domain default vrf** *vrf-name* **master policy**

### DETAILED STEPS

**Step 1** **show domain default master status**

Displays the status of the hub master controller.

**Step 2** **show domain default master channel**

Displays channel information of the hub master controller.

**Step 3** **show domain default border status**

Displays the status of the hub border routers.

**Step 4** **show domain default border channel**

Displays the information of border router channels at the hub site.

**Step 5** **show domain default master site-capability**

Displays the capability information of master controller.

**Example:**

```
Device# show domain default master site-capability

Device Capability

------------------------------------------------------------
|       Capability          |     Major     |     Minor      |
------------------------------------------------------------
|     Domain                |     2         |      0         |
------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
------------------------------------------------------------
```

```
Site id  :10.2.10.10

------------------------------------------------------------
|       Capability          |     Major     |     Minor      |
------------------------------------------------------------
|     Domain                |     2         |      0         |
------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
------------------------------------------------------------
Site id  :10.2.12.12

------------------------------------------------------------
|     Capability            |     Major     |     Minor      |
------------------------------------------------------------
|     Domain                |     2         |      0         |
------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
------------------------------------------------------------
```

*Table 15:* ***show domain default master site-capability*** *Field Descriptions*

| Field | Description |
|---|---|
| Capability | Features supported by PfR v3 domain. |
| Domain | Domain version.<br>Major - Means the major release version number for PfR v3.<br>Minor - Means the minor release version number for PfR v3. |
| Zero-SLA | Zero-SLA feature support.<br>Major - Means the major release version of the Zero-SLA feature on the master controller.<br>Minor - Means the minor release version of the Zero-SLA feature on the master controller. |

**Step 6** **show domain default vrf** *vrf-name* **master status**

Displays the master status of the hub border routers.

**Example:**

```
Device# show domain default vrf vrf1 master status

Borders:
  IP address: 10.204.1.4
  Version: 2
  Connection status: CONNECTED (Last Updated 00:59:16 ago )
  Interfaces configured:
   Name: Tunnel20 | type: external | Service Provider: ISP2 | Status: UP | Zero-SLA: NO | Path of
Last Resort: Disabled
    Number of default Channels: 0
  Tunnel if: Tunnel1
  IP address: 10.203.1.3
  Version: 2
  Connection status: CONNECTED (Last Updated 00:59:16 ago )
```

```
  Interfaces configured:
    Name: Tunnel10 | type: external | Service Provider: ISP1 | Status: UP | Zero-SLA: YES | Path
of
Last Resort: Standby
      Number of default Channels: 0
  Tunnel if: Tunnel1
```

**Step 7** **show domain default vrf** *vrf-name* **border status**

Displays the master status of the hub border routers.

**Example:**

```
Device# show domain default vrf vrf1 border status

------------------------------------------------------------------------
**** Border Status ****
Instance Status: UP
Present status last updated: 01:01:42 ago
Loopback: Configured Loopback1 UP (30.209.1.9)
Master: 30.209.1.9
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 01:01:42
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
    Name: Tunnel10 Interface Index: 16 SNMP Index: 13 SP: ISP1 path-id: 0 Status: UP Zero-SLA: YES
Path of Last Resort: Standby Path-id List: 0:0
  Name: Tunnel20 Interface Index: 18 SNMP Index: 15 SP: ISP2 Status: UP Zero-SLA: NO Path of Last
Resort: Disabled Path-id List: 0:0


Auto Tunnel information:


   Name:Tunnel1 if_index: 21
   Borders reachable via this tunnel:
------------------------------------------------------------------------
```

**Step 8** **show domain default vrf** *vrf-name* **master channels**

Displays the master status of the hub master controller.

**Example:**

```
Device# show domain default vrf vrf1 master channels

Channel Id: 9 Dst Site-Id: 30.209.1.9 Link Name: ISP1 DSCP: af41 [34] pfr-label: 0:0 | 0:0 [0x0]
TCs: 0
  Channel Created: 00:57:15 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: FALSE
  Interface Id: 16
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: Yes
  Muted by Path of Last Resort: Yes
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
    Total Performance Count: 0, Total BW Count: 0
```

```
  ODE Stats Bucket Number: 1
    Last Updated : 00:56:15 ago
     Packet Count : 505
     Byte Count : 42420
     One Way Delay : 229 msec*
     Loss Rate Pkts: 0.0 %
     Loss Rate Byte: 0.0 %
     Jitter Mean : 535 usec
     Unreachable : FALSE
    TCA Statistics:
     Received:1 ; Processed:1 ; Unreach_rcvd:0
  Latest TCA Bucket
    Last Updated : 00:56:15 ago
     One Way Delay : 229 msec*
     Loss Rate Pkts: NA
     Loss Rate Byte: NA
     Jitter Mean : NA
     Unreachability: FALSE
```

**Step 9** **show domain default vrf** *vrf-name* **border channels**

Displays the information of border router channels at the hub site.

**Example:**

```
Device# show domain default vrf vrf1 border channels

Channel id: 2
 Channel create time: 00:46:02 ago
 Site id : 255.255.255.255
 DSCP : default[0]
 Service provider : ISP1
 Pfr-Label : 0:0 | 0:0 [0x0]
 exit path-id: 0
 Exit path-id sent on wire: 0
 Number of Probes sent : 0
 Number of Probes received : 0
 Last Probe sent : 00:46:02 ago
 Last Probe received : - ago
 Channel state : Initiated and open
 Channel next_hop : 0.0.0.0
 RX Reachability : Initial State
 TX Reachability : Reachable
 Channel is sampling 0 flows
 Channel remote end point: 0.0.0.0
 Channel to hub: FALSE
 Version: 0
 Supports Zero-SLA: No
 Muted by Zero-SLA: No
 Muted by Path of Last Resort: Yes
 Probe freq with traffic : 1 in 10000 ms
```

**Step 10** **show domain default vrf** *vrf-name* **master policy**

Displays the status of the master policy.

**Example:**

```
Device# show domain default vrf vrf1 master policy

class VOICE sequence 10
  path-last-resort ISP1
  class type: Dscp Based
    match dscp ef policy custom
```

```
priority 1 one-way-delay threshold 200 msec
Number of Traffic classes using this policy: 2
```

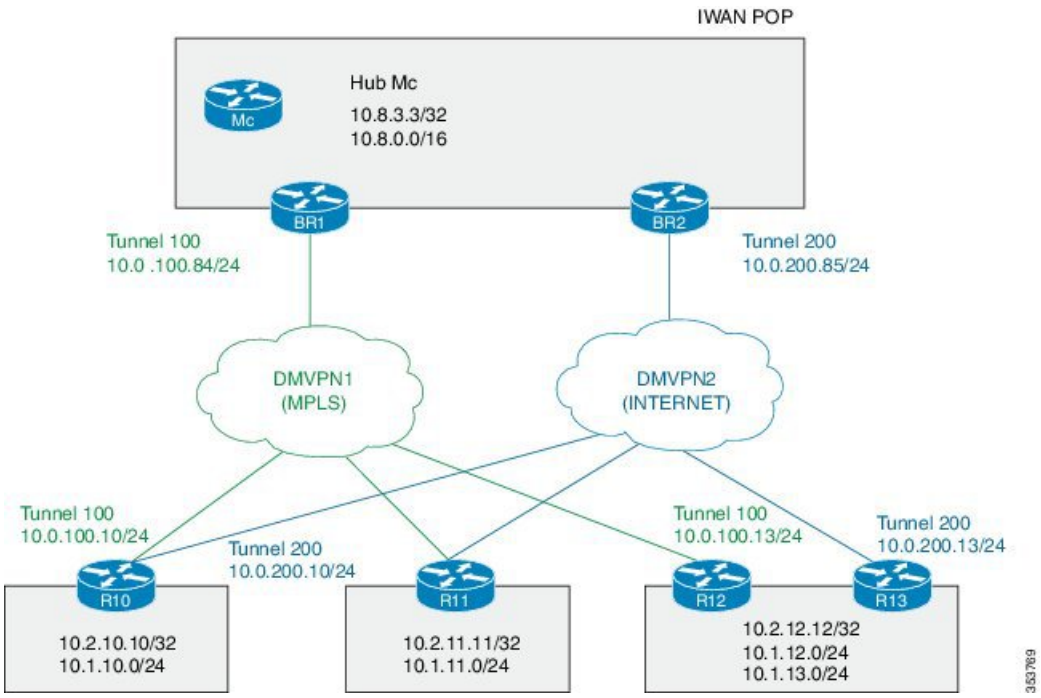
# Configuration Examples for PfRv3 Zero SLA Support

## Example: Configuring PfRv3 Zero SLA Support

Let us consider a use case scenario, where the service provider of a large enterprise network wants to reduce the probing frequency on all its channels. To reduce probing, Zero-SLA is configured on the ISP link from BR1.

**Note** In the following example, only the hub master controller, BR1 (border router 1), R10 and R11 (branch border router) configurations are described.

***Figure 9: PfRv3 Topology***




In this example, the following routers are used:

- Hub Master Controller — Cisco ASR 1002-X router configured with an embedded services processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps.
- Hub Border Routers — Cisco ASR 1000 Series Embedded Services Processor 2

- Branch Routers — Cisco 4451X Integrated Services Router.

### Configure the interfaces on hub master controller

```
HubMC> enable
HubMC# configure terminal
HubMC(config)# interface Loopback0
HubMC(config-if)# ip address 10.8.3.3 255.255.255.255
HubMC(config-if)# exit
```

### Configure the device as hub-master controller

```
HubMC(config)# domain one
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE
HubMC(config-domain-vrf-mc)# site-prefixes prefix-list DATA_CENTER_1
HubMC(config-domain-vrf-mc)# exit
```

### Configure IP prefix-lists

```
HubMC(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24
HubMC(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24
```

### Configure domain policies on hub master controller

```
HubMC(config)# domain one
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# monitor-interval 2 dscp ef
HubMC(config-domain-vrf-mc)# load-balance
HubMC(config-domain-vrf-mc)# class VOICE sequence 10
HubMC(config-domain-vrf-mc-class)# match dscp ef policy voice
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc)# class VIDEO sequence 20
HubMC(config-domain-vrf-mc-class)# match dscp af41 policy real-time-video
HubMC(config-domain-vrf-mc-class)# match dscp cs4 policy real-time-video
HubMC(config-domain-vrf-mc-class)# path-preference INET fallback MPLS
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc)# class CRITICAL sequence 30
HubMC(config-domain-vrf-mc-class)# match dscp af31 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600
HubMC(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 600
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
```

### Configure the interfaces on hub border router (BR1)

```
BR1> enable
BR1# configure terminal
BR1(config)# interface Loopback0
BR1(config-if)# ip address 10.8.1.1 255.255.255.255
BR1(config-if)exit
```

### Configure the device as border router (BR1)

```
BR1(config)# domain one
BR1(config-domain)# vrf default
BR1(config-domain-vrf)# border
BR1(config-domain-vrf-br)# source-interface Loopback0
BR1(config-domain-vrf-br)# master 10.8.3.3
BR1(config-domain-vrf-br)# exit
```

### Configure tunnel from BR1 to DMVPN1 (MPLS)Link

```
BR1(config)# interface Tunnel100
BR1(config-if)# bandwidth 100000
BR1(config-if)# ip address 10.0.100.84 255.255.255.0
BR1(config-if)# no ip redirects
BR1(config-if)# ip mtu 1400
BR1(config-if)# ip nhrp authentication cisco
BR1(config-if)# ip nhrp map multicast dynamic
BR1(config-if)# ip nhrp network-id 1
BR1(config-if)# ip nhrp holdtime 600
BR1(config-if)# ip tcp adjust-mss 1360
BR1(config-if)# load-interval 30
BR1(config-if)# tunnel source GigabitEthernet3
BR1(config-if)# tunnel mode gre multipoint
BR1(config-if)# tunnel key 100
BR1(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
BR1(config-if)# domain one path MPLS
```

### Configure Zero-SLA on BR1 to DMVPN1 (MPLS)Link

```
BR1(config-if)# domain one path MPLS zero-sla
```

### Configure the interfaces (R10)

```
R10> enable
R10# configure terminal
R10(config)# interface Loopback0
R10(config-if)# ip address 10.2.10.10 255.255.255.255
R10(config-if)exit
```

### Configure the device as branch master controller (R10)

```
R10(config)# domain one
R10(config-domain)# vrf default
R10(config-domain-vrf)# border
R10(config-domain-vrf-br)# source-interface Loopback0
R10(config-domain-vrf-br)# master local
R10(config-domain-vrf-br)# exit
R10(config-domain-vrf)# master branch
R10(config-domain-vrf-mc)# source-interface Loopback0
R10(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R10

```
R10(config)# interface Tunnel100
R10(config-if)# bandwidth 100000
R10(config-if)# ip address 10.0.100.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map 10.0.100.84 172.16.84.4
R10(config-if)# ip nhrp map multicast 172.16.84.4
R10(config-if)# ip nhrp network-id 1
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.100.84
R10(config-if)# ip nhrp registration timeout 60
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# tunnel source GigabitEthernet2
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 100
R10(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
R10(config-if)# domain one path MPLS
```

### Configure another tunnel path from R10

```
R10(config)# interface Tunnel200
R10(config-if)# bandwidth 50000
R10(config-if)# ip address 10.0.200.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R10(config-if)# ip nhrp multicast 172.16.85.5
R10(config-if)# ip nhrp network-id 2
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.200.85
R10(config-if)# ip tcp adjust-mss 1360
R10(config-if)# load-interval 30
R10(config-if)# delay 1000
R10(config-if)# tunnel source GigabitEthernet3
R10(config-if)# tunnel mode gre multipoint
R10(config-if)# tunnel key 200
R10(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
R10(config-if)# domain one path INET
```

### Configure the interfaces (R11)

```
R11> enable
R11# configure terminal
R11(config)# interface Loopback0
R11(config-if)# ip address 10.2.11.11 255.255.255.255
R11(config-if)# exit
```

### Configure the device as branch master controller (R11)

```
R11(config)# domain one
R11(config-domain)# vrf default
R11(config-domain-vrf)# border
R11(config-domain-vrf-br)# source-interface Loopback0
R11(config-domain-vrf-br)# master local
R11(config-domain-vrf-br)# exit
R11(config-domain-vrf)# master branch
R11(config-domain-vrf-mc)# source-interface Loopback0
R11(config-domain-vrf-mc)# hub 10.8.3.3
```

### Configure the tunnel interface and tunnel path from R11

```
R11(config)# interface Tunnel100
R11(config-if)# bandwidth 100000
R11(config-if)# ip address 10.0.100.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map 10.0.100.84 172.16.84.4
R11(config-if)# ip nhrp map multicast 172.16.84.4
R11(config-if)# ip nhrp network-id 1
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nhs 10.0.100.84
R11(config-if)# ip nhrp registration timeout 60
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# tunnel source GigabitEthernet2
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 100
R11(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
R11(config-if)# domain one path MPLS
```

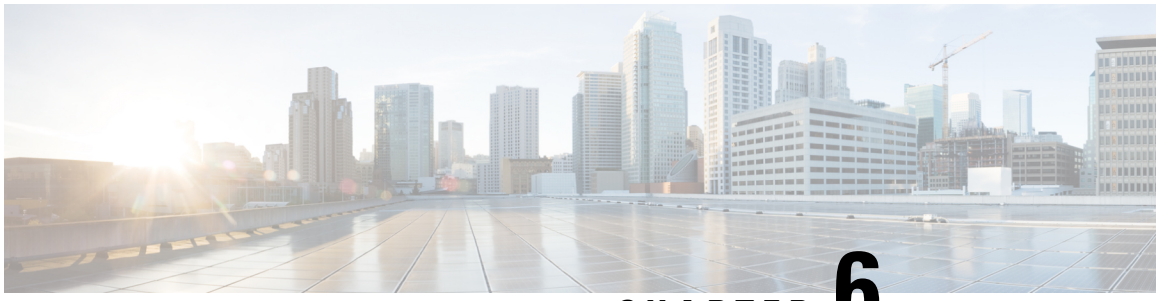
### Configure another tunnel path from R11

```
R11(config)# interface Tunnel200
R11(config-if)# bandwidth 50000
R11(config-if)# ip address 10.0.200.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R11(config-if)# ip nhrp multicast 172.16.85.5
R11(config-if)# ip nhrp network-id 2
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nhs 10.0.200.85
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# tunnel source GigabitEthernet3
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 200
R11(config-if)# tunnel vrf INET2
R11(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
R11(config-if)# domain one path INET
```

### Verifying PfRv3 Zero-SLA Configurations

To verify the PfRv3 Zero-SLA configuration, use the following show commands in any order:

- **show domain** *domain-name* **master status**
- **show domain** *domain-name* **border status**
- **show domain** *domain-name* **master channel**
- **show domain** *domain-name* **border channel**
- **show domain** *domain-name* **master site-capability**



CHAPTER 6

# PfRv3 Path of Last Resort

The PfRv3 path of last resort feature allows the traffic to be routed to the path of last resort.



## Feature Information for PfRv3 Path of Last Resort

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 16: Feature Information for PfRv3 Path of Last Resort***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Path of Last Resort | 15.5(3)M | The PfRv3 Path of Last Resort is a route used by the device when a service provider cannot be reached or the exits are out of bandwidth.<br><br>The following commands were modified or added by this feature: **domain path isp-name**, **show domain default vrf border**, **show domain default vrf master**. |

## Restrictions for PfRv3 Path of Last Resort

- Path of last resort supports probing per interface and not per channel.
- Path of last resort is not supported on multi next hop interfaces.

# Information About PfRv3 Path of Last Resort

## PfRv3 Path of Last Resort

The PfRv3 Path of Last Resort feature provides the ability to designate a service provider as a path of last resort such that when the primary and fallback service providers become unavailable due to unreadability or out of bandwidth situations, traffic is routed over the path of last resort service provider. This feature is used for metered links where data is charged on a per-usage basis and is used when no other service providers are available.

The following are the different supported modes:

- Standby mode—No traffic classes are currently routed over the path of last resort service provider.
- Active mode—Traffic classes are currently routed over the path of last resort service provider.
- Disabled mode—The path of last resort is not enabled.

The channels of the path of last resort are inactive when it is in standby mode. Once the path of last resort is active, smart probes are sent only on DSCP 0 (Zero SLA) to conserve bandwidth. In addition, smart probe frequency is reduced to 1 packet every 10 seconds from 20 packets per seconds, unreachable detection are extended to 60 seconds.

# How to Configure PfRv3 Path of Last Resort

## Configuring Policy for Path of Last Resort

To configure policy for path of last resort, perform the steps below.

### SUMMARY STEPS

1. **domain default**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **domain default**<br>**Example:**<br>`domain default`<br>`  vrf default`<br>`  master hub`<br>`  class foo seq 1`<br>`  match dscp ef policy voice`<br>`  path-preference ISP1 fallback ISP2`<br>`  path-last-resort ISP4` | The keyword specifics that the traffic for this policy is routed over the path of last resort when the primary and fallback service providers are unavailable. |

# Configuring Path of Last Resort

To configure path of last resort, perform the steps below.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **domain path** *isp-name* [**internet-bound** | **path-id** | **path-last-resort** | **zero-sla**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface tunnel** *tunnel-number*<br>**Example:**<br>`Device(config)# interface tunnel 100` | Enters interface configuration mode. |
| **Step 4** | **domain path** *isp-name* [**internet-bound** \| **path-id** \| **path-last-resort** \| **zero-sla**]<br>**Example:**<br>`Device(config-if)# domain path ISP1 path-last-resort` | Specifies a service provider for the interface.<br>• **internet-bound**—Configures an internet bound interface.<br>• **path-id**—Configures service provider's path-id for the interface.<br>• **path-last-resort**—Configures the interface to be a path of a last resort.<br>• **zero-sla**—Configures Zero SLA for the interface.<br>**Note** You can configure multiple Internet Service Providers (ISPs). If you are defining a specific domain name for an ISP (for example, domain_abc), you must specify the same domain name while configuring the ISP paths. |

# Verifying PfRv3 Path of Last Resort

The **show** commands can be entered in any order.

## SUMMARY STEPS

1. **show domain default vrf** *vrf-name* **master status**
2. **show domain default vrf** *vrf-name* **border status**
3. **show domain default vrf** *vrf-name* **master channels**
4. **show domain default vrf** *vrf-name* **border channels**
5. **show domain default vrf** *vrf-name* **master policy**

## DETAILED STEPS

### Step 1 show domain default vrf *vrf-name* master status

Displays the master status of the hub border routers.

**Example:**

```
Device# show domain default vrf vrf1 master status

Borders:
  IP address: 10.204.1.4
  Version: 2
  Connection status: CONNECTED (Last Updated 00:59:16 ago )
  Interfaces configured:
   Name: Tunnel20 | type: external | Service Provider: ISP2 | Status: UP | Zero-SLA: NO | Path of
Last Resort: Disabled
    Number of default Channels: 0
  Tunnel if: Tunnel1
  IP address: 10.203.1.3
  Version: 2
  Connection status: CONNECTED (Last Updated 00:59:16 ago )
  Interfaces configured:
    Name: Tunnel10 | type: external | Service Provider: ISP1 | Status: UP | Zero-SLA: YES | Path of
Last Resort: Standby
      Number of default Channels: 0
  Tunnel if: Tunnel1
```

### Step 2 show domain default vrf *vrf-name* border status

Displays the master status of the hub border routers.

**Example:**

```
Device# show domain default vrf vrf1 border status

------------------------------------------------------------------------
**** Border Status ****
Instance Status: UP
Present status last updated: 01:01:42 ago
Loopback: Configured Loopback1 UP (30.209.1.9)
Master: 30.209.1.9
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 01:01:42
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
    Name: Tunnel10 Interface Index: 16 SNMP Index: 13 SP: ISP1 path-id: 0 Status: UP Zero-SLA: YES
```

```
Path of Last Resort: Standby Path-id List: 0:0
  Name: Tunnel20 Interface Index: 18 SNMP Index: 15 SP: ISP2 Status: UP Zero-SLA: NO Path of Last
Resort: Disabled Path-id List: 0:0


Auto Tunnel information:


   Name:Tunnel1 if_index: 21
   Borders reachable via this tunnel:
---------------------------------------------------------------------
```

**Step 3** **show domain default vrf** *vrf-name* **master channels**

Displays the master status of the hub master controller.

**Example:**

```
Device# show domain default vrf vrf1 master channels

Channel Id: 9 Dst Site-Id: 30.209.1.9 Link Name: ISP1 DSCP: af41 [34] pfr-label: 0:0 | 0:0 [0x0]
TCs: 0
  Channel Created: 00:57:15 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: FALSE
  Interface Id: 16
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: Yes
  Muted by Path of Last Resort: Yes
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
    Total Performance Count: 0, Total BW Count: 0
  ODE Stats Bucket Number: 1
    Last Updated : 00:56:15 ago
     Packet Count : 505
     Byte Count : 42420
     One Way Delay : 229 msec*
     Loss Rate Pkts: 0.0 %
     Loss Rate Byte: 0.0 %
     Jitter Mean : 535 usec
     Unreachable : FALSE
    TCA Statistics:
     Received:1 ; Processed:1 ; Unreach_rcvd:0
  Latest TCA Bucket
    Last Updated : 00:56:15 ago
     One Way Delay : 229 msec*
     Loss Rate Pkts: NA
     Loss Rate Byte: NA
     Jitter Mean : NA
     Unreachability: FALSE
```

**Step 4** **show domain default vrf** *vrf-name* **border channels**

Displays the information of border router channels at the hub site.

**Example:**

```
Device# show domain default vrf vrf1 border channels

Channel id: 2
 Channel create time: 00:46:02 ago
 Site id : 255.255.255.255
 DSCP : default[0]
 Service provider : ISP1
```

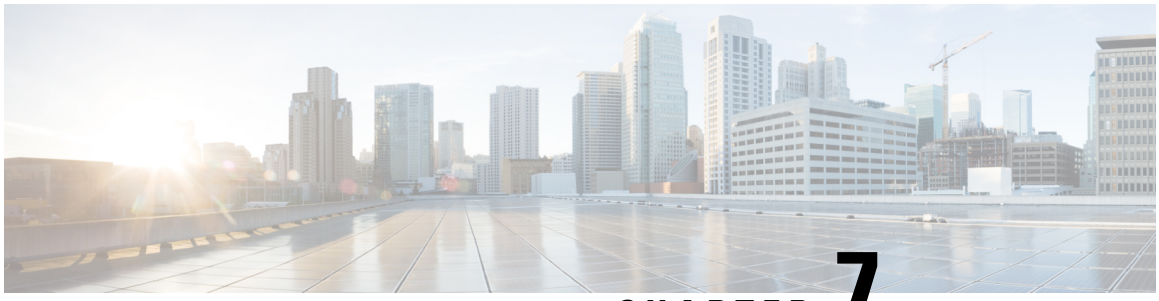
```
Pfr-Label : 0:0 | 0:0 [0x0]
exit path-id: 0
Exit path-id sent on wire: 0
Number of Probes sent : 0
Number of Probes received : 0
Last Probe sent : 00:46:02 ago
Last Probe received : - ago
Channel state : Initiated and open
Channel next_hop : 0.0.0.0
RX Reachability : Initial State
TX Reachability : Reachable
Channel is sampling 0 flows
Channel remote end point: 0.0.0.0
Channel to hub: FALSE
Version: 0
Supports Zero-SLA: No
Muted by Zero-SLA: No
Muted by Path of Last Resort: Yes
Probe freq with traffic : 1 in 10000 ms
```

**Step 5** **show domain default vrf** *vrf-name* **master policy**

Displays the status of the master policy.

**Example:**

```
Device# show domain default vrf vrf1 master policy

class VOICE sequence 10
  path-last-resort ISP1
  class type: Dscp Based
    match dscp ef policy custom
      priority 1 one-way-delay threshold 200 msec
      Number of Traffic classes using this policy: 2
```



CHAPTER 7

# PfRv3 Probe Reduction

This document provides information about the PfRv3 Probe Reduction feature that allows reducing traffic probe on channels that do not carrying any traffic.



## Feature Information for PfRv3 Probe Reduction

*Table 17: Feature Information for PfRv3 Probe Reduction*

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Probe Reduction | | This document provides information about the PfRv3 Probe Reduction feature that allows reducing traffic probe on channels that do not carrying any traffic.<br>The following command was introduced: **smart-probes burst** |

## Prerequisites for PfRv3 Probe Reduction

## Information About PfRv3 Probe Reduction

The PfRv3 Probe Reduction feature allows reducing traffic probe on channels that do not carry any traffic. Probing is used to compute important metrics such as reachability, one-way delay (OWD), jitter, and loss on channels that do not have user traffic. It helps PfRv3 algorithm to choose the best channel to use for a given traffic class.

A domain level parameter is defined to store the probing information. You need to store two sets of parameters; general monitor and quick monitor. In other words, one can specify the number of packets to be sent in a probe burst and the interval between such bursts.

Smart probe are of three types:

- **Active Channel Probe**—Active channel probe is sent out to measure network delay if no probe is sent out for past 10 seconds interval.
- **Unreachable Probe**—Unreachable probe is used to detect channel reachability when there is no traffic send out.
- **Burst Probe**—Burst probes are used to calculate delay, loss, jitter on a channel that is not carrying active user traffic.

# How to Configure PfRv3 Probe Reduction

## Configuring PfRv3 Probe Reduction

You can perform this task on a hub master or a border device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **domain default**
4. Do one of the following:
   - **master hub**
   - **border**
5. **advanced**
6. **smart-probes burst** [**quick**] *number-of-packets* **packets every** *interval* **seconds**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **domain default**<br>**Example:**<br>`Device(config)# domain default` | Enters domain configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Do one of the following:<br>• **master hub**<br>• **border**<br>**Example:**<br>`Device(config-domain)# master hub`<br>**Example:**<br>`Device(config-domain)# border` | Configures the device as a master hub and enters master controller configuration mode.<br>Configures the device as the border and enters border configuration mode.<br>**Note** If you select border configuration, it overwrites the master configuration. |
| **Step 5** | **advanced**<br>**Example:**<br>`Device(config-domain-mc)# advanced`<br>**Example:**<br>`Device(config-domain-br)# advanced` | Enters advanced configuration mode. |
| **Step 6** | **smart-probes burst** [**quick**] *number-of-packets* **packets every** *interval* **seconds**<br>**Example:**<br>`Device(config-domain-mc-advanced)# smart-probe burst 10 packets every 20 seconds`<br>**Example:**<br>`Device(config-domain-br-advanced)# smart-probe burst quick 10 packets every 1 seconds` | Specifies the number of packets to be sent in a probe burst and the interval between the bursts. The default values are as follows:<br>• 1 packet every 1 second for default monitor<br>• 20 packets every 1 second for quick monitor |

# Verifying PfRv3 Probe Reduction

### SUMMARY STEPS

1. **show domain** {**default** | *domain-name*} [**vrf** *vrf-name*] {**master** | **border**} **status**

### DETAILED STEPS

**show domain** {**default** | *domain-name*} [**vrf** *vrf-name*] {**master** | **border**} **status**

Use this command to verify the configuration.

**Example:**

```
Router# show domain default vrf green master status

Smart Probe Profile:
    General Monitor:
        Current Provision Level: Master Hub
            Master Hub:
                Packets per burst: 10
                Interval(secs): 20
    Quick Monitor:
        Current Provision Level: Master Hub
```

```
            Master Hub:
                Packets per burst: 10
                Interval(secs): 1
Smart Probe Inter-Packet Gap (ms) : 16
Smart Probe Timer Wheel Granularity (ms): 8
```

# Configuration Examples for PfRv3 Probe Reduction

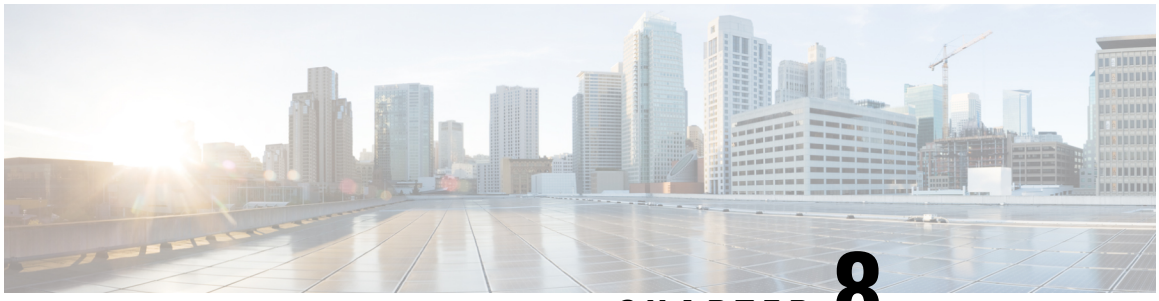
## Example: PfRv3 Probe Reduction

```
domain default
 master hub
  advanced
   smart-probe burst 10 packets every 20 seconds
   smart-probe burst quick 10 packets every 1 seconds
```

# Additional References for PfRv3 Probe Reduction

### Related Documents

| Related Topic | Document Title |
|---|---|
| Performance Routing Version 3 commands | Cisco IOS Performance Routing Version 3 Command Reference |



CHAPTER 8

# Path Preference Hierarchy

The Path Preference Hierarchy feature allows you to configure service providers per VRF for traffic classes.



# Feature Information for Path Preference Hierarchy

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 18: Feature Information for Path Preference Hierarchy***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Path Preference Hierarchy | Cisco IOS XE Denali 16.3.1 | The Path Preference Hierarchy feature allows you to configure service providers per VRF for traffic classes.<br>The following command was introduced or modified: **path-preference**. |

# Information About Path Preference Hierarchy

## Overview of Path Preference Hierarchy

In an enterprise network, you would need to configure service providers to interconnect the hub and branches. The Path Preference Hierarchy feature allows you to configure three service providers per VRF for traffic classes. The service providers could be primary service provider, fallback service provider, and next-fallback service provider respectively. As the name suggests, the primary service provider is the first preference in the network, followed by fallback and next-fallback, respectively. You cannot have the same service provider for

primary and fallback as this results in a “fallback backhole.” In other words, each service provider must be unique.

Use the **path-preference** command to specify the service provider order. Use the **blackhole** or **routing** keywords for a next-fallback service provider to drop the packet if fallback is unavailable or to specify there is no next-fallback service provider, respectively. When a packet reaches “blackhole,” the packet is discarded.

# How to Configure Path Preference Hierarchy

## Configuring Path Preference Hierarchy

Perform this task to configure Path Preference Hierarchy feature on a hub.

```
domain default
 vrf green
  master hub
   source-interface Loopback1
   site-prefixes prefix-list HUBPFX
   class HEIRARCHICAL sequence 100
    match dscp ef policy custom
     priority 1 loss threshold 10
    path-preference ISP1 ISP2 fallback ISP3 next-fallback blackhole
```

The following is a sample output on a device that displays the route change reason and history. In this example, the traffic class jumps from next-fallback service provider to primary service provider, when the fallback is unavailable.

```
Dst-Site-Prefix: 100.30.0.0/16       DSCP: ef [46] Traffic class id:2
  Clock Time:                 12:57:15 (PST) 03/30/2015
  TC Learned:                 00:22:14 ago
  Present State:              CONTROLLED
  Current Performance Status: in-policy
  Current Service Provider:   ISP2 path-id:2 since 00:03:28
  Previous Service Provider:  ISP3 pfr-label: 0:0 | 0:7 [0x7] for 180 sec
  (A fallback/next-fallback provider. Primary provider will be re-evaluated 00:02:34 later)

  BW Used:                    3 Kbps
  Present WAN interface:      Tunnel20 in Border 100.10.2.1
  Present Channel (primary):  46 ISP2 pfr-label:0:0 | 0:2 [0x2]
  Backup Channel:             42 ISP3 pfr-label:0:0 | 0:7 [0x7]
  Destination Site ID bitmap: 0
  Destination Site ID:        100.30.1.1
  Class-Sequence in use:      10
  Class Name:                 BUSINESS using policy User-defined
    priority 2 packet-loss-rate threshold 10.0 percent
    priority 2 byte-loss-rate threshold 10.0 percent
  BW Updated:                 00:00:14 ago
  Reason for Latest Route Change:    next-fallback to Higher Path Preference
  Route Change History:
              Date and Time                    Previous Exit                          Current
 Exit                      Reason

    1:  12:53:47 (PST) 03/30/2015   ISP3/100.10.1.1/Tu30 (Ch:42)
ISP2/100.10.2.1/Tu20 (Ch:46)            next-fallback to Higher Path Preference
    2:  12:50:47 (PST) 03/30/2015   None/0.0.0.0/None (Ch:0)
ISP3/100.10.1.1/Tu30 (Ch:42)            Uncontrolled to Controlled Transition
    3:  12:50:15 (PST) 03/30/2015   ISP3/100.10.1.1/Tu30 (Ch:42)          None/0.0.0.0/None
 (Ch:0)                No Channels Available
    4:  12:48:14 (PST) 03/30/2015   ISP2/100.10.4.1/Tu20 (Ch:43)
```

```
ISP3/100.10.1.1/Tu30 (Ch:42)            Exit down
    5:  12:47:57 (PST) 03/30/2015   ISP2/100.10.2.1/Tu20 (Ch:46)
ISP2/100.10.4.1/Tu20 (Ch:43)            Exit down
```

In the following example, continuation of the above example, the traffic class is now controlled by primary service provider.

```
 Route Change History:
             Date and Time                  Previous Exit                          Current
 Exit                      Reason

    1:  12:59:49 (PST) 03/30/2015   ISP2/100.10.2.1/Tu20 (Ch:46)
ISP1/100.10.1.1/Tu10 (Ch:41)            Backup to Primary path preference transition
    2:  12:53:47 (PST) 03/30/2015   ISP3/100.10.1.1/Tu30 (Ch:42)
ISP2/100.10.2.1/Tu20 (Ch:46)            next-fallback to Higher Path Preference
    3:  12:50:47 (PST) 03/30/2015   None/0.0.0.0/None (Ch:0)
ISP3/100.10.1.1/Tu30 (Ch:42)            Uncontrolled to Controlled Transition
    4:  12:50:15 (PST) 03/30/2015   ISP3/100.10.1.1/Tu30 (Ch:42)          None/0.0.0.0/None
 (Ch:0)                No Channels Available
    5:  12:48:14 (PST) 03/30/2015   ISP2/100.10.4.1/Tu20 (Ch:43)
ISP3/100.10.1.1/Tu30 (Ch:42)            Exit down
```

In the following example, continuation of the above example, the traffic class is discarded since the packet has reached a blackhole.

```
Route Change History:
             Date and Time                  Previous Exit                          Current
 Exit                      Reason

   1:  12:50:15 (PST) 03/30/2015   ISP3/100.10.1.1/Tu30 (Ch:42)          None/0.0.0.0/None
 (Ch:0)                No Channels Available
    2:  12:48:14 (PST) 03/30/2015   ISP2/100.10.4.1/Tu20 (Ch:43)
ISP3/100.10.1.1/Tu30 (Ch:42)            Exit down
    3:  12:47:57 (PST) 03/30/2015   ISP2/100.10.2.1/Tu20 (Ch:46)
ISP2/100.10.4.1/Tu20 (Ch:43)            Exit down
    4:  12:44:42 (PST) 03/30/2015   ISP1/100.10.1.1/Tu10 (Ch:41)
ISP2/100.10.2.1/Tu20 (Ch:46)            Exit down
    5:  12:44:13 (PST) 03/30/2015   ISP1/100.10.3.1/Tu10 (Ch:44)
ISP1/100.10.1.1/Tu10 (Ch:41)            Exit down
```

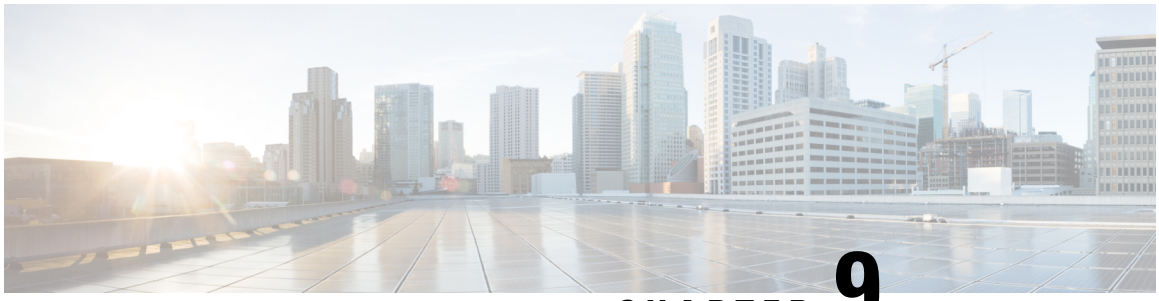
# Additional References for Path Preference Hierarchy

### Related Documents

| Related Topic | Document Title |
|---|---|
| Performance Routing Version 3 commands | Cisco IOS Performance Routing Version 3 Command Reference |

### 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 |



CHAPTER 9

# PfRv3 Remote Prefix Tracking

Performance Routing Version 3 (PfRv3) is an intelligent-path control mechanism for improving application delivery and WAN efficiency. The PfRv3 Remote Prefix Tracking feature enhances networks running Performance Routing Version 3 (PfRv3) to learn the prefix of a remote device from the Routing Information Base (RIB) table.



# Feature Information for PfRv3 Remote Prefix Tracking

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 19: Feature Information for PfRv3 Remote Prefix Tracking***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Remote Prefix Tracking | Cisco IOS release 3.16.6, 15.6M2, 15.5.3M6, 15.7M, 16.3.5, and Cisco IOS XE Everest 16.6.1. | Performance Routing Version 3 (PfRv3) is an intelligent-path control mechanism for improving application delivery and WAN efficiency. The PfRv3 Remote Prefix Tracking feature enhances networks running Performance Routing Version 3 (PfRv3) to learn the prefix of a remote device from the Routing Information Base (RIB) table.<br><br>The following command was modified: **show domain default vrf**. |

# Information About PfRv3 Remote Prefix Tracking

## Site Prefixes Database

Site Prefixes are LAN side prefixes owned by each site. The site prefix database is central to the site concept in PfRv3. Site prefix database reside on the master controller.

- The master site learns the remote site prefix through SAF advertised by remote MC. Master site learns the local site prefix from the local borders. The border learns the prefix from RIB and sends the prefix learned to the local master
- The border site prefix database is populated by SAF messages published by all the remote site master and local site master.
- By default, MCs and BRs delete site prefixes every 24 hours.

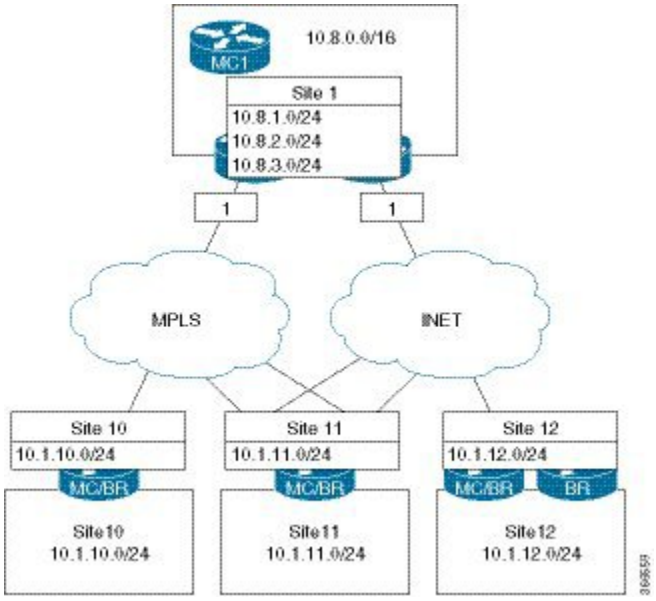
### Learning Local Site Prefixes

Border routers collect the prefix from the RIB table and send it to the local master controller. After receiving prefixes from a border router, the local master controller filters prefixes as per the following criteria.

1. If a prefix is learned on a tunnel interface, the prefix is marked remote and not added to local LAN list.
2. If a prefix is learned from NHRP, the prefix is not added to LAN list.
3. If a prefix is learned on a physical interface of the tunnel interface. the prefix is not added to LAN list.
4. If an enterprise prefix is configured on the hub and the prefix is part of the enterprise prefix list configured on hub, the branch master adds the prefix from the RIB table to the LAN list.

The prefixes in the LAN list are added to the site prefix database as local site prefix list.

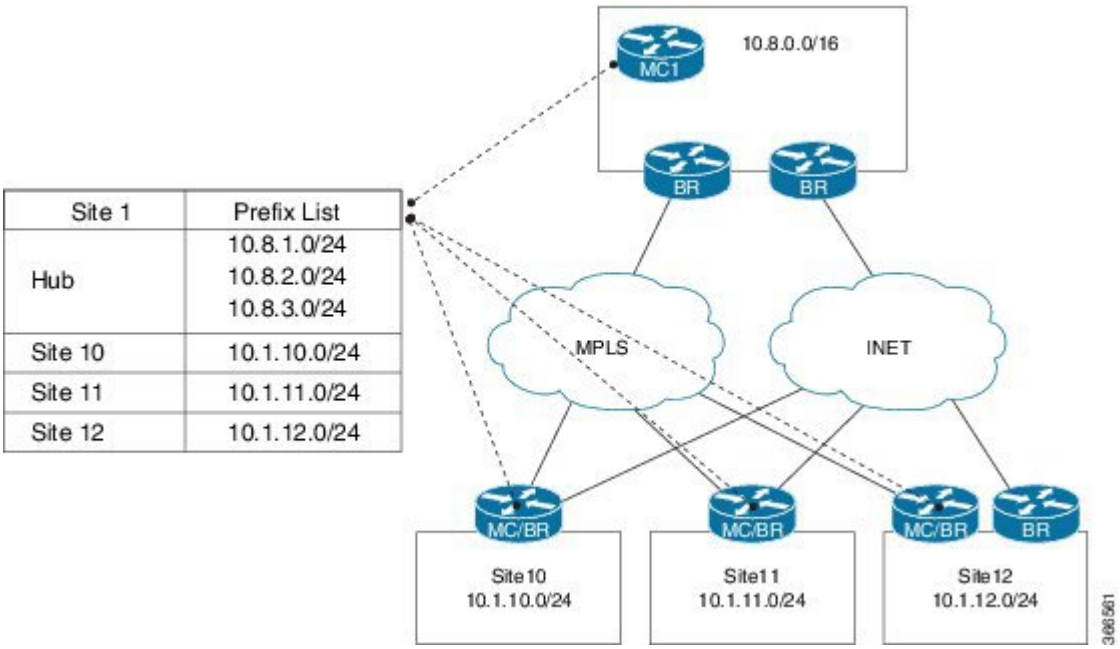
*Figure 10: Learning Local Site Prefixex*




## Learning Remote Site Prefixes

In order to learn from advertisements via the peering infrastructure from remote peers, every MC and BR subscribes to the peering service for the subservice of site prefix. MCs publish and receive site prefixes. BRs only receive site prefixes. MC learns prefixes from the border and filters the prefixes as explained in the previous section and publishes the prefixex to all sites. This message is received by all MCs and BRs that subscribe to the peering service. The message is decoded and added to the site prefix databases at those MCs and BRs.

*Figure 11: Pfrv3-discovery-site-prefix.png*




# PfRv3 Remote Prefix Tracking via Egress Flow

Prior to Cisco IOS XE Everest 16.6.1, the site prefix was learnt via the egress flow on the WAN interface. The prefix thus, learnt is published to all remote sites in the network using the EIGRP SAF message. If a remote site does not receive a new SAF message within 24 hours, the prefix is removed from the local-prefix database. If the routing is updated within 24 hours, corresponding prefix table will not be updated. Since, the prefix is learned from the egress traffic, sometimes-wrong prefixes are learnt due to redirected traffic. These wrongly learnt prefixes are not cleaned up until the 24 hour age out time.

Additionally, the prefix reachability is not tracked per channel. For example, if the prefix belongs to a specific site, it is assumed that prefix is reachable through all the channels available for that site. This results in a traffic blackhole when the prefix is not reachable through the selected channel.

# PfRv3 Remote Prefix Tracking via RIB table

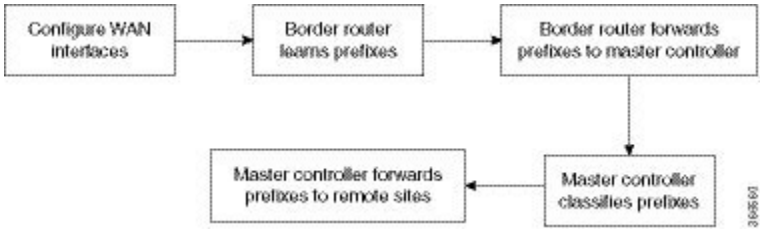
The PfRv3 Remote Prefix Tracking feature prevents the above scenarios by learning the local site prefixes from the RIB table instead of the egress flow. The prefixes are advertised to the remote sites. Changes to RIB table are tracked and are accordingly notified to all remote sites. Therefore, all sites are updated automatically with the precise site prefix information. Remote site tracks the prefix learnt via the WAN interface. While controlling the traffic, remote sites validate the reachability of the prefix on all channels available for a site.

There is no specific configuration required for this feature. You only need to configure the WAN interfaces.

# How Site Prefix is Learnt?

The following workflow illustrates the process of how site prefix is learnt.

*Figure 12: Site Prefix Learning Workflow*




## WAN Interfaces Configuration

You must configure the WAN interfaces on a border router in a branch using the **domain***domain-name* **dynamic-path** command. For more information, see "Configuring Branch Border Router" in the *Performance Routing Version 3* chapter.

## Prefix Learning on Border Router

On initialization, the border device learns the entire prefix from the RIB table and stores in the local prefix database, where the information is classified per VRF. Any changes in the RIB database, such as addition or deletion of prefixes, are accounted in the prefix database as appropriate. Prefixes learned from the RIB on the local border are forwarded to the local master controller. The prefix information in the border device can be viewed using the **show domain default vrf** *vrf name* **border route-import** command.

## Forwarding the Prefix to Master Controller

Master controller learns about a new prefix added or removed in the RIB table from the border device.

On a branch site, when the WAN interfaces are configured using the **domain***domain-name* **dynamic-path** command., the wan interface details are shared with the master controller by all border routers in a site. The master controller classifies this prefix information as WAN or LAN prefix, as appropriate.

On a hub site, The prefixes are learnt and classified similar to a branch site. The only difference is the command used to configure the WAN interface, which is **domain path service-provider-name path-id** *number* command.

**Note** It is mandatory to configure prefixes on the hub and the transit hub. It is also mandatory to configure the **domain** *domain-name* **dynamic-path** in branch tunnel interface.

## Prefix Classification by Master Controller

Master controller filters the prefix using the criteria described in the *Learning Local Site Prefixes* section and updates the local prefix database. The local prefix database is published to all the subscribers using the EIGRP SAF message.The prefix information in the border device can be viewed using the following commands:

- **show domain** {*domain-name* | **default**} **vrf** *vrf-name* **master route-import local all**
- **show domain** {*domain-name* | **default**} **vrf** *vrf-name* **master route-import border** *border-ip*
- **show domain** {*domain-name* | **default**} **vrf** *vrf-name* **master route-import local**
- **show domain** {*domain-name* | **default**} **vrf** *vrf-name* **master route-import remote**

- **show domain** {*domain-name* | *default*} **vrf** *vrf-name* **border route-import**
- **show domain** {*domain-name* | *default*} **vrf** *vrf-name* **border local-prefix interface** *interface-name*

## Path Preference

When a master controller receives prefixes from a border router, the master controller evaluates the traffic classes to a device, whose prefixes are listed in the RIB table and performs a policy decision to select a channel.

A channel is added to a channel list of a traffic class when a device associated with a prefix is reachable. The master controller decides on a path to a device based on the reachability of device (with a prefix in the RIB) on a channel. Prefixes are validated as follows:

- The list of interfaces on which prefixes are reachable is obtained from the prefix database and the prefix is verified for reachability via the same interface as the channel interface.
- A list of routes is obtained for a prefix that is reachable via an interface.

The channel is verified for the next hop address and if the next hop matches the appropriate prefix route. If the parent route of a device pertaining to a prefix matches the channel next hop, it indicates that the device with the prefix is reachable through a channel. If prefixes cannot be reached on a channel, a syslog message is displayed.

**Note** Maximum secondary paths must be configured on the border devices using the maximum-paths command so that prefixes are reachable. This command are enabled in the EIGRP or BGP router configuration mode.

# How to Display Site Prefixes

## Displaying Site Prefixes Learnt By a Border Router

### SUMMARY STEPS

1. **show domain** *domain-name* **vrf** *vrf-name* **border site-prefix**
2. **show domain default vrf** *vrf name* **border route-import**
3. **show domain default vrf** *vrf name* **border route-import interface**
4. **show monitor event-trace pfrv3 all**

### DETAILED STEPS

**Step 1** **show domain** *domain-name* **vrf** *vrf-name* **border site-prefix**

Use this command to verify the reachability of the prefix on all channels.

**Step 2** **show domain default vrf** *vrf name* **border route-import**

Use this command to view the prefix information learnt by a border device from the RIB table.

**Example:**

```
B1MCBR# show domain default vrf green border route-import

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Proto Prefix              Location   Next-Hop          Index      Interface                 In-RIB
-------------------------------------------------------------------------------------------------
L     10.20.0.1/32        Local      0.0.0.0           29         Ethernet0/2.30             YES
C     10.20.0.0/24        Local      0.0.0.0           29         Ethernet0/2.30             YES
L     10.20.1.1/32        Local      0.0.0.0           25         Ethernet0/1.30             YES
C     10.20.1.0/24        Local      0.0.0.0           25         Ethernet0/1.30             YES
D     10.20.2.0/24        Local      10.20.0.2         29         Ethernet0/2.30             YES
L     51.1.0.4/32         Local      0.0.0.0           24         Tunnel10                   YES
C     51.1.0.0/16         Local      0.0.0.0           24         Tunnel10                   YES
D     52.1.0.0/16         Local      10.20.0.2         29         Ethernet0/2.30             YES
C     100.20.1.1/32       Local      0.0.0.0           22         Loopback1                  YES
D     100.20.2.1/32       Local      10.20.0.2         29         Ethernet0/2.30             YES
S     100.20.3.1/32       Local      10.20.0.3         29         Ethernet0/2.30             YES
```

**Step 3** **show domain default vrf** *vrf name* **border route-import interface**

Use this command to view the prefix information associated with an interface.

**Example:**

```
B1MCBR# show domain default vrf green border route-import interface Loopback1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Proto Prefix              Location   Next-Hop          Index      Interface                 In-RIB
-------------------------------------------------------------------------------------------------
C     100.20.1.1/32       Local      0.0.0.0           22         Loopback1                  YES
```

**Step 4** **show monitor event-trace pfrv3 all**

Enables debugging by collecting trace.

# Displaying Site Prefixes Learnt By a Master Controller

## SUMMARY STEPS

1. **show domain default vrf** *vrf name* **master route-import**
2. **show domain default vrf** *vrf name* **master route-import interface**
3. **show domain default vrf** *vrf name* **master local-prefix**

## DETAILED STEPS

### Step 1 show domain default vrf *vrf name* master route-import

Use this command to view the prefix information learnt by a master controller.

**Example:**

```
B1MCBR# show domain default vrf green master route-import all

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
------------------------------------------------------------------------------------------------------------------------
Enterprise Prefix List:
Prefix: 100.20.0.0, Mask: 16
Prefix: 100.30.0.0, Mask: 16
Prefix: 100.0.0.0, Mask: 8
------------------------------------------------------------------------------------------------------------------------
Proto Prefix              Location   BR-IP            Next-Hop         Index      Interface
             IF-Role   In-RIB
------------------------------------------------------------------------------------------------------------------------
B     10.10.1.0/24         Remote     100.20.1.1       10.20.1.2        25         Ethernet0/1.30
             WAN       YES
B     10.10.2.0/24         Local      100.20.2.1       10.20.2.2        25         Ethernet0/1.32
             LAN       YES
B     10.10.3.0/24         Remote     100.20.1.1       10.20.1.2        25         Ethernet0/1.30
             WAN       YES
B     10.10.4.0/24         Local      100.20.2.1       10.20.2.2        25         Ethernet0/1.32
             LAN       YES
B     10.15.1.0/24         Remote     100.20.1.1       10.20.1.2        25         Ethernet0/1.30
             WAN       YES
B     10.15.2.0/24         Local      100.20.2.1       10.20.2.2        25         Ethernet0/1.32
             LAN       YES
L     10.20.0.1/32         Local      100.20.1.1       0.0.0.0          29         Ethernet0/2.30
             LAN       YES
L     10.20.0.2/32         Local      100.20.2.1       0.0.0.0          28         Ethernet0/2.30
             LAN       YES
C     10.20.0.0/24         Local      100.20.1.1       0.0.0.0          29         Ethernet0/2.30
             LAN       YES
C     10.20.0.0/24         Local      100.20.2.1       0.0.0.0          28         Ethernet0/2.30
             LAN       YES
L     10.20.1.1/32         Remote     100.20.1.1       0.0.0.0          25         Ethernet0/1.30
             WAN       YES
C     10.20.1.0/24         Remote     100.20.1.1       0.0.0.0          25         Ethernet0/1.30
             WAN       YES
D     10.20.1.0/24         Remote     100.20.2.1       10.20.0.1        28         Ethernet0/2.30
             LAN       YES
L     10.20.2.1/32         Local      100.20.2.1       0.0.0.0          25         Ethernet0/1.32
             LAN       YES
D     10.20.2.0/24         Local      100.20.1.1       10.20.0.2        29         Ethernet0/2.30
             LAN       YES
C     10.20.2.0/24         Local      100.20.2.1       0.0.0.0          25         Ethernet0/1.32
             LAN       YES
B     10.30.1.0/24         Remote     100.20.1.1       10.20.1.2        25         Ethernet0/1.30
             WAN       YES
B     10.30.2.0/24         Local      100.20.2.1       10.20.2.2        25         Ethernet0/1.32
```

```
              LAN       YES
L     51.1.0.4/32           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
              WAN       YES
C     51.1.0.0/16           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
              WAN       YES

B1MCBR# show domain default vrf green master route-import local

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
------------------------------------------------------------------------------------------------------------------------
Enterprise Prefix List:
Prefix: 100.20.0.0, Mask: 16
Prefix: 100.30.0.0, Mask: 16
Prefix: 100.0.0.0, Mask: 8
------------------------------------------------------------------------------------------------------------------------
Proto Prefix              Location   BR-IP             Next-Hop          Index       Interface
              IF-Role   In-RIB
------------------------------------------------------------------------------------------------------------------------
L     10.20.0.1/32          Local      100.20.1.1        0.0.0.0           29          Ethernet0/2.30
              LAN       YES
C     10.20.0.0/24          Local      100.20.1.1        0.0.0.0           29          Ethernet0/2.30
              LAN       YES
C     10.20.0.0/24          Local      100.20.2.1        0.0.0.0           28          Ethernet0/2.30
              LAN       YES
D     10.20.2.0/24          Local      100.20.1.1        10.20.0.2         29          Ethernet0/2.30
              LAN       YES
C     10.20.2.0/24          Local      100.20.2.1        0.0.0.0           25          Ethernet0/1.32
              LAN       YES
C     100.20.1.1/32         Local      100.20.1.1        0.0.0.0           22          Loopback1
              LAN       YES
D     100.20.1.1/32         Local      100.20.2.1        10.20.0.1         28          Ethernet0/2.30
              LAN       YES
D     100.20.2.1/32         Local      100.20.1.1        10.20.0.2         29          Ethernet0/2.30
              LAN       YES
C     100.20.2.1/32         Local      100.20.2.1        0.0.0.0           23          Loopback1
              LAN       YES
S     100.20.3.1/32         Local      100.20.1.1        10.20.0.3         29          Ethernet0/2.30
              LAN       YES

B1MCBR# show domain default vrf green master route-import remote

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
------------------------------------------------------------------------------------------------------------------------
Enterprise Prefix List:
Prefix: 100.20.0.0, Mask: 16
Prefix: 100.30.0.0, Mask: 16
Prefix: 100.0.0.0, Mask: 8
------------------------------------------------------------------------------------------------------------------------
Proto Prefix              Location   BR-IP             Next-Hop          Index       Interface
```

```
             IF-Role   In-RIB
-------------------------------------------------------------------------------------------------------------------------
L     10.20.1.1/32          Remote     100.20.1.1        0.0.0.0           25          Ethernet0/1.30
             WAN       YES
C     10.20.1.0/24          Remote     100.20.1.1        0.0.0.0           25          Ethernet0/1.30
             WAN       YES
L     51.1.0.4/32           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
             WAN       YES
C     51.1.0.0/16           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
             WAN       YES
D     52.1.0.0/16           Remote     100.20.1.1        10.20.0.2         29          Ethernet0/2.30
             LAN       NO
D     52.1.0.0/16           Remote     100.20.1.1        51.1.0.3          24          Tunnel10
             WAN       YES
B     10.10.1.0/24          Remote     100.20.1.1        10.20.1.2         25          Ethernet0/1.30
             WAN       YES
B     10.10.3.0/24          Remote     100.20.1.1        10.20.1.2         25          Ethernet0/1.30
             WAN       YES
B     10.15.1.0/24          Remote     100.20.1.1        10.20.1.2         25          Ethernet0/1.30
             WAN       YES
B     10.30.1.0/24          Remote     100.20.1.1        10.20.1.2         25          Ethernet0/1.30
             WAN       YES
D     100.10.0.0/16         Remote     100.20.1.1        10.20.0.2         29          Ethernet0/2.30
             LAN       NO
D     100.10.0.0/16         Remote     100.20.1.1        51.1.0.2          24          Tunnel10
             WAN       YES
```

```
B1MCBR# show domain default vrf green master route-import border 100.20.1.1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
-------------------------------------------------------------------------------------------------------------------------
Enterprise Prefix List:
Prefix: 100.20.0.0, Mask: 16
Prefix: 100.30.0.0, Mask: 16
Prefix: 100.0.0.0, Mask: 8
-------------------------------------------------------------------------------------------------------------------------
Proto Prefix              Location   BR-IP             Next-Hop          Index       Interface
             IF-Role   In-RIB
-------------------------------------------------------------------------------------------------------------------------
L     10.20.0.1/32          Local      100.20.1.1        0.0.0.0           29          Ethernet0/2.30
             LAN       YES
C     10.20.0.0/24          Local      100.20.1.1        0.0.0.0           29          Ethernet0/2.30
             LAN       YES
L     10.20.1.1/32          Remote     100.20.1.1        0.0.0.0           25          Ethernet0/1.30
             WAN       YES
C     10.20.1.0/24          Remote     100.20.1.1        0.0.0.0           25          Ethernet0/1.30
             WAN       YES
D     10.20.2.0/24          Local      100.20.1.1        10.20.0.2         29          Ethernet0/2.30
             LAN       YES
L     51.1.0.4/32           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
             WAN       YES
C     51.1.0.0/16           Remote     100.20.1.1        0.0.0.0           24          Tunnel10
             WAN       YES
D     52.1.0.0/16           Remote     100.20.1.1        10.20.0.2         29          Ethernet0/2.30
             LAN       NO
D     52.1.0.0/16           Remote     100.20.1.1        51.1.0.3          24          Tunnel10
             WAN       YES
```

```
C     100.20.1.1/32        Local      100.20.1.1        0.0.0.0           22         Loopback1
             LAN       YES
D     100.20.2.1/32        Local      100.20.1.1        10.20.0.2         29         Ethernet0/2.30
             LAN       YES
```

**Step 2** **show domain default vrf** *vrf name* **master route-import interface**

Use this command to view the prefix information associated with an interface.

**Example:**

```
Router# show domain default vrf green border local-prefix interface Ethernet0/0.10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B-BGP D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,
       E2 -   OSPF external type 2 i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area,
       * - candidate default, H- NHRP
Local  -- Prefix learned over LAN.
Remote -  Prefix learned over WAN.
Prefix          Interface       BR IP       Index   Prefix-site  Proto Next-Hop        Status
-------------------------------------------------------------------------
100.10.4.1/32   Ethernet0/0.10  100.20.1.1  12      Local         C                     -----
    Up
```

**Step 3** **show domain default vrf** *vrf name* **master local-prefix**

Use this command to view the prefix information associated with an border router.

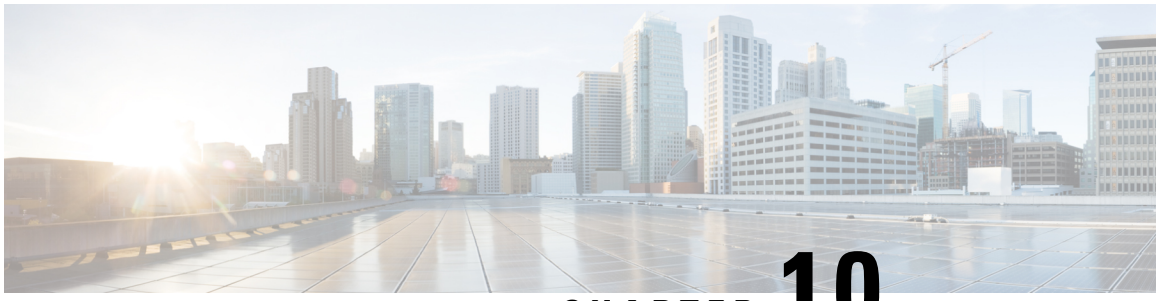
**Example:**

```
Router# show domain default vrf green master local-prefix border-ip 100.20.1.1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B-BGP D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,
       E2 -   OSPF external type 2 i - IS-IS, su - IS-IS summary,
       L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area,
       * - candidate default, H- NHRP
Local  -- Prefix learned over LAN.
Remote -  Prefix learned over WAN.
Prefix        Interface        BR IP       Index   Prefix-site  Proto      Next-Hop     Status
-------------------------------------------------------------------------
100.10.4.1/32  Ethernet0/0.10  100.20.1.1  12      Local        C
```

# Additional References for PfRv3 Remote Prefix Tracking

**Related Documents**

| Related Topic | Document Title |
|---|---|
| PfRv3commands | Cisco IOS Performance Routing Version 3 Command Reference |
| Site Prefix Splitting | Site Prefix Splitting |



CHAPTER 10

# PfRv3 Per Interface Probe Tuning

The PfRv3 Per Interface Probe Tuning feature provides the flexibility to specify different profiles for a channel associated with an interface thereby allowing you to measure the metrics of a channel.



# Feature Information for PfRv3 Per Interface Probe Tuning

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 20: Feature Information for PfRv3 Per Interface Probe Tuning***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Per Interface Probe Tuning | Cisco IOS XE Everest 16.6.1 | The PfRv3 Per Interface Probe Tuning feature provides the flexibility to specify different profiles for a channel associated with an interface thereby allowing you to measure the metrics of a channel.<br><br>The following commands were introduced or modified: **domain smart-probe**, **smart-probe**, **show platform hardware qfp active feature pfrv3**, **show platform software pfrv3**. |

# Prerequisites for PfRv3 Probe Reduction

# Restrictions for PfRv3 Per Interface Probe Tuning

- The profile parameters must be defined or enforced on all border hub routers. Configuring the profile on a hub master controller does not propagate the profile parameters to the border hub routers.
- The default data expiration value for a channel is 90 seconds.
- You must configure the Performance Routing v3 Zero SLA Support feature on the hub border router to suppress nonzero DSCP (Differentiated Services Code Point) channels.

# Information About PfRv3 Per Interface Probe Tuning

## Probe Reduction and Per Interface Probe Tuning

Probing helps in measuring the metrics of a channel. A “profile” is a set of probing parameters configured on a device to send a probe packet on a channel that must be monitored. Before sending a probe packets on a channel, the channel that is to be monitored must be understood because each monitor has different profiles. In most cases, there are two monitors—default and quick. Each probe has two parameters, namely, burst packets and burst interval, which can be configured to define the probe packets sent on a PfR channel.

The PfRv3 Probe Reduction feature allows reducing traffic probe on channels that do not carry any traffic. For more information see the *PfRv3 Probe Reduction* module.

The PfRv3 Probe Reduction feature enforces similar probing on all interfaces irrespective of an interface through which a channel goes out, whereas the PfRv3 Per Interface Probe Tuning feature provides the flexibility to enforce different profiles on channels associated with an interface.

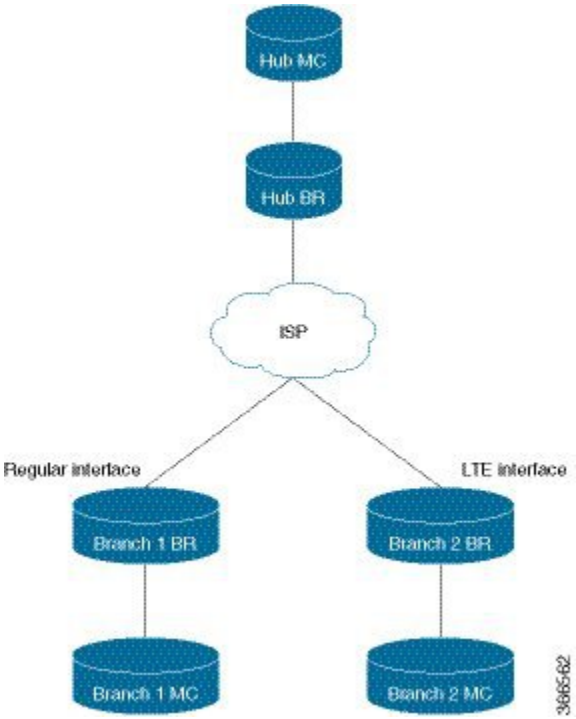
## How Per Interface Probe Tuning Works?

The PfRv3 Per Interface Probe Tuning feature is configured on border hub routers via the *profile-id* argument in the **smart-probes** command and applied to an interface via the **domain smart-probe profile** command.

If you do not configure these commands, the default profile 0, is set on a device. The default profile has predefined parameters of 1 packet every 1 second for a default monitor and 20 packets every 1 second for a quick monitor.

The following is a sample topology to explain the working of the PfRv3 Per Interface Probe Tuning feature.

*Figure 13: Per Interface Probe Tuning—Sample Topology*




A hub branch router communicates to two branch routers Branch 1 Router and Branch 2 Router via ISP. Branch 1 Router has a regular interface, while Branch 2 Router has an Long-Term Evolution (LTE) interface. The LTE interface requires different probing parameters on the channel connected to the interface as LTE radio channels are established when data needs to be transmitted over the interface and radio frequency band occupies the transmission.

The profile parameters for the LTE interface are 100 packets every 1200 seconds for default monitor and default values for quick monitor. The profile parameters for the regular interface is the default parameters, which is, one packet every one second for default monitor and 20 packets every one second for quick monitor.

The hub border router establishes channels through its WAN interface to Branch 1 Router and Branch 2 Router via the ISP. Based on the defined profile parameters, channels from the hub border router to the Branch 1 Router are probed at regular intervals. Channels from the hub border router to Branch 2 Router wil have not have incoming probes for 19 minutes. The following happens before data is transmitted to the LTE interface:

- Burst probe packets are sent over the channel to measure the metrics.
- The burst interval range is increased to allow a longer duration so that radio bandwidth is not stagnated.
- Unreachable probe packets are not sent after sending the burst probe packets. This is to free up the radio bandwidth. to transmit the data.
- The burst interval range is configured to a longer duration so that radio bandwidth is not occupied.
- Unreachability detection is suppressed to ensure that there is no unreachability from a remote device for a period of time.

## Profile—Channel Association

The profiles are associated with the channel and not the interface because it is possible that the same interface may host different channels, especially on border hub routers. If two channels have different profile numbers, the channel with a higher profile number is chosen to transmit data. The profile negotiation rule requires a profile with higher ID number to have a slower probing rate. The default profile (one packet every one second for default monitor and 20 packets every one second for quick monitor) has sufficient probing rate.When a channel probes at a slower rate (bigger profile ID number) another channel in the network probes at a higher rate (smaller profile ID number).

**Note** There is no automatic detection mechanism to calculate the rate of different profiles if the profile negotiation rule (higher-ID-slower-rate) is violated.

# How to Configure PfRv3 Per Interface Probe Tuning

## Defining a Profile on a Border Hub Router

```
domain domain1
 border
  advanced
   smart-probe 1 burst quick 10 packets every 20 seconds 1
```

## Applying a Profile to an Interface on a Border Hub Router

```
interface tunnel 100
 domain smart-probe profile 1
```

## Verifying Profile Parameters

The following is a sample output of the **show platform software pfrv3** command that displays the profile parameters applied to an device:

```
HubBr2# show platform software pfrv3 rp active smart-probe
PfRv3 smart probe parameters :
Profile ID: 0
Attribute: 0x0000
Probe Burst interval: 1 second
Probe Burst number: 1 packets
Quick Monitor Probe Burst interval: 1 second
Quick Monitor Probe Burst number: 20 packets
Unreachable interval: 4 second
Profile ID: 1
Attribute: 0x0000
Probe Burst interval: 0 second
Probe Burst number: 0 packets
Quick Monitor Probe Burst interval: 0 second
Quick Monitor Probe Burst number: 0 packets
Unreachable interval: 4 second
Profile ID: 2
Attribute: 0x0000
```

```
Probe Burst interval: 0 second
Probe Burst number: 0 packets
Quick Monitor Probe Burst interval: 0 second
Quick Monitor Probe Burst number: 0 packets
Unreachable interval: 4 second
```

# Verifying Profile Parameters Associated with a Channel

The following is a sample output of the **show platform hardware qfp** command that displays the profile parameters associated with a channel:

```
Branch100# show platform hardware qfp active feature pfrv3 client channel id 7 detail
Chan id: 7 tbl-id: 0, if_h: 14(Tunnel100), site-id: 10.3.1.1, in_uidb: 65528, dscp: 0,
pfr-label: 0:0 | 0:0 [00000000]
  Supports zero-sla: Yes
  Muted by zero-sla: No
  Plr rx state: No
  Plr tx state: No
  Plr establish state: No
  next hop: 100.1.1.1
  State:    Discovered and open
  rx state: Reachable
  tx state: Reachable
  Smart Probe in Burst: No
  Unreach Probing only: Off
  Profile_ID: 0
  V4 Smart Probe Received: Yes
  V4 Smart Probe Sent: Yes
  Current profile_id: 1 <<< different than "Profile ID" (two lines above), resulted from
negotiation
  Remote profile_id: 1
  hash val: 25699
  exmem info:
        PPE addr: 0xebd26000
  stats:
    RX pkts: 0  bytes: 0
    TX pkts: 0  bytes: 0
    Blackhole pkts: 0  bytes: 0
    Loop pkts: 0  bytes: 0
    Probes: rx: 6288 tx: 474
    Number of SMP Profile Bursts sent: 100
    Number of Active Channel Probes sent: 374
    Number of Reachability Probes sent: 0
    Number of Force Unreaches sent: 0
    Last Probe rx: 44115 ms Ago
    Last Probe tx: 3379 ms Ago
```

# Configuration Examples for PfRv3 Per Interface Probe Tuning

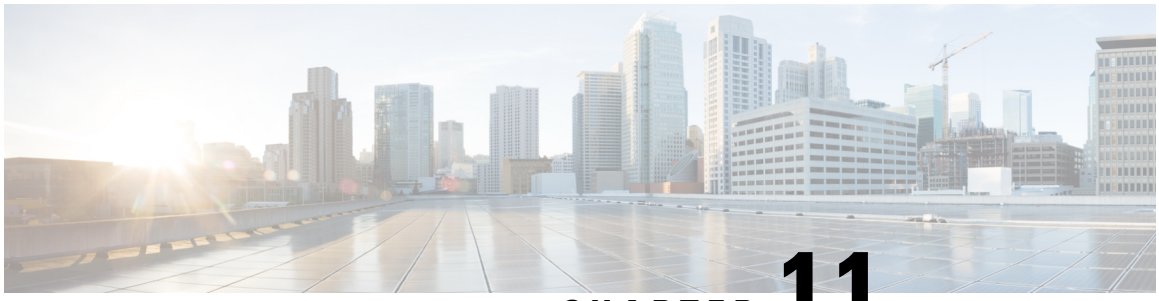
# Additional References for PfRv3 Per Interface Probe Tuning

### Related Documents

| Related Topic | Document Title |
|---|---|
| Performance Routing Version 3 commands | Cisco IOS Performance Routing Version 3 Command Reference |
| Probe Reduction | PfRv3 Probe Reduction |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| | |



CHAPTER 11

# PfRv3 Inter-DC Optimization

The PfRv3 Inter-DC (IDC) Optimization feature optimizes traffic between hub and transit hub sites over a WAN overlay or a DCI overlay. A path-preference policy specific to inter-DC Optimization is used for optimizing traffic between two or more hub sites. The PfRv3-Inter-DC-Optimization routs traffic from a hub site to another hub site for specific traffic types such as data, voice, video, and so on.



# Feature Information for PfRv3 Inter-DC Optimization

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 21: Feature Information for PfRv3 Inter-DC Optimization***

| Feature Name | Releases | Feature Information |
|---|---|---|
| PfRv3 Inter-DC Optimization | Cisco IOS XE Everest 16.6.1 | The following commands were introduced or modified: **domain**, **inter-dc**, **interdc-path-preference**. |

# Prerequisites for PfRv3 Inter-DC Optimization

- Hub sites must be upgraded for using the same version of IOS for the master and border devices.
- Static NHRP mapping must be used between hub sites. (NHRP shortcuts are not allowed between hub sites)

- Local LAN prefixes on each hub site (all borders) must have a specific route pointing to LAN interfaces and not to DCI or WAN interfaces.

# Limitations and Guidelines for Inter-DC Optimization

- The PfRv3 Inter-DC Optimization does not optimize routes using common prefixes.

**Note** A common prefix is a prefix which is configurared as a static prefix on all the hub sites, that include hub sites and transite hub sites.

- The command **domain dci-path** should be added in DCI tunnel interface, but normal WAN interface with **domain path** command can also be chosen as DCI path. But DCI interface using **domain dci-path** cannot be chosen as the path for normal hub to spoke traffic.
- We recommend to use static configuration under DCI tunnel interface to set up peer between DC sites. If **nhrp shortcut** is used, a forwarding loop may occur.
- After enabling the IDC feature using the inter-dc command, you can configure **path-preference** and **interdc-path-preference** under policy.

**Note** You should not configure DCI path in **global path-preference** because if you add DCI path into path-preference, there is no channel available between hub and spoke in the DCI path. The DCI path cannot be chosen for the normal traffic-classes.

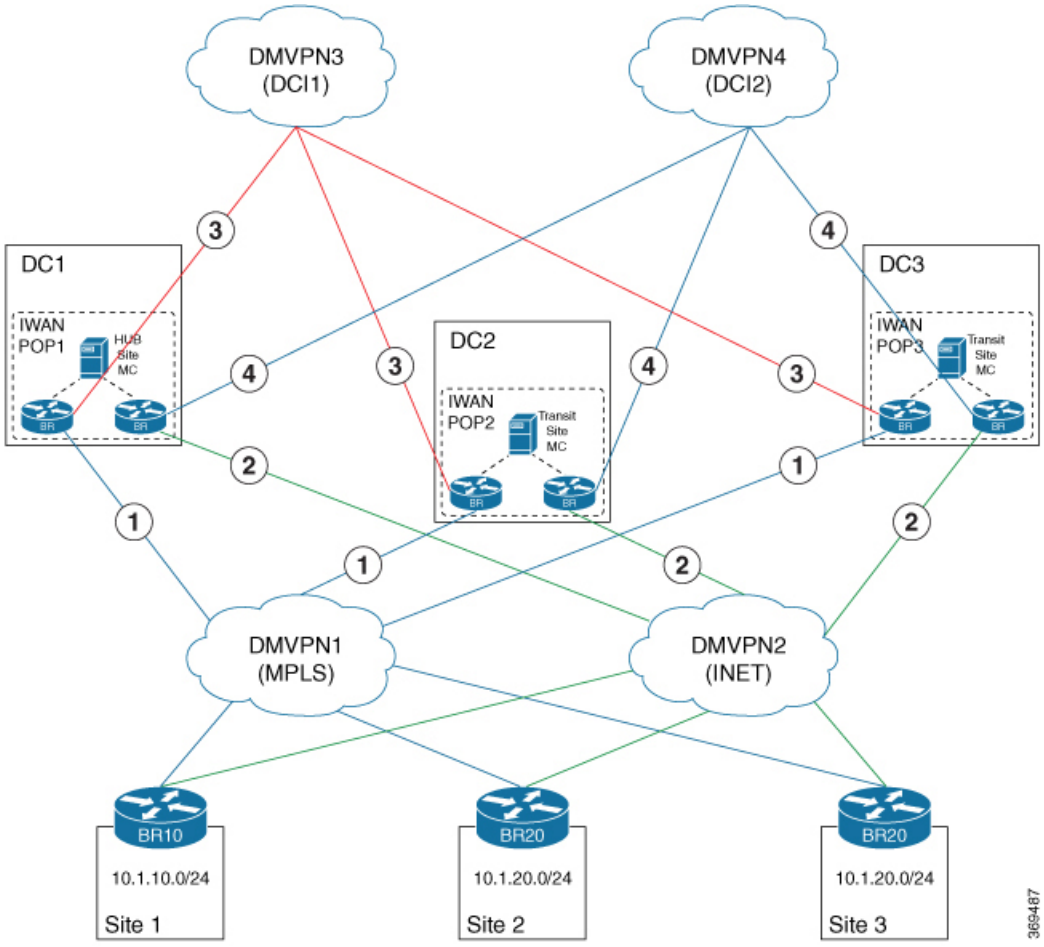
- The IDC feature must be enabled on both peer masters. It is recommended to use the same overlay routing protocol for all WAN and DCI tunnels.

# Information About PfRv3-Inter-DC-Optimization

## Datacenter Optimization

The following figure illustrates the PfRv3 Inter-DC Optimization feature where traffic between hub sites DC1, DC2 and DC3 are routed to forward specific traffic trough a specific hub. The figure shows four paths can be used as candidates for the traffic from DC1 to DC2. IDC1 and IDC2 are Inter-DC links those can be used for this traffic. MPLS and INET are normal WAN paths that can also be used for this traffic as candidates. It depends on the path-preference policy specific to inter-DC optimization.

*Figure 14: Datacenter Optimization*




The PfRv3 Inter-DC Optimization feature can be enabled with the **inter-dc** command in domain master controller advanced mode. All hubs in the network must be connected through WAN overlay or DCI overlay. All hub and transit hub masters must be enabled with this feature locally. WAN overlay is configured by defining a WAN interface using the **domain path** command. DCI overlay is configured by defining a DCI interface using the **domain dci-path** command.

The salient points of the PfRv3 Inter-DC Optimization feature are as follows:

- The **domain dci-path** command enables route control which routes the transit traffic on all DCI interfaces in ingress direction.
- Traffic classes are learnt based on the egress aggregate update and traffic channels over the WAN and DCI overlay.
- Tunnel addresses and path ID mapping are exchanged by site capability between the hub and transit masters.

**Note** The tunnel IP address for corresponding interface or path-id is advertised among the hub and transit masters when the PfRv3 Inter-DC Optimization feature is enabled.

## DCI Path Options

Based on the actual deployment requirement, you can choose any of the following options for providing the DCI path:

**Using the existing DMVPN overlay and the same tunnel interface:**

In the hub to spoke DMVPN tunnel interface configuration, there is no dmvpn peer between DC sites. So, if the normal hub tunnel interface is used as DCI path, some additional configuration should be added to set up the dmvpn peer between DC sites, such as ip nhrp nhs 161.1.0.5 nbma 155.155.155.5 multicast above.

**Using an independent DCI link(s) with independent DMVPN overlay**

When there is dedicated DCI links between DC sites, a dedicated DMVPN overlay can be used as DCI path. And ideally, the dedicated DCI links are more stable than the normal WAN links. Using the existing hub to spoke DMVPN, or using a dedicated DCI DMVPN built over dedicated DCI links will depend on the available interfaces in the network, and which solution will meet the need of the network

**Note** A third option of building a second set of DMVPN tunnels using the same transport as the existing DMVPN hub and spoke network is not recommended and it has not been validated.

# How to Configure PfRv3-Inter-DC-Optimization

## Specifying the DCI interface on a Hub Site

```
enable
configure terminal
interface tunnel155
 domain dci-path DCI path-id 11
   exit
```

## Configuring Inter-DC on Hub Master Controller

To configure the Inter-DC Optimization feature on the hub master controller, use the following commands:

```
enable
configure terminal
domain default
 vrf green
  master hub
   source-interface Loopback1
   site-prefixes prefix-list HUBPFX
```

```
   advanced
    inter-dc
     enterprise-prefix prefix-list ENTPFX
     class BUSINESS sequence 10
      match dscp ef policy custom
      priority 1 one-way-delay threshold 100
    interdc-path-preference DCI1 DCI2 fallback MPLS next-fallback INET
    exit
```

# Configuring Inter-DC on Transit Hub

To configure Inter-DC on the transit hub, use the following commands:

```
enable
Configure terminal
domain default
 vrf green
  master transit 2
   source-interface Loopback1
   site-prefixes prefix-list HUBPFX
   hub 100.10.1.1
   advanced
inter-dc
  class BUSINESS sequence 10
    interdc-path-preference DCI1 fallback MPLS next-fallback INET
exit
```

# Specifying IDC Local Policy

This is an optional task to overwrite the global path-preference.

```
enable
configure termainal
domain default
 vrf green
  master transit 2
   class BUSINESS sequence 10
    interdc-path-preference DCI1 fallback ISP1 next-fallback ISP2
exit
```

# Verifying Inter-DC Configuration

```
HMCBR# show domain default vrf green master status
  *** Domain MC Status ***
 Master VRF: green
  Instance Type:    Hub
  Instance id:      1
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 100.10.1.1
  Global Config Last Publish status: Peering Success
  Smart Probe Profile:
    General Monitor:
      Packets per burst: 1
      Interval(secs): 1
    Quick Monitor:
      Packets per burst: 20
      Interval(secs): 1
```

```
  Load Balancing:
   Admin Status: Disabled
   Operational Status: Down
   Enterprise top level prefixes configured: 0
  Route Control: Enabled
  Transit Site Affinity: Enabled
  Load Sharing: Enabled
  Path Pruning Depth: Disabled
  Inter-DC Optimization: Enabled
```

# Verifying Master Controller Configuration

```
HMCBR# show domain default vrf green master status

  *** Domain MC Status ***
 Master VRF: green
  Instance Type:    Hub
  Instance id:      1
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 100.10.1.1
  Global Config Last Publish status: Peering Success
..... .....
Minimum Packet Loss Calculation Threshold: 15 packets
  Minimum Bytes Loss Calculation Threshold: 1 bytes
  Borders:
    IP address: 100.10.3.1
    Version: 2
    Connection status: CONNECTED (Last Updated 15:44:28 ago )
    Interfaces configured:
      Name: Tunnel10 | type: external | Service Provider: ISP1 path-id:3 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0

      Name: Tunnel40 | type: external | Service Provider: ISP4 path-id:9 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
      Name: Tunnel155 | type: DCI | Service Provider: DCI1 path-id:103 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
    Tunnel if: Tunnel0
    IP address: 100.10.1.1
    Version: 2
    Connection status: CONNECTED (Last Updated 15:44:21 ago )
    Interfaces configured:
      Name: Tunnel10 | type: external | Service Provider: ISP1 path-id:1 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
      Name: Tunnel30 | type: external | Service Provider: ISP3 path-id:7 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
      Name: Tunnel155 | type: DCI | Service Provider: DCI1 path-id:101 | Status: UP |
Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
```

# Verifying the Channel Status

```
HMCBR# show domain default vrf green master channels
   Legend: * (Value obtained from Network delay:)
Channel Id: 7  Dst Site-Id: 100.20.1.1  Link Name: ISP1  DSCP: default [0] pfr-label: 0:0
```

```
| 0:3 [0x3] TCs: 0  BackupTCs: 0
  Channel Created: 15:43:53 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: FALSE
  Inter-DC Channel: FALSE
  Interface Id: 25
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Unreach Probing only: OFF
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
   ODE Statistics:
      Received: 0
   TCA Statistics:
      Received: 0 ; Processed: 0 ; Unreach_rcvd: 0 ; Local Unreach_rcvd: 0
      TCA lost byte rate: 0
      TCA lost packet rate: 0
      TCA one-way-delay: 0
      TCA network-delay: 0
      TCA jitter mean: 0
Channel Id: 117  Dst Site-Id: 100.16.1.1  Link Name: ISP1  DSCP: default [0] pfr-label:
3:13 | 0:3 [0x30D0003] TCs: 0  BackupTCs: 0
  Channel Created: 15:33:02 ago
  Provisional State: Initiated and open
  Operational state: Available
  Channel to hub: TRUE
  Inter-DC Channel: TRUE
  Interface Id: 25
  Supports Zero-SLA: Yes
  Muted by Zero-SLA: No
  Unreach Probing only: OFF
  Estimated Channel Egress Bandwidth: 0 Kbps
  Immitigable Events Summary:
   Total Performance Count: 0, Total BW Count: 0
  Site Prefix List
    100.16.1.1/32 (Routable)
    100.16.0.0/16 (Routable)
    100.10.0.0/16 (Routable)
    100.15.0.0/16 (Routable)
    100.0.0.0/8 (Routable)
   ODE Statistics:
      Received: 0
   TCA Statistics:
      Received: 0 ; Processed: 0 ; Unreach_rcvd: 0 ; Local Unreach_rcvd: 0
      TCA lost byte rate: 0
      TCA lost packet rate: 0
      TCA one-way-delay: 0
      TCA network-delay: 0
      TCA jitter mean: 0
```

# Example Configurations for PfRv3 Inter-DC

### Example for Policy Configured on the Hub MC with Inter DC

In this example, the policy can work on the normal hub-spoke traffic and the IDC traffic. For IDC traffic, the ‘interdc-path-preference’ takes effect. DCI1 and DCI2 are primary paths. If they are out-of-policy, the MPLS, which is a backup path, will be used. For normal hub-spoke traffic, the ‘path-preference’ takes effect. The other configuration is same as normal PfRv3 policy. For example, the threshold of delay is 100 ms for both the IDC traffic and the normal hub-spoke traffic.

```
class BUSINESS sequence 10
    match dscp ef policy custom
    priority 1 one-way-delay threshold 100
    path-preference MPLS fallback INET
    interdc-path-preference DCI1 DCI2 fallback MPLS next-fallback INET
```

### Example for Policy Configured on the Transit Hub MC with Inter DC

On transit hub master, you can see the same policy. But, if the **interdc-path-preference** is configured on this transit hub. The local interdc-path-preference will overwrite the policy from hub site

```
class BUSINESS sequence 10
    interdc-path-preference DCI1 fallback MPLS next-fallback INET
```

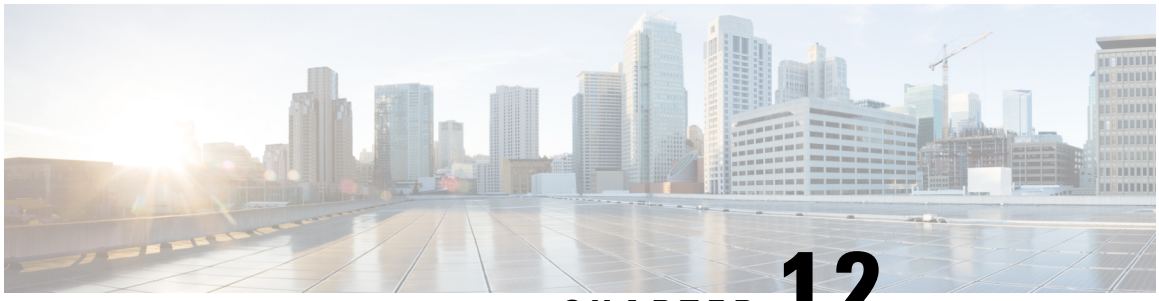
### Example for 'show domain vrf master policy' on hub master

```
------------------------------------------------------------------------------
Global-policy-list:

  class BUSINESS sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
      match dscp ef policy custom
        priority 1 one-way-delay threshold 100 msec
------------------------------------------------------------------------------
InterDC-policy-list:

  class BUSINESS sequence 10
interdc-path-preference DCI1 DCI2 fallback MPLS next-fallback INET
class type: Dscp Based
      match dscp ef policy custom
        priority 1 one-way-delay threshold 100 msec
```

# Additional References for PfRv3-Inter-DC-Optimization

### Related Documents

| Related Topic | Document Title |
|---|---|
| Performance Routing commands | Cisco IOS Performance Routing Version 3 Command Reference |



CHAPTER 12

# Direct Cloud Access

The Direct Cloud Access IWAN 2.3 feature enables users at branch sites to have best application experience to SaaS applications, such as, Office 365, Google services, with reduced cost. This feature helps in constantly monitoring network and application performance and select the optimized paths (usually local break out from branch to Cloud SaaS applications instead of back-haul to the data center). Non-SaaS traffic still back-haul to data center for further inspection.



## Feature Information for Configuring Direct Cloud Access

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 22: Feature Information for Direct Cloud Access IWAN 2.3***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Direct Cloud Access IWAN 2.3 | Cisco IOS XE Fuji 16.8.1 | The Direct Cloud Access (DCA) feature allows traffic from trusted applications, part of well-trusted domains, to pass the local Internet security check because traffic from these trusted applications have a lower security risk than untrusted Internet sites.<br><br>The following commands were introduced or modified: **domain path**, **path-preference**, **show domain dca-status**, **show domain default border**, **show domain default policy**, **show domain vrf border channels**, **show domain vrf master channels**. |

# Prerequisites for Configuring Direct Cloud Access

- Cisco Umbrella Branch must be enabled to intercept DNS to public DNS resolver.

**Note** By default OpenDNS is used as DNS resolver for SaaS traffic, but you can choose to use other DNS resolver such as Google DNS resolver 8.8.8.8. OpenDNS license/registration is not a must if you don't need OpenDNS security services.

# Restrictions for Configuring Direct Cloud Access

- IPv6 address is not supported.
- DCA is not supported if the DNS traffic does not pass through the router which is enabled with DCA.
- DCA does not work if SaaS applications use proxy. All traffic going to proxy server as DCA may not classify these applications and cannot perform local breakout for traffic that is bound to proxy.
- Applications that directly access the content and not through DNS resolution, NBAR may fail to classify as SaaS and cannot provide local break-out.
- DCA may not work on a device when NBAR classification results are not available on the device. You must customize NBAR to classify the results to support DCA.
- This feature depends on applications classification. SD-AVC helps in better classification with NBAR.
- To access SaaS applications, a public IP address is required. NAT helps translate the user’s private IP address to a public IP address. Configure NAT on the border router that has DCA enabled, or on other internet-facing devices.

# Information About Configuring Direct Cloud Access

## Direct Cloud Access Overview

The infrastructure of cloud-hosted services, such as Microsoft Office 365 and Google Apps, is in the cloud. Back-hauling traffic from remote users and sites through the private WAN to the data center via Internet imposes additional bandwidth requirements on the private WAN and may add latency to each connection. Moreover, private WAN connectivity is more expensive than direct Internet connections, which could add a tremendous amount of cost to the equation.

The Direct Cloud Access IWAN 2.3 feature implements direct cloud access (DCA) on Cisco IWAN networks and allows trusted SaaS traffic to be forwarded out over the optimized path (directly local break out) while other traffic still back-haul to headquarters over VPN. DCA monitors the candidate path (DCA path, back-haul path to headquarter) performance and chooses the optimized path in policy to get the best SaaS application performance. While adding direct Internet connectivity to the branch site without back hauling to data center,

IWAN DCA provides the security capability at branch site by enabling security features like NAT and Firewall (Zone-based Firewall, Snort IPS, etc.) at branch sites.

# Benefits of Direct Cloud Acces

- Reduced operation cost as SaaS traffic no longer needs to go to headquarters which consume additional headquarter network bandwidth.
- Business processes run faster through direct network access to the major cloud providers. A traffic classification mechanism is required in order to achieve direct Internet access for selected cloud applications.

# Direct Cloud Access Architecture

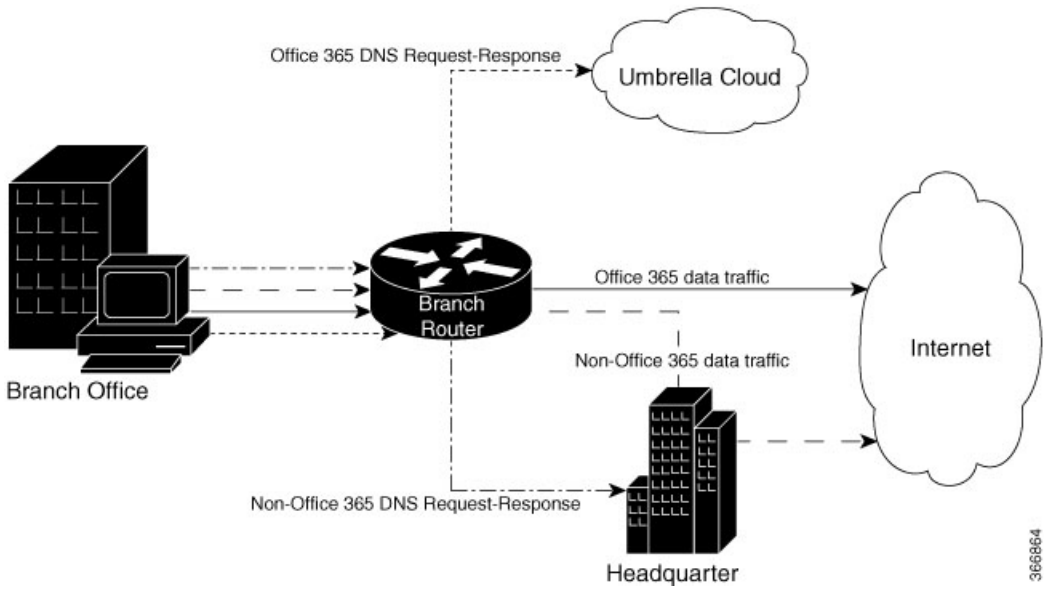
The overlay DMVPN WAN tunnels on a branch router are configured to dynamically learn the service provider they are connected to. An underlay interface is identified as a direct access interface via configuration.

Packets from the LAN side on a branch site are sent over the overlay when packets do not match the criteria of the configured application. When a flow matches the DCA criteria, the packets are directed to the DCA interface that is specified in the path preference. DCA interfaces can be listed in the order of priority in the path preference configuration of the policy for the application. The DCA interfaces are evaluated in the order of the configured path preference priority.

NBAR classification occurs at LAN ingress. NBAR provides the application ID, which is exported by the border router. If a match occurs on the Master Controller for an application, the policy for the application is applied to the traffic class for the specific flow.

The following figure explains the DCA functionality for Office365 application:

***Figure 15: DCA for Office365***




The following actions are performed to achieve DCA functionality:

- Classify all the cloud applications based on the DNS.

- Intercept DNS traffic and make decisions based on the classification.
  - If the traffic is from a trusted application, direct Internet access is provided. Ensure that security concerns are addressed for the breakout traffic, which include, constant application monitoring, choosing network performance over candidate paths (DCA path, back-haul path), selecting the optimized path according to policy (if DCA path is not good), back-hauling SaaS traffic to data center and reverting back if DCA path recovered.
  - If the traffic is not from a trusted application, the traffic is passed it to the Headquarter for further security inspection and processing.
- Route HTTP, HTTPS data traffic to Internet or Headquarter depending on the above decision.

## Designate an Underlay Interface as Direct Access Interface

An interface of the border router must be designated as direct access interface. **domain path** *path-name* **direct-cloud-access** command to specify the direct access interface. A service provider may have multiple links of direct access and each of the direct access interface is measured independently.

When an interface is selected to be the direct access interface, all traffic to the whitelisted applications is directed through the direct access interface. If there are multiple direct access interfaces, the traffic is directed on one direct access interface depending on the performance metrics and policy.

# Direct Cloud Access Components

Direct Cloud Access functionality has the following components:

## Cisco Umbrella Connector

To achieve location proximity, the SaaS server must be closer to the branch router to achieve better application performance. Generally, DNS requests for a SaaS application are destined to an enterprise DNS resolver. However, the DNS request must be changed from enterprise DNS resolver to a public DNS resolver, such as, OpenDNS resolver or Google DNS resolver. The public DNS resolver helps in placing the SaaS server closer to the branch router by using Cisco Umbrella connector. OpenDNS account and registration is not mandatory.

DNS requests must be unencrypted traffic from the endpoint to the DNS server. Each direct access interface must be configured with Open DNS.

## NBAR Classification

Network Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. NBAR uses several classification information metadata such as application name, ID, traffic class, business relevance, and so on.

For Direct Cloud Access functionality, once NBAR recognizes the DNS traffic as belonging to interesting cloud application, it attaches this information to DNS packet in a way so that the umbrella connector feature can extract and use the information.

Cisco NBAR provides the first packet classification for some applications. Cisco NBAR uses DNS learning for application recognition of user defined and predefined domains, Once the server is learned from the DNS response, traffic going to this server can be classified as FIFO. SD-AVC also improves the first packet classification result.

### Performance Routing Version 3

Performance Routing version 3 (PfRv3) delivers intelligent path control for application-aware routing across the WAN. Once a DNS response is received, the data traffic (HTTP, HTTPS etc.) from cloud application is provided direct Internet access (local break-out) or is sent to the headquarter for further security inspection.

### IPSLA

IPSLA is enabled automatically by PfRv3 to probe each SaaS application over candidate paths by using IPSLA HTTP operation. PfRv3 leverages the metrics reported by IPSLA to select the optimized path.

## SaaS Reachability and Performance Management

Performance and reachability of each whitelisted application determines the path that an application takes. PfR measures the reachability and performance of all VRFs and enables and shares one measurement across multiple VRFs.

## Next-Hop Reachability

One DSCP-agnostic channel is created as the next-hop for the direct access interface. The DSCP of DCA channel is configured as FF. The routing protocol configured on the direct access interface determines the next hop for the channel.

## Performance Measurement

After the channel next hop is up, the service is reached via next hop by using the following steps:

### Application Domain Mapping

Application to domain URL and Differentiated Services Code Point (DSCP) mapping must be configured on the master controller of each branch router so that IPSLA can measure the SaaS application using right domain and DSCP.

### Reachability and Performance Probing

Measuring network characteristics is performed using IPSLA. IPSLA probes are not sent per VRF, instead, PFR creates a probing layer for all the VRFs and path preferences in the VRFs in a domain. Reachability and performance can be verified per application by using the **show domain** *domain-name* **border dca** command. This command provides information per application, per interface for a border router.

## Traffic Steering and Flow Stickiness

When DCA is implemented on a network, traffic classes are automatically created for interested applications. The applications configured in the policy includes path preferences, which corresponds to the respective DSCP configured per application.

When selecting a path, PfR assigns a path to a flow that is destined to a service, for example, Offic365. These flows might traverse a NAT device or a firewall device that maintains the state for the flow sequence numbers. Changing the flow during packet traversal may lead to flow reset. Therefore, when a path is selected, flows

must align to that path only. If a path is unreachable, the flow is reset by the client and retried. If the path experiences packet loss but still usable, new flows are routed via alternate paths.

# How to Configure Direct Cloud Access

## Assign an Underlay Interface as Direct Access Interface

The following configuration snippet explains how to assign an Ethernet interface as direct access interface.

```
Router(config)# interface Ethernet 0/1
Router(config-interface)# domain path ATT-DCA direct-cloud-access
```

## Define PfR Policy for SaaS Application on Hub Master Controller

The following configuration snippet explains how SaaS application policies are defined on hub master controller at a central point and published to all branch sites. There is no need to define policies at each branch sites because branch sites still have the capability to customize the interested SaaS.

```
Router(config)# domain iwan Router
Router(config-domain)# vrf green
Router(config-domain-vrf)# master hub
Router(config-domain-vrf-master)# class BUSINESS-CRITICAL sequence 10
Router(config-domain-vrf-master-class)# match app-group ms-cloud-group policy custom
Router(config-domain-vrf-master-class-match)# priority 1 delay 500 ms
Router(config-domain-vrf-master-class-match)# exit
Router(config-domain-vrf-master-class)# path-preference ATT-DCA fallback ATT next-fallback
 INET
```

## Define SaaS Application Mapping on Branch Master Controller

To measure the SasS application's reachability and performance, the domain URL and DSCP must be specified for IPSLA probing for each SaaS application.

```
master branch
 domain-map
 application ms-lync-group domain http://www.office.com dscp default
 application ms-cloud-group domain http://www.office.com dscp default
 application ms-lync- group domain http://www.office.com dscp default
 application box domain http://www.box.com dscp default
 application dropbox domain http://www.dropbox.com dscp default
 application google-services domain http://www.google.com dscp default
 application google- group domain http://www.google.com dscp default
 application hangouts-group domain http://www.google.com dscp default
 application gtalk-group domain  http://www.google.com/ dscp default
```

## Verify and Monitor Direct Cloud Access Configuration

Use the following commands to verify and monitor DCA configuration.

- **show domain iwan master traffic-classes summary**
- **show domain iwan master traffic-classes detail**
- **show domain iwan master traffic-classes dca detail**

- **show domain iwan master traffic-classes dca application**
- **show domain** *domain-name* **border dca**

  Displays information about reachability and metrics collected for all paths towards a service. This command helps in understanding the behavior of various paths for a service and how PFR is selecting the best paths depending on the metrics.

```
Device# show domain iwan border dca

[*] PFR created IP SLA entry ID
IPSLA DNS Resolver:208.67.220.220

App    DSCP  RTT/ms  DCA2   MPLS1
        thresh  Gi0/0/2   Tu10 (0:1)
           RTT/ms[*]   RTT/ms[*]
share-point    default  1000  7 [31]   --
youtube    default  1000  78 [33]   --
box    default  1000  7 [39]   --
dropbox    default  1000  3 [41]   --
google-services default     1000  108 [49]   --
google-group    default  1000  109 [51]   --
gtalk-group    default  1000  112 [53]   --
hangouts-group    default  1000  115 [55]   --
ms-lync-group    default  1000  6 [57]   --
ms-cloud-group    default  1000  7 [59]   --
```

- **show domain default policy**

  Displays the default policy on the master controller.

```
Device# show domain default master policy
       No Policy publish pending
------------------------------------------------------------------------------
  class SOCIAL-NETWORKING sequence  11
        class type: Application Based
             match application skype policy custom
                   priority 1 delay threshold 500 msec
```

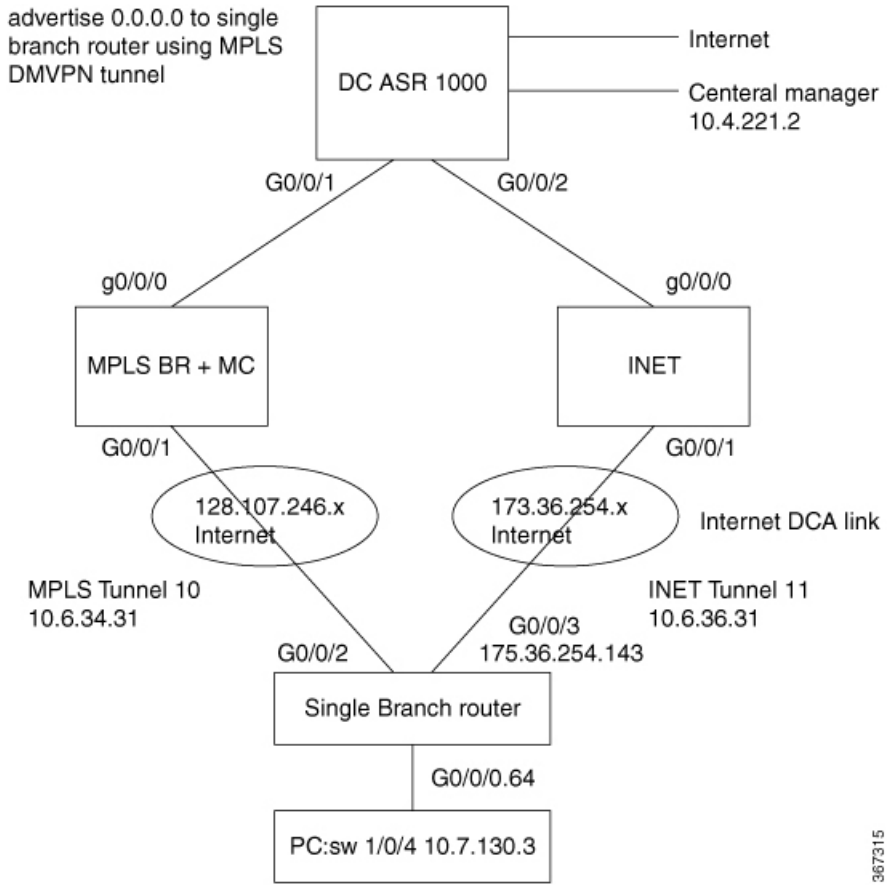
- To troubleshoot, use **debug domain default master dca** and *debug domain default border dca* commands.

# Configuration Examples for Configuring Direct Cloud Access

## Example: Configure DCA Link on a Single Branch Router

In this example, DCA is configured on Cisco IWAN network with a single branch router as shown in the following topology.

*Figure 16: DCA Link on a Single Branch Router*




The following configuration pertains to configuring Umbrella branch.

```
ip domain lookup vrf IWAN-TRANSPORT-2 source-interface GigabitEthernet0/0/3
ip domain name cisco.com //*This step is not required if OpenDNS Server is not used to
resolve dns request or if if other DNS server is configured for DNS resolution or registration
 with DNS is not required*//
ip host api.opendns.com 67.215.92.210 //*This step is not required if OpenDNS Server is not
 used to resolve dns request*//
ip name-server 8.8.8.8
ip name-server vrf IWAN-TRANSPORT-2 8.8.8.8
```

**Note** You need not specify the default static route if you have multi-VRF or if LAN is in different VRF. PfRv3 will automatically forward the whitelisted traffic to DCA interface.

The commands **ip domain name cisco.com** and **ip host api.opendns.com 67.215.92.210** are not required if OpenDNS Server is not used to resolve dns request or if another DNS server is configured for DNS resolution or registration with DNS is not required

Navigate to this link to log in to the OpenDNS portal (https://login.opendns.com/?return_to=https://dashboard2.opendns.com) to obtain API token and import the certificate on the device.

```
crypto pki trustpool import terminal
 % Enter PEM-formatted CA certificate.
-----BEGIN CERTIFICATE----- MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bdK
pPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz-----END CERTIFICATE-----
```

Optionally, the local domains and the token can be configured. DNS queries destined to local domain will remain untouched and will not be redirected to OpenDNS cloud.

```
parameter-map type umbrella global
 token F3F195ADD8160A3A4E42BB6B3722A5770022BF2F
 no dnscrypt
 udp-timeout 5
```

You may include the **resolver ipv4** *dns-server IP address* command, if you are not registering with the OpenDNS server or using another DNS server.

The hub master controller configuration is as follows:

```
domain iwan
 vrf default
  master hub
  class saasapp sequence 55
    match application share-point policy custom     !  For Office 365 Application
      priority 1 one-way-delay threshold 500
     match app-group ms-lync-group policy custom  ! For Office 365 Application
      priority 1 one-way-delay threshold 500
     match app-group ms-cloud-group policy custom  !  For Office 365 Application
      priority 1 one-way-delay threshold 500
      match application google-services policy custom  !  For google Application
       priority 1 one-way-delay threshold 1000
      match app-group google-group policy custom  !  For google Application
        priority 1 one-way-delay threshold 500
       match app-group gtalk-group policy custom  !  For google Application
      priority 1 one-way-delay threshold 500
     match app-group hangouts-group policy custom  !  For google Application
      priority 1 one-way-delay threshold 500
     match application youtube policy custom  !  For youtube Application
      priority 1 one-way-delay threshold 500
     match application box policy custom
      priority 1 one-way-delay threshold 500
     match application dropbox policy custom
```

```
      priority 1 one-way-delay threshold 500
     path-preference DCA1 fallback DCA2 next-fallback MPLS1
```

The configuration for class-map and policy for umbrella branch on the branch master controller is as follows:

```
class-map match-any umbrella-direct-access
 match protocol share-point
 match protocol attribute application-group ms-lync-group
 match protocol attribute application-group ms-cloud-group
 match protocol skype
 match protocol dropbox
 match protocol google-services
 match protocol attribute application-group google-group
 match protocol attribute application-group gtalk-group
 match protocol attribute application-group hangouts-group
 match protocol youtube
policy-map type umbrella umbrella-direct-access
 class umbrella-direct-access
  direct-cloud-access
```

The above created policy is assigned to an LAN interface.

```
interface GigabitEthernet0/0/0.64  ! INET branch LAN interface
 umbrella in direct-cloud-access umbrella-direct-access lan064
```

DCA is configured on WAN underlay interface in order to distinguish tunnel WAN interface.

```
interface GigabitEthernet0/0/3  ! INET branch WAN DCA interface
domain iwan path DCA1 direct-cloud-access
umbrella out
```

Optionally, a second DCA can be created as WAN underlay interface.

```
interface GigabitEthernet0/0/2  ! INET branch DCA2 interface
 domain iwan path DCA2 direct-cloud-access
 umbrella out
```

The following configuration creates domain map, which must match the hub configuration.

```
domain iwan
master branch
  domain-map
   application ms-lync-group domain http://www.office.com dscp default
   application ms-cloud-group domain http://www.office.com dscp default
   application ms-lync-group domain http://www.office.com dscp default
   application box domain http://www.box.com dscp default
   application dropbox domain http://www.dropbox.com dscp default
   application google-services domain http://www.google.com dscp default
   application google-group domain http://www.google.com dscp default
   application hangouts-group domain http://www.google.com dscp default
   application gtalk-group domain http://www.google.com/ dscp default
```

**Note** If there are multiple VRFs, IP SLA probing is performed for all domains defined for each VRF and the same IP SLA ID is used for each domain group in the VRF.

The following commands are used to verify the configuration. To verify OpenDNS configuration, use the **show umbrella deviceid** and **show umbrella configuration** commands.

```
router# show umbrella deviceid

Device registration details
Interface Name                  Tag                 Status                Device-id
```

```
GigabitEthernet3.64     inside-network   200 SUCCESS     010a3d458c172b8b

router# show umbrella configuration
Umbrella Configuration
=======================
   Token: 7772166EF2E473ADE8FA2204B37D0BD7001FE4F5
   OrganizationID: 2090229
   Local Domain Regex parameter-map name: dns_bypass
   DNSCrypt: Enabled
  Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
Umbrella Interface Config:
       Number of interfaces with "umbrella out" config: 2
         1. GigabitEthernet0/0/0
             Mode     :  OUT
             VRF      : IWAN-TRANSPORT-2(Id: 3)
         2. GigabitEthernet0/0/1
             Mode     :  OUT
             VRF      : IWAN-TRANSPORT-1(Id: 2)
       Number of interfaces with "umbrella in" config: 1
         1. GigabitEthernet3.64
             Mode       : IN
             DCA        : Enabled
             Policy Name: umbrella-direct-access
             Tag        : lan064
             Device-id  : 010a3d458c172b8b
             VRF        : global(Id: 0)
```

To verify DCA configuration, use the following commands:

- **show domain iwan border dca**
- **show domain iwan master traffic-classes summary**
- **show domain iwan master traffic-classes detail**
- **show ip sla summary**
- **show ip sla configuration**
- **show ip sla statistics**
- **show flow monitor name flow-monitor cache format table**

Use the **show ip sla summary**, **show ip sla configuration**, and **show ip sla statistics** commands to verify the probe functions.

Use the **show flow monitor** command to verify that the flow is passes through the DCA path.

```
Router# show domain iwan master traffic-classes summary

APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
Current-EXIT - Service-Provider(PFR-label)/Border/Interface(Channel-ID)
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN

Dst-Site-Pfx      Dst-Site-Id       State DSCP        TC-ID      APP-ID    APP
Current-Exit
```

```
DCA               Internet          CN    default[0]  30         9424      ms-cloud-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  29         4478      ms-lync-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  28         8388      hangouts-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  27         4692      gtalk-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  26         4456      google-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  25         218104328 google-service
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  21         50349148  dropbox
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  20         218104882 box
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)
DCA               Internet          CN    default[0]  17         218103890 youtube
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

Router# show domain iwan border dca

[*] PFR created IP SLA entry ID
IPSLA DNS Resolver:208.67.220.220

App    DSCP  RTT/ms  DCA2   MPLS1
        thresh  Gi0/0/2   Tu10 (0:1)
           RTT/ms[*]   RTT/ms[*]
share-point    default  1000  7 [31]   --
youtube    default  1000  78 [33]   --
box    default  1000  7 [39]   --
dropbox    default  1000  3 [41]   --
google-services default     1000  108 [49]   --
google-group    default  1000  109 [51]   --
gtalk-group    default  1000  112 [53]   --
hangouts-group    default  1000  115 [55]   --
ms-lync-group    default  1000  6 [57]   --
ms-cloud-group    default  1000  7 [59]   --

Router# show domain iwan master traffic-classes detail

 Dst-Site-Prefix: DCA               Application: ms-cloud-group   DSCP: default [0] Traffic
 class id:30 app_id:9424
  Clock Time:                 22:13:32 (UTC) 01/17/2018
  TC Learned:                 4d23h ago
  Present State:              CONTROLLED
  Current Performance Status: not monitored (internet)
  Current Service Provider:   DCA1 since 4d23h
  Previous Service Provider:  Unknown
  BW Used:                    0 bps
  Present WAN interface:      GigabitEthernet0/0/3 in Border 10.255.241.31
  Present Channel (primary):  6 DCA1 pfr-label:0:0 | 0:0 [0x0]
  Backup Channel:             4 DCA2 pfr-label:0:0 | 0:0 [0x0]
  Destination Site ID:        Internet
  DNS Primary Channel:        6 DCA1 pfr-label:0:0 | 0:0 [0x0]
  DNS Backup Channel:         4 DCA2 pfr-label:0:0 | 0:0 [0x0]
  Class-Sequence in use:      55
  Class Name:                 saasapp using policy User-defined
    priority 1 one-way-delay threshold 500 msec
  BW Updated:                 - ago
  Method for choosing channel: Random
  Reason for Latest Route Change:    Uncontrolled to Controlled Transition
  Route Change History

Router# show ip sla sum
```

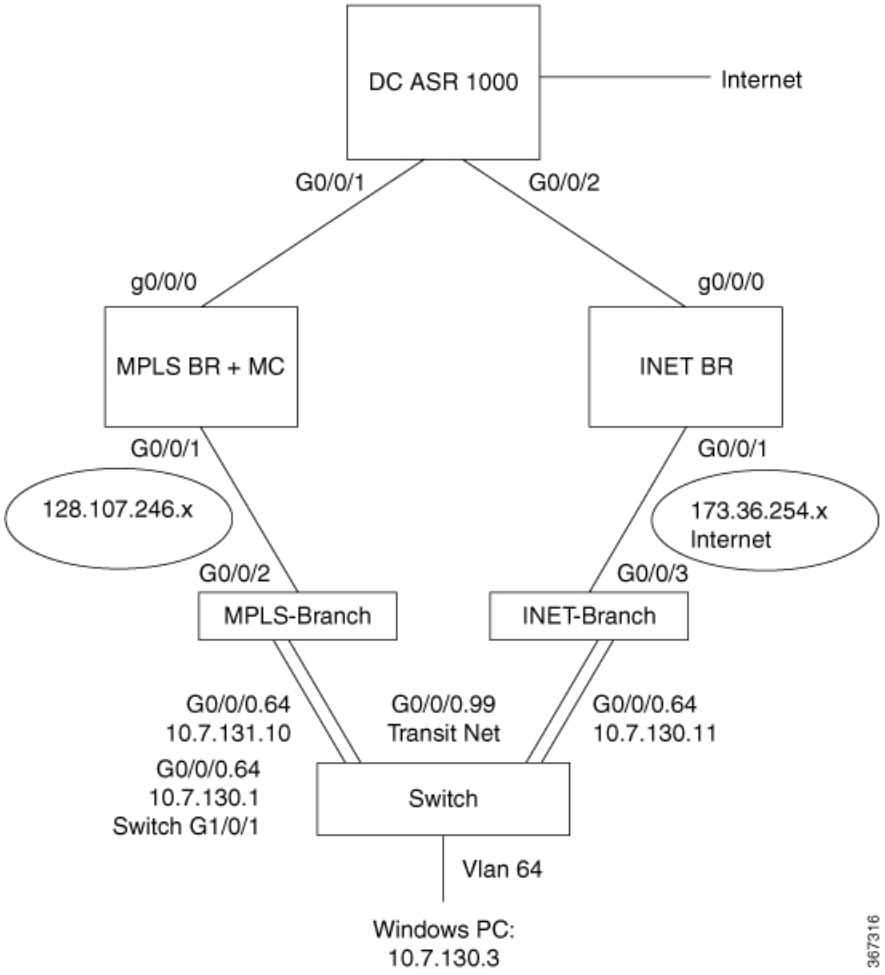
```
ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------

*1255        http        216.58.217.164    RTT=198     OK          30 seconds ago
*1256        http        216.58.217.164    RTT=184     OK          30 seconds ago
*1257        http        216.58.217.164    RTT=219     OK          30 seconds ago

*1258        http        216.58.217.164    RTT=219     OK          30 seconds ago

*1259        http        13.107.7.190      RTT=76      Http Error  30 seconds ago

Router# show ip sla config 1255

Entry number: 1255
Type of operation to perform: http
Target address/Source address: 216.58.217.164/172.16.1.1
Target port/Source port: 80/0
Type Of Service parameters: 0x0
Vrf Name: IWAN-TRANSPORT-2
HTTP Operation: get
HTTP Server Version: 1.0
URL: http://www.google.com
Proxy:
Raw String(s):
Cache Control: enable
Owner:
Tag:
Operation timeout (milliseconds): 30000
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 20000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None

Router# show ip sla statistics 1255

IPSLA operation id: 1255
        Latest RTT: 179 milliseconds
Latest operation start time: 19:09:14 UTC Fri Jan 26 2018
Latest operation return code: OK
Latest DNS RTT: 6 ms
Latest TCP Connection RTT: 62 ms
Latest HTTP Transaction RTT: 111 ms
Number of successes: 29
Number of failures: 0
Operation time to live: Forever

Router# show flow monitor Monitor-FNF-IWAN cache format table | i office
```

```
54.209.129.73    172.31.1.2                  80          62102  Gi0/0/0               Input
            6  layer7 ms-office-365              0.0.0.0                          /30  Null
                        4                   0x00
172.31.1.2       52.109.2.14               5110            443  Gi0/0/2.101           Output
           6  layer7 ms-office-web-apps          172.31.1.1                       /0  Gi0/0/0
                        7                   0x00
10.30.32.200     104.91.217.163           50319            443  Gi0/0/2.101           Input
            6  layer7 ms-office-365              172.31.1.1                       /0  Gi0/0/0
                        9                   0x00
172.31.1.2       208.67.222.222           52262             53  Null                  Output
          17  layer7 ms-office-365              172.31.1.1                      /30  Gi0/0/0
                        1  www.office.com    0x00
10.30.32.200     104.91.188.182           50341            443  Gi0/0/2.101           Input
            6  layer7 ms-office-365              172.31.1.1                       /0  Gi0/0/0
                       11                   0x00
10.30.32.200     104.91.188.182           50310            443  Gi0/0/2.101           Input
            6  layer7 ms-office-365              172.31.1.1                       /0  Gi0/0/0
                       11                   0x00
172.31.1.2       52.109.2.14               5108            443  Gi0/0/2.101           Output
           6  layer7 ms-office-web-apps          172.31.1.1                       /0  Gi0/0/0
                        8                   0x00
```

# Example: Configure DCA Link on a Dual Branch Router

In this example, DCA is configured on Cisco IWAN network with a dual branch router as shown in the following topology.

*Figure 17: DCA Link on a Dual Branch Router*




The following is the hub master controller configuration.

```
domain iwan
 vrf default
  master hub
  class saasapp sequence 55
    match application share-point policy custom     !  For Office 365 Application
      priority 1 one-way-delay threshold 500
     match app-group ms-lync-group policy custom  ! For Office 365 Application
      priority 1 one-way-delay threshold 500
     match app-group ms-cloud-group policy custom  !  For Office 365 Application
      priority 1 one-way-delay threshold 500
      match application google-services policy custom  !  For google Application
       priority 1 one-way-delay threshold 1000
      match app-group google-group policy custom  !  For google Application
        priority 1 one-way-delay threshold 500
       match app-group gtalk-group policy custom  !  For google Application
      priority 1 one-way-delay threshold 500
     match app-group hangouts-group policy custom  !  For google Application
      priority 1 one-way-delay threshold 500
     match application youtube policy custom  !  For youtube Application
      priority 1 one-way-delay threshold 500
     match application box policy custom
```

```
     priority 1 one-way-delay threshold 500
    match application dropbox policy custom
     priority 1 one-way-delay threshold 500
    path-preference DCA1 fallback DCA2 next-fallback MPLS1
```

The following is the domain map configuration on the MPLS branch master controller. The domain map must match the hub configuration.

```
domain iwan
master branch
  domain-map
   application ms-lync-group domain http://www.office.com dscp default
   application ms-cloud-group domain http://www.office.com dscp default
   application ms-lync-group domain http://www.office.com dscp default
   application box domain http://www.box.com dscp default
   application dropbox domain http://www.dropbox.com dscp default
   application google-services domain http://www.google.com dscp default
   application google-group domain http://www.google.com dscp default
   application hangouts-group domain http://www.google.com dscp default
   application gtalk-group domain http://www.google.com/ dscp default
```

The following is the configuration on INET branch router to create class-map and policy for umbrella branch.

```
class-map match-any umbrella-direct-access
 match protocol share-point
 match protocol attribute application-group ms-lync-group
 match protocol attribute application-group ms-cloud-group
 match protocol skype
 match protocol dropbox
 match protocol google-services
 match protocol attribute application-group google-group
 match protocol attribute application-group gtalk-group
 match protocol attribute application-group hangouts-group
 match protocol youtube
policy-map type umbrella umbrella-direct-access
class umbrella-direct-access
  direct-cloud-access
```

The policy created above is assigned to a LAN interface.

```
GigabitEthernet0/0/0.64  ! INET branch LAN interface
 umbrella in direct-cloud-access umbrella-direct-access lan064
```

The DCA is assigned to WAN interface as follows:

```
interface GigabitEthernet0/0/3  ! INET branch WAN DCA interface
domain iwan path DCA1 direct-cloud-access
umbrella out
```

Optionally, a second DCA (on another WAN interface) can be configured as follows:

```
interface GigabitEthernet0/0/2  ! MPLS branch WAN DCA interface
domain iwan path DCA2 direct-cloud-access
umbrella out
```

The following adds the interface to IWAN border source-interface configuration and enables the feature.

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nat inside
 umbrella in direct-cloud-access umbrella-direct-access inetAT
domain iwan
 vrf default
  border
```

```
source-interface Loopback0 virtual-template 1
shut
no shut
```

In DCA dual branch scenario, to apply features like NAT or Umbrella on PfR auto-tunnel interface, a virtual template is configured and bound to IWAN domain configuration.

To effect configuration changes on virtual template interface, you must execute the **shut** or **no shut** command on the branch router.

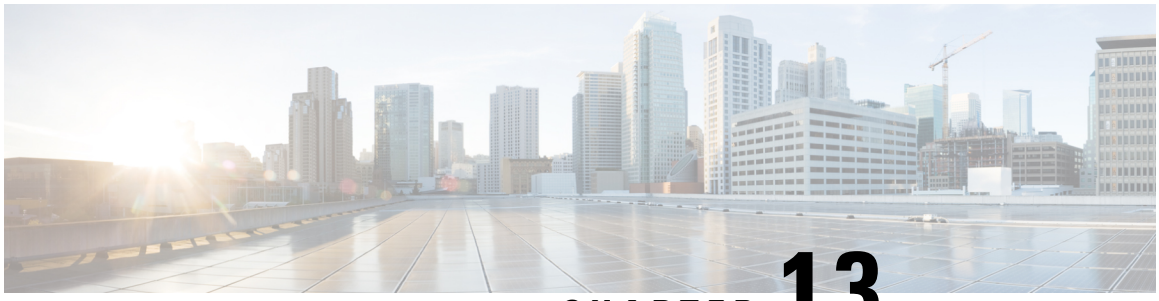
# Additional References for Configuring Direct Cloud Access

### Related Documents

| Related Topic | Document Title |
|---|---|
| Performance Routing Version 3 commands | Cisco IOS Performance Routing Version 3 Command Reference |

### 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 |



CHAPTER 13

# PfRv3 Command References

The following tables lists various Cisco IOS commands that are used for PfRv3 along with the command mode from which they are entered.

***Table 23: Configuration Commands for PfRv3***

| Command mode | Command name | Description |
|---|---|---|
| Interface configuration | **bandwidth** *bandwidth-value* | Configures inherited and received bandwidth values for the tunnel interface. The bandwidth value is in kilobits and the valid values are 1 to 10000000. |
| Border configuration | **border** | Defines a device as a border. |
| Domain master controller configuration | **branch-to-branch** | Disable branch to branch PfR optimization. This is configured on Branch Masters.<br>**Note** Configuring the command results in two different bahaviors for the different releases. See, PfRv3 Command Reference guide. |
| Configuration | **domain** *domain name* | Configures a top level domain for PfRv3. |
| Configuration interface | **domain** *domain name* **path***path-name* | Configures a path for the domain for PfRv3. |
| Global configuration | **domain** *domain name* **path***path-name* **path-id***path-id* | Configures a path and path-id for a specified domain. |
| Global configuration | **domain path** *isp-name* **zero-sla** | Configures Zero SLA on tunnel interface for an ISP path. |
| Master controller configuration | **hub** *ip-address* | Configures an IP address for the hub. |
| Domain class configuration | **match {application \| dscp}** | Specifies applications or DSCP policies to be associated with a class. |

| Command mode | Command name | Description |
|---|---|---|
| Master controller configuration | **master** *ip-address* | Configures an IP address for the master controller. |
| Domain VRF configuration | **master {hub \| branch \| transit}** | Defines a device as a master type. You can configure a master device as a hub, border, or a transit. |
| Domain VRF configuration | **master transit** *pop-id* | Configures an ID for the master transit branch. |
| Domain-class configuration | **path-preference** *path-name* **fallback** *path-name* | Specifies a path preference for a traffic class policy. |
| Master controller class type | **priority** *priority-number* **[jitter \| loss \| one-way-delay] threshold** *thershold-value* | Specifies threshold values for user-defined policies. |
| Domain configuration | **vrf** *vrf- name* | Configures a Virtual Routing and Forwarding (VRF) instance for a domain. |

***Table 24: Show Commands for PfRv3***

| Command mode | Command name | Description |
|---|---|---|
| Privileged EXEC | **show domain** *domain-name* **border peering** | Displays the border router peering status. |
| Privileged EXEC | **show domain** *domain-name* **border pmi \| begin prefix-learn** | Displays the automatically learned site-prefix status information of the hub-border router. |
| Privileged EXEC | **show domain** *domain-name* **border status** | Displays the status of the border routers configured at the hub site. |
| Privileged EXEC | **show domain** *domain-name* **border site-prefix** | Displays the site-prefix status information of the hub- border router. |
| Privileged EXEC | **show domain** *domain-name* **border channels** | Displays channel information from the hub-border site. |
| Privileged EXEC | **show domain** *domain-name* **border parent route** | Displays the parent route information of a border channel. |
| Privileged EXEC | **show domain** *domain-name* **border channels parent route** | Displays the parent route information of a channel. |
| Privileged EXEC | **show domain** *domain-name* **master exits** | Displays the summary of the external interfaces configured at the hub site. |
| Privileged EXEC | **show domain** *domain-name* **master peering** | Displays the peering information of the hub-master controller. |

| Command mode | Command name | Description |
|---|---|---|
| Privileged EXEC | **show domain** *domain-name* **master discovered-sites** | Displays branch sites that are remotely connected to the hub site. |
| Privileged EXEC | **show domain** *domain-name* **master site-prefix** | Displays the site-prefix status information of the hub- master controller. |
| Privileged EXEC | **show platform pfrv3 rp active smart-probe** | Displays the PfRv3 smart probe status on a Cisco ASR 1000 Series Aggregation Services Router configured at the hub site. |
| Privileged EXEC | **show platform pfrv3 fp active smart-probe** | Displays the PfRv3 active smart probes status of a embedded-service-processor on Cisco ASR 1000 Series Aggregation Services Routers. |
| Privileged EXEC | **show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail** | Displays the platform hardware information on a Cisco ASR 1000 Series Aggregation Services Routers. |
| Privileged EXEC | **show flow monitor type performance-monitor** | Displays the flow monitor information for passive performance monitoring on the egress interface of WAN. |
| Privileged EXEC | **show domain** *domain-name* **master traffic-classes summary** | Displays the summary information of all the traffic classes. |
| Privileged EXEC | **show domain** *domain-name* **master traffic-classes** | Displays the status information of the traffic class for the hub-master controller. |
| Privileged EXEC | **show domain** *domain-name* **master traffic-classes policy** *policy-name* | Displays the occurrence of performance issues in a policy traffic class. |
| Privileged EXEC | **show domain** *domain-name* **master channels** | Displays channel information from the hub site. |
| Privileged EXEC | **show domain** *domain-name* **master channels link-name** *path-name* | Displays channel status information and the unreachable threshold crossing alerts (TCA) and on demand export (ODE) instances on a hub-master controller. |
| Privileged EXEC | **show domain** *domain-name* **master channels dst-site-id** *destination-site-id* | Displays the details of destination site-ids configured with hub-master controller. |
| Privileged EXEC | **show domain** *domain-name* **default master site-capability** | Displays the capability information of master controller. |

*Table 25: Debug Commands for PfRv3*

| Command mode | Command name | Description |
|---|---|---|
| Privileged EXEC | **debug platform hardware qfp active feature pfrv3 client** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) client debug logging. |
| Privileged EXEC | **debug platform hardware qfp active feature pfrv3 datapath** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) data path debug logging. |
| Privileged EXEC | **debug platform hardware qfp active feature pfrv3 pal** | Enables debug logging for PfRv3 in the Cisco Quantum Flow Processor (QFP). |
| Privileged EXEC | **debug platform software pfrv3** | Enables PfRv3 platform debug commands. |