# CONTENTS

## CHAPTER 1

**Read Me First** 1

## CHAPTER 2

**About this Guide** 3

- **Audience** 3
- **Document Organization** 3
- **Document Conventions** 4
- **New and Changed Information** 5
- **Additional References for PfRv3** 6

## CHAPTER 3

**Performance Routing Version 3** 9

- **Performance Routing Version 3** 9
- **Feature Information for PfRv3** 9
- **Hardware and Software Support** 10
- **Restrictions for Configuring Performance Routing v3** 10
- **Information About PfRv3** 11
  - **Performance Routing v3 Overview** 11
  - **Benefits of PfRv3** 11
  - **PfRv3 Design Overview** 12
  - **PfRv3 Configuration Components** 13
  - **Device Setup and Role** 13
  - **Domain Policies** 14
  - **PfRv3 and Link Group Configuration** 15
- **Configuring Performance Routing Version 3** 15
  - **Configuring PfRv3** 15
  - **Configuring Hub Master Controller** 15
  - **Configuring Hub Border Router** 18
Contents

CHAPTER 9 PfRv3 Intelligent Load Balance 155
Feature Information for PfRv3 Intelligent Load Balance 155
Prerequisites for PfRv3 Intelligent Load Balance 156
Restrictions for PfRv3 Intelligent Load Balance 156
Information About PfRv3 Intelligent Load Balance 156
How to Configure PfRv3 Intelligent Load Balance 156
Configuring PfRv3 Intelligent Load Balance 156
Verifying PfRv3 Intelligent Load Balance 158
Example: Configuring PfRv3 Intelligent Load Balance 158
Example: Verifying PfRv3 Intelligent Load Balance 158
Additional References for PfRv3 Intelligent Load Balance 158

CHAPTER 10 Path Preference Hierarchy 161
Feature Information for Path Preference Hierarchy 161
Information About Path Preference Hierarchy 161
Overview of Path Preference Hierarchy 161
How to Configure Path Preference Hierarchy 162
Configuring Path Preference Hierarchy 162
Additional References for Path Preference Hierarchy 163

CHAPTER 11 PfRv3 Remote Prefix Tracking 165
Feature Information for PfRv3 Remote Prefix Tracking 165
Information About PfRv3 Remote Prefix Tracking 166
Site Prefixes Database 166
Learning Local Site Prefixes 166
Learning Remote Site Prefixes 167
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter Optimization</td>
<td>184</td>
</tr>
<tr>
<td>DCI Path Options</td>
<td>186</td>
</tr>
<tr>
<td>How to Configure PfRv3-Inter-DC-Optimization</td>
<td>186</td>
</tr>
<tr>
<td>Specifying the DCI interface on a Hub Site</td>
<td>186</td>
</tr>
<tr>
<td>Configuring Inter-DC on Hub Master Controller</td>
<td>186</td>
</tr>
<tr>
<td>Configuring Inter-DC on Transit Hub</td>
<td>187</td>
</tr>
<tr>
<td>Specifying IDC Local Policy</td>
<td>187</td>
</tr>
<tr>
<td>Verifying Inter-DC Configuration</td>
<td>187</td>
</tr>
<tr>
<td>Verifying Master Controller Configuration</td>
<td>188</td>
</tr>
<tr>
<td>Verifying the Channel Status</td>
<td>188</td>
</tr>
<tr>
<td>Example Configurations for PfRv3 Inter-DC</td>
<td>189</td>
</tr>
<tr>
<td>Additional References for PfRv3-Inter-DC-Optimization</td>
<td>190</td>
</tr>
<tr>
<td><strong>CHAPTER 14</strong></td>
<td></td>
</tr>
<tr>
<td>Direct Cloud Access</td>
<td>191</td>
</tr>
<tr>
<td>Feature Information for Configuring Direct Cloud Access</td>
<td>191</td>
</tr>
<tr>
<td>Prerequisites for Configuring Direct Cloud Access</td>
<td>192</td>
</tr>
<tr>
<td>Restrictions for Configuring Direct Cloud Access</td>
<td>192</td>
</tr>
<tr>
<td>Information About Configuring Direct Cloud Access</td>
<td>193</td>
</tr>
<tr>
<td>Direct Cloud Access Overview</td>
<td>193</td>
</tr>
<tr>
<td>Benefits of Direct Cloud Access</td>
<td>193</td>
</tr>
<tr>
<td>Direct Cloud Access Architecture</td>
<td>193</td>
</tr>
<tr>
<td>Designate an Underlay Interface as Direct Access Interface</td>
<td>194</td>
</tr>
<tr>
<td>Direct Cloud Access Components</td>
<td>195</td>
</tr>
<tr>
<td>Cisco Umbrella Connector</td>
<td>195</td>
</tr>
<tr>
<td>NBAR Classification</td>
<td>195</td>
</tr>
<tr>
<td>Performance Routing Version 3</td>
<td>195</td>
</tr>
<tr>
<td>IPSLA</td>
<td>195</td>
</tr>
<tr>
<td>SaaS Reachability and Performance Management</td>
<td>196</td>
</tr>
<tr>
<td>Next-Hop Reachability</td>
<td>196</td>
</tr>
<tr>
<td>Performance Measurement</td>
<td>196</td>
</tr>
<tr>
<td>Application Domain Mapping</td>
<td>196</td>
</tr>
<tr>
<td>Reachability and Performance Probing</td>
<td>196</td>
</tr>
<tr>
<td>Traffic Steering and Flow Stickiness</td>
<td>196</td>
</tr>
<tr>
<td>Local Policy Configuration</td>
<td>196</td>
</tr>
</tbody>
</table>
How to Configure Direct Cloud Access 197
Assign an Underlay Interface as Direct Access Interface 197
Define PfR Policy for SaaS Application on Hub Master Controller 197
Define SaaS Application Mapping on Branch Master Controller 197
Configure a DNS Resolver 198
Configure the HTTP Ping Probe Interval 198
Verify and Monitor Direct Cloud Access Configuration 199
Configuration Examples for Configuring Direct Cloud Access 200
Example: Configure DCA Link on a Single Branch Router 200
Example: Configure DCA Link on a Dual Branch Router 206
Example: Configuring Umbrella Branch for OpenDNS 208
Additional References for Configuring Direct Cloud Access 210

CHAPTER 15
Channel-based Metrics Measurement 211
Feature Information for Channel-based Metrics 211
Prerequisites for Channel-based Metrics Measurement 211
Information About Channel-based Metrics Measurement 212
   Overview 212
How to Configure Channel-based Metrics Measurement 212
   Channel-based Metrics Measurement Configuration 212
Configuration Examples 213
   Examples: Channel-based Metrics Measurement 213
Additional References 213
   References 213

CHAPTER 16
PfRv3 Event Tracing 215
Prerequisites for PfRv3 Event Tracing 215
Restrictions for PfRv3 Event Tracing 215
Information About PfRv3 Event Tracing 215
   PfRv3 Event Tracing Options 215
   Benefits of PfRv3 Event Tracing 216
How to Display PfRv3 Event Tracing 216
Additional References for PfRv3 Event Tracing 234
Feature Information for PfRv3 Event Tracing 235
Read Me First

Important Information about Cisco IOS XE 16

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

Feature Information

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

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.
CHAPTER 2

About this Guide

- Audience, on page 3
- Document Organization, on page 3
- Document Conventions, on page 4
- New and Changed Information, on page 5
- Additional References for PfRv3, on page 6

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

## 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. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</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><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>Courier font</strong>.</td>
</tr>
<tr>
<td><strong>Bold Courier font</strong></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 syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string 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>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**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></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.13S</td>
<td></td>
<td></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></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></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.15S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel-based Measurement of performance metrics</td>
<td>IOS XE Gibraltar 16.11</td>
<td>Configures the performance monitors used by PfRv3 to employ a data collection method which is typically more accurate, sampling traffic at intervals and using metadata together to provide traffic metrics.</td>
<td></td>
</tr>
</tbody>
</table>

**Additional References for PfRv3**

<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>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> <a href="http://www.cisco.com/support">http://www.cisco.com/support</a></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

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></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: domain default, vrf default, master, source-interface, site-prefixes, password, monitor-interval, route-control, load-balance, enterprise-prefix, advanced, minimum-mask-length, mitigation-mode, threshold-variance, smart-probes, collector, class, match, priority, path-preference, border, domain-path.</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>
<tr>
<td></td>
<td>Cisco IOS 15.4(3)M1 or later</td>
<td></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).

---

**Note**

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

---

**Note**

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

---

**Information About PfRv3**

**Performance Routing v3 Overview**

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

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

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

**Benefits of PfRv3**

Performance Routing Version 3 provides the following benefits:

- Centralized provisioning — Policies are defined on the hub-master controller and then distributed to all branches. Hence, per-site provisioning is not required in PfRv3.
• Simple provisioning — PfRv3 has simplified policies with pre-existing templates that a user can choose from.

• Enterprise domain — All sites belong to an enterprise domain and are connected with peering.

• Application and DSCP-based policies — Policies are provisioned based on applications. PfRv3 provides application visibility such as bandwidth, performance, and correlation to Quality of Service (QoS) queues by using Unified Monitoring.

• Automatic discovery — PfRv3 site are discovered using peering. Each site peers with the hub site. The WAN interfaces are automatically discovered on the branch sites.

• Scalable passive monitoring — PfRv3 uses Unified Monitor to monitor traffic going into WAN links and traffic coming from the WAN links. It monitors performance metrics based on per DSCP instead of per flow or per prefix basis.

• Smart probing — PfRv3 uses probing mechanism that generates traffic only when there 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>
<tbody>
<tr>
<td><strong>Voice</strong></td>
<td>Priority 1 one-way-delay threshold 150 threshold 150 (msec)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 packet-loss-rate threshold 1 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 byte-loss-rate threshold 1 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 3 jitter 30 (msec)</td>
</tr>
<tr>
<td><strong>Real-time-video</strong></td>
<td>Priority 1 packet-loss-rate threshold 1 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 1 byte-loss-rate threshold 1 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 one-way-delay threshold 150 (msec)</td>
</tr>
<tr>
<td></td>
<td>Priority 3 jitter 20 (msec)</td>
</tr>
<tr>
<td><strong>Low-latency-data</strong></td>
<td>Priority 1 one-way-delay threshold 100 (msec))</td>
</tr>
<tr>
<td></td>
<td>Priority 2 byte-loss-rate threshold 5 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 packet-loss-rate threshold 5 (%)</td>
</tr>
<tr>
<td><strong>Bulk-data</strong></td>
<td>Priority 1 one-way-delay threshold 300 (msec)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 byte-loss-rate threshold 5 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 packet-loss-rate threshold 5 (%)</td>
</tr>
<tr>
<td><strong>Best-effort</strong></td>
<td>Priority 1 one-way-delay threshold 500 (msec)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 byte-loss-rate threshold 10 (%)</td>
</tr>
<tr>
<td></td>
<td>Priority 2 packet-loss-rate threshold 10 (%)</td>
</tr>
<tr>
<td><strong>Scavenger</strong></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><strong>Custom</strong></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.

**Configuring Performance Routing Version 3**

**Configuring PfRv3**

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

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

![Figure 2: PfRv3 Workflow](image)

**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 \textit{interface-number}
4. ip address \textit{ip-address-mask}
5. exit
6. domain \{\textit{domain-name} | default\}
7. vrf \{\textit{vrf-name} | default\}
8. master \{\textit{hub} | branch | transit\}
9. source-interface loopback \textit{interface-number}
10. enterprise-prefix prefix-list \textit{site-list}
11. site-prefixes prefix-list \textit{site-list}
12. exit
13. ip prefix-list \textit{ip-list} seq \textit{sequence-number} permit \textit{ip-prefix-network} le \textit{le-length}
14. end
15. (Optional) show domain \textit{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>- 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> interface loopback \textit{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> ip address \textit{ip-address-mask}</td>
<td>Configures an IP address for an interface on the hub-master controller.</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip address 10.8.3.3 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# exit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>domain {domain-name</td>
<td>default}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# domain default</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vrf {vrf-name</td>
<td>default}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-domain)# vrf default</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>master {hub</td>
<td>branch</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf)# master hub</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>source-interface loopback interface-number</td>
<td>Configures the loopback used as a source for peering with other sites or master controller.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# source-interface Loopback0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enterprise-prefix prefix-list site-list</td>
<td>Configures an enterprise prefix-list with static site targets.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>site-prefixes prefix-list site-list</td>
<td>Configures the prefix-list containing list of site prefixes.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-domain-vrf-mc)# site-prefixes prefix-list Data_Center_1</td>
<td></td>
</tr>
</tbody>
</table>

| Note | You can either configure a default domain or define a specific domain for the master controller configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration. |

| Note | You can configure specific VRF definition also for the hub-master controller configuration. |

| Note | The source-interface loopback also serves as a site ID of a particular site (hub or branch) on the master controller. |

| Note | The `enterprise-prefix prefix-list` command defines the boundary for all the internal enterprise prefixes. A prefix that is not from the prefix-list is considered as internet prefix and is routed over internet-bound links. |

| Note | The `site-prefix prefix-list` defines static site-prefix for the local site and disables automatic site-prefix learning on the border router. The static-site prefix list is only required for hub and transit sites. |
**Command or Action**

<table>
<thead>
<tr>
<th>Step 12</th>
<th><code>exit</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>device(config-domain-vrf-mc)# exit</code></td>
<td>Exits from master controller configuration mode and returns to domain configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th><code>ip prefix-list ip-list seq sequence-number permit ip-prefix-network le le-length</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>device(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24</code>&lt;br&gt;<code>device(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24</code></td>
<td>Configures the IP prefix list to filter traffic based on the IP network defined in the configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th><code>end</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>device(config)# end</code></td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>(Optional) <code>show domain domain-name master status</code></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>device# show domain one master status</code></td>
<td>Use this show command to display the status of a master controller.</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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
|  | Example: Device> enable | • Enter your password if prompted. |
| 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 | |
| Step 5 | exit | Exits interface configuration mode and returns to global configuration mode. |
|  | Example: | |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>`domain {domain-name</td>
<td>default}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# domain one</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>`vrf {vrf-name</td>
<td>default}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain)# vrf default</td>
<td><strong>Note</strong> You can also configure specific VRF definition for hub-border configuration.</td>
</tr>
<tr>
<td>8</td>
<td><code>border</code></td>
<td>Enters border configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain-vrf)# border</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>source-interface loopback interface-number</code></td>
<td>Configures the loopback used as a source for peering with other sites or master controller.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain-vrf-br)# source-interface Loopback0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>`master [ip-address</td>
<td>local]`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain-vrf-br)# master 10.8.3.3</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>exit</code></td>
<td>Exits border configuration mode and enters VRF configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain-vrf-br)# exit</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>exit</code></td>
<td>Exits VRF configuration mode and enters domain configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain-vrf)# exit</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><code>exit</code></td>
<td>Exits domain configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-domain)# exit</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>interface tunnel-name</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# interface Tunnel100</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>ip address ip-address mask</code></td>
<td>Configures an IP address for the tunnel interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# ip address 10.0.100.84 255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
**Step 16** |  |
| **domain domain-name path path-name** | 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.

We recommend using front VRF on the tunnel interface for enterprise links over internet ISP 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.

**Example:**

Device(config-if)# domain one path MPLS

**Step 17** |  |
| **end** | Exits interface configuration mode and returns to privileged EXEC mode.

**Example:**

Device(config-if)# end

**Step 18** |  |
| *(Optional)* **show domain domain-name border status** | 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]**
### Configuring Domain Policies

#### Commands and Actions

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>monitor-interval seconds dscp ef</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>load-balance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>class class-name sequence sequence-number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>match {application</td>
<td>dscp} services-value policy</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>path-preference path-name fallback path-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>priority priority-number [jitter</td>
<td>loss</td>
<td>one-way-delay] threshold threshold-value</td>
</tr>
<tr>
<td>10.</td>
<td>end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>domain {domain-name</td>
<td>default}</td>
<td>Enters domain configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# domain default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>vrf {vrf-name</td>
<td>default}</td>
<td>Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain)# vrf default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>master [hub</td>
<td>branch</td>
<td>transit]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf)# master hub</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>monitor-interval seconds dscp ef</td>
<td>Configures interval time that defines monitoring interval on ingress monitors.</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf-mc)# monitor-interval 2 dscp ef</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>load-balance</td>
<td>Configures load balancing.</td>
<td>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.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
<td>Note</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 6</td>
<td>class class-name sequence sequence-number</td>
<td>Enters policy class configuration mode.</td>
<td>Class-name value must be in all capitals.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-domain-vrf-mc)# class VOICE sequence 10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Step 7 | match {application | dscp} services-value policy                                        | Configures policy on per DSCP basis. You can select a DSCP value from 0 to 63. You can select the following policy types: | - best-effort  
- bulk-data  
- custom  
- low-latency-data  
- real-time-video  
- scavenger  
- voice |
| Example: | Device(config-domain-vrf-mc-class)# match dscp ef policy voice                    | In this example, the domain policy type is configured for voice.                            |                                                                      |
| Step 8 | path-preference path-name fallback path-name                                       | Configures the path preference for applications.                                           | 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. |
| Example: | Device(config-domain-vrf-mc-class)# path-preference MPLS fallback INET           |                                                                                            |                                                                      |
| Step 9 | priority priority-number [jitter | loss | one-way-delay] threshold threshold-value                                           | Enters class type configuration mode. Configures the user-defined threshold value for loss, jitter, and one-way-delay for the policy type. Threshold values are defined in usec. | You can configure class type priorities only for a custom policy. You can configure multiple priorities for custom policies. |
| Example: | Device(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10             |                                                                                            |                                                                      |
|                             | Device(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600 |                                                                                            |                                                                      |
|                             | Device(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 200         |                                                                                            |                                                                      |
| Step 10 | end                                                                               | Exits configuration mode and returns to privileged EXEC mode.                              |                                                                      |

Example:  
Device(config)# end
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>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> ip address ip-address-mask</td>
<td>Configures an IP address for an interface on the branch-master controller.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Device(config-if)# ip address 10.2.10.10 255.255.255</code></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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`domain {domain-name</td>
<td>default}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# domain default</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`vrf {vrf-name</td>
<td>default}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-domain)# vrf default</code></td>
<td><strong>Note</strong> You can also configure specific VRF definition for the branch-border configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>border</code></td>
<td>Enters border configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-domain-vrf)# border</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>source-interface loopback interface-number</code></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><code> </code></td>
<td></td>
</tr>
</tbody>
</table>
### 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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</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 branch master controller.

**Example:**

```
Device(config-if)# ip address 10.2.12.12 255.255.255.255
```

**Step 5**

```
exit
```

Exits interface configuration mode and returns to global configuration mode.

**Example:**

```
Device(config-if)# exit
```

**Step 6**

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

Enters domain configuration mode.

**Example:**

```
Device(config)# domain default
```

**Step 7**

```
vrf {vrf-name | default}
```

Configures Virtual Routing and Forwarding (VRF) for the default domain.

**Example:**

```
Device(config-domain)# vrf default
```

**Step 8**

```
border
```

Enters border configuration mode.

**Example:**

```
Device(config-domain-vrf)# border
```

**Step 9**

```
source-interface loopback  interface-number
```

Configures the loopback used as a source for peering with other sites or master controller.

**Example:**

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

**Step 10**

```
master local
```

Configures the local IP address of the device as branch-master controller.

**Example:**

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

Command or Action | Purpose
--- | ---
**Step 11** | master branch
**Example:**
Device(config-domain-vrf-mc)# master branch

**Step 12** | source-interface loopback *interface-number*
**Example:**
Device(config-domain-vrf-mc)# source-interface Loopback0

**Step 13** | hub *ip-address*
**Example:**
Device(config-domain-vrf-mc)# hub 10.8.3.3

**Step 14** | end
**Example:**
Device(config-domain-vrf-mc)# end

What to do next

Verifying PfRv3 Configuration

Verifying PfRv3 Configuration

Verifying Hub Master Controller Configurations

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

**Step 1**

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

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

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

- Policy publishing status to remote sites
• Policy threshold per class based on either DSCP or application
• Class default is enabled

Example:

HubMC# show domain one master policy
No Policy publish pending

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

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

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

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

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

Table 3: show domain master policy Field Descriptions

<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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>class</td>
<td>Name of the class type. In this example, the following classes are listed: • VOICE • VIDEO • 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>

**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 Kbps
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 5: show domain master exits Field Descriptions

<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
*** Domain MC Status ***

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

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

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

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

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

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

<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)
```
The fields shown above are self-explanatory.

**Step 6**

`show domain domain-name master discovered-sites`

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

**Example:**

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

*** Domain MC DISCOVERED sites ***

Number of sites: 3

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

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

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

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

The fields shown above are self-explanatory.
Verifying Hub Border Router Configurations

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

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

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

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

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

**Example:**

```
HubBR# show domain one border status

****Border Status****
Instance Status: UP
Present status last updated: 02:07:43 ago
Loopback: Configured Loopback0 UP (10.8.2.2)
Master: 10.8.3.3
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:07:42
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
  Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
  Name: Tunnel200 Interface Index: 154 SNMP Index: 10 SP:INET Status: UP
Auto Tunnel information:
  Name: Tunnel0 if_index: 15
  Borders reachable via this tunnel: 10.8.2.2
```
The following table describes the significant fields shown in the command output.

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

<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
```

---

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

Published service:

---

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

<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 PfRv3 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 Kpbs
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 9: `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 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
```
class type: Dscp Based
   match dscp af41 policy custom
       priority 2 packet-loss-rate threshold 5.0 percent
       priority 1 one-way-delay threshold 150 msec
       priority 2 byte-loss-rate threshold 5.0 percent
   Number of Traffic classes using this policy: 1
match dscp cs4 policy custom
   priority 2 packet-loss-rate threshold 5.0 percent
   priority 1 one-way-delay threshold 150 msec
   priority 2 byte-loss-rate threshold 5.0 percent
   Number of Traffic classes using this policy: 1
class CRITICAL sequence 30
   path-preference MPLS fallback INET
   class type: Dscp Based
      match dscp af31 policy custom
          priority 2 packet-loss-rate threshold 10.0 percent
          priority 1 one-way-delay threshold 600 msec
          priority 2 byte-loss-rate threshold 10.0 percent
      Number of Traffic classes using this policy: 1
class default
   match dscp all
   ----------------------------------------------------------------------------------------------------------------------------------------------------------------

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

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

Auto Tunnel information:
   Name:Tunnel0 if_index: 19
   Borders reachable via this tunnel:
```

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

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

<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>
### Field

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

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

<table>
<thead>
<tr>
<th>EIGRP-SFv4 VR(#AUTOCFG#) Service-Family Neighbors for AS(59501)</th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Cnt</th>
<th>Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 10.8.3.3</td>
<td>Lo0</td>
<td></td>
<td>497 02:12:18</td>
<td>5 100</td>
<td>0</td>
<td>31</td>
<td></td>
<td></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:**

```
BR# show domain one master peering
```

Peering state: Enabled
Origin:     Loopback0(10.2.10.10)
Peering type: Listener, Peer(With 10.8.3.3)
Subscribed service:
  cent-policy (2) :
    Last Notification Info: 00:24:15 ago, Size: 2244, Compressed size: 488, Status: No Error, Count: 5
  site-prefix (1) :
    Last Notification Info: 00:24:15 ago, Size: 128, Compressed size: 134, Status: No Error, Count: 35
  service-provider (4) :
    globals (5) :
      Last Notification Info: 00:24:15 ago, Size: 325, Compressed size: 218, Status: No Error, Count: 19

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

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

Table 12: show domain master peering Field Descriptions

<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-Egress-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
```
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>10.1.10.0/24</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>
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</td>
<td>*10.0.0.0/8</td>
<td>01:30:22 ago</td>
<td>S,T,</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/NA</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/NA</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: 00:00:14 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
```

The fields shown above are self-explanatory.
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>show platform software pfrv3 rp active route-control traffic-class</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show platform software pfrv3 fp active route-control traffic-class</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show platform hardware qfp active feature pfrv3 client route-control traffic-class detail</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show platform software interface rp active name interface-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show platform software interface fp active name interface-name</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
Immitigable 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 Statistics:
  Received:4 ; Processed:1 ; Unreach_rcvd:4
Latest TCA Bucket
  Last Updated : 00:00:01 ago

The fields shown above are self-explanatory.

Step 3 show domain domain-name border channels

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

Example:

HubBR# show domain one border channels

Border Smart Probe Stats:

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

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

Configure the device as hub-master controller

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

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

Example: Configuring Domain Policies on Hub Master Controller

HubMC(config)# domain one
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf)# monitor-interval 2 dscp ef
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 10.0.100.84 255.255.255.255
BR1(config-if)# no ip redirects
BR1(config-if)# ip mtu 1400
Example: Configuring Performance Routing Version 3

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)
Configure the tunnel interface and tunnel path from R10

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

Configure another tunnel path from R10

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

Configure the interfaces (R11)

R11> enable
R11# configure terminal
R11(config)# interface Loopback0
R11(config-if)# ip address 10.2.11.11 255.255.255.255
R11(config-if)# exit
Configure the device as branch master controller (R11)

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

Configure the tunnel interface and tunnel path from R11

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

Configure another tunnel path from R11

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

Example: Configuring Branch Routers (Dual CPE)

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

```plaintext
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

```plaintext
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 nhftp authentication cisco
R12(config-if)# ip nhftp map 10.0.100.84 172.16.84.4
R12(config-if)# ip nhftp map multicast 172.16.84.4
R12(config-if)# ip nhftp network-id 1
R12(config-if)# ip nhftp holdtime 600
R12(config-if)# ip nhftp nhs 10.0.100.84
R12(config-if)# ip nhftp 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)

```plaintext
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)

```plaintext
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

```plaintext
R13(config)# interface Tunnel200
R13(config-if)# bandwidth 50000
```
Example: Configuring Performance Routing Version 3

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: Enabled
  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 Kbps
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
Minimum Mask Length: 28
Sampling: off

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

Tunnel if: Tunnel0

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

Tunnel if: Tunnel0

```
show domain  domain-name  master discovered-sites
```

*** 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
```

****Border Status****

Instance Status: UP
Present status last updated: 02:07:43 ago
Loopback: Configured Loopback0 UP (10.8.2.2)
Master: 10.8.3.3
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:07:42
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
   Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
Auto Tunnel information:
   Name:Tunnel0 if_index: 15
   Borders reachable via this tunnel: 10.8.2.2

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

PfrV3 smart probe parameters :
Total number of PfrV3 smart probe: 1
Parameters :
   vrf id = 0
   Probe src = 10.8.3.3
   Src port = 18000, Dst port = 19000
   Unreach time = 1000, Probe period = 500
   Discovery = false
   Dscp bitmap = 0xffffffffffffffff
   interval = 10000
   Discovery_probe = true
   minimum prefix length = 28

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

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

show domain  domain-name  master policy
HubMC# show domain one master policy
No Policy publish pending

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

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

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

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

show domain  domain-name  border pmi
BR# show domain one border pmi

****Pfrv3 PMI INFORMATION****
Ingress policy Pfrv3-Policy-Ingress-0-4:
Ingress policy activated on:
  Tunnel200 Tunnel100
[SNIP]

Egress policy Pfrv3-Policy-Egress-0-3:
Egress policy activated on:
  Tunnel200 Tunnel100

PMI[Egress-aggregate]-FLOW MONITOR[MON-Egress-aggregate-0-48-1]
  Trigger Nbar:No

PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-2]
  With application based policy:

show ip access-lists dynamic
BR# show ip access-lists dynamic

Extended IP access list mma-dvmc-acl#3
  10 deny ip any 224.0.0.0 15.255.255.255
  20 deny ip any any dscp cs6
30 permit tcp any any
40 permit udp any neq 18000 any neq 19000
50 permit icmp any any

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

HubMC# show domain one master site-prefix

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

<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>10.2.11.11</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</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>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>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>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>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>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>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>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>
</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: CONTROLLED
Current Performance Status: in-policy
Current Service Provider: MPLS since 00:00:30 (hold until 59 sec)
Previous Service Provider: INET for 117 sec
(A fallback provider. Primary provider will be re-evaluated 00:02:30 later)
BW Used: 309 Kbps
Present WAN interface: Tunnel100 in Border 10.8.2.2
Present Channel (primary): 76
Backup Channel: 73
Destination Site ID: 10.2.10.10
Class-Sequence in use: 20
Class Name: VIDEO using policy User-defined
  priority 2 packet-loss-rate threshold 5.0 percent
  priority 1 one-way-delay threshold 150 msec
  priority 2 byte-loss-rate threshold 5.0 percent
BW Updated: 00:00:03 ago
Reason for Route Change: Delay

-----------------------------------------------------------------------------------------------------------------
show running-config

HubMC#  show running-config

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

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
clock timezone CST 8 0
!
!
no ip domain lookup
!
!
subscriber templating
!
multilink bundle-name authenticated
!
domain one
vrf default
master hub
source-interface Loopback0
site-prefixes prefix-list DC1_PREFIX
monitor-interval 2 dscp cs5
monitor-interval 2 dscp ef
load-balance
enterprise-prefix prefix-list ENTERPRISE_PREFIX
class VOICE sequence 10
match dscp ef policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
path-preference MPLS fallback INET
class VIDEO sequence 20
match dscp af41 policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
match dscp cs4 policy custom
priority 2 loss threshold 5
priority 1 one-way-delay threshold 150
path-preference INET fallback MPLS
class CRITICAL sequence 30
match dscp af31 policy custom
priority 2 loss threshold 10
priority 1 one-way-delay threshold 600
path-preference MPLS fallback INET
!
!
license udi pid CSR1000V sn 90KU0SDCWNB
license boot level ax
spanning-tree extend system-id

!
redundancy
mode none
!
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
interface Loopback0
ip address 10.8.3.3 255.255.255.255
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.208 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
no ip address
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet2.100
encapsulation dot1Q 100
ip address 10.8.101.1 255.255.255.0
!
interface GigabitEthernet2.101
encapsulation dot1Q 101
ip address 10.8.102.1 255.255.255.0
!
interface GigabitEthernet2.102
encapsulation dot1Q 102
ip address 10.8.103.1 255.255.255.0
!
interface GigabitEthernet2.103
encapsulation dot1Q 103
ip address 10.8.104.1 255.255.255.0
!
interface GigabitEthernet3
description --INTERNAL--
ip address 10.8.24.2 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet4
description --INTERNAL--
ip address 10.8.25.2 255.255.255.0
speed 1000
no negotiation auto
!
router eigrp 100
network 10.8.3.3 0.0.0.0
network 10.8.24.0 0.0.0.255
network 10.8.25.0 0.0.0.255
redistribute connected
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
!!
ip prefix-list DCL_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
Example: Configuring Performance Routing Version 3

```
!
!
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 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 an 952V3LQECED  
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  
mismatch identity address 0.0.0.0  
!  
crypto ipsec security-association replay disable  
crypto ipsec security-association replay window-size 1024  
!  
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac  
mode transport  
!  
crypto ipsec profile DMVPN-PROFILE1  
set transform-set AES256/SHA/TRANSPORT  
set isakmp-profile ISAKMP-INET1  
!
interface Loopback0
ip address 10.8.1.1 255.255.255.255
!

interface Tunnel100
bandwidth 100000
ip address 10.0.100.84 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 600
ip nhrp redirect
ip tcp adjust-mss 1360
load-interval 30
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel key 100
tunnel protection ipsec profile DMVPN-PROFILE1
domain one path MPLS
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.124.19.210 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description --INTERNAL--
ip address 10.8.24.4 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet3
description --MPLS--
ip address 172.16.84.4 255.255.255.0
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet4
no ip address
load-interval 30
speed 1000
no negotiation auto
!
interface GigabitEthernet5
ip address 101.1.4.1 255.255.255.0
speed 1000
no negotiation auto
!
interface GigabitEthernet6
no ip address
speed 1000
no negotiation auto
!
router eigrp 100
network 10.8.2.2 0.0.0.0
network 10.8.24.0 0.0.0.255
redistribute bgp 10 metric 100000 1 255 255 1500
distance eigrp 90 210

router ospf 100
router-id 10.8.1.1
network 172.16.84.4 0.0.0.0 area 0

router bgp 10
bgp router-id 10.8.1.1
bgp log-neighbor-changes
bgp listen range 10.0.100.0/24 peer-group MPLS-SPOKES
neighbor MPLS-SPOKES peer-group
neighbor MPLS-SPOKES remote-as 10
neighbor MPLS-SPOKES timers 20 60

! address-family ipv4
bgp redistribute-internal
network 10.8.1.1 mask 255.255.255.255
network 10.8.3.3 mask 255.255.255.255
network 10.8.101.0 mask 255.255.255.0
network 10.8.102.0 mask 255.255.255.0
network 10.8.103.0 mask 255.255.255.0
network 10.8.104.0 mask 255.255.255.0
aggregate-address 10.8.0.0 255.255.0.0 summary-only
neighbor MPLS-SPOKES activate
neighbor MPLS-SPOKES send-community
neighbor MPLS-SPOKES default-originate
neighbor MPLS-SPOKES route-map MPLS-DC1-IN in
neighbor MPLS-SPOKES route-map MPLS-DC1-OUT out
distance bgp 20 109 109
exit-address-family

! virtual-service csr_mgmt
! ip forward-protocol nd
! ip bgp-community new-format
ip community-list standard MPLS-DMVPN permit 10:100
ip community-list standard INET-DMVPN permit 10:200
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1

! ip prefix-list DC1-LOCAL-ROUTES seq 10 permit 0.0.0.0/0
ip prefix-list DC1-LOCAL-ROUTES seq 20 permit 10.8.0.0/16 le 32
no service-routing capabilities-manager
!
route-map MPLS-DC1-IN deny 10
match ip address prefix-list DC1-LOCAL-ROUTES
!
route-map MPLS-DC1-IN permit 20
set community 10:100
!
route-map TO-PEER permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set ip next-hop self
set community no-advertise
!
route-map site_prefixes permit 10
match ip address prefix-list site_prefixes
!
route-map MPLS-DC1-OUT permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set community 10:100
!
route-map MPLS-DC1-OUT permit 20
description readvertise routes learned from MPLS DMVPN cloud
match community MPLS-DMVPN
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login
!
ntp source Loopback0
ntp server 10.8.3.3
!
end
------------------------------------------------------------
show running-config

HubBR2# show running-config

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

exit-address-family
!
no logging console
!
no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
![Performance Routing Version 3: Example]
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
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
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
!
!
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
!
routemap INET-DC1-IN deny 10
match ip address prefix-list DC1-LOCAL-ROUTES
!
routemap INET-DC1-IN permit 20
set community 10:200
!
routemap TO-PEER permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set ip next-hop self
set community no-advertise

route-map site_prefixes permit 10
match ip address prefix-list site_prefixes

route-map INET-DC1-OUT permit 10
match ip address prefix-list DC1-LOCAL-ROUTES
set community 10:200

route-map INET-DC1-OUT permit 20
description readvertise routes learned from INTERNET DMVPN cloud
match community INET-DMVPN

control-plane

line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
exec-timeout 0 0
privilege level 15
no login
line vty 5 15
exec-timeout 0 0
privilege level 15
no login

ntp source Loopback0
ntp server 10.8.3.3

end

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

show running-config

BR10# show running-config

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

Building configuration...
Current configuration : 8517 bytes

! Last configuration change at 02:29:54 CST Mon Nov 3 2014

version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial

hostname Branch10

boot-start-marker
boot-end-marker

vrf definition INET2
rd 65512:2

address-family ipv4
exit-address-family
! vrf definition Mgmt-intf
! address-family ipv4 exit-address-family
! no logging console
! no aaa new-model
clock timezone CST 8 0
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

Example: Configuring Performance Routing Version 3
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
!
!
!
!
!
in Loopback0
ip address 10.2.10.10 255.255.255.255
!
in 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 ns 10.0.200.85
  ip nhrp registration timeout 60
  ip tcp adjust-mss 1360
  load-interval 30
  delay 1000
  tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel key 200
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
  ip address 10.124.19.212 255.255.255.0
  negotiation auto
!
interface GigabitEthernet2
description --MPLS--
  ip address 172.16.101.10 255.255.255.0
  speed 1000
  no negotiation auto
!
interface GigabitEthernet3
description --INET--
vrf forwarding INET2
  ip address 172.16.102.10 255.255.255.0
  load-interval 30
  speed 1000
  no negotiation auto
!
interface GigabitEthernet4
no ip address
  speed 1000
  no negotiation auto
!
interface GigabitEthernet5
no ip address
  speed 1000
  no negotiation auto
!
interface GigabitEthernet5.100
  encapsulation dot1Q 100
  ip address 10.1.10.1 255.255.255.0
!
router ospf 200 vrf INET2
network 172.16.102.10 0.0.0.0 area 0
!
router ospf 100
router-id 10.2.10.10
network 101.7.7.2 0.0.0.0 area 0
network 172.16.101.10 0.0.0.0 area 0
!
router bgp 10
bgp router-id 10.2.10.10
bgp log-neighbor-changes
neighbor MPLS-HUB peer-group
neighbor MPLS-HUB remote-as 10
neighbor MPLS-HUB timers 20 60
neighbor INET-HUB peer-group
neighbor INET-HUB remote-as 10
neighbor INET-HUB timers 20 60
neighbor 10.0.100.84 peer-group MPLS-HUB
neighbor 10.0.200.85 peer-group INET-HUB
!
address-family ipv4
network 10.1.10.0 mask 255.255.255.0
network 10.2.10.0 mask 255.255.255.255
neighbor MPLS-HUB send-community
neighbor MPLS-HUB route-map MPLS-SPOKE-IN in
neighbor MPLS-HUB route-map MPLS-SPOKE-OUT out
neighbor INET-HUB send-community
neighbor INET-HUB route-map INET-SPOKE-IN in
neighbor INET-HUB route-map INET-SPOKE-OUT out
neighbor 10.0.100.84 activate
neighbor 10.0.100.84 soft-reconfiguration inbound
neighbor 10.0.200.85 activate
neighbor 10.0.200.85 soft-reconfiguration inbound
exit-address-family
!
virtual-service csr_mgmt
!
ip forward-protocol nd
!
ip bgp-community new-format
!
ip community-list standard MPLS-HUB1 permit 10:100
ip community-list standard MPLS-HUB2 permit 10:101
ip community-list standard INET-HUB1 permit 10:200
ip community-list standard INET-HUB2 permit 10:201
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.124.19.1
!
ip access-list extended RC
permit tcp host 10.1.10.2 any
ip access-list extended SMP
permit udp any eq 18000 any eq 19000
!
ip prefix-list INET-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list INET-DMVPN seq 10 permit 10.8.0.0/16
!
ip prefix-list MPLS-DMVPN seq 5 permit 0.0.0.0/0
ip prefix-list MPLS-DMVPN seq 10 permit 10.8.0.0/16
no service-routing capabilities-manager
!
route-map MPLS-SPOKE-OUT deny 10
match ip address prefix-list INET-DMVPN
!
version 15.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
no platform punt-keepalive disable-kernel-core
platform shell
platform console serial
!
hostname Branch11
!
boot-start-marker
boot-end-marker
!
!
vrf definition INET2
rd 65512:2
!
address-family ipv4
exit-address-family
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
no logging console
!
no aaa new-model
!
clock timezone CST 8 0
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
master branch
source-interface Loopback0
hub 10.8.3.3
!
license udi pid CSR1000V sn 9YRYPG7XWOA
license boot level ax
spanning-tree extend system-id
!
redundancy
mode none
!
!
!
ip ftp source-interface GigabitEthernet1
ip ftp username mgcusr
ip ftp password mgcusr
ip tftp source-interface GigabitEthernet1
!
crypto keyring DMVPN-KEYRING1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring DMVPN-KEYRING2 vrf INET2
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 40 5
crypto isakmp profile ISAKMP-INET1
keyring DMVPN-KEYRING1
match identity address 0.0.0.0
crypto isakmp profile ISAKMP-INET2
keyring DMVPN-KEYRING2
match identity address 0.0.0.0 INET2
!
crypto ipsec security-association idle-time 60
crypto ipsec security-association replay window-size 512
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET1
!
crypto ipsec profile DMVPN-PROFILE2
set transform-set AES256/SHA/TRANSPORT
set isakmp-profile ISAKMP-INET2
!
interface Loopback0
 ip address 10.2.11.11 255.255.255.255
!
interface Tunnel100
 bandwidth 100000
 ip address 10.0.100.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.100.84 172.16.84.4
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nh 10.0.100.84
 ip nhrp registration timeout 60
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source GigabitEthernet3
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE1
!
interface Tunnel200
 bandwidth 50000
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 10.0.200.85 172.16.85.5
 ip nhrp network-id 2
 ip nhrp holdtime 600
 ip nhrp nh 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 10.1.7.8.2 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 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

Performance Routing Version 3

Example: Configuring Performance Routing Version 3
Example: Configuring Performance Routing Version 3
**CHAPTER 4**

**PfRv3 Transit Site Support**

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

- Feature Information for PfRv3 Transit Site Support, 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](http://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.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.15S</td>
<td>The following commands were modified by this feature: master (domain VRF configuration), domain (interface configuration).</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

Information About Transit Site Support

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

PfRv3 Transit Site Use Case Scenarios

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

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

Single Data Center with Multiple Borders

In the following illustration, spoke A (R10) is connected to two (BR1 and BR2) DMVPN hubs in a single Dynamic Multipoint VPN (DMVPN) domain. There are two paths and two next-hops to the hub site from the spoke A. To differentiate traffic from different ISP paths, a path-id is added on each domain path. Use the `domain domain-name path path-name path-id` command to configure the path-ids.
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><strong>Example:</strong> 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> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface loopback <code>interface-number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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><strong>Example:</strong> Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> domain `{domain-name</td>
<td>default}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config)# domain default</td>
<td>You can either configure a default domain or define a specific domain for the transit hub configuration. If you are defining a specific domain, for example &quot;domain-cisco&quot;, you must configure the same domain for all devices for PfRv3 configuration. <strong>Note</strong></td>
</tr>
</tbody>
</table>

**Step 6**  
**vrf {vrf-name | default}**  
**Example:**  
Device(config-domain)# vrf default  
Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain.  

**Step 7**  
**master transit pop-id**  
**Example:**  
Device(config-domain-vrf)# master transit 1  
Enters master-controller configuration mode and configures the master as a transit hub. The valid range for a pop-id is from 1 to 62.  

**Step 8**  
**source-interface loopback interface-number**  
**Example:**  
Device(config-domain-vrf)# source-interface loopback0  
Configures the loopback used as a source for peering with other sites or master controller.  
**Note** The source-interface loopback also serves as a site ID of a particular site (hub or branch) on the master controller.  

**Step 9**  
**site-prefixes prefix-list site-list**  
**Example:**  
Device(config-domain-vrf)# site-prefixes prefix-list Data_Center_1  
Configures the prefix-list containing list of site prefixes.  
**Note** You must configure the static-site prefix list for a hub and transit sites.  

**Step 10**  
**hub ip-address**  
**Example:**  
Device(config-domain-vrf)# hub 10.8.3.3  
Configures the hub for the transit site.  

**Step 11**  
**exit**  
**Example:**  
Device(config-domain-vrf)# exit  
Exits from master controller configuration mode and returns to domain configuration mode.  
**Note** Exit from domain configuration mode and enter in global configuration mode using the `exit` command.  

**Step 12**  
**end**  
**Example:**  
Device(config)# end  
Exits configuration mode and returns to privileged EXEC mode.  

**Step 13**  
(Optional) **show domain domain-name master status**  
**Example:**  
Device# show domain one master status  
Use this show command to display the status of a master controller.
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>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:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal  
**Example:**  
Device# configure terminal

Enters global configuration mode.

**Step 3**

interface loopback  
**Example:**  
Device(config)# interface Loopback0

Enters interface configuration mode.

**Step 4**

ip address  
**Example:**  
Device(config-if)# ip address 10.9.4.4 255.255.255.255

Configures an IP address for an interface on the hub-border router (Border Router 1).

**Step 5**

exit  
**Example:**  
Device(config-if)# exit

Exits interface configuration mode and returns to global configuration mode.

**Step 6**

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

Enters domain configuration mode.

**Step 7**

vrf  
**Example:**  
Device(config-domain)# vrf default  
**Note** You can configure specific VRF definition for the hub-border configuration.

Configures Virtual Routing and Forwarding (VRF) for the default domain.

**Step 8**

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

Enters border configuration mode and configures the device as border.

**Step 9**

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

Configures the loopback used as a source for peering with other sites or master controller.

**Step 10**

master  
**Example:**  
Device(config-domain-vrf-br)# master 10.9.3.3

Configures the IP address of the hub-master controller.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong> exit</td>
<td>Exits border configuration mode and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-domain-vrf-br)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exits VRF configuration mode and enters domain configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-domain-vrf)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> exit</td>
<td>Exits domain configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-domain)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> interface tunnel-name</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface Tunnel100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> ip address ip-address mask</td>
<td>Configures an IP address for the tunnel interface.</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip address 10.0.100.84 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> description description-line</td>
<td>Configures a description to associate with an ISP path.</td>
</tr>
<tr>
<td>Example: Device1(config-if)# description primary path Device2(config-if)# description secondary path</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> domain domain-name path path-name path-id path-id</td>
<td>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.</td>
</tr>
<tr>
<td>Example: Device(config-if)# domain default path MPLS path-id 1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong> end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Device(config-if)# end

**Device# show domain default border status**

<table>
<thead>
<tr>
<th>Step 19</th>
<th>(Optional) show domain domain-name border status Example: Device# show domain default border status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Use this show command to display the status of a border router.</td>
</tr>
</tbody>
</table>

### What to do next

Verifying PfRv3 Transit Site Support

### Verifying PfRv3 Transit Site Support

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

**Before you begin**

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

**Step 1**  

**show domain domain-name master channels**

Displays channel information of the hub-master controller.

**Example:**

HubMC# show domain default master channels

```
Channel Id: 8  Dst Site-Id: 10.2.11.11  Link Name: MPLS  DSCP: default 0  pfr-label: 0:0 | 2:30 [0x21E]  TCs: 0
Channel Created: 03:19:14 ago
Provisional State: Initiated and open
Operational state: Available but unreachable
Channel to hub: FALSE
Interface Id: 11
Supports Zero-SLA: Yes
Muted by Zero-SLA: No
Estimated Channel Egress Bandwidth: 0 Kbps
Immitigable Events Summary:
  Total Performance Count: 0, Total BW Count: 0
ODE Stats Bucket Number: 1
Last Updated : 00:00:21 ago
Packet Count : 0
Byte Count : 0
```
One Way Delay : N/A
Loss Rate Pkts : N/A
Loss Rate Bytes: N/A
Jitter Mean : N/A
Unreachable : TRUE
ODE Stats Bucket Number: 2
Last Updated : 00:00:52 ago
Packet Count : 0
Byte Count : 0
One Way Delay : N/A
Loss Rate Pkts : N/A
Loss Rate Bytes: N/A
Jitter Mean : N/A
Unreachable : TRUE
TCA Statistics:
- Received:355 ; Processed:354 ; Unreach_rcvd:355
Latest TCA Bucket
- Last Updated : 00:00:21 ago
  - Local unreachable TCA received(Check for stale TCA 00:00:09 later)

Step 2  
show domain  domain-name  border channel

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

Example:
HubBR# show domain default border channels

Border Smart Probe Stats:

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

Channel id: 20
Channel create time: 06:42:54 ago
Site id : 10.2.11.11
DSCP : default[0]
Service provider : MPLS
Frfr-Label : 0:0 | 0:0 [0x0]
exit path-id sent on wire: 0
exit path-id: 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>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>10.8.0.0/16</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>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>10.9.0.0/16</td>
<td>01:28:47 ago</td>
<td>0x5</td>
<td>C,M</td>
</tr>
<tr>
<td>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>

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>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>
</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.

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

**Example:**

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

---

<table>
<thead>
<tr>
<th>Channel Id</th>
<th>Dst Site Id</th>
<th>Link Name</th>
<th>DSCP</th>
<th>pfr-label</th>
<th>TCs</th>
<th>Last Updated</th>
<th>Packet Count</th>
<th>Byte Count</th>
<th>One Way Delay</th>
<th>Loss Rate Pkts</th>
<th>Loss Rate Byte</th>
<th>Jitter Mean</th>
<th>Unreachable</th>
<th>ODE Stats Bucket Number</th>
<th>TCA Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>10.8.3.3</td>
<td>INET</td>
<td>default [0]</td>
<td>0x0</td>
<td>0x140000</td>
<td>0</td>
<td>00:00:24 ago</td>
<td>562</td>
<td>47208</td>
<td>71 msec*</td>
<td>0.0%</td>
<td>0.0%</td>
<td>619 usec</td>
<td>FALSE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>10.8.0.0/16</td>
<td></td>
<td></td>
<td>0x5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.9.0.0/16</td>
<td></td>
<td></td>
<td>0x5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:** * (Value obtained from Network delay:)

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

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

Configuration Examples for PfRv3 Transit Site Support

Example: Configuring Transit Site Support

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

*Figure 7: PfRv3 Transit Hub Topology*

In this example, the following routers are used:

- Hub Master Controller — Cisco ASR 1002-X router configured with an embedded services processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps.
• Hub Border Routers — Cisco ASR 1000 Series Embedded Services Processor 2
• Branch Routers — Cisco 4451X Integrated Services Router.

Example: Configuring Data Center 1 (DC1) Devices

Configure the interfaces on master hub controller (R82)

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

Configure the device as hub-master controller

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

Configure IP prefix-lists

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

Configure domain policies on hub master controller

HubMC(config)# domain default
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master hub
HubMC(config-domain-vrf-mc)# source-interface Loopback0
HubMC(config-domain-vrf-mc)# 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)**

```
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)Link

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

Example: Configuring Data Center 2 (DC2) Devices

Configure the interfaces on master hub controller (R92)

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

Configure the device as transit-hub master controller

HubMC(config)# domain default
HubMC(config-domain)# vrf default
HubMC(config-domain-vrf)# master transit 2
HubMC(config-domain-vrf)# source-interface Loopback0
HubMC(config-domain-vrf)# site-prefixes prefix-list DC2_PREFIX
HubMC(config-domain-vrf)# hub 10.8.3.3
HubMC(config-domain-vrf)# 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 hub border routers on DC2 (R95)

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

Configure the device as border router (BR95)

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

Configure tunnel from BR95 to DMVPN2 (INET)Link

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

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

Configure the device as branch-master controller (R10)
R10(config)# domain default
R10(config-domain)# vrf default
R10(config-domain-vrf)# border
R10(config-domain-vrf-br)# source-interface Loopback0
R10(config-domain-vrf-br)# master local
R10(config-domain-vrf-br)# exit
R10(config-domain-vrf)# master branch
R10(config-domain-vrf-mc)# source-interface Loopback0
R10(config-domain-vrf-mc)# hub 10.8.3.3

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

R10(config)# interface Tunnel200
R10(config-if)# bandwidth 5000
R10(config-if)# ip address 10.0.200.10 255.255.255.0
R10(config-if)# no ip redirects
R10(config-if)# ip mtu 1400
R10(config-if)# ip nhrp authentication cisco
R10(config-if)# ip nhrp map multicast dynamic
R10(config-if)# ip nhrp network-id 2
R10(config-if)# ip nhrp holdtime 600
R10(config-if)# ip nhrp nhs 10.0.200.85 nbma 172.16.85.5 multicast
R10(config-if)# ip nhrp nhs 10.0.200.95 nbma 172.16.95.5 multicast
R10(config-if)# ip nhrp registration no-unique
R10(config-if)# ip nhrp registration timeout 60
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 nh 10.0.100.84 nbma 172.16.84.4 multicast
R11(config-if)# ip nhrp nh 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
Example: Configuring Transit Site Support

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

Configure the interfaces (R12)

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

Configure the device as branch-master controller (R12)

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

Configure the tunnel interface and tunnel path from R12

R12(config)# interface Tunnel100
R12(config-if)# bandwidth 400
R12(config-if)# ip address 10.0.100.12 255.255.255.0
R12(config-if)# no ip redirects
R12(config-if)# ip mtu 1400
R12(config-if)# ip nhrp authentication cisco
R12(config-if)# ip nhrp map multicast dynamic
R12(config-if)# ip nhrp network-id 1
R12(config-if)# ip nhrp holdtime 600
R12(config-if)# ip nhrp nhs 10.0.100.84 nbma 172.16.84.4 multicast
R12(config-if)# ip nhrp nhs 10.0.100.94 nbma 172.16.94.4 multicast
R12(config-if)# ip nhrp registration no-unique
R12(config-if)# ip nhrp registration timeout 60
R12(config-if)# ip nhrp shortcut
R12(config-if)# ip tcp adjust-mss 1360
R12(config-if)# load-interval 30
R12(config-if)# delay 1000
R12(config-if)# no nhrp route-watch
R12(config-if)# if-state nhrp
R12(config-if)# tunnel source Ethernet0/1
R12(config-if)# tunnel mode gre multipoint
```
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 nh 10.0.200.85 nbma 172.16.85.5 multicast
R13(config-if)# ip nhrp nh 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

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
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>10.8.0.0/16</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>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>10.9.0.0/16</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

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
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
BR94# show domain default border status

**** Border Status ****

Instance Status: UP
Present status last updated: 06:39:21 ago
Loopback: Configured Loopback0 UP (10.9.4.4)
Master: 10.9.3.3
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 06:39:15
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
  Name: Tunnel100 Interface Index: 11 SNMP Index: 8 SP: MPLS path-id: 30 Status: DOWN Zero-SLA: NO
Auto Tunnel information:
  Name: Tunnel0 if_index: 12
  Borders reachable via this tunnel: 10.9.5.5

BR94# show domain default border site-prefix

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

<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,C,M</td>
</tr>
<tr>
<td>10.8.3.3</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>
R10# show domain default master channels dst-site-id 10.8.3.3

Legend: * (Value obtained from Network delay:)

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

R10# show domain default border status

**** Border Status ****
Instance Status: UP
Present status last updated: 3d14h ago
Loopback: Configured Loopback0 UP (10.2.10.10)
Master: 10.2.10.10
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 3d14h
Route-Control: Enabled
Asymmetric Routing: Disabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
Name: Tunnel100 Interface Index: 14 SNMP Index: 8 SP: MPLS Status: UP Zero-SLA: NO Path-id List: 0:10, 1:30
Name: Tunnel200 Interface Index: 15 SNMP Index: 9 SP: INET Status: UP Zero-SLA: NO Path-id List: 0:20, 1:40
Auto Tunnel information:
Name:Tunnel0 if_index: 13
Borders reachable via this tunnel:

R10# show domain default master status

*** Domain MC Status ***

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

Borders:
IP address: 10.2.10.10
Version: 2
Connection status: CONNECTED (Last Updated 3d14h ago )
Interfaces configured:
Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP | Zero-SLA: NO
Number of default Channels: 0
Path-id list: 0:10 1:30
Name: Tunnel200 | type: external | Service Provider: INET | Status: UP | Zero-SLA: NO
Number of default Channels: 0
Path-id list: 0:20 1:40
Tunnel if: Tunnel0

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

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

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

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

R10# show domain default border channels service-provider INET

Tue Mar 24 04:53:39.968
Border Smart Probe Stats:

Smart probe parameters:
Source address used in the Probe: 10.2.10.10
Unreach time: 1000 ms
Probe source port: 18000
Probe destination port: 19000
Interface Discovery: ON
Probe freq for channels with traffic :10 secs
Discovery Probes: OFF
Number of transit probes consumed :0
Number of transit probes re-routed: 0
[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

---------------------------------------------------------------------------------------------
Example: Configuring Transit Site Support
PfRv3 Zero SLA Support

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

- Feature Information for PfRv3 Zero SLA Support, on page 123
- Prerequisites for PfRv3 Zero SLA Support, on page 124
- Restrictions for PfRv3 Zero SLA Support, on page 124
- Information About PfRv3 Zero SLA Support, on page 124
- How to Configure PfRv3 Zero SLA Support, on page 127
- Configuration Examples for PfRv3 Zero SLA Support, on page 132

Feature Information for PfRv3 Zero SLA Support

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

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

Table 14: Feature Information for PfRv3 Zero SLA Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Path of Last Resort Support</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>
### Prerequisites for PfRv3 Zero SLA Support

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

### Restrictions for PfRv3 Zero SLA Support

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

### Information About PfRv3 Zero SLA Support

#### Information About Zero SLA

The Zero SLA (0-SLA) feature enables users to reduce probing frequency in their network infrastructure. Reduction in probing process helps in reducing cost especially when ISPs charge based on traffic, and helps in optimizing network performance when ISPs provide limited bandwidth. When this feature is configured, probe is sent only on the DSCP-0 channel. For all other DSCPs, channels are created if there is traffic, but no probing is performed. The reachability of other channels is learnt from the DSCP-0 channel that is available at the same branch site.
In the above illustration, the branch and hub sites are connected with red and blue ISP links. On the red ISP link, Zero SLA is configured at the hub site. Traffic exists on DSCP-0, DSCP AF31, and DSCP-EF channels on both ISP links, but on the red link probing is sent only on the DSCP-0 channel. A probe sent during the WAN discovery signals if a link is a Zero SLA link or a normal link.

**Information About Path of Last Resort**

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

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

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

**Compatibility Matrix for Zero SLA Support**

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

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

The following table shows the devices with various Cisco IOS/XE release versions and its support for Zero SLA within a single branch.
If the master controller and border routers have the same Cisco IOS release versions, the Zero SLA feature is enabled.

If the master controller has the latest Cisco IOS release and the border router has the earlier release version, the Zero SLA feature is disabled.

Zero SLA is not supported on Cisco IOS XE release 3.13.

The release versions are not compatible and hence, Zero SLA cannot be enabled.

The following table shows the various Cisco IOS/XE release versions and its support for Zero SLA between different sites.

<table>
<thead>
<tr>
<th>Hub</th>
<th>Branch</th>
<th>Compatibility Between Release Versions</th>
<th>Zero SLA Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.14 or later</td>
<td>Cisco IOS XE Release 3.14 or later</td>
<td>Yes</td>
<td>If the hub and branch sites have the same Cisco IOS release versions, the Zero SLA feature is enabled.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 15.5(1)T or later</td>
<td>Cisco IOS XE Release 15.5(1)T or later</td>
<td>Yes</td>
<td>If the hub has the latest Cisco IOS release and the branch has the older release version, the Zero SLA feature is disabled.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.13 or earlier</td>
<td>Cisco IOS XE Release 3.13 or earlier</td>
<td>Yes</td>
<td>Zero SLA is not supported on Cisco IOS XE Release 3.13 and earlier versions.</td>
</tr>
</tbody>
</table>
Zero SLA Support
Compatibility Between Release Versions

<table>
<thead>
<tr>
<th>Hub</th>
<th>Branch</th>
<th>Compatibility Between Release Versions</th>
<th>Zero SLA Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.13 or earlier</td>
<td>Cisco IOS XE Release 3.14 or later</td>
<td>Yes</td>
<td>Zero SLA is not supported on Cisco IOS XE Release 3.13 and earlier versions.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.4 T or earlier</td>
<td>Cisco IOS Release 15.5(1)T or later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**How to Configure PfRv3 Zero SLA Support**

Configuring PfRv3 Zero SLA Support

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

**Before you begin**

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface tunnel</code> <code>tunnel-number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>interface tunnel</code> <code>100</code></td>
<td></td>
</tr>
</tbody>
</table>
## Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** | **bandwidth** *bandwidth-value*  
**Example:**  
Device(config-if)# bandwidth 10000000 | Configures inherited and received bandwidth values for the tunnel interface. The bandwidth value is in kilobits and the valid values are 1 to 10000000. |

**Step 5** | **ip address** *ip-address* *mask*  
**Example:**  
Device(config-if)# ip address 10.32.1.1 255.0.0.0 | Configures an IP address of the border router at the hub site. |

**Step 6** | **domain path** *isp-name* [internet-bound | path-id | path-last-resort | zero-sla]  
**Example:**  
Device(config-if)# domain path ISP1 zero-sla | Specifies a service provider for the interface. |

- **internet-bound**—Configures an internet bound interface.  
- **path-id**—Configures service provider's path-id for the interface.  
- **path-last-resort**—Configures the interface to be a path of a last resort.  
- **zero-sla**—Configures Zero SLA for the interface. |

**Note** You can configure multiple Internet Service Providers (ISPs). If you are defining a specific domain name for an ISP (for example, domain_abc), you must specify the same domain name while configuring the ISP paths. |

## Verifying PfRv3 Zero SLA Support

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

**Before you begin**  
Configure Zero SLA on the hub-border router.

**SUMMARY STEPS**

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

**Step 1**  
**show domain default master status**  
Displays the status of the hub master controller.

**Step 2**  
**show domain default master channel**  
Displays channel information of the hub master controller.

**Step 3**  
**show domain default border status**  
Displays the status of the hub border routers.

**Step 4**  
**show domain default border channel**  
Displays the information of border router channels at the hub site.

**Step 5**  
**show domain default master site-capability**  
Displays the capability information of master controller.

**Example:**  
Device# show domain default master site-capability

```
Device Capability

<table>
<thead>
<tr>
<th>Capability</th>
<th>Major</th>
<th>Minor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Zero-SLA</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Site id : 10.2.10.10

<table>
<thead>
<tr>
<th>Capability</th>
<th>Major</th>
<th>Minor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Zero-SLA</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Site id : 10.2.12.12

<table>
<thead>
<tr>
<th>Capability</th>
<th>Major</th>
<th>Minor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Zero-SLA</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>Features supported by PfR v3 domain.</td>
</tr>
</tbody>
</table>
### Verifying PfRv3 Zero SLA Support

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Domain version. Major - Means the major release version number for PfR v3.</td>
</tr>
<tr>
<td></td>
<td>Minor - Means the minor release version number for PfR v3.</td>
</tr>
<tr>
<td>Zero-SLA</td>
<td>Zero-SLA feature support. Major - Means the major release version of the Zero-SLA feature on the master controller.</td>
</tr>
<tr>
<td></td>
<td>Minor - Means the minor release version of the Zero-SLA feature on the master controller.</td>
</tr>
</tbody>
</table>

#### Step 6

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

Displays the master status of the hub border routers.

**Example:**

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

Borders:
- IP address: 10.204.1.4
- Version: 2
- Connection status: CONNECTED (Last Updated 00:59:16 ago)
- Interfaces configured:
  - Name: Tunnel20 | type: external | Service Provider: ISP2 | Status: UP | Zero-SLA: NO | Path of Last Resort: Disabled
- Number of default Channels: 0
- Tunnel if: Tunnel2
- IP address: 10.203.1.3
- Version: 2
- Connection status: CONNECTED (Last Updated 00:59:16 ago)
- Interfaces configured:
  - Name: Tunnel10 | type: external | Service Provider: ISP1 | Status: UP | Zero-SLA: YES | Path of Last Resort: Standby
  - Number of default Channels: 0
- Tunnel if: Tunnel2

#### Step 7

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

Displays the master status of the hub border routers.

**Example:**

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

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

Auto Tunnel information:

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

Step 8  show domain default vrf  vrf-name  master channels
Displays the master status of the hub master controller.

Example:
Device# show domain default vrf vrf1 master channels

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

Step 9  show domain default vrf  vrf-name  border channels
Displays the information of border router channels at the hub site.

Example:
Device# show domain default vrf vrf1 border channels

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

Step 10

show domain default vrf \ vrf-name  master policy

Displays the status of the master policy.

Example:

Device# show domain default vrf vrf1 master policy

class VOICE sequence 10
  path-last-resort ISP1
  class type: Dscp Based
    match dscp ef policy custom
      priority 1 one-way-delay threshold 200 msec

  Number of Traffic classes using this policy: 2

Configuration Examples for PfRv3 Zero SLA Support

Example: Configuring PfRv3 Zero SLA Support

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

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

- Hub Master Controller — Cisco ASR 1002-X router configured with an embedded services processor (ESP) default bandwidth of 5 Gbps upgradable with software licensing options to 10 Gbps, 20 Gbps, and 36 Gbps.
- Hub Border Routers — Cisco ASR 1000 Series Embedded Services Processor 2
- Branch Routers — Cisco 4451X Integrated Services Router.

**Configure the interfaces on hub master controller**

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

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

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

**Configure IP prefix-lists**

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

**Configure domain policies on hub master controller**
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)# master hub
BR1(config-domain-vrf-mc)# monitor-interval 2 dscp ef
```

```
HubMC(config-domain-vrf-mc)# load-balance
HubMC(config-domain-vrf-mc)# class VOICE sequence 10
HubMC(config-domain-vrf-mc-class)# match dscp ef policy voice
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
```

```
HubMC(config-domain-vrf-mc)# class VIDEO sequence 20
HubMC(config-domain-vrf-mc-class)# match dscp af41 policy real-time-video
HubMC(config-domain-vrf-mc-class)# match dscp cs4 policy real-time-video
HubMC(config-domain-vrf-mc-class)# path-preference INET fallback MPLS
```

```
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc)# class CRITICAL sequence 30
HubMC(config-domain-vrf-mc-class)# match dscp af31 policy custom
HubMC(config-domain-vrf-mc-class-type)# priority 2 loss threshold 10
HubMC(config-domain-vrf-mc-class-type)# priority 1 one-way-delay threshold 600
HubMC(config-domain-vrf-mc-class-type)# priority 2 jitter threshold 600
```

```
HubMC(config-domain-vrf-mc-class)# exit
HubMC(config-domain-vrf-mc-class)# path-preference MPLS fallback INET
```

Configure tunnel from BR1 to DMVPN1 (MPLS) Link

```
BR1(config)# interface Tunnel100
BR1(config-if)# bandwidth 100000
```

```
BR1(config-if)# ip address 10.0.100.84 255.255.255.0
BR1(config-if)# no ip redirects
```

```
BR1(config-if)# ip mtu 1400
```

```
BR1(config-if)# ip nhrp authentication cisco
```

```
BR1(config-if)# ip nhrp map multicast dynamic
```

```
BR1(config-if)# ip nhrp network-id 1
```

```
BR1(config-if)# ip nhrp holdtime 600
```

```
BR1(config-if)# ip tcp adjust-mss 1360
```

```
BR1(config-if)# load-interval 30
```

```
BR1(config-if)# tunnel source GigabitEthernet3
```

```
BR1(config-if)# tunnel mode gre multipoint
```

```
BR1(config-if)# tunnel key 100
```

```
BR1(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
```

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

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

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

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

Configure the device as branch master controller (R10)
R10(config)# domain one
R10(config-domain)# vrf default
R10(config-domain-vrf)# border
R10(config-domain-vrf-br)# source-interface Loopback0
R10(config-domain-vrf-br)# master local
R10(config-domain-vrf-br)# exit
R10(config-domain-vrf)# master branch
R10(config-domain-vrf-mc)# source-interface Loopback0
R10(config-domain-vrf-mc)# hub 10.8.3.3

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

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

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

Configure the device as branch master controller (R11)
R11(config)# domain one
R11(config-domain)# vrf default
R11(config-domain-vrf)# border
R11(config-domain-vrf-br)# source-interface Loopback0
R11(config-domain-vrf-br)# master local
R11(config-domain-vrf-br)# exit
R11(config-domain-vrf)# master branch
R11(config-domain-vrf-mc)# source-interface Loopback0
R11(config-domain-vrf-mc)# hub 10.8.3.3

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

Configure another tunnel path from R11
R11(config)# interface Tunnel200
R11(config-if)# bandwidth 50000
R11(config-if)# ip address 10.0.200.11 255.255.255.0
R11(config-if)# no ip redirects
R11(config-if)# ip mtu 1400
R11(config-if)# ip nhrp authentication cisco
R11(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R11(config-if)# ip nhrp multicast 172.16.85.5
R11(config-if)# ip nhrp network-id 2
R11(config-if)# ip nhrp holdtime 600
R11(config-if)# ip nhrp nh 10.0.200.85
R11(config-if)# ip tcp adjust-mss 1360
R11(config-if)# load-interval 30
R11(config-if)# delay 1000
R11(config-if)# tunnel source GigabitEthernet3
R11(config-if)# tunnel mode gre multipoint
R11(config-if)# tunnel key 200
R11(config-if)# tunnel vrf INET2
R11(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
R11(config-if)# domain one path INET
Verifying PfRv3 Zero-SLA Configurations

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

- `show domain domain-name master status`
- `show domain domain-name border status`
- `show domain domain-name master channel`
- `show domain domain-name border channel`
- `show domain domain-name master site-capability`
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 139
- Restrictions for PfRv3 Path of Last Resort, on page 139
- Information About PfRv3 Path of Last Resort, on page 140
- How to Configure PfRv3 Path of Last Resort, on page 140

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: <code>domain path isp-name</code>, <code>show domain default vrf border</code>, <code>show domain default vrf master</code>.</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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>domain default</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>
</tbody>
</table>

Example:

```
domain default
  vrf default
  master hub
  class foo seq 1
  match dscp ef policy voice
  path-preference ISP1 fallback ISP2
  path-last-resort ISP4
```
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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>enable</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><em>configure terminal</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><em>interface tunnel tunnel-number</em></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface tunnel 100</td>
</tr>
<tr>
<td></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>*domain path isp-name [internet-bound</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# domain path ISP1 path-last-resort</td>
</tr>
<tr>
<td></td>
<td>Specifies a service provider for the interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>internet-bound</strong>—Configures an internet bound interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>path-id</strong>—Configures service provider's path-id for the interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>path-last-resort</strong>—Configures the interface to be a path of a last resort.</td>
</tr>
<tr>
<td></td>
<td>• <strong>zero-sla</strong>—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: 10.203.1.3
    Version: 2
    Connection status: CONNECTED (Last Updated 00:59:16 ago )
    Interfaces configured:
      Name: Tunnel10 | type: external | Service Provider: ISP1 | Status: UP | Zero-SLA: YES | Path of Last Resort: Standby
      Number of default Channels: 0
      Tunnel if: Tunnel1

Step 2  show domain default vrf vrf-name border status
Displays the master status of the hub border routers.

Example:
Device# show domain default vrf vrf1 border status

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

Auto Tunnel information:

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

Step 3 show domain default vrf vrf-name master channels
Displays the master status of the hub master controller.
Example:
Device# show domain default vrf vrf1 master channels
Channel Id: 9 Dst Site-Id: 30.209.1.9 Link Name: ISP1 DSCP: af41 [34] pf-r-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
Verifying PfRv3 Path of Last Resort

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

Step 5

show domain default vrf  vrf-name  master policy

Displays the status of the master policy.

Example:

Device# show domain default vrf vrf1 master policy

class VOICE sequence 10
    path-last-resort ISP1
    class type: Dscp Based
        match dscp ef policy custom
            priority 1 one-way-delay threshold 200 msec
    Number of Traffic classes using this policy: 2
PfRv3 Fallback Timer

PfRv3 can move a specific traffic class (TC) from a primary, preferred path to a backup path to optimize performance. Use fallback-timer to set the time interval (called timeout) for the next re-evaluation of the primary path. Increasing the time interval causes PfRv3 to wait longer before reassessing. This can help to prevent excessive switching between the primary and secondary paths.

- Feature Information for PfRv3 Fallback Timer, on page 145
- Prerequisites for PfRv3 Fallback Timer, on page 146
- Information About PfRv3 Fallback Timer, on page 146
- How to Configure PfRv3 Fallback Timer, on page 148
- Configuration Examples for PfRv3 Fallback Timer, on page 149

Feature Information for PfRv3 Fallback Timer

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 17: Feature Information for PfRv3 Fallback Timer**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Fallback Timer</td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>The PfRv3 Fallback Timer sets the re-evaluation interval for re-evaluating the primary path after a traffic class has been changed to a backup path. The following commands were modified or added by this feature: fallback-time, show domain vrf master.</td>
</tr>
</tbody>
</table>
Prerequisites for PfRv3 Fallback Timer

- Latest Cisco IOS XE image

Information About PfRv3 Fallback Timer

Overview of Fallback Timer

As part of its intelligent path selection, PfRv3 can move a specific traffic class (TC) from a primary, preferred path to a backup path to optimize performance. After changing the TC to a backup path, PfRv3 re-evaluates the primary path to determine when to return the TC to the primary path. The re-evaluation occurs in cycles of a specific period of time, and continues for as long as the traffic is not on the primary path.

In some situations, if the primary path alternates between meeting the performance requirements specified for the TC and not meeting the requirements, the TC may be switched excessively between the primary and backup paths. This “bouncing” between paths reduces the stability of the TC.

To prevent excessive switching between paths, you can increase the evaluation interval (called timeout) and apply a dampening algorithm.

Figure 10: Default Timeout
Figure 11: Longer Timeout Interval

**Longer Timeout, Less Bouncing**

Re-evaluate

Primary Path OK

Timeout Duration

Use Primary Path

Use Backup Path

Time (minutes)

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Applicable to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase evaluation interval</td>
<td>Use fallback-timer to set the time interval (called timeout) for the next re-evaluation of the primary path. Increasing the time interval causes PfRv3 to wait longer before reassessing. This prevents excessive switching between the primary and secondary paths. Possible values: 1 to 1440 minutes Default: 3 minutes</td>
<td>Global (per VRF) Traffic class</td>
</tr>
<tr>
<td>Dampening</td>
<td>Use fallback-timer to enable automatic adjustment of the re-evaluation time interval to prevent excessive switching between paths. When enabled, dampening temporarily increases the evaluation period if a traffic class has been switched more than once from the primary path to a backup path within a short time. It then gradually reduces the evaluation period over time if the primary path meets the performance requirements specified for the traffic class. Possible values: enable, disable Default: enable (if fallback-timer is configured)</td>
<td>Traffic class</td>
</tr>
</tbody>
</table>
How to Configure PfRv3 Fallback Timer

PfRv3 Fallback Timer Configuration

To configure the fallback timer, use:

```
fallback-timer  time-in-minutes  [ dampening  { enable / disable } ]
```

See the examples below.

Fallback Timer Configuration Priority

Priority of fallback timer configuration:

```
per class (policy) > global > default
```

**Example**

Configuration:

- Traffic class A configuration: `fallback-timer 4 dampening enable`
- Global configuration: `fallback-timer 6`

**Result:**

Traffic class A will operate with a timeout of 4 minutes and dampening. Other traffic classes will have a fixed timeout (no dampening) of 6 minutes.

Viewing PfRv3 Fallback Timer Status

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

**Before you begin**

Perform on hub master controller.

**SUMMARY STEPS**

1. `show domain  domain-name  vrf  vrf-name  master policy`
2. `show domain  domain-name  vrf  vrf-name  master traffic-classes detail`

**DETAILED STEPS**

**Step 1**

```
show domain  domain-name  vrf  vrf-name  master policy
```

**Example**

Sections of the output in bold are relevant to fallback timer.
Device# show domain default vrf green master policy
  No Policy publish pending
  Last publish Status : Peering Success
  Total publish errors : 0

Global-policy-list:

class SER_CS1 sequence 10
  path-preference ISP1 fallback ISP2
    fallback timer timeout 5 minutes, dampening Enabled
  class type: Dscp Based
    match dscp cs1 policy custom
    priority 1 packet-loss-rate threshold 10.0 percent
    priority 1 byte-loss-rate threshold 10.0 percent
    Number of Traffic classes using this policy: 1

class SER_EF sequence 20
  path-preference ISP1 fallback ISP2
    fallback timer timeout 6 minutes, dampening Disabled
  class type: Dscp Based
    match dscp ef policy custom
    priority 1 packet-loss-rate threshold 10.0 percent
    priority 1 byte-loss-rate threshold 10.0 percent

Step 2

Example

Sections of the output in bold are relevant to fallback timer.

Example: Configuring PfRv3 Fallback Timer Globally

  Configure the global fallback timer settings on a hub master controller.

  Configure global fallback timer to 4 minutes

domain iwan
vrf default
master hub
advanced
fallback-timer 4
Disable fallback timer globally

Use `fallback-timer off` to disable re-evaluation of the primary path after a traffic class switches to a backup path. In this mode, traffic does not switch back to the primary path.

Example: Configuring PfRv3 Fallback Timer for Traffic Class

Configure the global fallback timer settings on a hub master controller.

### Fallback 5 minutes, dampening enabled by default

```
domain iwan
vrf default
master hub
advanced
fallback-timer off
```

### Fallback 10 minutes, dampening disabled

```
class REAL_TIME_VIDEO sequence 20
match dscp cs4 policy real-time-video
match dscp af41 policy real-time-video
path-preference MPLS1 fallback INET1
fallback-timer 10 dampening disable
```

### Fallback timer off

Use `fallback-timer off` to disable re-evaluation of the primary path after a traffic class switches to a backup path. In this mode, traffic does not switch back to the primary path.

Note Consider restoring the fallback timer to the default 3 minutes instead of disabling.

```
class LOW_LATENCY_DATA sequence 30
match dscp cs2 policy real-time-video
match dscp af21 policy real-time-video
path-preference INET1 fallback MPLS1
fallback-timer off
```
CHAPTER 8

PfRv3 Probe Reduction

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

- Feature Information for PfRv3 Probe Reduction, on page 151
- Prerequisites for PfRv3 Probe Reduction, on page 151
- Information About PfRv3 Probe Reduction, on page 151
- How to Configure PfRv3 Probe Reduction, on page 152
- Configuration Examples for PfRv3 Probe Reduction, on page 154
- Additional References for PfRv3 Probe Reduction, on page 154

Feature Information for PfRv3 Probe Reduction

Table 18: 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></td>
<td>This document provides information about the PfRv3 Probe Reduction feature that allows reducing traffic probe on channels that do not carrying any traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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> <code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>domain default</code></td>
<td>Enters domain configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# domain default</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 4** | **Configure the device as a master hub and enters master controller configuration mode.**  
Do one of the following:  
• **master hub**  
• **border**  
**Example:**  
Device(config-domain)# master hub  
**Example:**  
Device(config-domain)# border |

| **Step 4** | **Configure the device as the border and enters border configuration mode.**  
**Note**  
If you select border configuration, it overwrites the master configuration.  
**Example:**  
Device(config-domain)# border |

| **Step 5** | **Enters advanced configuration mode.**  
**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:**  
• 1 packet every 1 second for default monitor  
• 20 packets every 1 second for quick monitor  
**Example:**  
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**

```show domain {default | domain-name} [vrf vrf-name] {master | border} status```  
Use this command to verify the configuration.  
**Example:**  
Router# show domain default vrf green master status

**Smart Probe Profile:**  
**General Monitor:**  
Current Provision Level: Master Hub  
Master Hub:  
• Packets per burst: 10  
• Interval(secs): 20  
**Quick Monitor:**  
Current Provision Level: Master Hub
Configuration Examples for PfRv3 Probe Reduction

Example: PfRv3 Probe Reduction

domain default
master hub
advanced
  smart-probe burst 10 packets every 20 seconds
  smart-probe burst quick 10 packets every 1 seconds

Additional References for PfRv3 Probe Reduction

<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>
The Performance Routing v3 (PfRv3) Intelligent Load Balance feature helps to move the traffic-classes based on the remote ingress interface, if the remote interface is overrun the bandwidth threshold. It validates remote interface ingress bandwidth when choosing the path. The PfRv3 Intelligent Load Balance feature detects the remote bandwidth overrun at the earliest and helps to reduce the packet drop caused by per tunnel QoS and increases the bandwidth utilization.

- Feature Information for PfRv3 Intelligent Load Balance, on page 155
- Prerequisites for PfRv3 Intelligent Load Balance, on page 156
- Restrictions for PfRv3 Intelligent Load Balance, on page 156
- Information About PfRv3 Intelligent Load Balance, on page 156
- How to Configure PfRv3 Intelligent Load Balance, on page 156

### Feature Information for PfRv3 Intelligent Load Balance

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

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

**Table 19: Feature Information for PfRv3 Intelligent Load Balance**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Intelligent Load Balance</td>
<td>Cisco IOS XE 16.11</td>
<td>The Performance Routing v3 (PfRv3) Intelligent Load Balance feature helps to move the traffic-classes (TC) based on the remote ingress interface, if the remote interface is overrun the bandwidth threshold. The following command was introduced: remote-ingress-bandwidth-check.</td>
</tr>
</tbody>
</table>
Prerequisites for PfRv3 Intelligent Load Balance

You must upgrade master hub software version to 16.11 or later. The spoke sites that require PfRv3 Intelligent Load Balance feature must be upgraded to version 16.11 or later. However, it is not mandatory to upgrade the spoke sites that do not use the PfRv3 intelligent Load Balance feature to the recommended versions.

Restrictions for PfRv3 Intelligent Load Balance

• The PfRv3 Intelligent Load balance supports the traffic only from hub to spoke.
• Only the default traffic classes are load-balanced among paths when the WAN interface is overrun in remote spoke sites.
• Remote bandwidth check is only supported on the hub or on the transit hub.
• Remote bandwidth TCA is sent from branch to hub or from branch to transit hub only.

Information About PfRv3 Intelligent Load Balance

How to Configure PfRv3 Intelligent Load Balance

Configuring PfRv3 Intelligent Load Balance

SUMMARY STEPS

1. enable
2. configure terminal
3. domain iwan
4. vrf default
5. master hub
6. load-balance
7. load-balance advanced
8. path-preference INET1 fallback MPLS1
9. advanced
10. remote-ingress-bandwidth-check max 75
11. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
**Example:**  
Device> enable  
- Enter your password if prompted.

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

**Step 3**  
domain iwan  
**Example:**  
Device(config)# domain iwan  
Enter domain iwan configuration mode.

**Step 4**  
vrf default  
**Example:**  
Device(config-domain)# vrf default  
Configures Virtual Routing and Forwarding (VRF) for the default domain.

**Step 5**  
master hub  
**Example:**  
Device(config-domain-vrf)# master hub  
Configures the device as a master hub and enters master controller configuration mode.

**Step 6**  
load-balance  
**Example:**  
Device(config-domain-vrf-mc)# load-balance  
Enables load balance.

**Step 7**  
load-balance advanced  
**Example:**  
Device(config-domain-vrf-mc)# load-balance advanced  
(Optional) Enables advanced mode of VRF on master hub.

**Step 8**  
path-preference **INET1** fallback **MPLS1**  
**Example:**  
Device(config-domain-vrf-mc-load-balance)# path-preference INET1 fallback MPLS1  
Specifies the path preference name and the fallback path(s) preference to use when the primary path(s) are out of policy.

**Step 9**  
advanced  
**Example:**  
Device(config-domain-vrf-mc-load-balance)# advanced  
Enter advanced configuration mode.

**Step 10**  
remote-ingress-bandwidth-check max 75  
**Example:**  
Device(config-domain-vrf-mc-advanced)# remote-ingress-bandwidth-check max 75  
(Optional) Enables to change the value of remote bandwidth threshold. The default value of remote bandwidth threshold is 75%. You should change the remote bandwidth threshold followed by per tunnel QoS.

**Note**  
Remote spoke site sends out BW-TCA, if WAN interface BW utilization exceeds the threshold.
### Purpose

**Step 11**

**Command or Action**

| exit |

**Example:**

Device(config-domain-vrf-mc-advanced)exit

**Purpose**

Exits border configuration mode and returns to privileged EXEC mode.

---

### What to do next

The remote BW percentage must be configured after configuring PfRv3 Intelligent Load Balance.

### Verifying PfRv3 Intelligent Load Balance

Use the following commands to verify PfRv3 intelligent load balance configuration:

- `show domain domain-name vrf vrf-name master exits`
- `show domain domain-name vrf vrf-name master exists site-id path-id`

### Example: Configuring PfRv3 Intelligent Load Balance

```plaintext
domain iwan
vrf default
master hub
load-balance advanced
path-preference INET1 fallback MPLS1
advanced
remote-ingress-bandwidth-check max 75
```

### Example: Verifying PfRv3 Intelligent Load Balance

The following is an example output from the `show domain iwan master exits` command.

```
Device# show domain iwan master exits
BR address: 168.254.0.2 | Name: Tunnel10 | type: external | Path: MPLS1 | path-id: 11 |
PLR TCs: 0

  Egress capacity: 1000000 Kbps | Egress BW: 2 Kbps | Ideal:1078 Kbps | under: 1076 Kbps
  Ingress capacity: 1000000 Kbps | Ingress BW: 1076 Kbps | Ingress Utilization: 0 %

BR address: 168.254.0.3 | Name: Tunnel120 | type: external | Path: INET1 | path-id: 12 |
PLR TCs: 0

  Egress capacity: 1000000 Kbps | Egress BW: 1076 Kbps | Ideal:1078 Kbps | under: 2 Kbps
  Ingress capacity: 1000000 Kbps | Ingress BW: 2 Kbps | Ingress Utilization: 0 %

DSCP: default[0]-Number of Traffic Classes[1]
```

The following is an example output from the `show domain iwan master exits 168.254.0.9 path-id` command.

```
Device# show domain iwan master exits 168.254.0.9 path-id
Site id : 168.254.0.9
Site mc type : Branch
Border Address : 168.254.0.9
Service provider: MPLS1 path-id: 11 if_index: 28 bandwidth: 2000Kbps
bw-from-local-to-remote: 0Kbps Address: NA
```
Example: Verifying PfRv3 Intelligent Load Balance

Service provider: INET1 path-id: 12 if_index: 29 bandwidth: 300000Kbps
bw-from-local-to-remote: 1040Kbps  Address: NA
Example: Verifying PfRv3 Intelligent Load Balance
CHAPTER 10

Path Preference Hierarchy

The Path Preference Hierarchy feature allows you to configure service providers per VRF for traffic classes.

- Feature Information for Path Preference Hierarchy, on page 161
- Information About Path Preference Hierarchy, on page 161
- How to Configure Path Preference Hierarchy, on page 162
- Additional References for Path Preference Hierarchy, on page 163

Feature Information for Path Preference Hierarchy

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Preference Hierarchy</td>
<td>Cisco IOS XE Denali</td>
<td>The Path Preference Hierarchy feature allows you to configure service providers per VRF for traffic classes. The following command was introduced or modified: path-preference.</td>
</tr>
<tr>
<td></td>
<td>16.3.1</td>
<td></td>
</tr>
</tbody>
</table>

Information About Path Preference Hierarchy

Overview of Path Preference Hierarchy

In an enterprise network, you would need to configure service providers to interconnect the hub and branches. The Path Preference Hierarchy feature allows you to configure three service providers per VRF for traffic classes. The service providers could be primary service provider, fallback service provider, and next-fallback service provider respectively. As the name suggests, the primary service provider is the first preference in the network, followed by fallback and next-fallback, respectively. You cannot have the same service provider for
primary and fallback as this results in a “fallback backhole.” In other words, each service provider must be unique.

Use the **path-preference** command to specify the service provider order. Use the **blackhole** or **routing** keywords for a next-fallback service provider to drop the packet if fallback is unavailable or to specify there is no next-fallback service provider, respectively. When a packet reaches “blackhole,” the packet is discarded.

### How to Configure Path Preference Hierarchy

#### Configuring Path Preference Hierarchy

Perform this task to configure Path Preference Hierarchy feature on a hub.

```plaintext
domain default
vrf green
master hub
  source-interface Loopback1
  site-prefixes prefix-list HUBPFX
  class HEIRARCHICAL sequence 100
    match dscp ef policy custom
    priority 1 loss threshold 10
  path-preference ISP1 ISP2 fallback ISP3 next-fallback blackhole
```

The following is a sample output on a device that displays the route change reason and history. In this example, the traffic class jumps from next-fallback service provider to primary service provider, when the fallback is unavailable.

```plaintext
Dst-Site-Prefix: 100.30.0.0/16  DSCP: ef [46] Traffic class id:2
Clock Time: 12:57:15 (PST) 03/30/2015
TC Learned: 00:22:14 ago
Present State: CONTROLLED
Current Performance Status: in-policy
Current Service Provider: ISP2 path-id:2 since 00:03:28
Previous Service Provider: ISP3 pfr-label: 0:0 | 0:7 [0x7] for 180 sec
(A fallback/next-fallback provider. Primary provider will be re-evaluated 00:02:34 later)
BW Used: 3 Kbps
Present WAN interface: Tunnel20 in Border 100.10.2.1
Present Channel (primary): 46 ISP2 pfr-label:0:0 | 0:2 [0x2]
Backup Channel: 42 ISP3 pfr-label:0:0 | 0:7 [0x7]
Destination Site ID bitmap: 0
Destination Site ID: 100.30.1.1
Class-Sequence in use: 10
Class Name: BUSINESS using policy User-defined
  priority 2 packet-loss-rate threshold 10.0 percent
  priority 2 byte-loss-rate threshold 10.0 percent
BW Updated: 00:00:14 ago
Reason for Latest Route Change: next-fallback to Higher Path Preference
Route Change History:

<table>
<thead>
<tr>
<th>Date and Time</th>
<th>Previous Exit</th>
<th>Current Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: 12:53:47 (PST)</td>
<td>ISP3/100.10.1.1/Tu30 (Ch:42)</td>
<td>ISP2/100.10.1.1/Tu20 (Ch:46)</td>
</tr>
<tr>
<td>ISP2/100.10.2.1/Tu20 (Ch:46)</td>
<td>next-fallback to Higher Path Preference</td>
<td></td>
</tr>
<tr>
<td>2: 12:50:47 (PST)</td>
<td>None/0.0.0.0/None (Ch:0)</td>
<td>ISP3/100.10.1.1/Tu30 (Ch:42)</td>
</tr>
<tr>
<td>ISP3/100.10.1.1/Tu20 (Ch:42)</td>
<td>Uncontrolled to Controlled Transition</td>
<td></td>
</tr>
<tr>
<td>3: 12:50:15 (PST)</td>
<td>None/0.0.0.0/None (Ch:0)</td>
<td>ISP2/100.10.1.1/Tu20 (Ch:43)</td>
</tr>
<tr>
<td>ISP3/100.10.4.1/Tu20 (Ch:43)</td>
<td>No Channels Available</td>
<td></td>
</tr>
</tbody>
</table>
```
ISP3/100.10.1.1/Tu30 (Ch:42) Exit down
5: 12:47:57 (PST) 03/30/2015 ISP2/100.10.2.1/Tu20 (Ch:46)
ISP2/100.10.4.1/Tu20 (Ch:43) Exit down

In the following example, continuation of the above example, the traffic class is now controlled by primary service provider.

Route Change History:

<table>
<thead>
<tr>
<th>Exit</th>
<th>Date and Time</th>
<th>Previous Exit</th>
<th>Current Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>12:50:15 (PST) 03/30/2015</td>
<td>ISP3/100.10.1.1/Tu30 (Ch:42)</td>
<td>None/0.0.0.0/None (Ch:0) No Channels Available</td>
</tr>
<tr>
<td>2:</td>
<td>12:48:14 (PST) 03/30/2015</td>
<td>ISP2/100.10.4.1/Tu20 (Ch:43)</td>
<td>Exit down</td>
</tr>
<tr>
<td>3:</td>
<td>12:47:57 (PST) 03/30/2015</td>
<td>ISP2/100.10.2.1/Tu20 (Ch:46)</td>
<td>Exit down</td>
</tr>
<tr>
<td>4:</td>
<td>12:44:42 (PST) 03/30/2015</td>
<td>ISP1/100.10.1.1/Tu10 (Ch:41)</td>
<td>Exit down</td>
</tr>
<tr>
<td>5:</td>
<td>12:44:13 (PST) 03/30/2015</td>
<td>ISP1/100.10.3.1/Tu10 (Ch:44)</td>
<td>Exit down</td>
</tr>
</tbody>
</table>

In the following example, continuation of the above example, the traffic class is discarded since the packet has reached a blackhole.

Route Change History:

<table>
<thead>
<tr>
<th>Exit</th>
<th>Date and Time</th>
<th>Previous Exit</th>
<th>Current Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>12:50:15 (PST) 03/30/2015</td>
<td>ISP3/100.10.1.1/Tu30 (Ch:42)</td>
<td>None/0.0.0.0/None (Ch:0) No Channels Available</td>
</tr>
<tr>
<td>2:</td>
<td>12:48:14 (PST) 03/30/2015</td>
<td>ISP2/100.10.4.1/Tu20 (Ch:43)</td>
<td>Exit down</td>
</tr>
<tr>
<td>3:</td>
<td>12:47:57 (PST) 03/30/2015</td>
<td>ISP2/100.10.2.1/Tu20 (Ch:46)</td>
<td>Exit down</td>
</tr>
<tr>
<td>4:</td>
<td>12:44:42 (PST) 03/30/2015</td>
<td>ISP1/100.10.1.1/Tu10 (Ch:41)</td>
<td>Exit down</td>
</tr>
<tr>
<td>5:</td>
<td>12:44:13 (PST) 03/30/2015</td>
<td>ISP1/100.10.3.1/Tu10 (Ch:44)</td>
<td>Exit down</td>
</tr>
</tbody>
</table>

Additional References for Path Preference Hierarchy

<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>
### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</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>
</tbody>
</table>
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 165
- Information About PfRv3 Remote Prefix Tracking, on page 166
- How to Display Site Prefixes, on page 170
- Additional References for PfRv3 Remote Prefix Tracking, on page 175

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>
<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, 15.6M2, 15.5.3M6, 15.7M, 16.3.5, and Cisco IOS XE Everest 16.6.1.</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: <strong>show domain default vrf</strong>.</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 learnt 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`
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>L</td>
<td>51.1.0.4/32</td>
<td>Local</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
<td>YES</td>
</tr>
<tr>
<td>C</td>
<td>51.1.0.0/16</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>52.1.0.0/16</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>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>D</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 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
```

<table>
<thead>
<tr>
<th>Codes:</th>
<th>L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area</td>
</tr>
<tr>
<td></td>
<td>N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2</td>
</tr>
<tr>
<td></td>
<td>E1 - OSPF external type 1, E2 - OSPF external type 2</td>
</tr>
<tr>
<td></td>
<td>i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2</td>
</tr>
<tr>
<td></td>
<td>ia - IS-IS inter area, * - candidate default, U - per-user static route</td>
</tr>
<tr>
<td></td>
<td>o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP</td>
</tr>
<tr>
<td></td>
<td>a - application route</td>
</tr>
<tr>
<td></td>
<td>+ - replicated route, % - next hop override, p - overrides from PfR</td>
</tr>
</tbody>
</table>

---

**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>Local</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>Local</td>
<td>10.20.2.1</td>
<td>10.20.2.2</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>B</td>
<td>10.10.3.0/24</td>
<td>Local</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>Local</td>
<td>10.20.2.1</td>
<td>10.20.2.2</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>B</td>
<td>10.15.1.0/24</td>
<td>Local</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>10.15.2.0/24</td>
<td>Local</td>
<td>10.20.2.1</td>
<td>10.20.2.2</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>L</td>
<td>10.20.1.32</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>L</td>
<td>10.20.2.32</td>
<td>Local</td>
<td>10.20.2.1</td>
<td>0.0.0.0</td>
<td>28</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>10.20.0.0/24</td>
<td>Local</td>
<td>10.20.2.1</td>
<td>0.0.0.0</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.1.32</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>C</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>10.20.1.0/24</td>
<td>Remote</td>
<td>10.20.2.1</td>
<td>10.20.0.1</td>
<td>28</td>
<td>Ethernet0/2.30</td>
</tr>
<tr>
<td>L</td>
<td>10.20.2.32</td>
<td>Local</td>
<td>10.20.2.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.32</td>
</tr>
<tr>
<td>D</td>
<td>10.20.2.0/24</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>10.30.1.0/24</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>10.20.2.1</td>
<td>10.20.2.2</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

B1MCRB# 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 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 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 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 10.20.0.0/24</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 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 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 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 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 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 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 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>

B1MCRB# 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 Prefix</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
</table>

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
B1MCRB# show domain default vrf green master route-import border 100.20.1.1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, L - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Enterprise Prefix List:
Prefix: 100.20.0.0, Mask: 16
Prefix: 100.30.0.0, Mask: 16
Prefix: 100.0.0.0, Mask: 8

<table>
<thead>
<tr>
<th>Proto Prefix</th>
<th>IF-Rule</th>
<th>Location</th>
<th>BR-IP</th>
<th>Next-Hop</th>
<th>Index</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L 10.20.1.1/32</td>
<td>Remote 100.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C 10.20.1.0/24</td>
<td>Remote 100.20.1.1</td>
<td>0.0.0.0</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L 51.1.0.4/32</td>
<td>Remote 100.20.1.1</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C 51.1.0.0/16</td>
<td>Remote 100.20.1.1</td>
<td>0.0.0.0</td>
<td>24</td>
<td>Tunnel10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D 52.1.0.0/16</td>
<td>Remote 100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D 52.1.0.0/16</td>
<td>Remote 100.20.1.1</td>
<td>51.1.0.2</td>
<td>24</td>
<td>Tunnel10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 10.10.1.0/24</td>
<td>Remote 100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 10.10.3.0/24</td>
<td>Remote 100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 10.15.1.0/24</td>
<td>Remote 100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B 10.30.1.0/24</td>
<td>Remote 100.20.1.1</td>
<td>10.20.1.2</td>
<td>25</td>
<td>Ethernet0/1.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D 100.10.0.0/16</td>
<td>Remote 100.20.1.1</td>
<td>10.20.0.2</td>
<td>29</td>
<td>Ethernet0/2.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D 100.10.0.0/16</td>
<td>Remote 100.20.1.1</td>
<td>51.1.0.2</td>
<td>24</td>
<td>Tunnel10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
Step 2  show domain default vrf vrf name master route-import interface

Use this command to view the prefix information associated with an interface.

Example:

Router# show domain default vrf green border local-prefix interface Ethernet0/0.10

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, H - NHRP

Local -- Prefix learned over LAN. Remote -- Prefix learned over WAN.
Prefix Interface BR IP Index Prefix-site Proto Next-Hop Status
----------------------------------------------------------------------
100.10.4.1/32 Ethernet0/0.10 100.20.1.1 12 Local C Up

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

Use this command to view the prefix information associated with an border router.

Example:

Router# show domain default vrf green master local-prefix border-ip 100.20.1.1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, H - NHRP

Local -- Prefix learned over LAN. Remote -- Prefix learned over WAN.
Prefix Interface BR IP Index Prefix-site Proto Next-Hop Status
----------------------------------------------------------------------
100.10.4.1/32 Ethernet0/0.10 100.20.1.1 12 Local C

Additional References for PfRv3 Remote Prefix Tracking

<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>
CHAPTER 12

PfRv3 Per Interface Probe Tuning

The PfRv3 Per Interface Probe Tuning feature provides the flexibility to specify different profiles for a channel associated with an interface thereby allowing you to measure the metrics of a channel.

- Feature Information for PfRv3 Per Interface Probe Tuning, on page 177
- Prerequisites for PfRv3 Probe Reduction, on page 178
- Restrictions for PfRv3 Per Interface Probe Tuning, on page 178
- Information About PfRv3 Per Interface Probe Tuning, on page 178
- How to Configure PfRv3 Per Interface Probe Tuning, on page 180
- Configuration Examples for PfRv3 Per Interface Probe Tuning, on page 182
- Additional References for PfRv3 Per Interface Probe Tuning, on page 182

Feature Information for PfRv3 Per Interface Probe Tuning

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

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

Table 22: Feature Information for PfRv3 Per Interface Probe Tuning

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Per Interface Probe Tuning</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The PfRv3 Per Interface Probe Tuning feature provides the flexibility to specify different profiles for a channel associated with an interface thereby allowing you to measure the metrics of a channel. The following commands were introduced or modified: domain smart-probe, smart-probe, show platform hardware qfp active feature pfvr3, show platform software pfvr3.</td>
</tr>
</tbody>
</table>
Prerequisites for PfRv3 Probe Reduction

Restrictions for PfRv3 Per Interface Probe Tuning

- The profile parameters must be defined or enforced on all border hub routers. Configuring the profile on a hub master controller does not propagate the profile parameters to the border hub routers.

- The default data expiration value for a channel is 90 seconds.

- You must configure the Performance Routing v3 Zero SLA Support feature on the hub border router to suppress nonzero DSCP (Differentiated Services Code Point) channels.

Information About PfRv3 Per Interface Probe Tuning

Probe Reduction and Per Interface Probe Tuning

Probing helps in measuring the metrics of a channel. A “profile” is a set of probing parameters configured on a device to send a probe packet on a channel that must be monitored. Before sending a probe packets on a channel, the channel that is to be monitored must be understood because each monitor has different profiles. In most cases, there are two monitors—default and quick. Each probe has two parameters, namely, burst packets and burst interval, which can be configured to define the probe packets sent on a PfR channel.

The PfRv3 Probe Reduction feature allows reducing traffic probe on channels that do not carry any traffic. For more information see the PfRv3 Probe Reduction module.

The PfRv3 Probe Reduction feature enforces similar probing on all interfaces irrespective of an interface through which a channel goes out, whereas the PfRv3 Per Interface Probe Tuning feature provides the flexibility to enforce different profiles on channels associated with an interface.

How Per Interface Probe Tuning Works?

The PfRv3 Per Interface Probe Tuning feature is configured on border hub routers via the profile-id argument in the smart-probes command and applied to an interface via the domain smart-probe profile command.

If you do not configure these commands, the default profile 0, is set on a device. The default profile has predefined parameters of 1 packet every 1 second for a default monitor and 20 packets every 1 second for a quick monitor.

The following is a sample topology to explain the working of the PfRv3 Per Interface Probe Tuning feature.
A hub branch router communicates to two branch routers Branch 1 Router and Branch 2 Router via ISP. Branch 1 Router has a regular interface, while Branch 2 Router has an Long-Term Evolution (LTE) interface. The LTE interface requires different probing parameters on the channel connected to the interface as LTE radio channels are established when data needs to be transmitted over the interface and radio frequency band occupies the transmission.

The profile parameters for the LTE interface are 100 packets every 1200 seconds for default monitor and default values for quick monitor. The profile parameters for the regular interface is the default parameters, which is, one packet every one second for default monitor and 20 packets every one second for quick monitor.

The hub border router establishes channels through its WAN interface to Branch 1 Router and Branch 2 Router via the ISP. Based on the defined profile parameters, channels from the hub border router to the Branch 1 Router are probed at regular intervals. Channels from the hub border router to Branch 2 Router will have not have incoming probes for 19 minutes. The following happens before data is transmitted to the LTE interface:

- Burst probe packets are sent over the channel to measure the metrics.
- The burst interval range is increased to allow a longer duration so that radio bandwidth is not stagnated.
- Unreachable probe packets are not sent after sending the burst probe packets. This is to free up the radio bandwidth to transmit the data.
- The burst interval range is configured to a longer duration so that radio bandwidth is not occupied.
- Unreachability detection is suppressed to ensure that there is no unreachability from a remote device for a period of time.
Profile—Channel Association

The profiles are associated with the channel and not the interface because it is possible that the same interface may host different channels, especially on border hub routers. If two channels have different profile numbers, the channel with a higher profile number is chosen to transmit data. The profile negotiation rule requires a profile with higher ID number to have a slower probing rate. The default profile (one packet every one second for default monitor and 20 packets every one second for quick monitor) has sufficient probing rate. When a channel probes at a slower rate (bigger profile ID number) another channel in the network probes at a higher rate (smaller profile ID number).

Note
There is no automatic detection mechanism to calculate the rate of different profiles if the profile negotiation rule (higher-ID-slower-rate) is violated.

How to Configure PfRv3 Per Interface Probe Tuning

Defining a Profile on a Border Hub Router

```plaintext
domain  domain1
  border
    advanced
      smart-probe 1 burst quick 10 packets every 20 seconds 1
```

Applying a Profile to an Interface on a Border Hub Router

```plaintext
interface tunnel 100
  domain smart-probe profile 1
```

Verifying Profile Parameters

The following is a sample output of the `show platform software pfrv3` command that displays the profile parameters applied to an device:

```plaintext
HubBr2# show platform software pfrv3 rp active smart-probe
PfRv3 smart probe parameters :
  Profile ID: 0
  Attribute: 0x0000
  Probe Burst interval: 1 second
  Probe Burst number: 1 packets
  Quick Monitor Probe Burst interval: 1 second
  Quick Monitor Probe Burst number: 20 packets
  Unreachable interval: 4 second
  Profile ID: 1
  Attribute: 0x0000
  Probe Burst interval: 0 second
  Probe Burst number: 0 packets
  Quick Monitor Probe Burst interval: 0 second
  Quick Monitor Probe Burst number: 0 packets
  Unreachable interval: 4 second
  Profile ID: 2
  Attribute: 0x0000
```
Verifying Profile Parameters Associated with a Channel

The following is a sample output of the `show platform hardware qfp` command that displays the profile parameters associated with a channel:

```
Branch100# show platform hardware qfp active feature pfrv3 client channel id 7 detail
Chan id: 7 tbl-id: 0, if_h: 14(Tunnel100), site-id: 10.3.1.1, in_uidb: 65528, dscp: 0, pfr-label: 0:0 | 0:0 [00000000]
  Supports zero-sla: Yes
  Muted by zero-sla: No
  Plr rx state: No
  Plr tx state: No
  Plr establish state: No
  next hop: 100.1.1.1
  State: Discovered and open
  rx state: Reachable
  tx state: Reachable
  Smart Probe in Burst: No
  Unreach Probing only: Off
  Profile_ID: 0
  V4 Smart Probe Received: Yes
  V4 Smart Probe Sent: Yes
  Current profile_id: 1 <<< different than "Profile ID" (two lines above), resulted from negotiation
  Remote profile_id: 1
  hash val: 25699
  exmem info:
    PPE addr: 0xebd26000
  stats:
    RX pkts: 0  bytes: 0
    TX pkts: 0  bytes: 0
    Blackhole pkts: 0  bytes: 0
    Loop pkts: 0  bytes: 0
    Probes: rx: 6288 tx: 474
    Number of SMP Profile Bursts sent: 100
    Number of Active Channel Probes sent: 374
    Number of Reachability Probes sent: 0
    Number of Force Unreaches sent: 0
    Last Probe rx: 44115 ms Ago
    Last Probe tx: 3379 ms Ago
```
Configuration Examples for PfRv3 Per Interface Probe Tuning

Additional References for PfRv3 Per Interface Probe Tuning

### Related Documents

<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>
<tr>
<td>Probe Reduction</td>
<td>PfRv3 Probe Reduction</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
</table>
CHAPTER 13

PfRv3 Inter-DC Optimization

The PfRv3 Inter-DC (IDC) Optimization feature optimizes traffic between hub and transit hub sites over a WAN overlay or a DCI overlay. A path-preference policy specific to inter-DC Optimization is used for optimizing traffic between two or more hub sites. The PfRv3-Inter-DC-Optimization routs traffic from a hub site to another hub site for specific traffic types such as data, voice, video, and so on.

- Feature Information for PfRv3 Inter-DC Optimization, on page 183
- Prerequisites for PfRv3 Inter-DC Optimization, on page 183
- Limitations and Guidelines for Inter-DC Optimization, on page 184
- Information About PfRv3-Inter-DC-Optimization, on page 184
- How to Configure PfRv3-Inter-DC-Optimization, on page 186
- Additional References for PfRv3-Inter-DC-Optimization, on page 190

Feature Information for PfRv3 Inter-DC Optimization

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PfRv3 Inter-DC Optimization</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The following commands were introduced or modified: domain, inter-dc, interdc-path-preference.</td>
</tr>
</tbody>
</table>

Prerequisites for PfRv3 Inter-DC Optimization

- Hub sites must be upgraded for using the same version of IOS for the master and border devices.
- Static NHRP mapping must be used between hub sites. (NHRP shortcuts are not allowed between hub sites)
• Local LAN prefixes on each hub site (all borders) must have a specific route pointing to LAN interfaces and not to DCI or WAN interfaces.

**Limitations and Guidelines for Inter-DC Optimization**

• The PfRv3 Inter-DC Optimization does not optimize routes using common prefixes.

  **Note**
  
  A common prefix is a prefix which is configurared as a static prefix on all the hub sites, that include hub sites and transite hub sites.

• The command `domain dci-path` should be added in DCI tunnel interface, but normal WAN interface with `domain path` command can also be chosen as DCI path. But DCI interface using `domain dci-path` cannot be chosen as the path for normal hub to spoke traffic.

• We recommend to use static configuration under DCI tunnel interface to set up peer between DC sites. If `nhrp shortcut` is used, a forwarding loop may occur.

• After enabling the IDC feature using the inter-dc command, you can configure `path-preference` and `interdc-path-preference` under policy.

  **Note**
  
  You should not configure DCI path in `global path-preference` because if you add DCI path into path-preference, there is no channel available between hub and spoke in the DCI path. The DCI path cannot be chosen for the normal traffic-classes.

• The IDC feature must be enabled on both peer masters. It is recommended to use the same overlay routing protocol for all WAN and DCI tunnels.

**Information About PfRv3-Inter-DC-Optimization**

**Datacenter Optimization**

The following figure illustrates the PfRv3 Inter-DC Optimization feature where traffic between hub sites DC1, DC2 and DC3 are routed to forward specific traffic through a specific hub. The figure shows four paths that can be used as candidates for the traffic from DC1 to DC2. IDC1 and IDC2 are Inter-DC links that can be used for this traffic. MPLS and INET are normal WAN paths that can also be used for this traffic as candidates. It depends on the path-preference policy specific to inter-DC optimization.
The PfRv3 Inter-DC Optimization feature can be enabled with the `inter-dc` command in domain master controller advanced mode. All hubs in the network must be connected through WAN overlay or DCI overlay. All hub and transit hub masters must be enabled with this feature locally. WAN overlay is configured by defining a WAN interface using the `domain path` command. DCI overlay is configured by defining a DCI interface using the `domain dci-path` command.

The salient points of the PfRv3 Inter-DC Optimization feature are as follows:

- The `domain dci-path` command enables route control which routes the transit traffic on all DCI interfaces in ingress direction.

- Traffic classes are learnt based on the egress aggregate update and traffic channels over the WAN and DCI overlay.

- Tunnel addresses and path ID mapping are exchanged by site capability between the hub and transit masters.
DCI Path Options

Based on the actual deployment requirement, you can choose any of the following options for providing the DCI path:

**Using the existing DMVPN overlay and the same tunnel interface:**

In the hub to spoke DMVPN tunnel interface configuration, there is no dmvpn peer between DC sites. So, if the normal hub tunnel interface is used as DCI path, some additional configuration should be added to set up the dmvpn peer between DC sites, such as ip nhp nhs 161.1.0.5 nbma 155.155.155.5 multicast above.

**Using an independent DCI link(s) with independent DMVPN overlay**

When there is dedicated DCI links between DC sites, a dedicated DMVPN overlay can be used as DCI path. And ideally, the dedicated DCI links are more stable than the normal WAN links. Using the existing hub to spoke DMVPN, or using a dedicated DCI DMVPN built over dedicated DCI links will depend on the available interfaces in the network, and which solution will meet the need of the network.

A third option of building a second set of DMVPN tunnels using the same transport as the existing DMVPN hub and spoke network is not recommended and it has not been validated.

How to Configure PfRv3-Inter-DC-Optimization

**Specifying the DCI interface on a Hub Site**

```config
enable
configure terminal
interface tunnel155
  domain dci-path DCI path-id 11
exit
```

**Configuring Inter-DC on Hub Master Controller**

To configure the Inter-DC Optimization feature on the hub master controller, use the following commands:

```config
enable
configure terminal
domain default
vrf green
master hub
  source-interface Loopback1
  site-prefixes prefix-list HUBPFX
```
Configuring Inter-DC on Transit Hub

To configure Inter-DC on the transit hub, use the following commands:

```
enable
configure terminal
domain default
vrf green
master transit 2
source-interface Loopback1
site-prefixes prefix-list HUBPFX
hub 100.10.1.1
advanced
inter-dc
class BUSINESS sequence 10
interdc-path-preference DCI1 fallback MPLS next-fallback INET
exit
```

Specifying IDC Local Policy

This is an optional task to overwrite the global path-preference.

```
enable
configure terminal
domain default
vrf green
master transit 2
class BUSINESS sequence 10
interdc-path-preference DCI1 fallback ISP1 next-fallback ISP2
exit
```

Verifying Inter-DC Configuration

```
HMCBR# show domain default vrf green master status
*** Domain MC Status ***
Master VRF: green
Instance Type: Hub
Instance id: 1
Operational status: Up
Configured status: Up
Loopback IP Address: 100.10.1.1
Global Config Last Publish status: Peering Success
Smart Probe Profile:
  General Monitor:
    Packets per burst: 1
    Interval (secs): 1
  Quick Monitor:
    Packets per burst: 20
    Interval (secs): 1
```
Verifying Master Controller Configuration

Verifying the Channel Status
Example Configurations for PfRv3 Inter-DC

Example for Policy Configured on the Hub MC with Inter DC

In this example, the policy can work on the normal hub-spoke traffic and the IDC traffic. For IDC traffic, the ‘interdc-path-preference’ takes effect. DCI1 and DCI2 are primary paths. If they are out-of-policy, the MPLS, which is a backup path, will be used. For normal hub-spoke traffic, the ‘path-preference’ takes effect. The other configuration is same as normal PfRv3 policy. For example, the threshold of delay is 100 ms for both the IDC traffic and the normal hub-spoke traffic.
class BUSINESS sequence 10
  match dscp ef policy custom
  priority 1 one-way-delay threshold 100
  path-preference MPLS fallback INET
  interdc-path-preference DCI1 DCI2 fallback MPLS next-fallback INET

Example for Policy Configured on the Transit Hub MC with Inter DC

On transit hub master, you can see the same policy. But, if the interdc-path-preference is configured on this transit hub. The local interdc-path-preference will overwrite the policy from hub site

```plaintext
class BUSINESS sequence 10
  interdc-path-preference DCI1 fallback MPLS next-fallback INET
```

Example for 'show domain vrf master policy' on hub master

```
Global-policy-list:

  class BUSINESS sequence 10
    path-preference MPLS fallback INET
    class type: Dscp Based
    match dscp ef policy custom
    priority 1 one-way-delay threshold 100 msec

InterDC-policy-list:

  class BUSINESS sequence 10
  interdc-path-preference DCI1 DCI2 fallback MPLS next-fallback INET
  class type: Dscp Based
  match dscp ef policy custom
  priority 1 one-way-delay threshold 100 msec
```

Additional References for PfRv3-Inter-DC-Optimization

### Related Documents

<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 commands</td>
<td>Cisco IOS Performance Routing Version 3 Command Reference</td>
</tr>
</tbody>
</table>
Direct Cloud Access

The Direct Cloud Access IWAN 2.3 feature enables users at branch sites to have best application experience to SaaS applications, such as, Office 365, Google services, with reduced cost. This feature helps in constantly monitoring network and application performance and select the optimized paths (usually local break out from branch to Cloud SaaS applications instead of back-haul to the data center). Non-SaaS traffic still back-haul to data center for further inspection.

- Feature Information for Configuring Direct Cloud Access, on page 191
- Prerequisites for Configuring Direct Cloud Access, on page 192
- Restrictions for Configuring Direct Cloud Access, on page 192
- Information About Configuring Direct Cloud Access, on page 193
- How to Configure Direct Cloud Access, on page 197
- Configuration Examples for Configuring Direct Cloud Access, on page 200
- Additional References for Configuring Direct Cloud Access, on page 210

Feature Information for Configuring Direct Cloud Access

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

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

Table 24: Feature Information for Direct Cloud Access IWAN 2.3

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Cloud Access IWAN 2.3</td>
<td>Cisco IOS XE</td>
<td>The Direct Cloud Access (DCA) feature allows traffic from trusted applications, part of well-trusted domains, to pass the local Internet security check because traffic from these trusted applications have a lower security risk than untrusted Internet sites. The following commands were introduced or modified: <strong>domain path, path-preference, show domain dca-status, show domain default border, show domain default policy, show domain vrf border channels, show domain vrf master channels.</strong></td>
</tr>
<tr>
<td></td>
<td>Fuji 16.8.1</td>
<td></td>
</tr>
</tbody>
</table>
### Feature Information

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Direct Cloud Access Phase 2| Cisco IOS XE Gibraltar 16.10.1   | Simplification of configuration, automatic configuration of Cisco Umbrella Branch component.  
|                            |                                  | The following commands were introduced or modified:                              
|                            |                                  | `dca-probe-http-interval`, `dns-redirect`, `policy local type dca`, `show domain master dca domain-map`, `show domain vrf master dca status`, `umbrella in direct-cloud-access default` |

### Prerequisites for Configuring Direct Cloud Access

- **NAT:**
  
  To enable a host that typically operates in a private network directly communicate with a SaaS application in a public network, use a NAT. Enable NAT on the same router that has DCA enabled or other devices in the path.

- **Firewall security:**
  
  To improve security, you can enable a firewall, such as a zone-based firewall (ZBFW), in the path.

**Note**

By default OpenDNS is used as DNS resolver for SaaS traffic, but you can choose to use other DNS resolver such as Google DNS resolver 8.8.8.8. OpenDNS license/registration is not a must if you don't need OpenDNS security services.

### Restrictions for Configuring Direct Cloud Access

- **IPv6 address is not supported.**

- **DCA is not supported if the DNS traffic does not pass through the router which is enabled with DCA.**

- **DCA does not work if SaaS applications use proxy.** All traffic going to proxy server as DCA may not classify these applications and cannot perform local breakout for traffic that is bound to proxy.

- **Applications that directly access the content and not through DNS resolution, NBAR may fail to classify as SaaS and cannot provide local break-out.**

- **DCA may not work on a device when NBAR classification results are not available on the device.** You must customize NBAR to classify the results to support DCA.

- **This feature depends on applications classification.** SD-AVC helps in better classification with NBAR.
Information About Configuring Direct Cloud Access

Direct Cloud Access Overview

The infrastructure of cloud-hosted services, such as Microsoft Office 365 and Google Apps, is in the cloud. Back-hauling traffic from remote users and sites through the private WAN to the data center via Internet imposes additional bandwidth requirements on the private WAN and may add latency to each connection. Moreover, private WAN connectivity is more expensive than direct Internet connections, which could add a tremendous amount of cost to the equation.

The Direct Cloud Access IWAN 2.3 feature implements direct cloud access (DCA) on Cisco IWAN networks and allows trusted SaaS traffic to be forwarded out over the optimized path (directly local break out) while other traffic still back-haul to headquarters over VPN. DCA monitors the candidate path (DCA path, back-haul path to headquarters) performance and chooses the optimized path in policy to get the best SaaS application performance. While adding direct Internet connectivity to the branch site without back hauling to data center, IWAN DCA provides the security capability at branch site by enabling security features like NAT and Firewall (Zone-based Firewall, Snort IPS, etc.) at branch sites.

Features

DCA features include:

• Automatic configuration of Cisco Umbrella Connector (supported from Cisco IOS XE Gibraltar 16.10.1)

• Support for policy configured on a centralized hub, or per-site customized local policy
  • Customized local policy overrides global policy.
  • If a hub connection goes down, local policy remains in effect.

• Support for P2P interface, such as dialer interface, as DCA interface

Benefits of Direct Cloud Access

• Reduced operation cost as SaaS traffic no longer needs to go to headquarters which consume additional headquarters network bandwidth.

• Business processes run faster through direct network access to the major cloud providers. A traffic classification mechanism is required in order to achieve direct Internet access for selected cloud applications.

Direct Cloud Access Architecture

The overlay DMVPN WAN tunnels on a branch router are configured to dynamically learn the service provider they are connected to. An underlay interface is identified as a direct access interface via configuration.

Packets from the LAN side on a branch site are sent over the overlay when packets do not match the criteria of the configured application. When a flow matches the DCA criteria, the packets are directed to the DCA interface that is specified in the path preference. DCA interfaces can be listed in the order of priority in the
path preference configuration of the policy for the application. The DCA interfaces are evaluated in the order of the configured path preference priority.

NBAR classification occurs at LAN ingress. NBAR provides the application ID, which is exported by the border router. If a match occurs on the Master Controller for an application, the policy for the application is applied to the traffic class for the specific flow.

The following figure explains the DCA functionality for Office365 application:

*Figure 17: DCA for Office365*

The following actions are performed to achieve DCA functionality:

- Classify all the cloud applications based on the DNS.
- Intercept DNS traffic and make decisions based on the classification.
  - If the traffic is from a trusted application, direct Internet access is provided. Ensure that security concerns are addressed for the breakout traffic, which include, constant application monitoring, choosing network performance over candidate paths (DCA path, back-haul path), selecting the optimized path according to policy (if DCA path is not good), back-hauling SaaS traffic to data center and reverting back if DCA path recovered.
  - If the traffic is not from a trusted application, the traffic is passed it to the Headquarter for further security inspection and processing.
- Route HTTP, HTTPS data traffic to Internet or Headquarter depending on the above decision.

**Designate an Underlay Interface as Direct Access Interface**

An interface of the border router must be designated as direct access interface. `domain path path-name direct-cloud-access` command to specify the direct access interface. A service provider may have multiple links of direct access and each of the direct access interface is measured independently.
When an interface is selected to be the direct access interface, all traffic to the whitelisted applications is directed through the direct access interface. If there are multiple direct access interfaces, the traffic is directed on one direct access interface depending on the performance metrics and policy.

**Direct Cloud Access Components**

Direct Cloud Access functionality has the following components:

**Cisco Umbrella Connector**

To achieve location proximity, the SaaS server must be closer to the branch router to achieve better application performance. Generally, DNS requests for a SaaS application are destined to an enterprise DNS resolver. However, the DNS request must be changed from enterprise DNS resolver to a public DNS resolver, such as, OpenDNS resolver or Google DNS resolver. The public DNS resolver helps in placing the SaaS server closer to the branch router by using Cisco Umbrella connector. OpenDNS account and registration is not mandatory.

**Note**

Beginning with Cisco IOS XE Gibraltar 16.10.1, the Cisco Umbrella connector component is configured automatically to redirect SaaS DNS requests to a public DNS server. You can also configure Umbrella connector manually; manual configuration overrides auto configuration.

DNS requests must be unencrypted traffic from the endpoint to the DNS server. Each direct access interface must be configured with Open DNS.

**NBAR Classification**

Network Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. NBAR uses several classification information metadata such as application name, ID, traffic class, business relevance, and so on.

For Direct Cloud Access functionality, once NBAR recognizes the DNS traffic as belonging to interesting cloud application, it attaches this information to DNS packet in a way so that the umbrella connector feature can extract and use the information.

Cisco NBAR provides the first packet classification for some applications. Cisco NBAR uses DNS learning for application recognition of user defined and predefined domains. Once the server is learned from the DNS response, traffic going to this server can be classified as FIFO. SD-AVC also improves the first packet classification result.

**Performance Routing Version 3**

Performance Routing version 3 (PfRv3) delivers intelligent path control for application-aware routing across the WAN. Once a DNS response is received, the data traffic (HTTP, HTTPS etc.) from cloud application is provided direct Internet access (local break-out) or is sent to the headquarter for further security inspection.

**IPSLA**

IPSLA is enabled automatically by PfRv3 to probe each SaaS application over candidate paths by using IPSLA HTTP operation. PfRv3 leverages the metrics reported by IPSLA to select the optimized path.
SaaS Reachability and Performance Management

Performance and reachability of each whitelisted application determines the path that an application takes. PFR measures the reachability and performance of all VRFs and enables and shares one measurement across multiple VRFs.

Next-Hop Reachability

One DSCP-agnostic channel is created as the next-hop for the direct access interface. The DSCP of DCA channel is configured as FF. The routing protocol configured on the direct access interface determines the next hop for the channel.

Performance Measurement

After the channel next hop is up, the service is reached via next hop by using the following steps:

Application Domain Mapping

Application to domain URL and Differentiated Services Code Point (DSCP) mapping must be configured on the master controller of each branch router so that IPSLA can measure the SaaS application using right domain and DSCP.

Reachability and Performance Probing

Measuring network characteristics is performed using IPSLA. IPSLA probes are not sent per VRF, instead, PFR creates a probing layer for all the VRFs and path preferences in the VRFs in a domain. Reachability and performance can be verified per application by using the `show domain domain-name border dca` command. This command provides information per application, per interface for a border router.

Traffic Steering and Flow Stickiness

When DCA is implemented on a network, traffic classes are automatically created for interested applications. The applications configured in the policy includes path preferences, which corresponds to the respective DSCP configured per application.

When selecting a path, PFR assigns a path to a flow that is destined to a service, for example, Office365. These flows might traverse a NAT device or a firewall device that maintains the state for the flow sequence numbers. Changing the flow during packet traversal may lead to flow reset. Therefore, when a path is selected, flows must align to that path only. If a path is unreachable, the flow is reset by the client and retried. If the path experiences packet loss but still usable, new flows are routed via alternate paths.

Local Policy Configuration

Direct Cloud Access (DCA) policy can be configured on a centralized hub, or it can be configured on any individual site as a customized local policy. To configure local DCA policy, use the `policy local type DCA` command.

- Customized local policy overrides global policy.
- If a hub connection goes down, local policy remains in effect.
Example of Local Policy Configuration

```
policy local type DCA
  class DCA sequence 4
    match application ms-cloud-group saas-dca
    path-preference DCA1 fallback DCA2
```

How to Configure Direct Cloud Access

Assign an Underlay Interface as Direct Access Interface

The following configuration snippet explains how to assign an Ethernet interface as direct access interface.

```
Router(config)# interface Ethernet 0/1
Router(config-interface)# domain path ATT-DCA direct-cloud-access
```

Define PfR Policy for SaaS Application on Hub Master Controller

The following configuration snippet explains how SaaS application policies are defined on hub master controller at a central point and published to all branch sites. There is no need to define policies at each branch sites because branch sites still have the capability to customize the interested SaaS.

```
Router(config)# domain iwan Router
Router(config-domain)# vrf green
Router(config-domain-vrf)# master hub
Router(config-domain-vrf-master)# class BUSINESS-CRITICAL sequence 10
Router(config-domain-vrf-master-class)# match app-group ms-cloud-group policy saas-dca
Router(config-domain-vrf-master-class-match)# exit
Router(config-domain-vrf-master-class)# path-preference ATT-DCA fallback ATT next-fallback INET
```

Define SaaS Application Mapping on Branch Master Controller

To measure the SaaS application’s reachability and performance, the domain URL and DSCP must be specified for IPSLA probing for each SaaS application.

Use HTTP ping to probe a specific SaaS to determine reachability and performance. The system has built-in default URL domains for popular SaaS applications. For a complete list, use `show domain xxx master dca domain-map`.

**Note**

If there are multiple VRFs, IP SLA probing is performed for all domains defined for each VRF and the same IP SLA ID is used for each domain group in the VRF.

If a desired SaaS is not included in the list, create a domain map for the service in PfRv3. For example, to add Servicenow:

```
master branch
domain-map
  application servicenow-group domain http://www.servicenow.com dscp af21
```
Configure a DNS Resolver

By default, DNS requests for white-listed SaaS are intercepted by Umbrella, and the OpenDNS resolver is used to achieve location proximity.

Optionally, configure a specific DNS resolver, either on a hub master controller or on an specific branch master controller. Configuring a DNS resolver on a specific branch overrides, for that branch, the DNS resolver configured on the hub.

**Hub**

Use the following on a hub master controller to configure a DNS resolver for all DCA branches.

```
domain default
  master hub
  advanced
    dns-redirect dns-server-address
```

**Example:**

```
domain default
  master hub
  advanced
    dns-redirect 8.8.8.8
```

**Branch**

Use the following on a branch master controller to configure a DNS resolver for the branch, overriding the hub setting.

```
domain default
  master branch
  dns-redirect dns-server-address
```

**Example:**

```
domain default
  master branch
  dns-redirect 8.8.8.8
```

Configure the HTTP Ping Probe Interval

The HTTP ping probe uses a default probe interval of 30 seconds.

Optionally, you can configure a specific interval on the hub master controller, which applies the change to all DCA branches, or to a branch master controller, to change the interval for a specific branch.

**Hub**

Use the following on a hub master controller to configure the interval for all DCA branches.

```
domain default
  master hub
  advanced
    dca-probe-http-interval interval-in-seconds
```

**Example:**

```
domain default
  master hub
```

advanced
  dca-probe-http-interval 20

Branch

Use the following on a branch master controller to configure the interval for a specific branch. The branch setting overrides a setting made at the hub.

```
domain default
  master branch
    dca-probe-http-interval interval-in-seconds
```

Example:

```
domain default
  master branch
    dca-probe-http-interval 20
```

Verify and Monitor Direct Cloud Access Configuration

Use the following commands to verify and monitor DCA configuration.

- `show domain iwan master traffic-classes summary`
- `show domain iwan master traffic-classes detail`
- `show domain iwan master traffic-classes dca detail`
- `show domain iwan master traffic-classes dca application`
- `show domain iwan master dca domain-map`
- `show domain iwan master dca status`
- `show domain domain-name border dca`

Displays information about reachability and metrics collected for all paths towards a service. This command helps in understanding the behavior of various paths for a service and how PFR is selecting the best paths depending on the metrics.

```
Device# show domain iwan border dca
[*] PFR created IP SLA entry ID
IPSLA DNS Resolver:208.67.220.220
App      DSCP  RTT/ms  DCA2  MPLS1
         thresh  Gi0/0/2   Tu10 (0:1)
         RTT/ms[*]  RTT/ms[*]
share-point default  1000 7 [31]  --
youtube    default  1000  78 [33]  --
box        default  1000 7 [39]  --
dropbox    default  1000 3 [41]  --
google-services default 1000 108 [49]  --
google-group default 1000 109 [51]  --
gtalk-group default 1000 112 [53]  --
hangouts-group default 1000 115 [55]  --
ms-lync-group default 1000 6 [57]  --
ms-cloud-group default 1000 7 [59]  --
```

- `show domain default policy`

Displays the default policy on the master controller.
Device# show domain default master policy
No Policy publish pending

class SOCIAL-NETWORKING sequence 11
class type: Application Based
match application skype policy custom
priority 1 delay threshold 500 msec

- To troubleshoot, use `debug domain default master dca` and `debug domain default border dca` commands.

Configuration Examples for Configuring Direct Cloud Access

Example: Configure DCA Link on a Single Branch Router

Overview

In this example, DCA is configured on Cisco IWAN network with a single branch router as shown in the following topology.

Figure 18: DCA Link on a Single Branch Router

![Diagram of DCA Link on a Single Branch Router](image)

- advertise 0.0.0.0 to single branch router using MPLS DMVPN tunnel.
- DC ASR 1000 to Internet
- Central manager 10.4.221.2
- MPLS BR + MC
- G0/0/1 to G0/0/1
- Internet Tunnel 10 10.6.34.31
- 128.107.246.x Internet
- INET Tunnel 11 10.6.36.31
- 173.36.254.x Internet
- INET
- Single Branch router
- G0/0/0.64
- PC:sw 1/0/4 10.7.130.3
Umbrella Service

Beginning with Cisco IOS XE Gibraltar 16.10.1, the Umbrella service configuration is automatic.

Underlay Interface

DCA is configured on WAN underlay interface in order to distinguish tunnel WAN interface.

```
interface GigabitEthernet0/0/3 ! INET branch WAN DCA interface
domain iwan path DCA1 direct-cloud-access umbrella out
```

Optionally, a second DCA can be created as WAN underlay interface.

```
interface GigabitEthernet0/0/2 ! INET branch DCA2 interface
domain iwan path DCA2 direct-cloud-access umbrella out
```

Create Domain Map

Optionally, create a domain map for a specific SaaS not included by default.

```
master branch
domain-map
application servicenow-group domain http://www.servicenow.com dscp af21
```

Hub Master Controller Configuration

The policy can be local or from a centralized hub master controller. Configure a hub master controller as follows:

```
Note
Configure only one master controller, either at a hub site or a branch site.

domain default
vrf default
master hub

class DCA sequence 4
  match application ms-cloud-group saas-dca
  path-preference DCA1 fallback DCA2
```

Branch 1 and Master Controller Configuration

A branch site can serve as master controller instead of a hub site. In this example, Branch 1 serves as master controller. The configuration includes LAN interface and WAN (DCA) interface.

```
Note
Configure only one master controller, either at a hub site or a branch site.

domain default
vrf default
  border
  master local
  master branch
  source-interface Loopback0
```
LAN interface configuration:

interface GigabitEthernet3.30
description B1MCBR-LAN
capsulation dot1Q 30
ip address 10.20.0.1 255.255.255.0
ip nat inside

Assigning the DCA to a WAN interface:

interface GigabitEthernet2.30
capsulation dot1Q 30
ip vrf forwarding fvrf
ip address 10.20.1.1 255.255.255.0
ip nat outside
domain path DCA1 direct-cloud-access

Branch 2 Configuration

This branch configuration includes LAN interface and WAN (DCA) interface.

domain default
vrf default
border
source-interface Loopback0
master 192.168.3.22

LAN interface configuration:

interface GigabitEthernet3.30
description B1MCBR-LAN
capsulation dot1Q 30
ip address 10.20.0.1 255.255.255.0
ip nat inside

Assigning the DCA to a WAN interface:

interface GigabitEthernet2.30
capsulation dot1Q 30
ip vrf forwarding fvrf
ip address 10.20.1.1 255.255.255.0
ip nat outside
domain path DCA2 direct-cloud-access

Verifying the Configuration

The following commands are used to verify the configuration. To verify OpenDNS configuration, use the show umbrella deviceid and show umbrella configuration commands.

router# show umbrella deviceid

Device registration details
Interface Name Tag Status Device-id
GigabitEthernet3.64 inside-network 200 SUCCESS 010a3d458c172b8b

router# show umbrella configuration

Umbrella Configuration

------------------------
Token: 7772166EF2E473ADE8FA2204B37D0BD7001FE4F5
To verify the DCA configuration, use the following commands:

- `show domain iwan border dca`
- `show domain iwan master dca status`
- `show domain iwan master traffic-classes summary`
- `show domain iwan master traffic-classes detail`
- `show ip sla summary`
- `show ip sla configuration`
- `show ip sla statistics`
- `show flow monitor name flow-monitor cache format table`

Use the `show ip sla summary`, `show ip sla configuration`, and `show ip sla statistics` commands to verify the probe functions.

Use the `show flow monitor` command to verify that the flow is passes through the DCA path.
Example: Configure DCA Link on a Single Branch Router

DCA Internet CN default[0] 28 8388 hangouts-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 27 4692 gtalk-group
d
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 26 4456 google-group
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 25 218104328 google-service
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 21 50349148 dropbox
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 20 218104882 box
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

DCA Internet CN default[0] 17 218103890 youtube
DCA1(0:0|0:0)/10.255.241.31/Gi0/0/3(Ch:6)

Router# show domain iwan border dca

[*] PFR created IP SLA entry ID
IP SLA DNS Resolver:208.67.220.220

App DSCP RTT/ms DCA2 MPLS1
thresh Gi0/0/2 Tu10 (0:1)

share-point default 1000 7 [31] --
youtube default 1000 78 [33] --
box default 1000 7 [39] --
dropbox default 1000 3 [41] --
googles-services default 1000 108 [49] --
googles-group default 1000 109 [51] --
gtalk-group default 1000 112 [53] --
hangouts-group default 1000 115 [55] --
ms-lync-group default 1000 6 [57] --
ms-cloud-group default 1000 7 [59] --

Router# show domain iwan master traffic-classes detail

Dat-Site-Prefix: DCA Application: ms-cloud-group DSCP: default [0] Traffic
class id:30 app_id:9424
Clock Time: 22:13:32 (UTC) 01/17/2018
TC Learned: 4d23h ago
Present State: CONTROLLED
Current Performance Status: not monitored (internet)
Current Service Provider: DCA1 since 4d23h
Previous Service Provider: Unknown
BW Used: 0 bps
Present WAN interface: GigabitEthernet0/0/3 in Border 10.255.241.31
Present Channel (primary): 6 DCA1 pfr-label:0:0 | 0:0 [0x0]
Backup Channel: 4 DCA2 pfr-label:0:0 | 0:0 [0x0]
Destination Site ID: Internet
DNS Primary Channel: 6 DCA1 pfr-label:0:0 | 0:0 [0x0]
DNS Backup Channel: 4 DCA2 pfr-label:0:0 | 0:0 [0x0]
Class-Sequence in use: 55
Class Name: saasapp using policy User-defined
priority 1 one-way-delay threshold 500 msec
BW Updated: - ago
Method for choosing channel: Random
Reason for Latest Route Change: Uncontrolled to Controlled Transition
Route Change History

Router# show ip sla sum
Show IP SLA Configuration

Entry number: 1255
Type of operation to perform: http
Target address/Source address: 216.58.217.164/172.16.1.1
Target port/Source port: 80/0
Type Of Service parameters: 0x0
Vrf Name: IWAN-TRANSPORT-2
HTTP Operation: get
HTTP Server Version: 1.0
URL: http://www.google.com
Proxy:
Raw String(s):
Cache Control: enable
Owner:
Tag:
Operation timeout (milliseconds): 30000
Schedule:
Operation frequency (seconds): 60 (not considered if randomly scheduled)
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Randomly Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 20000

Distribution Statistics:
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20

History Statistics:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None

Show IP SLA Statistics

IPS LA operation id: 1255
Latest RTT: 179 milliseconds
Latest operation start time: 19:09:14 UTC Fri Jan 26 2018
Latest operation return code: OK
Latest DNS RTT: 6 ms
Latest TCP Connection RTT: 62 ms
Latest HTTP Transaction RTT: 111 ms
Number of successes: 29
Number of failures: 0
Operation time to live: Forever

Show Flow Monitor

Router# show flow monitor Monitor-FNF-IWAN cache format table | i office

54.209.129.73  172.31.1.2  80  62102  G10/0/0  /30Null
   6 layer7 ms-office-365  0.0.0.0
   4 0x00
172.31.1.2  52.109.2.14  5110  443  G10/0/2.101

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

Direct Cloud Access
Example: Configure DCA Link on a Single Branch Router
Example: Configure DCA Link on a Dual Branch Router

Overview

In this example, DCA is configured on Cisco IWAN network with a dual branch router as shown in the following topology.

The policy can be local or from a centralized hub. This example illustrates the use of a local policy in a non-IWAN scenario.
Branch 1 and Master Controller Configuration

A branch site can serve as master controller instead of a hub site. In this example, Branch 1 serves as master controller. The configuration includes LAN interface and WAN (DCA) interface.

Configure only one master controller, either at a hub site or a branch site.

domain default
vrf default
  border
    master local
    master branch
    source-interface Loopback0
    hub 100.20.1.1

policy local type DCA
class DCA sequence 4
  match application ms-cloud-group saas-dca
  path-preference DCA1 fallback DCA2
LAN interface configuration:

interface GigabitEthernet3.30
description B1MCBR-LAN
encapsulation dot1Q 30
ip address 10.20.0.1 255.255.255.0
ip nat inside

Assigning the DCA to a WAN interface:

interface GigabitEthernet2.30
encapsulation dot1Q 30
ip vrf forwarding fvrf
ip address 10.20.1.1 255.255.255.0
ip nat outside
domain path DCA1 direct-cloud-access

Branch 2 Configuration

This branch configuration includes LAN interface and WAN (DCA) interface.

domain default
vrf default
border
source-interface Loopback0
master 192.168.3.22

LAN interface configuration:

interface GigabitEthernet3.30
description B1MCBR-LAN
encapsulation dot1Q 30
ip address 10.20.0.1 255.255.255.0
ip nat inside

Assigning the DCA to a WAN interface:

interface GigabitEthernet2.30
encapsulation dot1Q 30
ip vrf forwarding fvrf
ip address 10.20.1.1 255.255.255.0
ip nat outside
domain path DCA2 direct-cloud-access

Example: Configuring Umbrella Branch for OpenDNS

Overview

Beginning with Cisco IOS XE Gibraltar 16.10.1, DCA configures the Cisco Umbrella Connector automatically on the router. However, it is still possible to configure Umbrella manually.

For example, if it is necessary to validate OpenDNS, you must configure Cisco Umbrella Connector on the branch, as shown in the example below.

Procedure

1. Configure the DNS server, setting the router's clock and time zone correctly.
   
   ip domain name cisco.com
   ip host api.opendns.com 67.215.92.210

2. Log into the OpenDNS portal to get an API token.
3. Import the certificate, entering a PEM-formatted CA certificate.

```
(config)# crypto pki trustpool import terminal
```

Enter a PEM-formatted CA certificate.

```
(config)# crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627Kdcis1QtsyS8+8ktTANBgkqhkiG9w0BAQfasDAbh
MQowCQYDVQQGEwJVUzEEMBMGA1UEChMNMRGlnaUNl.cnQg5WJsMRkwFwYDVQQLEwB3
d3cuzLgnaWNlcnQuY29tMTcAwgYDVQQDEwEDEjYzLjIwMjIyMB4xKDAwCAYGCSqG
SIb3DQEJMAkGA1UEBhMGAkIwDASBgNVBAcTIE5Od2VseCB3d3cuZGlnaWNlcnQuY2
9tMRQwEwYDVQQDEwRSVEZkMTYuMjEyMDcyNzE3MjYyNVFUVTIyMjAyGDE3MjYuMj
EyMDcyNzE3MjYyNVFUVTIyMjAyGDE3MjYuMjEyMDcyNzE3MjYyNVFUVTIyMjAyGDE
3d3cuZGlnaWNlcnQuY29tMTcAwgYDVQQDEwEDEjYzLjIwMjIyMB4xKDAwCAYGCSqG
SIb3DQEJMAkGA1UEBhMGAkIwDASBgNVBAcTIE5Od2VseCB3d3cuZGlnaWNlcnQuY2
9tMRQwEwYDVQQDEwRSVEZkMTYuMjEyMDcyNzE3MjYyNVFUVTIyMjAyGDE3MjYuMj
EyMDcyNzE3MjYyNVFUVTIyMjAyGDE3MjYuMjEyMDcyNzE3MjYyNVFUVTIyMjAyGDE
-----END CERTIFICATE-----
```

This is the PEM-formatted version. Keep the "END CERTIFICATE" portion. Without this, the certificate will be lost after a router reloads.

4. (Optional) Configure local domains.

DNS queries directed to a local domain will remain untouched and will not be redirected to OpenDNS cloud.

```
parameter-map type regex dns_bypass
pattern .eisg.cisco.*
```

5. Configure the token.

```
parameter-map type umbrella global
token 0F32C32FEC26991C2B562D3C7FF844EO0001C70E7
```

Cisco OpenDNS is used by default. To use a different DNS resolver, add the following line:

```
resolver ipv4 DNS-server-IP
```
Note
Enter a fake token for this step if you are using another DNS server or do not want to register with OpenDNS server.

6. Assign the above policy to a LAN interface.

   GigabitEthernet0/0/0.100  ! INET branch LAN interface
   umbrella in direct-cloud-access default lan100

7. Assign the Umbrella to a WAN interface.

   interface GigabitEthernet0/0/3  ! INET branch WAN DCA interface
   domain iwan path DCA1 direct-cloud-access
   umbrella out

8. Apply umbrella out on all DCA interfaces. This includes the MPLS branch of a dual branch if the MPLS branch has a DCA interface.

   interface GigabitEthernet0/0/2  ! MPLS branch WAN DCA interface
   domain iwan path DCA2 direct-cloud-access
   umbrella out

   interface GigabitEthernet0/0/0.100  ! MPLS branch LAN interface
   umbrella in direct-cloud-access default lan100

**Additional References for Configuring Direct Cloud Access**

<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>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</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>
</tbody>
</table>
Chapter 15

Channel-based Metrics Measurement

Channel-based metrics measurement configures the performance monitors used by PfRv3 to employ a data collection method that combines the use of metadata and traffic sampled at intervals to provide traffic metrics.

• Feature Information for Channel-based Metrics, on page 211
• Prerequisites for Channel-based Metrics Measurement, on page 211
• Information About Channel-based Metrics Measurement, on page 212
• How to Configure Channel-based Metrics Measurement, on page 212
• Configuration Examples, on page 213
• Additional References, on page 213

Feature Information for Channel-based Metrics

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>Channel-based measurement of performance metrics</td>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>Configures the performance monitors used by PfRv3 to employ a data collection method that combines the use of metadata and traffic sampled at intervals to provide traffic metrics. New command: channel-based-measurement</td>
</tr>
</tbody>
</table>

Prerequisites for Channel-based Metrics Measurement

• Cisco IOS XE Gibraltar 16.11.1 or later
Information About Channel-based Metrics Measurement

Overview

As part of its intelligent path selection, PfRv3 uses performance monitors to gather traffic metrics. Channel-based measurement typically provides improved accuracy for metrics. The method samples packets in the traffic stream, and uses packet metadata, such as timestamp and sequence information, to generate traffic metrics. This feature uses packet-based loss measurement, not byte-loss.

Channel-based measurement of metrics provides the following benefits:

- Packets of any protocol are acceptable.
- Overcomes inaccuracies caused by methods that aggregate data from individual flows that are carried across different channels.
- Provides better tolerance of out-of-order packets.
- Reduces false threshold crossing alarms (TCAs): Previously, performance metrics have been calculated based on the samples collected in one interval. Typically, a TCA for lost packets is set for about 1% to 2%. In such a case, if there are, for example, only 30 samples in the interval and 1 packet is lost, then the packet loss rate is 3.3% and the TCA is triggered. This would be considered a false TCA because it was triggered by a single lost packet. Channel-based measurement ensures that at least 100 samples (even if these samples must be taken from different intervals) are used to calculate metrics, reducing the occurrence of false TCA.

Migration

During migration of multiple sites to a later Cisco IOS version, it may occur that the hub site and branch sites are upgraded at different times. Migrate the hub site and transit hub site first. After upgrading a hub site, if channel-based-measurement is enabled on the hub site, some branch sites might still be using IOS versions that do not support channel-based-measurement. Channel-based measurement of traffic between two branch sites requires both sites to be using Cisco IOS XE Gibraltar 16.11 or later.

How to Configure Channel-based Metrics Measurement

Channel-based Metrics Measurement Configuration

To configure the channel-based metrics measurement, use:

```bash
config terminal
domain iwan
master hub
advanced
channel-based-measurement
[sampling-rate sampling-rate] [quick sampling-rate-for-quick-monitoring]
```
Configuration Examples

Examples: Channel-based Metrics Measurement

Configure channel-based metrics measurement on a hub master controller, regardless of the number of branch sites.

Enable channel-based measurement for traffic metrics.

```
Device# config terminal
Device(config)# domain iwan
Device(config-domain)# master hub
Device(config-domain-mc)# advanced
Device(config-domain-mc-advanced)# channel-based-measurement
```

Enable channel-based measurement and configure a sampling packet size of 1300 and a sampling rate of 20 samples per second.

```
Device# config terminal
Device(config)# domain iwan
Device(config-domain)# master hub
Device(config-domain-mc)# advanced
Device(config-domain-mc-advanced)# channel-based-measurement
Device(config-domain-mc-advanced-channel-measure)# sample-packet-size 1300
Device(config-domain-mc-advanced-channel-measure)# sampling-rate 20
```

Additional References

References

<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 Pfr 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 documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="https://www.cisco.com/c/en/us/support/index.html">https://www.cisco.com/c/en/us/support/index.html</a></td>
</tr>
</tbody>
</table>
PfRv3 Event Tracing

The Event Trace for PfRv3 feature provides a trace facility for troubleshooting Performance Routing Version 3 (PfRv3). This feature enables you to monitor PfRv3 events and channels. During runtime, the event trace mechanism logs trace information in a buffer space. A display mechanism extracts and decodes the debug data.

- Prerequisites for PfRv3 Event Tracing, on page 215
- Restrictions for PfRv3 Event Tracing, on page 215
- Information About PfRv3 Event Tracing, on page 215
- How to Display PfRv3 Event Tracing, on page 216
- Additional References for PfRv3 Event Tracing, on page 234
- Feature Information for PfRv3 Event Tracing, on page 235

Prerequisites for PfRv3 Event Tracing

PfRv3 event trace is enabled by default. When PfRv3 features are enabled on the route, PfRv3 writes event trace data into PfRv3’s event trace buffer.

Restrictions for PfRv3 Event Tracing

By default, PfRv3 event trace can store 4096 entries of event traces. The entry size can be adjusted from 1 to 1000000 entries. Event traces are stored in memory and every event trace entry uses the memory size. The greater the number of entries, more memory is consumed. In PfRv3, each entry consumes 104 bytes. This indicates that PfRv3 event trace will consume about 416K bytes memory. Per design, the memory will have a delay allocation until first entry is written.

Information About PfRv3 Event Tracing

PfRv3 Event Tracing Options

Event Tracing uses event-trace infra framework by providing the ability to retrieve relevant part of event trace by providing show commands, such as, `show monitor event-trace pfrv3 sub-comp channel` command.

In Cisco IOS XE Fuji 16.9.1, PfRv3 supports event trace for the following subcomponents:
You can use the Event Trace for PfRv3 feature to analyze the cause of a device failure. When you configure PfRv3 features, the device records PfRv3 setup workflow and logs messages from specific subsystem components into the device memory. You can view trace messages stored in the memory by using the commands or save them to a file.

**Benefits of PfRv3 Event Tracing**

- Displays debug information on the console during runtime.
- Avoids multiple debug calls, and, therefore, improves device performance.
- Saves memory space.

**How to Display PfRv3 Event Tracing**

**SUMMARY STEPS**

1. `show monitor event-trace pfrv3 sub-comp channel {all | back duration | clock duration | from-boot seconds | latest} [detail]`
2. `show monitor event-trace pfrv3 sub-comp pdp {all | back duration | clock duration | from-boot seconds | latest} [detail]`
3. `show monitor event-trace pfrv3 sub-comp policy {all | back duration | clock duration | from-boot seconds | latest} [detail]`
4. `show monitor event-trace pfrv3 sub-comp process {all | back duration | clock duration | from-boot seconds | latest} [detail]`

**DETAILED STEPS**

**Step 1**

`show monitor event-trace pfrv3 sub-comp channel {all | back duration | clock duration | from-boot seconds | latest} [detail]`

**Example:**

```
Router# show monitor event-trace pfrv3 sub-comp channel all
```


Jul 12 02:03:02.469: CHANNEL: INFO: BR[3] Tunnel0 interface line protocol is coming back


How to Display PfRv3 Event Tracing

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
label[0x9] intf_type[External] IDC channel[NO] MHOP channel[NO] To-HUB channel[NO] reason[default channel to branch] op state[Initiated and open]


Jul 12 02:08:47.175: CHANNEL: INFO: BR[2] Tunnel1 interface line protocol is going down, may enqueue ALL_CHAN_UNREACH msg


state[Reachable] muted-by-0-sla[NO] op state[Initiated and open]
dscp[0] intf_index[27] label[0x4] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[29] label[0x1] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[27] label[0x4] intf_type[External] channel status[Not-Available(no next-hop)] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x7] intf_type[External] channel status[Not-Available(no next-hop)] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[27] label[0x2] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x7] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x9] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
 backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x9] intf_type[External] channel status[Not-Available(no next-hop)] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x9] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
dscp[0] intf_index[31] label[0x9] intf_type[External] channel status[Not-Available] TC count[0] backup-TC count[0] op state[Initiated and open]
Step 2

**How to Display PfRv3 Event Tracing**

- Show monitor event-trace pfrv3 sub-comp pdp {all | back duration | clock duration | from-boot seconds | latest} [detail]

**Example:**

Router# show monitor event-trace pfrv3 sub-comp pdp all

How to Display PfRv3 Event Tracing

Displays event trace for PfRv3 policy decision points (PDP).

**Step 3**

**show monitor event-trace pfrv3 sub-comp policy {all | back duration | clock duration | from-boot seconds | latest} [detail]**

**Example:**
```
Router# show monitor event-trace pfrv3 sub-comp policy all
```

```
Jul 12 02:02:42.727: POLICY: INFO: MC[2]: Pol_map seq 10: Set sp pref to ISP1 at index 0
Jul 12 02:02:42.727: POLICY: INFO: MC[2]: Pol_map seq 10: Set sp fallback to ISP2 at index 0
Jul 12 02:02:42.890: POLICY: INFO: MC[2]: Pol_map seq 20: Set sp pref to ISP1 at index 0
Jul 12 02:03:01.959: POLICY: INFO: BR[3]: Create C3PL policy for Egress direction
Jul 12 02:03:01.959: POLICY: INFO: BR[3]: Create C3PL policy for Ingress direction
Jul 12 02:03:01.967: POLICY: INFO: BR[3]: Create C3PL policy for Egress direction
Jul 12 02:03:08.212: POLICY: INFO: MC[2]: MC policy downloaded: site id[10.10.1.1], domain[default], vrf[green]
Jul 12 02:03:08.212: POLICY: INFO: MC[2]: Policy publish max allowed xml size[3030], exact xml size[2099]
Jul 12 02:03:09.355: POLICY: INFO: MC[3]: MC policy downloaded: site id[10.10.1.1], domain[default], vrf[red]
Jul 12 02:03:09.355: POLICY: INFO: MC[3]: Policy publish max allowed xml size[2303], exact xml size[1571]
Jul 12 02:03:10.927: POLICY: INFO: BR[2]: Updating PMI policies
Jul 12 02:03:10.927: POLICY: INFO: BR[2]: Create C3PL policy for Ingress direction
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Create filter dscp:46, appid:0
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Create filter dscp:40, appid:0
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Create class CENT-Class-Ingress-DSCP-cs4-2-4
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react packet-loss-rate val=100 id=2
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react one-way-delay val=20 id=3
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react network-delay-avg val=40 id=4
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react jitter val=5000 id=5
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react byte-loss-rate val=100 id=6
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react jitter val=5000 id=7
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Create react for class CENT-Class-Ingress-DSCP-cs4-2-4
Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Provision react one-way-delay val=20 id=8
```

How to Display PfRv3 Event Tracing

Jul 12 02:03:10.950: POLICY: INFO: BR[2]: Create C3PL policy for Egress direction
Jul 12 02:03:10.976: POLICY: INFO: BR[2]: Create filter dscp:0,appid:0
Jul 12 02:03:12.013: POLICY: INFO: BR[3]: Updating PMI policies
Jul 12 02:03:12.013: POLICY: INFO: BR[3]: Create C3PL policy for Ingress direction
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Create filter dscp:46,appid:0
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Create class CENT-Class-Ingress-DSCP-ef-3-6
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Create filter dscp:40,appid:0
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Create class CENT-Class-Ingress-DSCP-cs5-3-7
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Create react for class CENT-Class-Ingress-DSCP-ef-3-6
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Provision react packet-loss-rate val=100 id=10
Jul 12 02:03:12.014: POLICY: INFO: BR[3]: Provision react byte-loss-rate val=100 id=11
Jul 12 02:03:12.015: POLICY: INFO: BR[3]: Create class CENT-Class-Ingress-DSCP-cs5-3-7
Jul 12 02:03:12.015: POLICY: INFO: BR[3]: Create react for class CENT-Class-Ingress-DSCP-cs5-3-7
Jul 12 02:03:12.015: POLICY: INFO: BR[3]: Provision react packet-loss-rate val=100 id=12
Jul 12 02:03:12.015: POLICY: INFO: BR[3]: Provision react byte-loss-rate val=100 id=13
Jul 12 02:03:12.094: POLICY: INFO: BR[3]: Activate PMI policy CENT-Policy-Ingress-3-4 on Tunnel31
Jul 12 02:03:12.094: POLICY: INFO: BR[3]: Activate PMI policy CENT-Policy-Ingress-3-4 on Tunnel11
Jul 12 02:03:12.094: POLICY: INFO: BR[3]: Create C3PL policy for Egress direction
Jul 12 02:08:47.201: POLICY: INFO: BR[2]: De-activate PMI policy CENT-Policy-Egress-2-3 on Tunnel10
Jul 12 02:08:47.201: POLICY: INFO: BR[2]: Delete class CENT-Class-Ingress-DSCP-cs4-2-4
**Step 4** show monitor event-trace pfrv3 sub-comp process {all | back duration | clock duration | from-boot seconds | latest} [detail]

**Example:**

Router# show monitor event-trace pfrv3 sub-comp process all


Jul 12 02:02:57.970: PROCESS: INFO: MC server listening on: 10.10.1.1, port: 17749


Jul 12 02:02:58.501: PROCESS: INFO: MC server listening on: 10.10.1.1, port: 17749
Jul 12 02:03:01.739: PROCESS: INFO: BR[3] SAF peering succeed: 10.10.1.1 to 10.10.1.1
Jul 12 02:03:01.958: PROCESS: INFO: BR[3] Register CMD IDB : idb Tunnel0, client id 4, result Succeed
PfRv3 Event Tracing

How to Display PfRv3 Event Tracing

Jul 12 02:03:05.257: PROCESS: INFO: BR[3] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.10.1.1
Jul 12 02:03:05.258: PROCESS: INFO: BR[3] SAF peering site prefix update: prefix 10.16.0.0/16 from 10.10.1.1
Jul 12 02:03:05.258: PROCESS: INFO: BR[3] SAF peering site prefix update: prefix 10.0.0.0/8 from 10.10.1.1
Jul 12 02:03:09.610: PROCESS: INFO: MC[3] SAF peering site prefix update: prefix 10.10.0.0/16 from 10.15.1.1
Jul 12 02:03:09.610: PROCESS: INFO: MC[3] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.15.1.1
Jul 12 02:03:09.610: PROCESS: INFO: MC[3] SAF peering site prefix update: prefix 10.0.0.0/8 from 10.15.1.1
Jul 12 02:03:09.614: PROCESS: INFO: BR[3] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.15.1.1
Jul 12 02:03:10.979: PROCESS: INFO: BR[2] SAF peering site prefix update: prefix 10.0.0.0/8 from 10.10.1.1


Jul 12 02:03:24.577: PROCESS: INFO: MC[2] SAF peering site prefix update: prefix 10.10.0.0/16 from 10.15.1.1
Jul 12 02:03:24.577: PROCESS: INFO: MC[2] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.15.1.1
Jul 12 02:03:24.577: PROCESS: INFO: MC[2] SAF peering site prefix update: prefix 10.0.0.0/8 from 10.15.1.1
Jul 12 02:03:24.578: PROCESS: INFO: BR[2] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.15.1.1
Jul 12 02:03:24.582: PROCESS: INFO: BR[2] SAF peering site prefix update: prefix 10.10.0.0/16 from 10.15.1.1
Jul 12 02:03:24.582: PROCESS: INFO: BR[2] SAF peering site prefix update: prefix 10.15.0.0/16 from 10.15.1.1
Jul 12 02:03:24.582: PROCESS: INFO: BR[2] SAF peering site prefix update: prefix 10.0.0.0/8 from 10.15.1.1
Jul 12 02:05:00.536: PROCESS: INFO: BR[3] SAF peering received sub-service: site-prefix, from: 10.30.1.1, data size: 184, data seq: 3
Jul 12 02:05:00.537: PROCESS: INFO: MC[3] SAF peering site prefix update: prefix 10.30.0.0/24 from 10.30.1.1

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
Jul 12 02:05:00.537: PROCESS: INFO: MC[3] SAF peering site prefix update: prefix 10.30.0.0/24 from 10.30.1.1
Jul 12 02:05:00.539: PROCESS: INFO: BR[3] SAF peering site prefix update: prefix 10.30.0.0/24 from 10.30.1.1
Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

PfRv3 Event Tracing

How to Display PfRv3 Event Tracing

Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x
Performance Routing Version 3 Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

PfRv3 Event Tracing

How to Display PfRv3 Event Tracing

Additional References for PfRv3 Event Tracing

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

Displays event trace for PfRv3 processes.
Feature Information for PfRv3 Event Tracing

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 26: Feature Information for PfRv3 Event Tracing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Trace for PfRv3 Errors and PfRv3 Channels</td>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The Event Trace for PfRv3 feature provides a trace facility for troubleshooting Performance Routing Version 3 (PfRv3). This feature enables you to monitor PfRv3 events and channels. During runtime, the event trace mechanism logs trace information in a buffer space. A display mechanism extracts and decodes the debug data. The following commands were introduced or modified: show monitor event-trace pfrv3 sub-comp channel, show monitor event-trace pfrv3 sub-comp pdp, show monitor event-trace pfrv3 sub-comp policy, show monitor event-trace pfrv3 sub-comp process.</td>
</tr>
</tbody>
</table>
PfRv3 Command References

The following tables lists various Cisco IOS commands that are used for PfRv3 along with the command mode from which they are entered.

Table 27: Configuration Commands for PfRv3

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Command name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration</td>
<td>bandwidth bandwidth-value</td>
<td>Configures inherited and received bandwidth values for the tunnel interface. The bandwidth value is in kilobits and the valid values are 1 to 1000000.</td>
</tr>
<tr>
<td>Border configuration</td>
<td>border</td>
<td>Defines a device as a border.</td>
</tr>
<tr>
<td>Domain master hub advanced</td>
<td>channel-based-measurement</td>
<td>Configures the performance monitors used by PfRv3 to employ a data collection method which is typically more accurate, sampling traffic at intervals and using metadata together to provide traffic metrics.</td>
</tr>
<tr>
<td></td>
<td>[sampling-rate sampling-rate]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[quick samples-for-quick-monitoring]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[sample-packet-size maximum-packet-size]</td>
<td></td>
</tr>
<tr>
<td>Domain master controller</td>
<td>branch-to-branch</td>
<td>Disable branch to branch PfR optimization. This is configured on Branch Masters.</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td>Note Configuring the command results in two different behaviors for the different releases. See, PfRv3 Command Reference guide.</td>
</tr>
<tr>
<td>Configuration</td>
<td>domain domain name</td>
<td>Configures a top level domain for PfRv3.</td>
</tr>
<tr>
<td>Configuration interface</td>
<td>domain domain name pathpath-name</td>
<td>Configures a path for the domain for PfRv3.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>domain domain name pathpath-name path-id</td>
<td>Configures a path and path-id for a specified domain.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>domain path isp-name zero-sla</td>
<td>Configures Zero SLA on tunnel interface for an ISP path.</td>
</tr>
<tr>
<td>Command mode</td>
<td>Command name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Master controller configuration</td>
<td>hub ip-address</td>
<td>Configures an IP address for the hub.</td>
</tr>
<tr>
<td>Domain class configuration</td>
<td>match {application</td>
<td>dscp}</td>
</tr>
<tr>
<td>Master controller configuration</td>
<td>master ip-address</td>
<td>Configures an IP address for the master controller.</td>
</tr>
<tr>
<td>Domain VRF configuration</td>
<td>master {hub</td>
<td>branch</td>
</tr>
<tr>
<td>Domain VRF configuration</td>
<td>master transit pop-id</td>
<td>Configures an ID for the master transit branch.</td>
</tr>
<tr>
<td>Domain-class configuration</td>
<td>path-preference path-name fallback path-name</td>
<td>Specifies a path preference for a traffic class policy.</td>
</tr>
<tr>
<td>Master controller class type</td>
<td>priority priority-number</td>
<td>Specifies threshold values for user-defined policies.</td>
</tr>
<tr>
<td></td>
<td>jitter</td>
<td>loss</td>
</tr>
<tr>
<td>Domain configuration</td>
<td>vrf vrf-name</td>
<td>Configures a Virtual Routing and Forwarding (VRF) instance for a domain.</td>
</tr>
</tbody>
</table>

Table 28: Show Commands for PfRv3

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Command name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border peering</td>
<td>Displays the border router peering status.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border pmi</td>
<td>Displays the automatically learned site-prefix status information of the hub-border router.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border status</td>
<td>Displays the status of the border routers configured at the hub site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border site-prefix</td>
<td>Displays the site-prefix status information of the hub-border router.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border channels</td>
<td>Displays channel information from the hub-border site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border parent route</td>
<td>Displays the parent route information of a border channel.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>show domain domain-name border channels parent route</td>
<td>Displays the parent route information of a channel.</td>
</tr>
<tr>
<td>Command mode</td>
<td>Command name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master exits</code></td>
<td>Displays the summary of the external interfaces configured at the hub site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master peering</code></td>
<td>Displays the peering information of the hub-master controller.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master discovered-sites</code></td>
<td>Displays branch sites that are remotely connected to the hub site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master site-prefix</code></td>
<td>Displays the site-prefix status information of the hub-master controller.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show platform pfrv3 rp active smart-probe</code></td>
<td>Displays the PfRv3 smart probe status on a Cisco ASR 1000 Series Aggregation Services Router configured at the hub site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show platform pfrv3 fp active smart-probe</code></td>
<td>Displays the PfRv3 active smart probes status of an embedded-service-processor on Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show platform hardware qfp active feature pfrv3 client global pfrv3-instance detail</code></td>
<td>Displays the platform hardware information on a Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show flow monitor type performance-monitor</code></td>
<td>Displays the flow monitor information for passive performance monitoring on the egress interface of WAN.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master traffic-classes summary</code></td>
<td>Displays the summary information of all the traffic classes.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master traffic-classes</code></td>
<td>Displays the status information of the traffic class for the hub-master controller.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master traffic-classes policy policy-name</code></td>
<td>Displays the occurrence of performance issues in a policy traffic class.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master channels</code></td>
<td>Displays channel information from the hub site.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master channels link-name path-name</code></td>
<td>Displays channel status information and the unreachable threshold crossing alerts (TCA) and on demand export (ODE) instances on a hub-master controller.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name master channels dst-site-id destination-site-id</code></td>
<td>Displays the details of destination site-ids configured with hub-master controller.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show domain domain-name default master site-capability</code></td>
<td>Displays the capability information of master controller.</td>
</tr>
</tbody>
</table>
### Table 29: Debug Commands for PfRv3

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Command name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td><code>debug platform hardware qfp active feature pfrv3 client</code></td>
<td>Enables PfRv3 Cisco Quantum Flow Processor (QFP) client debug logging.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>debug platform hardware qfp active feature pfrv3 datapath</code></td>
<td>Enables PfRv3 Cisco Quantum Flow Processor (QFP) data path debug logging.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>debug platform hardware qfp active feature pfrv3 pal</code></td>
<td>Enables debug logging for PfRv3 in the Cisco Quantum Flow Processor (QFP).</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>debug platform software pfrv3</code></td>
<td>Enables PfRv3 platform debug commands.</td>
</tr>
</tbody>
</table>

### Table 30: Troubleshooting Commands for PfRv3

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Command name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
<td><code>show tech-support iwan</code></td>
<td>Displays data useful for troubleshooting, including information related to FNF, PfRv3, MMA, and NBAR.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td><code>show tech-support pfrv3</code></td>
<td>Displays data useful for troubleshooting, including information related to PfRv3.</td>
</tr>
</tbody>
</table>