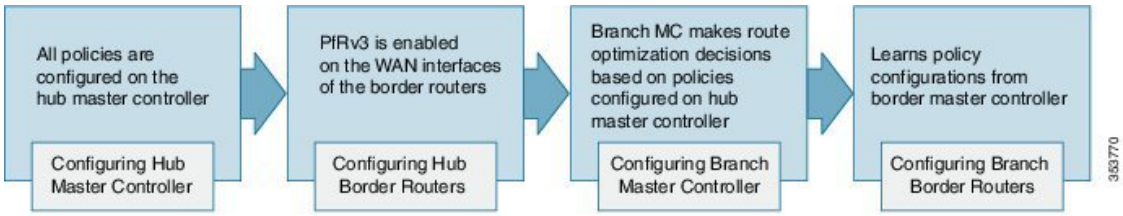
How to Configure PfRv3

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 1: PfRv3 Workflow



How to Configure Performance Routing Version 3

Configuring Hub Master Controller

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**ip address** *ip-address-mask* **Example:** `Device(config-if)# ip address 10.8.3.3 255.255.255.255`	Configures an IP address for an interface on the hub-master controller.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**domain** {*domain-name* | **default**} **Example:** `Device(config)# domain default`	Enters domain configuration mode. **Note** You can either configure a default domain or define a specific domain for the master controller configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration.
Step 7	**vrf** {*vrf-name* | **default**} **Example:** `Device(config-domain)# vrf default`	Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain. **Note** You can configure specific VRF definition also for the hub-master controller configuration.
Step 8	**master** {**hub** |**branch**|**transit**} **Example:** `Device(config-domain-vrf)# master hub`	Enters master controller configuration mode and configures the master as a hub. When the master hub is configured, EIGRP SAF auto-configuration is enabled by default and requests from remote sites are sent to the hub-master controller.
Step 9	**source-interface loopback** *interface-number* **Example:** `Device(config-domain-vrf-mc)# 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 10	**enterprise-prefix prefix-list** *site-list* **Example:** `Device(config-domain-vrf-mc)# enterprise-prefix prefix-list ENTERPRISE`	Configures an enterprise prefix-list with static site targets. **Note** The **enterprise-prefix prefix-list** command defines the boundary for all the internal enterprise prefixes. A prefix that is not from the prefix-list is considered as internet prefix and is routed over internet-bound links.
Step 11	**site-prefixes prefix-list** *site -list* **Example:** `Device(config-domain-vrf-mc)# site-prefixes prefix-list Data_Center_1`	Configures the prefix-list containing list of site prefixes. **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	Purpose
Step 12	**exit** **Example:** `Device(config-domain-vrf-mc)# 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 13	**ip prefix-list** *ip-list* **seq** *sequence-number* **permit** *ip-prefix-network* **le** *le-length*
	
	Example:
	`Device(config)# ip prefix-list DATA_CENTER_1 seq 5 permit 10.8.0.0/16 le 24`
	`Device(config)# ip prefix-list ENTERPRISE seq 5 permit 10.0.0.0/8 le 24`
		Configures the IP prefix list to filter traffic based on the IP network defined in the configuration.

Step 14	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 15	**show domain** *domain-name* **master status** **Example:** `Device# show domain one master status`	(Optional) Use this show command to display the status of a master controller.

What to Do Next

Configuring Domain Policies

Configuring Hub Border Routers

Configuring Branch Routers

Verifying PfRv3 Configuration

Configuring Hub Border Router

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

	Command or Action	Purpose
Step 14	**interface** *tunnel-name* **Example:** `Device(config)# interface Tunnel100`	Enters interface configuration mode.
Step 15	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.0.100.84 255.255.255.0`	Configures an IP address for the tunnel interface.
Step 16	**domain** *domain-name* **path** *path-name* **Example:** `Device(config-if)# domain one path MPLS`	Configures the Internet Service Provider (ISP). There are two types of external interfaces, enterprise link such as DMVPN tunnel interface and internet-bound interface. Internet-bound external interface is configured only on the hub site for the internet edge deployment and cannot be discovered by any branch site. 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.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 18	**show domain** *domain-name* **border status** **Example:** `Device# show domain one border status`	(Optional) Use this show command to display the status of a border router.

What to Do Next

Configuring Branch Master Controller

Configuring Branch Border Router

Verifying PfRv3 Configuration

Configuring Domain Policies

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

Before You Begin

Configure a device as hub-master controller at the hub site. To know more about how to configure a hub-master controller, see Configuring Hub Master Controller, on page 1 section.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**domain** {*domain-name* | **default**} **Example:** `Device(config)# domain default`	Enters domain configuration mode. **Note** You can either configure a default domain or define a specific domain for the border configuration. If you are defining a specific domain, for example "domain-cisco", you must configure the same domain for all devices for PfRv3 configuration.
Step 2	**vrf** {*vrf-name* | **default**} **Example:** `Device(config-domain)# vrf default`	Configures default Virtual Routing and Forwarding (VRF) instances for the default or specific domain. **Note** You can configure specific VRF definition also for the hub-master controller configuration.
Step 3	**master** [**hub** | **branch** | **transit**] **Example:** `Device(config-domain-vrf)# master hub`	Enters master controller configuration mode and configures the master as a hub. When the master hub is configured, EIGRP SAF auto-configuration is enabled by default and requests from remote sites are sent to the hub master controller.

	Command or Action	Purpose
Step 4	**monitor-interval** *seconds* **dscp ef** **Example:** `Device(config-domain-vrf-mc)# monitor-interval 2 dscp ef`	Configures interval time that defines monitoring interval on ingress monitors. **Note** For critical applications monitor interval is set to 2 seconds. Default value is 30 seconds. You can lower the monitor interval for critical applications to achieve a fast fail over to the secondary path. This is known as quick monitor.
Step 5	**load-balance** **Example:** `Device(config-domain-vrf-mc)# load-balance`	Configures load balancing. **Note** When load balancing is enabled, all the traffic that falls in the default class is load balanced. When load balancing is disabled, PfRv3 deletes this default class and traffic is not load balanced and is routed based on the routing table information.
Step 6	**class** *class-name* **sequence** *sequence-number* **Example:** `Device(config-domain-vrf-mc)# class VOICE sequence 10`	Enters policy class configuration mode. **Note** Class-name value must be in all capitals.
Step 7	**match {application | dscp}** *services-value* **policy** **Example:** `Device(config-domain-vrf-mc-class)# match dscp ef policy voice`	Configures policy on per DSCP basis. You can select a DSCP value from 0 to 63. You can select the following policy types: • **best-effort** • **bulk-data** • **custom** • **low-latency-data** • **real-time-video** • **scavenger** • **voice** In this example, the domain policy type is configured for voice.
Step 8	**path-preference** *path-name* **fallback** *path-name* **Example:** `Device(config-domain-vrf-mc-class)# path-preference MPLS fallback INET`	Configures the path preference for applications. **Note** You can configure up to five primary path preferences and four fallback preferences. Group policies sharing the same purpose can be defined under the same class path preference. You cannot configure different path preference under the same class.

Step 9	**priority** *priority-number* [**jitter** | **loss** | **one-way-delay**] **threshold** *threshold-value*
	
	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`
		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.
		Note You can configure class type priorities only for a custom policy. You can configure multiple priorities for custom policies.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

What to Do Next

- Verifying PfRv3 Configurations

Configuring Branch Master Controller

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface loopback** *interface-number* **Example:** `Device(config)# interface Loopback0`	Enters interface configuration mode.
Step 4	**ip address** *ip-address-mask* **Example:** `Device(config-if)# ip address 10.2.10.10 255.255.255.255`	Configures an IP address for an interface on the branch-master controller.
Step 5	**domain** {*domain-name* | **default**} **Example:** `Device(config)# domain default`	Enters domain configuration mode. **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`	Configures Virtual Routing and Forwarding (VRF) for the default domain. **Note** You can also configure specific VRF definition for branch border configuration.
Step 7	**master branch** **Example:** `Device(config-domain-vrf)# master branch`	Configures the device as master branch.
Step 8	**source-interface loopback** *interface-number* **Example:** `Device(config-domain-vrf-mc)# source-interface Loopback0`	Configures the loopback used as a source for peering with other sites or master controller.
Step 9	**hub** *ip-address* **Example:** `Device(config-domain-vrf-mc)# hub 10.8.3.3`	Specifies the IP address of the hub master controller.
Step 10	**end** **Example:** `Device(config-domain-vrf-mc)# end`	Exits master controller domain configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 11	**show domain** *domain-name* **master status** **Example:** `Device# show domain one master status`	(Optional) Use this show command to display the status of a master controller.

What to Do Next

Configuring Branch Border Router

Verifying Border Router

Configuring Branch Border

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**domain** {*domain-name* | **default**} **Example:** `Device(config)# domain default`	Enters domain configuration mode.
Step 4	**vrf** {*vrf-name* | **default**} **Example:** `Device(config-domain)# vrf default`	Configures Virtual Routing and Forwarding (VRF) for the default domain. **Note** You can also configure specific VRF definition for the branch-border configuration.
Step 5	**border** **Example:** `Device(config-domain-vrf)# border`	Enters border configuration mode.
Step 6	**source-interface loopback** *interface-number* **Example:** `Device(config-domain-vrf-br)# source-interface Loopback0`	Configures the loopback address used as a source for peering with other sites or the master controller.
Step 7	**master** *ip-address* **Example:** `Device(config-domain-vrf-br)# master 10.1.1.1`	Specifies the IP address of the branch-master controller.
Step 8	**end** **Example:** `Device(config-domain-vrf-br)# end`	Exits border configuration mode and returns to privileged EXEC mode.
Step 9	**show domain** *domain-name* **border status** **Example:** `Device# show domain one border status`	(Optional) Use this show command to display the status of a border router.

What to Do Next

Verifying PfRv3 Configurations

Configuring Branch Master Controller and Border

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**ip address** *ip-address-mask* **Example:** `Device(config-if)# ip address 10.2.12.12 255.255.255.255`	Configures an IP address for an interface on the branch master controller.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**domain** {*domain-name* | **default**} **Example:** `Device(config)# domain default`	Enters domain configuration mode.
Step 7	**vrf** {*vrf-name* | **default**} **Example:** `Device(config-domain)# vrf default`	Configures Virtual Routing and Forwarding (VRF) for the default domain.
Step 8	**border** **Example:** `Device(config-domain-vrf)# border`	Enters border configuration mode.
Step 9	**source-interface loopback** *interface-number* **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 local** **Example:** `Device(config-domain-vrf-br)# master local`	Configures the local IP address of the device as branch-master controller.
Step 11	**master branch** **Example:** `Device(config-domain-vrf-mc)# master branch`	Configures the master type of the device as a branch.
Step 12	**source-interface loopback** *interface-number* **Example:** `Device(config-domain-vrf-mc)# source-interface Loopback0`	Configures the loopback used as a source for peering with other sites or master controller.
Step 13	**hub** *ip-address* **Example:** `Device(config-domain-vrf-mc)# hub 10.8.3.3`	Configures the IP address of the hub-master controller.

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

What to Do Next

Verifying PfRv3 Configuration

Verifying Performance Routing Version 3 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 1: show domain master policy Field Descriptions

Field	Description
No policy publish pending	Specifies if the policy publishing is pending to remote sites.
class	Name of the class type. In this example, the following classes are listed: • VOICE • VIDEO • CRITICAL
path-preference	Specifies the path preferred for the class type.
match	Specifies the DSCP value to match for a policy type.
priority	Specifies the detailed policy threshold per class, based on the DSCP or application.

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

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

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

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

Example:

```
HubMC# show domain one master status

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

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

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

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

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

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

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

Example:

```
HubMC# show domain one master exits

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

*** Domain MC Status ***

BR address: 10.8.2.2 | Name: Tunnel200 | type: external | Path: INET |
Egress capacity: 50000 Kbps | Egress BW: 17514 Kbps | Ideal:17948 Kbps | under: 434 Kbps | Egress
Utilization: 35 %
DSCP: cs4[32]-Number of Traffic Classes[1]
DSCP: af41[34]-Number of Traffic Classes[1]
DSCP: cs5[40]-Number of Traffic Classes[1]
BR address: 10.8.1.1 | Name: Tunnel100 | type: external | Path: MPLS |
Egress capacity: 100000 Kbps | Egress BW: 36331 Kbps | Ideal:35896 Kbps | over: 435 Kbps | Egress
Utilization: 36 %
DSCP: cs1[8]-Number of Traffic Classes[1]
DSCP: af11[10]-Number of Traffic Classes[1]
DSCP: af31[26]-Number of Traffic Classes[1]
DSCP: ef[46]-Number of Traffic Classes[1]
```

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

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

Table 3: show domain master exits Field Descriptions

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

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

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

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

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

Example:

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

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

*** Domain MC Status ***

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

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

Published service:
site-prefix (1) :
Last Publish Info: 00:03:10 ago, Size: 209, Compressed size: 138, Status: No Error
cent-policy (2) :
```

```
Last Publish Info: 00:02:58 ago, Size: 2244, Compressed size: 468, Status: No Error
pmi (3) :
Last Publish Info: 02:03:12 ago, Size: 2088, Compressed size: 458, Status: No Error
globals (5) :
Last Publish Info: 00:03:09 ago, Size: 325, Compressed size: 198, Status: No Error

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

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

Table 4: show domain master peering Field Descriptions

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

Step 5 **show derived-config | section eigrp**
This command displays if EIGRP SAF is automatically configured.

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

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

Example:

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

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

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

The fields shown above are self-explanatory.

Step 6 **show domain** *domain-name* **master discovered-sites**
This command displays the sites that are remotely connected to the hub site.

Example:

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

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

*** Domain MC DISCOVERED sites ***

Number of sites: 3

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

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

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

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

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

The fields shown above are self-explanatory.

Verifying Hub Border Router Configurations

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

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

Example:

```
HubBR# show domain one border status

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

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

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

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

This command displays the border router peering status.

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

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

Example:

```
HubBR# show domain one border peering

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

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

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

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

Table 6: show domain border peering Field Descriptions

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

Step 3

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.

show platform software pfrv3 rp active smart-probe

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

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.

show platform software pfrv3 fp active smart-probe

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

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

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

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

Example:

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

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

PfRv3 QFP CLIENT GLOBAL INFO

Number of Instances: 1
Instance
hash val: 5
tbl id: 0
symmetry: Off
discovery: Off
discovery_probe: On
probe info:
probe src: 10.8.3.3, src port: 18000, dst port: 19000
unreach time: 1000, probe period: 500
dscp bitmap: 0xffffffffffffffff, interval: 10000
mml: 28
exmem info:
PPE addr: 0xe80b7830
------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

Verifying Branch Master Controller Configurations

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

- External interfaces are listed with correct path names

- Minimum requirements are met
- Path names are correct

Example:

```
BRMC#show domain one master status

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

Master VRF: Global
Instance Type: Branch
Instance id: 0
Operational status: Up
Configured status: Up
Loopback IP Address: 10.2.10.10
Load Balancing:

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

Borders:
IP address: 10.2.10.10
Connection status: CONNECTED (Last Updated 02:03:22 ago )
Interfaces configured:
Name: Tunnel100 | type: external | Service Provider: MPLS | Status: UP
Number of default Channels: 0
Name: Tunnel200 | type: external | Service Provider: INET | Status: UP
Number of default Channels: 0
Tunnel if: Tunnel0

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

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

Table 7: show domain master status Field Descriptions

Field	Description
Instance Type	Displays the instance type of the device. In this output, the device is configured as a branch.
Operational Status	Displays the operational status of the branch-master controller.
Configured Status	Displays the configuration status of the branch-master controller.

Field	Description
Load Balancing	Displays the load balancing status. If load balancing is enabled on the hub-master controller, the branch master controller receives load balanced traffic.
Borders	Displays the information of border routers connected to the branch-master controller, and external interfaces connected to path names.

Step 2 **show domain** *domain-name* **master policy**
This command displays the policy information received from the hub-master controller.

Example:

```
BRMC# show domain one master policy

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

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

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

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

Table 8: show domain master policy Field Descriptions

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

Verifying Branch Border Configurations

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

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

Example:

```
BR#show domain one border status

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

*** Border Status ***

Instance Status: UP
Present status last updated: 02:11:47 ago
Loopback: Configured Loopback0 UP (10.2.10.10)
Master: 10.2.10.10
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 02:11:41
Route-Control: Enabled
Minimum Mask length: 28
Sampling: off
Minimum Requirement: Met
External Wan interfaces:
Name: Tunnel100 Interface Index: 14 SNMP Index: 9 SP:MPLS Status: UP
Name: Tunnel200 Interface Index: 15 SNMP Index: 10 SP:INET Status: UP
Auto Tunnel information:
Name:Tunnel0 if_index: 19
Borders reachable via this tunnel:

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

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

Table 9: show domain border status Field Descriptions

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

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

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

Example:

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

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

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

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

The fields shown above are self-explanatory.

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

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

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

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

Example:

```
BR# show domain one master peering

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

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

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

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

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

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

Table 10: show domain master peering Field Descriptions

Field	Description
Peering state	Status of peering.

Field	Description
Subscribed services	Displays the subscribed services list.
Published services	Displays the services published by the branch-master controller to the branch-border routers.

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

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

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

- Ingress policy activation
- Egress policy activation
- PMI status

Example:

```
BR# show domain one border pmi

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

The fields shown above are self-explanatory.

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

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

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

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

Example:

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

Flow Monitor type performance-monitor MON-Egress-aggregate-0-48-9:
```

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

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

Flow Monitor type performance-monitor MON-Ingress-per-DSCP-0-48-11:
      Description :User defined
      Flow Record :CENT-FLOWREC-Ingress-per-DSCP-0-13
    Flow Exporter :not configured
       Cache type :synchronized
          entries :2000
         interval :30 (seconds)
     history size :0 (intervals)
          timeout :1 (intervals)
  export spreading:FALSE
Interface applied :2
```

The fields shown above are self-explanatory.

Monitoring Performance Routing Version 3

Monitoring Site Prefix

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show domain** *domain-name* **master site-prefix**
This command displays the site- prefix status information of the hub master controller.

Example:

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

Change will be published between 5-60 seconds
Next Publish 00:54:41 later
Prefix DB Origin: 10.8.3.3
Prefix Flag: S-From SAF; L-Learned; T-Top Level; C-Configured;
Site-id Site-prefix Last Updated Flag
------------------------------------------------------------------------------------------------------------
10.2.10.10 10.1.10.0/24 00:42:07 ago S,
10.2.10.10 10.2.10.10/32 00:42:07 ago S,
10.2.11.11 10.2.11.11/32 00:18:25 ago S,
10.8.3.3 10.8.3.3/32 1d05h ago L,
10.8.3.3 10.8.0.0/16 1d05h ago C,
255.255.255.255 *10.0.0.0/8 1d05h ago T,


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

The fields shown above are self-explanatory.

Step 2 **show domain** *domain-name* **border site-prefix**
This command displays the site- prefix status information of the hub-border router.

Example:

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

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

The fields shown above are self-explanatory.

Step 3 **show domain** *domain-name* **border pmi | begin prefix-learn**
This command displays the automatically learned site- prefix status information of the hub-border router.

Example:

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

-----------------------------------------------------------------------------------------------
PMI[Egress-prefix-learn]-FLOW MONITOR[MON-Egress-prefix-learn-0-48-29]
monitor-interval:30
minimum-mask-length:28
key-list:
ipv4 source prefix
ipv4 source mask
routing vrf input
Non-key-list:
counter bytes long
counter packets long
timestamp absolute monitoring-interval start
DSCP-list:N/A
Class:CENT-Class-Egress-ANY-0-51
Exporter-list:
10.2.10.10
-----------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

Monitoring Traffic Classes

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

Traffic classes are divided in the following groups:

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

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show domain** *domain-name* **master traffic-classes summary**
This command displays the summary information of all the traffic classes.

Example:

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

------------------------------------------------------------------------------------------------------------
APP - APPLICATION, TC-ID - TRAFFIC-CLASS-ID, APP-ID - APPLICATION-ID
SP - SERVICE PROVIDER, PC = PRIMARY CHANNEL ID,
BC - BACKUP CHANNEL ID, BR - BORDER, EXIT - WAN INTERFACE
UC - UNCONTROLLED, PE - PICK-EXIT, CN - CONTROLLED, UK - UNKNOWN
Dst-Site-Pfx Dst-Site-Id APP DSCP TC-ID APP-ID State SP PC/BC BR/EXIT
10.1.10.0/24 10.2.10.10 N/A af11 193 N/A CN MPLS 59/60 10.8.2.2/Tunnel100
10.1.10.0/24 10.2.10.10 N/A cs1 192 N/A CN MPLS 57/58 10.8.2.2/Tunnel100
10.1.10.0/24 10.2.10.10 N/A cs5 191 N/A CN MPLS 55/NA 10.8.2.2/Tunnel100
10.1.10.0/24 10.2.10.10 N/A ef 190 N/A CN MPLS 52/NA 10.8.2.2/Tunnel100
10.1.10.0/24 10.2.10.10 N/A af41 195 N/A CN INET 64/63 10.8.1.1/Tunnel200
10.1.10.0/24 10.2.10.10 N/A cs4 189 N/A CN INET 54/53 10.8.1.1/Tunnel200
10.1.10.0/24 10.2.10.10 N/A af31 194 N/A CN MPLS 61/62 10.8.2.2/Tunnel100
Total Traffic Classes: 7 Site: 7 Internet: 0

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

The fields shown above are self-explanatory.

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

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

Example:

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

------------------------------------------------------------------------------------------------
Dst-Site-Prefix: 10.1.10.0/24 DSCP: af11 [10] Traffic class id:193
TC Learned: 00:22:13 ago
Present State: CONTROLLED
Current Performance Status: not monitored (default class)
Current Service Provider: MPLS since 00:12:10
Previous Service Provider: INET for 298 sec
BW Used: 9195 Kbps
Present WAN interface: Tunnel100 in Border 10.8.2.2
Present Channel (primary): 59
Backup Channel: 60
Destination Site ID: 10.2.10.10
Class-Sequence in use: default
Class Name: default
BW Updated: 00:00:14 ago
Reason for Route Change: Load Balance
------------------------------------------------------------------------------------------------
Dst-Site-Prefix: 10.1.10.0/24 DSCP: cs1 [8] Traffic class id:192
TC Learned: 00:22:14 ago
Present State: CONTROLLED
Current Performance Status: not monitored (default class)
Current Service Provider: MPLS since 00:12:40
Previous Service Provider: INET for 184 sec
BW Used: 9251 Kbps
Present WAN interface: Tunnel100 in Border 10.8.2.2
Present Channel (primary): 57
Backup Channel: 58
Destination Site ID: 10.2.10.10
Class-Sequence in use: default
Class Name: default
BW Updated: 00:00:12 ago
Reason for Route Change: Load Balance
.
.
.
------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

Step 3 **show domain** *domain-name* **master traffic-classes policy** *policy-name*
This command displays the occurrence of performance issues in a policy traffic class.

Example:

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

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

The fields shown above are self-explanatory.

Cisco IOS XE Platform Commands

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show platform software pfrv3 rp active route-control traffic-class**	This command displays the traffic class information for a platform.
Step 2	**show platform software pfrv3 fp active route-control traffic-class**	This command displays the traffic class information for a platform.
Step 3	**show platform hardware qfp active feature pfrv3 client route-control traffic-class detail**	This command displays the hardware information for the configured policy.
Step 4	**show platform software interface rp active name** *interface-name*	This command displays the ingress interface information for PfRv3.
Step 5	**show platform software interface fp active name** *interface-name*	This command displays the ingress interface information for PfRv3.
Step 6	**show platform hardware qfp active interface if-name** *interface-name*	This command displays the interface information in a data plane path for PfRv3.

Monitoring Channels

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

SUMMARY STEPS

1. **show domain** *domain-name* **master channels dscp ef**
2. **show domain** *domain-name* **master channels link-name** *path-name*
3. **show domain** *domain-name* **border channels**
4. **show domain** *domain-name* **border exporter statistics**
5. **show domain** *domain-name* **border 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:)
```

```
49
Channel Id: 89 Dst Site-Id: 10.2.10.10 Link Name: MPLS DSCP: ef [46] TCs: 1
Channel Created: 00:01:15 ago
Provisional State: Initiated and open
Operational state: Available
Interface Id: 14
Estimated Channel Egress Bandwidth: 5380 Kbps
Immitigable Events Summary:
Total Performance Count: 0, Total BW Count: 0
TCA Statitics:
Received 0 ; Processed 0 ; Unreach_rcvd:0

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

The fields shown above are self-explanatory.

Step 2 **show domain** *domain-name* **master channels link-name** *path-name*
This command displays channel status information and the unreachable threshold crossing alerts (TCA) and on demand export (ODE) on a hub-master controller.

Example:

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

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

The fields shown above are self-explanatory.

Step 3 **show domain** *domain-name* **border channels**
This command displays channel information from the hub-border site.

Example:

```
HubBR#show domain one border channels


------------------------------------------------------------------------------------------------
Border Smart Probe Stats:
Channel id: 21
Channel dscp: 0
Channel site: 255.255.255.255
Channel interface: Tunnel200
Channel operation state: Initiated_n_open
Channel RX state: reachable
Channel TX state: reachable
Channel next hop: 0.0.0.0
Channel recv_probes: 0
Channel send_probes: 0
Channel recv_packets: 0
Channel send_packets: 0
Channel recv_bytes: 0
Channel send_bytes 0
Last Probe Received: N/A
Last Probe Sent: N/A
.
.
.
------------------------------------------------------------------------------------------------------------
```

The fields shown above are self-explanatory.

Step 4 **show domain** *domain-name* **border exporter statistics**
This command displays the border site exporter statistics information.

Example:

```
BR#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 parent-route**
This command displays the parent route information of a channel.

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 channels parent route

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

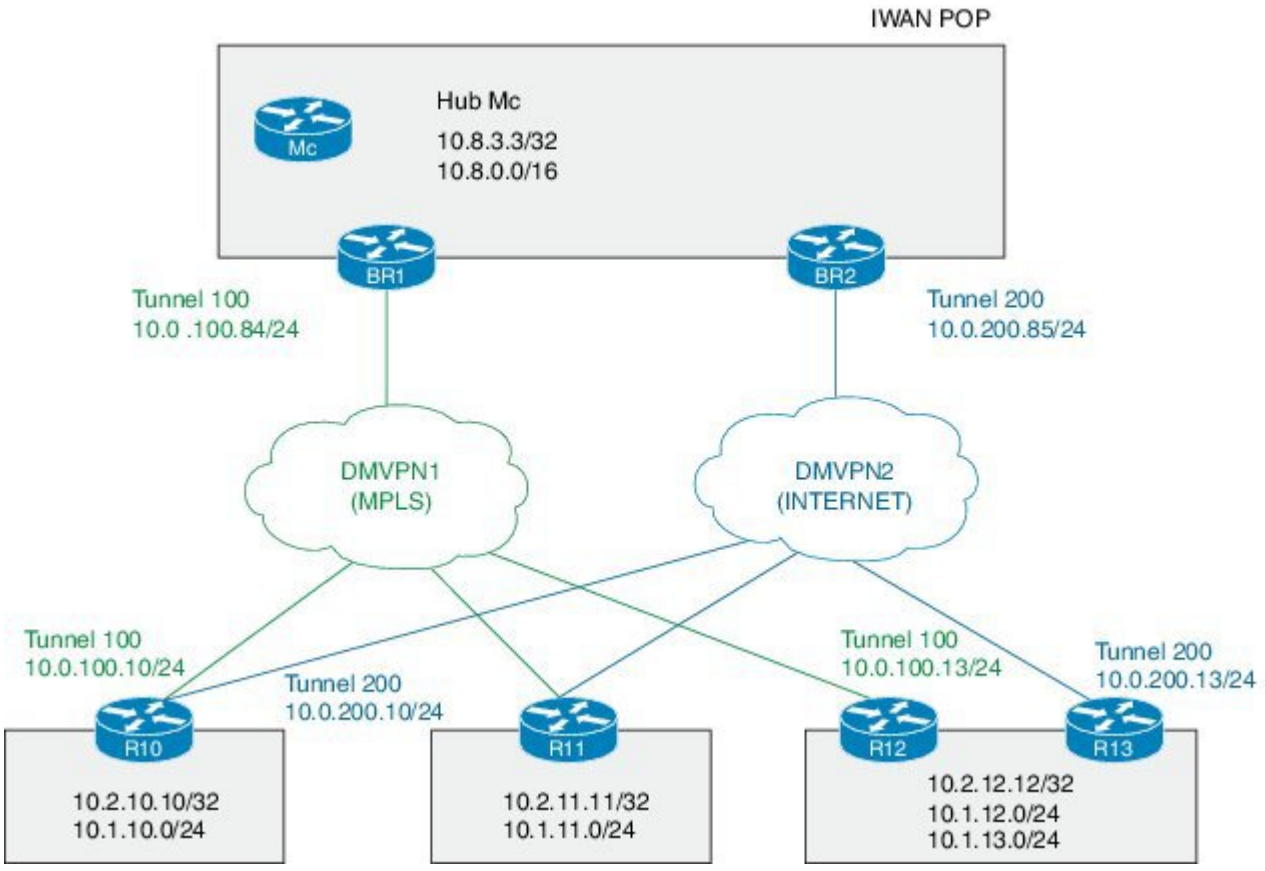
The fields shown above are self-explanatory.

Example: Configuring Performance Routing Version 3

Let us consider a use case scenario, where the service provider of a large enterprise network wants to optimize the WAN reliability and bandwidth of its network infrastructure based on applications between the head

quarter site and branch sites. The service provider wants the network to intelligently choose a path that meets the performance requirement of its video-based applications over non-critical applications.

Figure 2: PfRv3 Topology



In this example, the following routers are used:

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

Example: Configuring Hub Master Controller

```
! Configure the interfaces on hub master controller

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

! Configure the device as hub-master controller
```

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

! Configure IP prefix-lists

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

Example: Configuring Domain Policies on Hub Master Controller

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

Example: Configuring Hub Border Routers

```
! Configure the interfaces on hub border router (BR1)

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

! Configure the device as border router (BR1)

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


! Configure tunnel from BR1 to DMVPN1 (MPLS)Link

BR1(config)# interface Tunnel100
BR1(config-if)# bandwidth 100000
BR1(config-if)# ip address 10.0.100.84 255.255.255.0
BR1(config-if)# no ip redirects
BR1(config-if)# ip mtu 1400
BR1(config-if)# ip nhrp authentication cisco
BR1(config-if)# ip nhrp map multicast dynamic
BR1(config-if)# ip nhrp network-id 1
BR1(config-if)# ip nhrp holdtime 600
```

```
BR1(config-if)# ip tcp adjust-mss 1360
BR1(config-if)# load-interval 30
BR1(config-if)# tunnel source GigabitEthernet3
BR1(config-if)# tunnel mode gre multipoint
BR1(config-if)# tunnel key 100
BR1(config-if)# tunnel protection ipsec profile DMVPN-PROFILE1
BR1(config-if)# domain one path MPLS


! Configure the interfaces on hub border router (BR2)

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

! Configure the device as border router (BR2)

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

! Configure tunnel from BR2 to DMVPN2 (INTERNET)Link

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

Example: Configuring Branch Routers (Single CPE)

```
! Configure the interfaces (R10)

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

! Configure the device as branch master controller (R10)

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

! Configure the tunnel interface and tunnel path from R10
```

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


!Configure another tunnel path from R10


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



! Configure the interfaces (R11)

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

! Configure the device as branch master controller (R11)

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

! Configure the tunnel interface and tunnel path from R11

R11(config)# interface Tunnel100
```

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


!Configure another tunnel path from R11


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

Example: Configuring Branch Routers (Dual CPE)

```
! Configure the interfaces (R12)

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

! Configure the device as branch master controller (R12)

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


! Configure the tunnel interface and tunnel path from R12
```

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

! Configure the interfaces (R13)

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

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

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


! Configure the tunnel interface and tunnel path from R13

R13(config)# interface Tunnel200
R13(config-if)# bandwidth 50000
R13(config-if)# ip address 10.0.200.13 255.255.255.0
R13(config-if)# no ip redirects
R13(config-if)# ip mtu 1400
R13(config-if)# ip nhrp authentication cisco
R13(config-if)# ip nhrp map 10.0.200.85 172.16.85.5
R13(config-if)# ip nhrp multicast 172.16.85.5
R13(config-if)# ip nhrp network-id 2
R13(config-if)# ip nhrp holdtime 600
R13(config-if)# ip nhrp nhs 10.0.200.85
R13(config-if)# ip tcp adjust-mss 1360
R13(config-if)# load-interval 30
R13(config-if)# delay 1000
R13(config-if)# tunnel source GigabitEthernet6
R13(config-if)# tunnel mode gre multipoint
R13(config-if)# tunnel key 200
R13(config-if)# tunnel vrf INET2
R13(config-if)# tunnel protection ipsec profile DMVPN-PROFILE2
R13(config-if)# domain one path INET
```

Verifying PfR v3 Configuration on Cisco IOS XE Platform

To verify the PfR v3 configuration, use the following show commands in any order:

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

- **show domain** *domain-name* **border status**
- **show platform software pfrv3 rp active smart-probe**
- **show derived-config | section eigrp**
- **show domain** *domain-name* **master policy**
- **show domain** *domain-name* **border pmi**
- **show domain** *domain-name* **master channels**
- **show ip access-lists dynamic**
- **show domain** *domain-name* **master site-prefix**
- **show domain** *domain-name* **border site-prefix**
- **show domain** *domain-name* **master traffic-classess summary**
- **show domain** *domain-name* **master traffic-classess policy**