<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Branch Border Router</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Branch Master Controller and Border Router</td>
<td>27</td>
</tr>
<tr>
<td>Verifying PfRv3 Configuration</td>
<td>29</td>
</tr>
<tr>
<td>Verifying Hub Master Controller Configurations</td>
<td>29</td>
</tr>
<tr>
<td>Verifying Hub Border Router Configurations</td>
<td>36</td>
</tr>
<tr>
<td>Verifying Branch Master Controller Configurations</td>
<td>40</td>
</tr>
<tr>
<td>Verifying Branch Border Configurations</td>
<td>42</td>
</tr>
<tr>
<td>Monitoring PfRv3</td>
<td>47</td>
</tr>
<tr>
<td>Monitoring Site Prefix</td>
<td>47</td>
</tr>
<tr>
<td>Monitoring Traffic Classes</td>
<td>49</td>
</tr>
<tr>
<td>Monitoring Channels</td>
<td>52</td>
</tr>
<tr>
<td>Example: Configuring Performance Routing Version 3</td>
<td>55</td>
</tr>
</tbody>
</table>

---

**CHAPTER 4**  

**PfRv3 Transit Site Support**  
91

- Feature Information for PfRv3 Transit Site Support  
  91
- Prerequisites for PfRv3 Transit Site Support  
  92
- Restrictions for PfRv3 Transit Site Support  
  92
- Information About PfRv3 Transit Site Support  
  92
  - Information About Transit Site Support  
    92
  - PfRv3 Transit Site Use Case Scenarios  
    92
- How to Configure Transit Site Support  
  95
  - Configuring Transit Hub  
    95
  - Configuring Transit Site Border Routers  
    98
  - Verifying PfRv3 Transit Site Support  
    101
- Configuration Examples for PfRv3 Transit Site Support  
  105
  - Example: Configuring Transit Site Support  
    105

---

**CHAPTER 5**  

**PfRv3 Path of Last Resort**  
123

- Feature Information for PfRv3 Path of Last Resort  
  123
- Restrictions for PfRv3 Path of Last Resort  
  123
- Information About PfRv3 Path of Last Resort  
  124
- PfRv3 Path of Last Resort  
  124
- How to Configure PfRv3 Path of Last Resort  
  124
  - Configuring Policy for Path of Last Resort  
    124
About this Guide

- Audience, on page 1
- Document Organization, on page 1
- Document Conventions, on page 2
- New and Changed Information, on page 3
- Additional References for PfRv3, on page 4

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:

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

This document uses the following conventions:

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Routing v3</td>
<td>15.5(1)T</td>
<td>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.</td>
<td>• Overview of Performance Routing v3</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.13S</td>
<td></td>
<td>• Configuring Basic PfRv3</td>
</tr>
<tr>
<td>Performance Routing v3 Zero SLA Support</td>
<td>15.5(1)T</td>
<td>The PfRv3 zero SLA support feature enables users to reduce probing frequency on various ISP links.</td>
<td>Performance Routing v3 Zero SLA Support</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.14S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Routing v3 Transit Site Support</td>
<td>15.5(2)T</td>
<td>The PfRv3 transit site support feature enables enterprise organizations to configure multiple data centers at the hub site.</td>
<td>PfRv3 Transit Site Support</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.15S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional References for PfRv3**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Cisco PfRv3 commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples</td>
<td>Cisco IOS Performance Routing Command Reference</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com</td>
<td></td>
</tr>
<tr>
<td>user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
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, on page 7
- Hardware and Software Support, on page 8
- Restrictions for Configuring Performance Routing v3, on page 8
- Information About PfRv3, on page 9

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3</td>
<td>15.4(3)M</td>
<td>Performance Routing v3 (PfRv3) is the evolution of Performance Routing. 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. The following commands were modified by this feature: <code>domain default</code>, <code>vrf default</code>, <code>master</code>, <code>source-interface</code>, <code>site-prefixes</code>, <code>password</code>, <code>monitor-interval</code>, <code>route-control</code>, <code>load-balance</code>, <code>enterprise-prefix</code>, <code>advanced</code>, <code>minimum-mask-length</code>, <code>mitigation-mode</code>, <code>threshold-variance</code>, <code>smart-probes</code>, <code>collector</code>, <code>class</code>, <code>match</code>, <code>priority</code>, <code>path-preference</code>, <code>border</code>, <code>domain-path</code>.</td>
</tr>
</tbody>
</table>

Hardware and Software Support

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

<table>
<thead>
<tr>
<th>Device</th>
<th>Cisco IOS Software Release</th>
<th>Hub/Remote Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISR 4000 Series Routers</td>
<td>Cisco IOS XE 3.13 or later</td>
<td>Hub or remote site</td>
</tr>
<tr>
<td>Cisco ASR 1000 Series Routers</td>
<td>Cisco IOS XE 3.13 or later</td>
<td>Hub site</td>
</tr>
<tr>
<td>Cisco CSR 1000v Series Routers</td>
<td>Cisco IOS XE 3.14 or later</td>
<td>Hub site (master controller only)</td>
</tr>
<tr>
<td>Cisco ISR-G2 Series Routers</td>
<td>Cisco IOS 15.5(1)T1 or later</td>
<td>Remote site</td>
</tr>
</tbody>
</table>

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).

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 is 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:

<table>
<thead>
<tr>
<th>Pre-defined Template</th>
<th>Threshold Definition</th>
</tr>
</thead>
</table>
| Voice                | Priority 1 one-way-delay threshold 150 threshold 150 (msec)  
|                      | Priority 2 packet-loss-rate threshold 1 (%)  
|                      | Priority 2 byte-loss-rate threshold 1 (%)  
|                      | Priority 3 jitter 30 (msec) |
| Real-time-video      | Priority 1 packet-loss-rate threshold 1 (%)  
|                      | Priority 1 byte-loss-rate threshold 1 (%)  
|                      | Priority 2 one-way-delay threshold 150 (msec)  
|                      | Priority 3 jitter 20 (msec) |
| Low-latency-data     | Priority 1 one-way-delay threshold 100 (msec))  
|                      | Priority 2 byte-loss-rate threshold 5 (%)  
|                      | Priority 2 packet-loss-rate threshold 5 (%) |
| Bulk-data            | Priority 1 one-way-delay threshold 300 (msec)  
|                      | Priority 2 byte-loss-rate threshold 5 (%)  
|                      | Priority 2 packet-loss-rate threshold 5 (%) |
| Best-effort          | Priority 1 one-way-delay threshold 500 (msec)  
|                      | Priority 2 byte-loss-rate threshold 10 (%)  
<p>|                      | Priority 2 packet-loss-rate threshold 10 (%) |</p>
<table>
<thead>
<tr>
<th>Pre-defined Template</th>
<th>Threshold Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scavenger</td>
<td>Priority 1 one-way-delay threshold 500 (msec)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 byte-loss-rate threshold 50 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 packet-loss-rate threshold 50 (%)</td>
</tr>
<tr>
<td>Custom</td>
<td>Defines customized user-defined policy values</td>
</tr>
</tbody>
</table>

**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.
CHAPTER 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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enters your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>interface loopback  <em>interface-number</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures an IP address for an interface on the hub-master controller.</td>
</tr>
<tr>
<td>ip address  <em>ip-address-mask</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 10.8.3.3 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# exit</td>
</tr>
<tr>
<td>6</td>
<td>domain {domain-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# domain default</td>
</tr>
<tr>
<td>7</td>
<td>vrf {vrf-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-domain)# vrf default</td>
</tr>
<tr>
<td>8</td>
<td>master {hub</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf)# master hub</td>
</tr>
<tr>
<td>9</td>
<td>source-interface loopback interface-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# source-interface Loopback0</td>
</tr>
<tr>
<td>10</td>
<td>enterprise-prefix prefix-list site-list</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE</td>
</tr>
<tr>
<td>11</td>
<td>site-prefixes prefix-list site-list</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# site-prefixes prefix-list Data_Center_1</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Exit from master controller configuration mode and returns to domain configuration mode.</strong></td>
</tr>
<tr>
<td>Step 12</td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-domain-vrf-mc)# exit</code></td>
</tr>
<tr>
<td>Step 13</td>
<td><code>ip prefix-list</code> *ip-list seq sequence-number permit ip-prefix-network le le-length`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24</code></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24</code></td>
</tr>
<tr>
<td>Step 14</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# end</code></td>
</tr>
<tr>
<td>Step 15</td>
<td><em>(Optional)</em> <code>show domain domain-name master status</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Device# show domain one master status</code></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2**        |         |
| configure terminal | Enters global configuration mode. |
| **Example:**      |         |
| Device# configure terminal |

| **Step 3**        |         |
| interface loopback interface-number | Enters interface configuration mode. |
| **Example:**      |         |
| Device(config)# interface Loopback0 |

| **Step 4**        |         |
| ip address ip-address-mask | Configures an IP address for an interface on the hub-border router (Border Router 1). |
| **Example:**      |         |
| Device(config-if)# ip address 10.8.1.1 255.255.255.255 |

<p>| <strong>Step 5</strong>        |         |
| exit              | Exits interface configuration mode and returns to global configuration mode. |
| <strong>Example:</strong>      |         |
|                   |         |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# exit</td>
<td>Enters domain configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>`domain {domain-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# domain one</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>`vrf {vrf-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain)# vrf default</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>border</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf)# border</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>source-interface loopback interface-number</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf-br)# source-interface Loopback0</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>`master [ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf-br)# master 10.8.3.3</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf-br)# exit</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf)# exit</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain)# exit</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><code>interface tunnel-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface Tunnel100</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><code>ip address ip-address  mask</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip address 10.0.100.84 255.255.255.0</td>
</tr>
</tbody>
</table>

**Note** You can also configure specific VRF definition for hub-border configuration.
### Purpose

Command or Action | Purpose
--- | ---
Step 16 | 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.

Example: 
Device(config-if)# domain one path MPLS

**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 | Exits interface configuration mode and returns to privileged EXEC mode.

Example: 
Device(config-if)# end

---

Step 18 | Use this show command to display the status of a border router.

Example: 
Device# show domain one border status

---

### 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]`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | domain \{domain-name | default\} | Enters domain configuration mode.  
**Example:**  
Device(config)# domain default |
| **Step 2** | vrf \{vrf-name | default\} | Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain.  
**Example:**  
Device(config-domain)# vrf default |
| **Step 3** | master [hub | branch | transit] | 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.  
**Example:**  
Device(config-domain-vrf)# master hub |
| **Step 4** | monitor-interval \{seconds | dscp ef\} | Configures interval time that defines monitoring interval on ingress monitors.  
**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.  
**Example:**  
Device(config-domain-vrf-mc)# monitor-interval 2 dscp ef |
| **Step 5** | load-balance | Configures load balancing.  
**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.  
**Example:**  
Device(config-domain-vrf-mc)# load-balance |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> class class-name sequence sequence-number</td>
<td>Enters policy class configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc)# class VOICE sequence 10</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Class-name value must be in all capitals.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> match {application</td>
<td>dscp} services-value policy</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc-class)# match dscp ef policy voice</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> path-preference path-name fallback path-name</td>
<td>Configures the path preference for applications.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc-class)# path-preference MPLS fallback INET</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> priority priority-number [jitter</td>
<td>loss</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600</td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 200</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> You can configure class type priorities only for a custom policy. You can configure multiple priorities for custom policies.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface loopback interface-number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address ip-address-mask</td>
<td>Configures an IP address for an interface on the branch-master controller.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# ip address 10.2.10.10 255.255.255.255</td>
<td>Enters domain configuration mode.</td>
</tr>
</tbody>
</table>

### Step 5

**domain** `{domain-name | default}`

**Example:**
Device(config)# domain default

**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}`

**Example:**
Device(config-domain)# vrf default

**Note** You can also configure specific VRF definition for branch border configuration.

### Step 7

**master branch**

**Example:**
Device(config-domain-vrf)# master branch

### Step 8

**source-interface loopback interface-number**

**Example:**
Device(config-domain-vrf-mc)# source-interface Loopback0

### Step 9

**hub ip-address**

**Example:**
Device(config-domain-vrf-mc)# hub 10.8.3.3

### Step 10

**end**

**Example:**
Device(config-domain-vrf-mc)# end

### Step 11

(Optional) **show domain domain-name master status**

**Example:**
Device# show domain one master status

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> domain {domain-name</td>
<td>default}</td>
</tr>
<tr>
<td>Example: Device(config)# domain default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vrf {vrf-name</td>
<td>default}</td>
</tr>
<tr>
<td>Example: Device(config-domain)# vrf default</td>
<td>Note You can also configure specific VRF definition for the branch-border configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong> border</td>
<td>Enters border configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-domain-vrf)# border</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> source-interface loopback interface-number</td>
<td>Configures the loopback address used as a source for peering with other sites or the master controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-domain-vrf-br)# source-interface Loopback0</td>
<td>Specifies the IP address of the branch-master controller.</td>
</tr>
<tr>
<td><strong>Step 7</strong> master ip-address</td>
<td>Specifies the IP address of the branch-master controller.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-domain-vrf-br)# master 10.1.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Exits border configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-domain-vrf-br)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> (Optional) show domain domain-name border status</td>
<td>Use this show command to display the status of a border router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show domain one border status</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

- Enter your password if prompted.

### Command or Action

**Example:**

Device> enable

**Step 2**

configure terminal

**Example:**

Device# configure terminal

**Step 3**

interface loopback  *interface-number*

**Example:**

Device(config)# interface Loopback0

**Step 4**

ip address  *ip-address-mask*

**Example:**

Device(config-if)# ip address 10.2.12.12 255.255.255.255

**Step 5**

exit

**Example:**

Device(config-if)# exit

**Step 6**

domain  {*domain-name | default}*

**Example:**

Device(config)# domain default

**Step 7**

vrf  {*vrf-name | default}*

**Example:**

Device(config-domain)# vrf default

**Step 8**

border

**Example:**

Device(config-domain-vrf)# border

**Step 9**

source-interface loopback  *interface-number*

**Example:**

Device(config-domain-vrf-br)# source-interface Loopback0

**Step 10**

master local

**Example:**

Device(config-domain-vrf-br)# master local
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong></td>
<td>Configures the master type of the device as a branch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-domain-vrf-mc)# master branch</td>
</tr>
</tbody>
</table>

| **Step 12**       | Configures the loopback used as a source for peering with other sites or master controller. |
| **Example:**      | Device(config-domain-vrf-mc)# source-interface Loopback0 |

| **Step 13**       | Configures the IP address of the hub-master controller. |
| **Example:**      | Device(config-domain-vrf-mc)# hub 10.8.3.3 |

| **Step 14**       | Exits the configuration mode and returns to privileged EXEC mode. |
| **Example:**      | Device(config-domain-vrf-mc)# end |

### What to do next

**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

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

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

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

<table>
<thead>
<tr>
<th>class default</th>
<th>match dscp all</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of Traffic classes using this policy: 3</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy publish pending</td>
<td>Specifies if the policy publishing is pending to remote sites.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
class | Name of the class type. In this example, the following classes are listed:
• VOICE
• VIDEO
• 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
```
Verifying Hub Master Controller Configurations

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Type</td>
<td>Displays the instance type of the device. In this output, the device is configured as a hub.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays the operational status of the hub.</td>
</tr>
<tr>
<td>Configured Status</td>
<td>Displays the configuration status of the hub.</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>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.</td>
</tr>
<tr>
<td>Borders</td>
<td>Displays the information of border routers connected to the hub master controller.</td>
</tr>
<tr>
<td>Number of default Channels</td>
<td>Displays the number of channels configured.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR address</td>
<td>IP address of border routers configured at the hub site.</td>
</tr>
<tr>
<td>type</td>
<td>Type of interface. Internal or external. In this example, the type is external.</td>
</tr>
<tr>
<td>Path</td>
<td>Name of the path.</td>
</tr>
<tr>
<td>Egress capacity</td>
<td>Egress capacity of the interface.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Number of traffic classed configured per DSCP on external interfaces.</td>
</tr>
</tbody>
</table>

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
Verifying Hub Master Controller Configurations

*** 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peering state</td>
<td>Status of peering.</td>
</tr>
<tr>
<td>Subscribed services</td>
<td>Lists the status of services subscribed to.</td>
</tr>
<tr>
<td>Published services</td>
<td>Services published by the hub-master controller to the remote sites.</td>
</tr>
</tbody>
</table>

**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 :af4[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 :af4[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 :af4[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:Tunnel10 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Status</td>
<td>Displays the instance status.</td>
</tr>
<tr>
<td>Master</td>
<td>IP address of the master controller.</td>
</tr>
<tr>
<td>Minimum Requirement</td>
<td>Displays the minimum requirement status of the border router.</td>
</tr>
<tr>
<td>External Wan interfaces</td>
<td>Displays the information of external interfaces configured on border router.</td>
</tr>
<tr>
<td>Auto Tunnel information</td>
<td>Displays the information of auto-tunnel configuration.</td>
</tr>
</tbody>
</table>

**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-prefix status
- Globals service status

**Example:**

```
HubBR# show domain one border peering
```

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

**Published service:**

The following table describes the significant fields shown in the command output.
Table 8: show domain border peering Field Descriptions

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

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
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 Kbps
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
Minimum Mask Length: 28
Sampling: off
Minimum Requirement: Met
```
The following table describes the significant fields shown in the command output.

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

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

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

**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
```

---

```text
*** 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:Tunnel10 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Status</td>
<td>Displays the instance status of the device.</td>
</tr>
</tbody>
</table>
### Step 2

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

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

**Example:**

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

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.8.3.3</td>
<td>Lo0</td>
<td>497</td>
<td>02:12:18</td>
<td>5</td>
<td>100</td>
<td>31</td>
</tr>
</tbody>
</table>

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-prefix status
- Globals service status

**Example:**

```bash
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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peering state</td>
<td>Status of peering.</td>
</tr>
<tr>
<td>Subscribed services</td>
<td>Displays the subscribed services list.</td>
</tr>
<tr>
<td>Published services</td>
<td>Displays the services published by the branch-master controller to the branch-border routers.</td>
</tr>
</tbody>
</table>

**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-0-3:
Egress policy activated on:
  Tunnel1200 Tunnel1100

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;
```

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.10.10</td>
<td>10.2.10.10/24</td>
<td>00:42:07 ago</td>
<td>S</td>
</tr>
<tr>
<td>10.2.10.10</td>
<td>10.2.10.10/32</td>
<td>00:42:07 ago</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.2.11.11/32</td>
<td>00:18:25 ago</td>
<td>S</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.3.3/32</td>
<td>1d05h ago</td>
<td>L</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.0.0/16</td>
<td>1d05h ago</td>
<td>C</td>
</tr>
<tr>
<td>255.255.255</td>
<td>10.0.0.0/8</td>
<td>1d05h ago</td>
<td>T</td>
</tr>
</tbody>
</table>
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;

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

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

<table>
<thead>
<tr>
<th>Dst-Site-Pfx</th>
<th>Dst-Site-Id</th>
<th>APP</th>
<th>DSCP</th>
<th>TC-ID</th>
<th>APP-ID</th>
<th>State</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af11</td>
<td>193</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>59/60</td>
<td>10.8.2.2/Tunnel100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>cs1</td>
<td>192</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>57/58</td>
<td>10.8.2.2/Tunnel100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>cs5</td>
<td>191</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>55/58</td>
<td>10.8.2.2/Tunnel100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>ef</td>
<td>190</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>52/58</td>
<td>10.8.2.2/Tunnel100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af41</td>
<td>195</td>
<td>N/A</td>
<td>CN</td>
<td>INET</td>
</tr>
<tr>
<td>64/63</td>
<td>10.8.1.1/Tunnel1200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>cs4</td>
<td>189</td>
<td>N/A</td>
<td>CN</td>
<td>INET</td>
</tr>
<tr>
<td>54/53</td>
<td>10.8.1.1/Tunnel1200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af31</td>
<td>194</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>61/62</td>
<td>10.8.2.2/Tunnel100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
```

```
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
```

Performance Routing v3 Configuration Guide, Cisco IOS Release 15M&T
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>show platform software pfrv3 rp active route-control traffic-class</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show platform software pfrv3 fp active route-control traffic-class</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>show platform hardware qfp active feature pfrv3 client route-control traffic-class detail</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show platform software interface rp active name interface-name</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show platform software interface fp active name interface-name</code></td>
</tr>
</tbody>
</table>
### 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
Inmitigable Events Summary:
Total Performance Count: 0, Total BW Count: 0
TCA Statistics:
  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: Tunnel1200
  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

---

Performance Routing v3 Configuration Guide, Cisco IOS Release 15M&T

53
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.
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**

```bash
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**

```bash
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)# load-balance
HubMC(config-domain-vrf)# class VOICE sequence 10
HubMC(config-domain-vrf)# match dscp ef policy voice
HubMC(config-domain-vrf)# path-preference MPLS fallback INET
HubMC(config-domain-vrf)# exit
HubMC(config-domain-vrf)# class VIDEO sequence 20
HubMC(config-domain-vrf)# match dscp af41 policy real-time-video
HubMC(config-domain-vrf)# match dscp cs4 policy real-time-video
HubMC(config-domain-vrf)# path-preference INET fallback MPLS
HubMC(config-domain-vrf)# exit
HubMC(config-domain-vrf)# class CRITICAL sequence 30
HubMC(config-domain-vrf)# match dscp af31 policy custom
HubMC(config-domain-vrf)# priority 2 loss threshold 10
HubMC(config-domain-vrf)# priority 1 one-way-delay threshold 600
HubMC(config-domain-vrf)# priority 2 jitter threshold 600
HubMC(config-domain-vrf)# exit
HubMC(config-domain-vrf)# 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
**Example: Configuring Performance Routing Version 3**

**Configuring BR1**

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 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 key 100
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 key 200
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 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)# 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:
Example: Configuring Performance Routing Version 3

**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 pferv3 rp active smart-probe
HubBR# show platform software pferv3 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
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;

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.10.10</td>
<td>10.1.10.0/24</td>
<td>00:42:07 ago</td>
<td>S,</td>
</tr>
<tr>
<td>10.2.10.10</td>
<td>10.2.10.10/32</td>
<td>00:42:07 ago</td>
<td>S,</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.2.11.11/32</td>
<td>00:18:25 ago</td>
<td>S,</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.3.3/32</td>
<td>1d05h ago</td>
<td>L,</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.0.0/16</td>
<td>1d05h ago</td>
<td>C,</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>*10.0.0.0/8</td>
<td>1d05h ago</td>
<td>T,</td>
</tr>
</tbody>
</table>

```
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;

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

```
show domain  domain-name  master traffic-classes 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

<table>
<thead>
<tr>
<th>Dst-Site-Pfx</th>
<th>Dst-Site-Id</th>
<th>APP</th>
<th>DSCP</th>
<th>TC-ID</th>
<th>APP-ID</th>
<th>State</th>
<th>SP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC/BC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af11</td>
<td>193</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>59/60</td>
<td>10.8.2.2/Tunnel100</td>
<td>N/A</td>
<td>cs1</td>
<td>192</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>cs5</td>
<td>191</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>55/NA</td>
<td>10.8.2.2/Tunnel100</td>
<td>N/A</td>
<td>ef</td>
<td>190</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af41</td>
<td>195</td>
<td>N/A</td>
<td>CN</td>
<td>INET</td>
</tr>
<tr>
<td>64/63</td>
<td>10.8.1.1/Tunnel200</td>
<td>N/A</td>
<td>cs4</td>
<td>189</td>
<td>N/A</td>
<td>CN</td>
<td>INET</td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td>af31</td>
<td>194</td>
<td>N/A</td>
<td>CN</td>
<td>MPLS</td>
</tr>
<tr>
<td>54/53</td>
<td>10.8.1.1/Tunnel200</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.10.0/24</td>
<td>10.2.10.10</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61/62</td>
<td>10.8.2.2/Tunnel100</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show domain domain-name master traffic-classes 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: CONTROLED
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
domain one
class VIDEO sequence 20
match dscp ef policy custom
priority 1 one-way-delay threshold 150
path-preference MPLS fallback INET
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
!
```text
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
```

---

**Performance Routing v3 Configuration Guide, Cisco IOS Release 15M&T**

Page 69
Example: Configuring Performance Routing Version 3

```
control-plane

line con 0
eexec-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 952V3LWQEC9D
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/TRANSF Transport esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSF 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

Example: Configuring Performance Routing Version 3

Performance Routing v3 Configuration Guide, Cisco IOS Release 15M&T
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
!
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
eexec-timeout 0 0
stopbits 1
line vty 0 4
eexec-timeout 0 0
privilege level 15
no login
line vty 5 15
eexec-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
!
vrfs definition INET2
rd 65512:2
!
address-family ipv4

---

Example: Configuring Performance Routing Version 3

---
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
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
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
!
routing 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 INET-HUB route-map INET-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
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
! no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
master branch
source-interface Loopback0
hub 10.8.3.3
!
!
license udi pid CSR1000V sn 9YRYPG7XNOA
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

-------------------------------------------------------------
Example: Configuring Performance Routing Version 3
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, on page 91
- Prerequisites for PfRv3 Transit Site Support, on page 92
- Restrictions for PfRv3 Transit Site Support, on page 92
- Information About PfRv3 Transit Site Support, on page 92
- How to Configure Transit Site Support, on page 95
- Configuration Examples for PfRv3 Transit Site Support, on page 105

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

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

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.
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.

**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.
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.
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.
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface loopback interface-number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> domain {domain-name</td>
<td>default}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>6</td>
<td>vrf {vrf-name</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain) # vrf default</td>
</tr>
<tr>
<td>7</td>
<td>master transit  pop-id</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain-vrf) # master transit 1</td>
</tr>
<tr>
<td>8</td>
<td>source-interface loopback interface-number</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain-vrf-mc) # source-interface Loopback0</td>
</tr>
<tr>
<td>9</td>
<td>site-prefixes prefix-list site-list</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain-vrf-mc) # site-prefixes prefix-list Data_Center_1</td>
</tr>
<tr>
<td>10</td>
<td>hub ip-address</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain-vrf-mc) # hub 10.8.3.3</td>
</tr>
<tr>
<td>11</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-domain-vrf-mc) # exit</td>
</tr>
<tr>
<td>12</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config) # end</td>
</tr>
<tr>
<td>13</td>
<td>(Optional) show domain  domain-name  master status</td>
</tr>
</tbody>
</table>
Configuring Transit Site Border Routers

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface loopback  <em>interface-number</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address  <em>ip-address-mask</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# ip address 10.9.4.4 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>domain  {*domain-name</td>
<td>default*}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# domain default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>vrf  {*vrf-name</td>
<td>default*}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-domain)# vrf default</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can configure specific VRF definition for the hub-border configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>border</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-domain-vrf)# border</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>source-interface loopback  <em>interface-number</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-domain-vrf-br)# source-interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>master  <em>ip-address</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-domain-vrf-br)# master 10.9.3.3</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configures Virtual Routing and Forwarding (VRF) for the default domain.</td>
<td></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Configures the IP address of the hub-master controller.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> exit</td>
<td>Exits border configuration mode and enters VRF configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf-br)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exits VRF configuration mode and enters domain configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-domain-vrf)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> exit</td>
<td>Exits domain configuration mode and enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-domain)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> interface <strong>tunnel-name</strong></td>
<td>Enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Tunnel100</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> ip address <strong>ip-address</strong> <strong>mask</strong></td>
<td>Configures an IP address for the tunnel interface.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip address 10.0.100.84 255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> description <strong>description-line</strong></td>
<td>Configures a description to associate with an ISP path.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device1(config-if)# description primary path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device2(config-if)# description secondary path</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Step 17** domain **domain-name** **path-name** **path-id** **path-id** | 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. We recommend using front VRF on the tunnel interface for enterprise links.  
**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.  
You must assign a unique path-id for all the paths that are connected from hub-border routers to the same ISP domain. |
<p>| Example:                          |                                                                         |
| Device(config-if)# domain default path MPLS path-id 1 |                                                                         |
| <strong>Step 18</strong> end                  | Exits interface configuration mode and returns to privileged EXEC mode.  |
| Example:                          |                                                                         |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-if)# end</td>
<td>---------</td>
</tr>
</tbody>
</table>

**Step 19**

(Optional) show domain  *domain-name*  border status

**Example:**

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
### 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

<table>
<thead>
<tr>
<th>Border Smart Probe Stats:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart probe parameters:</td>
<td></td>
</tr>
<tr>
<td>Source address used in the Probe: 10.2.10.10</td>
<td></td>
</tr>
<tr>
<td>Unreach time: 1000 ms</td>
<td></td>
</tr>
<tr>
<td>Probe source port: 18000</td>
<td></td>
</tr>
<tr>
<td>Probe destination port: 19000</td>
<td></td>
</tr>
<tr>
<td>Interface Discovery: ON</td>
<td></td>
</tr>
<tr>
<td>Probe freq for channels with traffic :10 secs</td>
<td></td>
</tr>
<tr>
<td>Discovery Probes: OFF</td>
<td></td>
</tr>
<tr>
<td>Number of transit probes consumed :29</td>
<td></td>
</tr>
<tr>
<td>Number of transit probes re-routed: 0</td>
<td></td>
</tr>
<tr>
<td>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]</td>
<td></td>
</tr>
<tr>
<td>All the other DSCPs use the default interval: 10 secs</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.10.10</td>
<td>10.1.10.0/24</td>
<td>01:25:15 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.1.11.0/24</td>
<td>01:25:19 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.2.10.10</td>
<td>10.2.10.10/32</td>
<td>01:25:15 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.2.11.11/32</td>
<td>01:25:19 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.2.12.12</td>
<td>10.2.12.12/32</td>
<td>01:28:54 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.3.3/32</td>
<td>01:28:47 ago</td>
<td>0x01</td>
<td>S</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.8.0.0/16</td>
<td>01:28:47 ago</td>
<td>0x05</td>
<td>C,M</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.0.0/16</td>
<td>01:28:47 ago</td>
<td>0x05</td>
<td>C,M</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.9.3.3/32</td>
<td>03:29:04 ago</td>
<td>0x04</td>
<td>L</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.9.0.0/16</td>
<td>01:28:47 ago</td>
<td>0x05</td>
<td>C,M</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.9.0.0/16</td>
<td>01:28:47 ago</td>
<td>0x05</td>
<td>C,M</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>*10.0.0.0/8</td>
<td>01:28:47 ago</td>
<td>0x01</td>
<td>S,T</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.10.10</td>
<td>10.1.10.0/24</td>
<td>00:36:58 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.1.11.0/24</td>
<td>00:37:02 ago</td>
<td>0x00</td>
<td>S</td>
</tr>
</tbody>
</table>
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.

Example:
BN# 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
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.
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)# 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)# 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
Example: Configuring Transit Site Support

Configure tunnel from BR84 to DMVPN2 (INET)

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
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 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 authenticity 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
Configure the interfaces (R11)

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)# 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 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%
Example: Configuring Transit Site Support

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

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

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[0][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: 06:38:15
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

<table>
<thead>
<tr>
<th>Site-id</th>
<th>Site-prefix</th>
<th>Last Updated</th>
<th>DC Bitmap</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.10.10</td>
<td>10.1.10.0/24</td>
<td>00:36:58 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.1.11.0/24</td>
<td>00:37:02 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.2.10.10</td>
<td>10.2.10.10/32</td>
<td>00:36:58 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.2.11.11</td>
<td>10.2.11.11/32</td>
<td>00:37:02 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.2.12.12</td>
<td>10.2.12.12/32</td>
<td>00:40:37 ago</td>
<td>0x0</td>
<td>S</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.8.3.3/32</td>
<td>00:40:29 ago</td>
<td>0x1</td>
<td>S</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.8.0.0/16</td>
<td>00:38:40 ago</td>
<td>0x5</td>
<td>S</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.8.0.0/16</td>
<td>00:38:40 ago</td>
<td>0x5</td>
<td>S,C,M</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.9.3.3/32</td>
<td>00:38:40 ago</td>
<td>0x4</td>
<td>S</td>
</tr>
<tr>
<td>10.9.3.3</td>
<td>10.9.0.0/16</td>
<td>00:38:40 ago</td>
<td>0x5</td>
<td>S,C,M</td>
</tr>
<tr>
<td>10.8.3.3</td>
<td>10.9.0.0/16</td>
<td>00:38:40 ago</td>
<td>0x5</td>
<td>S,C,M</td>
</tr>
</tbody>
</table>
Example: Configuring Transit Site Support

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
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
Inmitigable 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 master channels dst-site-id 10.8.3.3
---------------------------------------------------------------------------------------------

Tue Mar 24 04:52:50.379
**** Border Status ****

Performance Routing v3 Configuration Guide, Cisco IOS Release 15M&T
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
[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
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, on page 123
- Restrictions for PfRv3 Path of Last Resort, on page 123
- Information About PfRv3 Path of Last Resort, on page 124
- How to Configure PfRv3 Path of Last Resort, on page 124

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Path of Last Resort</td>
<td>15.5(3)M</td>
<td>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. The following commands were modified or added by this feature: domain path isp-name, show domain default vrf border, show domain default vrf master.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>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.</td>
</tr>
<tr>
<td>domain default</td>
<td></td>
</tr>
<tr>
<td>vrf default</td>
<td></td>
</tr>
<tr>
<td>master hub</td>
<td></td>
</tr>
<tr>
<td>class foo seq 1</td>
<td></td>
</tr>
<tr>
<td>match dscp ef policy voice</td>
<td></td>
</tr>
<tr>
<td>path-preference ISP1 fallback ISP2 path-last-resort ISP4</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface tunnel  tunnel-number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface tunnel 100</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>domain path  isp-name [internet-bound</td>
<td>path-id</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# domain path ISP1 path-last-resort</td>
<td>• internet-bound—Configures an internet bound interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• path-id—Configures service provider's path-id for the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• path-last-resort—Configures the interface to be a path of a last resort.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• zero-sla—Configures Zero SLA for the interface.</td>
</tr>
</tbody>
</table>

**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:** 10.204.1.3
  - **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] pfrr-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
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
PFRv3 Probe Reduction

This document provides information about the PFRv3 Probe Reduction feature that allows reducing traffic probe on channels that do not carry any traffic.

- Feature Information for PFRv3 Probe Reduction, on page 129
- Prerequisites for PFRv3 Probe Reduction, on page 129
- Information About PFRv3 Probe Reduction, on page 129
- How to Configure PFRv3 Probe Reduction, on page 130
- Configuration Examples for PFRv3 Probe Reduction, on page 132
- Additional References for PFRv3 Probe Reduction, on page 132

Feature Information for PFRv3 Probe Reduction

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFRv3 Probe Reduction</td>
<td>15.6(3)M</td>
<td>This document provides information about the PFRv3 Probe Reduction feature that allows reducing traffic probe on channels that do not carry any traffic. The following command was introduced: <code>smart-probes burst</code></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> domain default</td>
<td>Enters domain configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# domain default</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the device as a master hub and enters master controller configuration mode.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td>Configures the device as the border and enters border configuration mode.</td>
</tr>
<tr>
<td>• master hub</td>
<td><strong>Note</strong> If you select border configuration, it overwrites the master configuration.</td>
</tr>
<tr>
<td>• border</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-domain)# master hub</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-domain)# border</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 5** | Enters advanced configuration mode. |
| advanced | |
| **Example:** | |
| Device(config-domain-mc)# advanced | |
| **Example:** | |
| Device(config-domain-br)# advanced | |

| **Step 6** | Specifies the number of packets to be sent in a probe burst and the interval between the bursts. The default values are as follows: |
| smart-probes burst [quick] number-of-packets packets every interval seconds | • 1 packet every 1 second for default monitor |
| **Example:** | • 20 packets every 1 second for quick monitor |
| Device(config-domain-mc-advanced)# smart-probe burst 10 packets every 20 seconds | |
| **Example:** | |
| Device(config-domain-br-advanced)# smart-probe burst quick 10 packets every 1 seconds | |

## Verifying PfRv3 Probe Reduction

### SUMMARY STEPS

1. `show domain {default | domain-name} [vrf vrf-name] {master | border} status`

### DETAILED STEPS

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

```plaintext
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Performance Routing Version 3 commands</td>
<td>Cisco IOS Performance Routing Version 3 Command Reference</td>
</tr>
</tbody>
</table>
CHAPTER 7

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, on page 133
- Information About PfRv3 Remote Prefix Tracking, on page 134
- How to Display Site Prefixes, on page 138
- Additional References for PfRv3 Remote Prefix Tracking, on page 143

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 16: Feature Information for PfRv3 Remote Prefix Tracking

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Remote Prefix Tracking</td>
<td>Cisco IOS release 3.16.6,</td>
<td>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. The following command was modified: show domain default vrf.</td>
</tr>
<tr>
<td></td>
<td>15.6M2, 15.5.3M6, 15.7M,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16.3.5, and Cisco IOS XE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Everest 16.6.1.</td>
<td></td>
</tr>
</tbody>
</table>
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.
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.
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.
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

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
<th>In-RIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
<tr>
<td>C</td>
<td>10.20.0.0/24</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
<tr>
<td>L</td>
<td>10.20.1.1/32</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td>YES</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td>YES</td>
</tr>
<tr>
<td>D</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
<tr>
<td>D</td>
<td>10.20.1.0/16</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
<td>YES</td>
</tr>
<tr>
<td>D</td>
<td>51.1.0.0/16</td>
<td>Local</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
<tr>
<td>C</td>
<td>52.1.0.0/16</td>
<td>Local</td>
<td>10.20.0.2</td>
<td>22</td>
<td>Loopback1</td>
<td>YES</td>
</tr>
<tr>
<td>D</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>22</td>
<td>Loopback1</td>
<td>YES</td>
</tr>
<tr>
<td>S</td>
<td>100.20.2.1/32</td>
<td>Local</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
<tr>
<td>S</td>
<td>100.20.3.1/32</td>
<td>Local</td>
<td>10.20.0.3</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td>YES</td>
</tr>
</tbody>
</table>

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 vrf name green border route-import interface Loopback1
```

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
<th>In-RIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>22</td>
<td>Loopback1</td>
<td>YES</td>
</tr>
</tbody>
</table>

Step 4  show monitor event-trace pfvr3 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, I - 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

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>10.10.1.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.10.3.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.10.2.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.10.4.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.10.5.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.0.0/24</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.0.0/24</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>B</td>
<td>10.20.1.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>D</td>
<td>10.20.2.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.0.1</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>L</td>
<td>10.20.2.1/32</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>C</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>B</td>
<td>10.30.1.0/24</td>
<td>Remote</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.30.2.0/24</td>
<td>Local</td>
<td>10.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.0.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>C</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>22</td>
<td>Loopback1</td>
</tr>
<tr>
<td>D</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>10.20.0.1</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>100.20.2.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>100.20.2.1/32</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>23</td>
<td>Loopback1</td>
</tr>
<tr>
<td>S</td>
<td>100.20.3.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.3</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.0.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.2.0/24</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>C</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>22</td>
<td>Loopback1</td>
</tr>
<tr>
<td>D</td>
<td>100.20.1.1/32</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>10.20.0.1</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>100.20.2.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>100.20.2.1/32</td>
<td>Local</td>
<td>100.20.2.1</td>
<td>0.0.0.0</td>
<td>23</td>
<td>Loopback1</td>
</tr>
<tr>
<td>S</td>
<td>100.20.3.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.3</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
</tbody>
</table>
### IF-Rule In-RIB

<table>
<thead>
<tr>
<th>IF-Rule</th>
<th>Role</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>L</td>
<td>51.1.0.4/32</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
<tr>
<td>C</td>
<td>51.1.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
<tr>
<td>D</td>
<td>52.1.0.0/16</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>52.1.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>51.1.0.3</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
<tr>
<td>B</td>
<td>10.10.1.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.10.3.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.15.1.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>B</td>
<td>10.30.1.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>D</td>
<td>100.10.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>100.10.0.0/16</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>51.1.0.3</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
</tbody>
</table>

B1MCR# 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, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default, U - per-user static route, O - OSSF external type 1, O2 - OSPF external type 2, i - 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, D - replicated route, % - next hop override, P - overrides from PfR

### Enterprise Prefix List:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.20.0.0</td>
<td>16</td>
</tr>
<tr>
<td>100.30.0.0</td>
<td>16</td>
</tr>
<tr>
<td>100.0.0.0</td>
<td>8</td>
</tr>
</tbody>
</table>

### Proto Prefix Location BR-IP Next-Hop Index Interface

<table>
<thead>
<tr>
<th>Proto</th>
<th>Prefix</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>10.20.0.1/32</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Local</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.1.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>C</td>
<td>10.20.1.0/24</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
</tr>
<tr>
<td>D</td>
<td>51.1.0.4/32</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>C</td>
<td>51.1.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
<tr>
<td>D</td>
<td>52.1.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>D</td>
<td>52.1.0.0/16</td>
<td>Remote</td>
<td>100.20.1.1</td>
<td>51.1.0.3</td>
<td>24</td>
<td>Tunnel10</td>
</tr>
</tbody>
</table>
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

Step 3  
show domain default vrf vrf-name master local-prefix

Use this command to view the prefix information associated with a 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List All Releases</td>
</tr>
<tr>
<td>PfRv3 commands</td>
<td>Cisco IOS Performance Routing Version 3 Command Reference</td>
</tr>
<tr>
<td>Site Prefix Splitting</td>
<td>Site Prefix Splitting</td>
</tr>
</tbody>
</table>