# Cisco IOS Performance Routing Version 3 Command Reference

**First Published:** 2017-04-07

**Last Modified:** 2019-03-11

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

# CONTENTS

# Performance Routing Version 3 Commands

# advanced

To enter advanced configuration mode and configure parameters for hub master controller configuration, use the **advanced** command in master controller configuration mode.

**advanced**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Default pre-defined parameters are used for hub master controller configuration.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

All configurable parameters under advanced configuration mode for hub master controller is pre-defined by default. You can choose to edit the parameters by entering into the advanced configuration mode. This is optional for hub master controller configuration.

### Example

The following example shows how to enter advanced configuration mode:

```
Device(config-domain-vrf-mc)# advanced
```

# bandwidth (interface configuration)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command in interface or virtual network interface config mode. To restore the default values, use the **no** form of this command.

**bandwidth** [{**receive**}] {*kbps*| **inherit** [{*kbps*}]}
**no bandwidth** [{**receive**}] {*kbps*| **inherit** [{*kbps*}]}

## Syntax Description

| | |
|---|---|
| *kbps* | Intended bandwidth, in kilobits per second. The range is from 1 to 10000000. For a full bandwidth DS3 line, enter the value 44736. |
| **inherit** | (Optional) Specifies how a subinterface inherits the bandwidth of its main interface. |
| **receive** | (Optional) Enables asymmetric transmit/receive operations so that the transmitted (**inherit** *kbps*) and received bandwidth are different. |

## Command Default

Default bandwidth values are set during startup. The bandwidth values can be displayed using the **show interfaces** or **show ipv6 interface** command. If the **receive** keyword is not used, by default, the transmit and receive bandwidths will be assigned the same value.

## Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2T | This command was modified. The **inherit** keyword was added. |
| 12.4(6)T | This command was modified. Support for IPv6 was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 Aggregation Services Series Routers. |
| Cisco IOS XE Release 3.2S | This command was modified. Support was added for this command in virtual network interface configuration mode. |
| 15.1(03)S | This command was modified. Support was added for the **receive** keyword. |

## Usage Guidelines

### Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

**Note** This is only a routing parameter. It does not affect the physical interface.

**Changing Bandwidth**

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting the hardware. For both classes of media, you can use the **bandwidth** command to communicate the current bandwidth to the higher-level protocols.

**Bandwidth Inheritance**

Before the introduction of the **bandwidth inherit** command option, when the bandwidth value was changed on the main interface, the existing subinterfaces did not inherit the bandwidth value. If the subinterface was created before the bandwidth was changed on the main interface, the subinterface would receive the default bandwidth of the main interface, and not the configured bandwidth. Additionally, if the router was subsequently reloaded, the bandwidth of the subinterface would then change to the bandwidth configured on the main interface.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface. This functionality eliminates inconsistencies related to whether the router has been reloaded and what the order was in entering the commands.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If the **bandwidth inherit** command is used without configuring a bandwidth on a subinterface, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the **bandwidth inherit** *kbps* command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an explicit bandwidth setting is configured on an interface, the interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

**Bandwidth Receipt**

Some interfaces (such as Asymmetric Digital Subscriber Line (ADSL), V.35, RS-449, and High-Speed Serial Interface (HSSI)) can operate with different transmit and receive bandwidths. The **bandwidth receive** command permits this type of asymmetric operation. For example, for ADSL, the lower layer detects the two bandwidth values and configures the Integrated Data Base (IDB) accordingly. Other interface drivers, particularly serial interface cards on low- and midrange-platforms, can operate in this asymmetric bandwidth mode but cannot measure their clock rates. In these cases, administrative configuration is necessary for asymmetric operations.

## Examples

The following example shows how to set the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

The following example shows how to set the receive bandwidth:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth receive 1000
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics for all interfaces configured on the router. |
| **show ipv6 interface** | Displays statistics for all interfaces configured on the IPv6 router. |

# border (VRF configuration)

To configure border devices for Performance Routing v3 configuration, use the **border** command in vrf configuration mode. To remove the configuration, use the **no** form of this command.

**border**
**no border**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Border is not configured for PfRv3 configuration.

## Command Modes

VRF configuration mode (config-domain-vrf)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

This command is available only on hub and regional hub master types.

### Example

The following example shows how to enter border configuration mode:

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

# branch-to-branch

To enable branch to branch PfRv3 optimization, use the **branch-to-branch** command in domain master controller configuration mode. To disable branch to branch PfRv3 optimizatin, use the **no** form of this command.

**branch-to-branch**
**no branch-to-branch**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Domain master controller configuration

| Release | Modification |
|---|---|
| 16.3.4 | This command was introduced. |
| 3.16.6 | This command was integrated. |
| 16.6.1 | This command was integrated. |
| Cisco IOS XE 16.8.1 | This command was integrated. |
| Cisco IOS XE 16.8.2 | This command was modified.<br>**Note** For this release and later releases, the **branch-to-branch** command will be published by default. So that local sites and remote sites will not establish spoke to spoke channels and traffic-classes. The 'branch-to-branch' command does not block traffic-classes learning and smart-probes that are sent to remote sites. |
| Cisco IOS XE 16.9.2 | This command was integrated. |
| Cisco IOS XE 16.10.1 | This command was integrated. |

## Usage Guidelines

The **branch-to-branch** command can be configured only on branch masters. Configuring this command results in two different behaviors for different releases.

**Behavior 1**

Spoke-to-spoke traffic class learning is enabled by default. The **no branch-to-branch** is an enhancement to make sure that no spoke to spoke channel is established. Spoke-to-spoke channles with limitation for small branch sites may be inundated in a scale condition due to a CPU malfunction or a bandwidth overhead.

**Behavior 2**

The**branch-to-branch** command will be published by default. So that local sites and remote sites will not build spoke to spoke channels and traffic-classes. The **branch-to-branch** command does not block traffic-classes learning and smart-probes that are sent to remote sites.

### Example

The following example for branch-to-branch configuration.

```
1. Enabled 'branch-to-branch' by default
domain iwan
 logging version v2 ime tca path
 vrf default
  border
   source-interface Loopback1
   master local
  master branch
   source-interface Loopback1
   traffic-class-max 4000
   hub 168.254.0.2
   branch-to-branch
   route-update-dampner 2

BRANCH2MCBR#show domain iwan master status

  *** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Branch
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 168.254.0.11
  Load Balancing:
   Operational Status: Up
   Max Calculated Utilization Variance: 0%
   Last load balance attempt: never
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kbps
  External Collector: 10.74.28.60 port: 9995
  Route Control: Enabled
  Transit Site Affinity: Enabled
  Load Sharing: Enabled
  Connection Keepalive: 10 seconds
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length Internet: 24
  Minimum Mask Length Enterprise: 24
  Syslog TCA suppress timer: 180 seconds
  Traffic-Class Ageout Timer: 5 minutes
  Minimum Packet Loss Calculation Threshold: 15 packets
  Minimum Bytes Loss Calculation Threshold: 1 bytes
  Branch to Branch Traffic Control: Enabled
  Maximum Traffic Classes Supported: 4000
  Minimum Requirement: Met

  Borders:
    IP address: 168.254.0.11
    Version: 2
    Connection status: CONNECTED (Last Updated 20:51:09 ago )
    Interfaces configured:
      Name: Tunnel10 | type: external | Service Provider: MPLS1 | Status: UP | Zero-SLA:
NO | Path of Last Resort: Disabled
          Number of default Channels: 0

          Path-id list: 0:11 3:31

2. Disabled 'branch-to-branch'
domain iwan
 logging version v2 ime tca path
 vrf default
```

```
  border
   source-interface Loopback1
   master local
  master branch
   source-interface Loopback1
   traffic-class-max 4000
   hub 168.254.0.2
   no branch-to-branch
   route-update-dampner 2

BRANCH2MCBR#show domain iwan master status

  *** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Branch
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 168.254.0.11
  Load Balancing:
   Operational Status: Up
   Max Calculated Utilization Variance: 0%
   Last load balance attempt: never
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kbps
  External Collector: 10.74.28.60 port: 9995
  Route Control: Enabled
  Transit Site Affinity: Enabled
  Load Sharing: Enabled
  Connection Keepalive: 10 seconds
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length Internet: 24
  Minimum Mask Length Enterprise: 24
  Syslog TCA suppress timer: 180 seconds
  Traffic-Class Ageout Timer: 5 minutes
  Minimum Packet Loss Calculation Threshold: 15 packets
  Minimum Bytes Loss Calculation Threshold: 1 bytes
  Branch to Branch Traffic Control: Disabled
  Maximum Traffic Classes Supported: 4000
  Minimum Requirement: Me

  Borders:
    IP address: 168.254.0.11
    Version: 2
    Connection status: CONNECTED (Last Updated 00:00:10 ago )
    Interfaces configured:
      Name: Tunnel10 | type: external | Service Provider: MPLS1 | Status: UP | Zero-SLA:
NO | Path of Last Resort: Disabled
          Number of default Channels: 0

          Path-id list: 3:31 0:11
```

# channel-based-measurement

To configure the performance monitors used by PfRv3 to employ a sampling method, use the **channel-based-measurement** command in domain master hub advanced mode. This data collection method is typically more accurate, combining the use of metadata and traffic sampled at intervals to provide traffic metrics.

**config terminal**
**domain iwan**
**master hub**
**advanced**
**channel-based-measurement**
[**sampling-rate** *sampling-rate*] [**quick** *sampling-rate-for-quick-monitoring*]
[**sample-packet-size** *maximum-packet-size*]

To disable:

**no channel-based-measurement**

## Syntax Description

| | |
|---|---|
| **sampling-rate** | (Optional) Manually sets the sampling rate (samples per second) for traffic packet samples.<br>Default: 10 (sample interval: 100 ms)<br>Possible sample rate values and corresponding sample intervals (note that sample intervals are rounded):<br>1 (sample interval 1000 ms)<br>2 (sample interval 500 ms)<br>3 (sample interval 330 ms)<br>4 (sample interval 250 ms)<br>5 (sample interval 200 ms)<br>6 (sample interval 160 ms)<br>7 (sample interval 140 ms)<br>8 (sample interval 120 ms)<br>9 (sample interval 110 ms)<br>10 (sample interval 100 ms)<br>20 (sample interval 50 ms)<br>25 (sample interval 40 ms)<br>33 (sample interval 30 ms)<br>50 (sample interval 20 ms) |

**quick** (Optional) Sampling rate (samples per second) for quick monitoring.

Possible sample rate values and corresponding sample intervals (note that sample intervals are rounded):

1 (sample interval 1000 ms)
2 (sample interval 500 ms)
3 (sample interval 330 ms)
4 (sample interval 250 ms)
5 (sample interval 200 ms)
6 (sample interval 160 ms)
7 (sample interval 140 ms)
8 (sample interval 120 ms)
9 (sample interval 110 ms)
10 (sample interval 100 ms)
20 (sample interval 50 ms)
25 (sample interval 40 ms)
33 (sample interval 30 ms)
50 (sample interval 20 ms)

The quick monitoring option provides a different sample rate for specific traffic designated by the **monitor-interval** command. So the sampling-rate interval is used for general traffic, and the quick interval is used for any traffic configured with **monitor-interval**. For example, if a specific interval is configured for DSCP traffic using...

```
monitor-interval 2 dscp ef
```

… then the quick interval would apply to metrics for DSCP traffic.

**Comparison of default monitoring and quick monitoring**: The default monitoring mode is optimized for efficient use of bandwidth. The quick monitoring mode is optimized for greater accuracy of metrics calculated for a specified subset of the total traffic. For example:

- If the **default** sample rate is configured to 10, then every 100 ms, the feature chooses one sampling packet from the user traffic. If there is no sample packet in that 100 ms interval, the feature does not send a sample packet. This reduces the bandwidth required for default monitoring. However, if there is no sampling available for a full 1 second interval, the feature generates a smart probe as a sampling packet.
- By contrast, with **quick** monitoring, if there is no sample available in a specific interval, the feature will generate a smart probe as a sample packet to help in calculating performance metrics. This consumes more bandwidth but provides a more accurate calculation of metrics for the specified traffic.

**sample-packet-size** (Optional) Maximum sample packet size.

The value should not be more than (MTU - metadata size). For example, if MTU is 1500 and packet metadata is 24, then the calculation is:

(1500 - 24) = 1476

Options:

- default

  Value: 1200

- Enter the maximum sample size in bytes.

  Possible values: 128 to 1400

- **interface-mtu**

  Get the maximum sample size from MTU on interface.

## Command Modes

Domain master hub advanced mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

## Usage Guidelines

To enable the feature, execute this command at the hub site, regardless of the number of branch sites.

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.

### Simple example

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
```

### Example with packet size and sampling rate options

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
```

### Displaying channel-based-measurement status

Use **show domain iwan border site-capability** to display the status of channel-based-measurement, as TRUE or FALSE. In the example below, the "Channel based measurement supported: TRUE" line indicates that channel-based-measurement is enabled.

```
Device-BR1#show domain iwan border site-capability
Device Capability

------------------------------------------------------------
|       Capability          |     Major     |     Minor      |
------------------------------------------------------------
|     Domain                |     2         |      0         |
------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
------------------------------------------------------------
|     Mul-Hop               |     1         |      0         |
------------------------------------------------------------
Site id  : 10.8.10.10

------------------------------------------------------------
|       Capability          |     Major     |     Minor      |
------------------------------------------------------------
|     Domain                |     2         |      0         |
------------------------------------------------------------
|     Zero-SLA              |     1         |      0         |
------------------------------------------------------------
|     Mul-Hop               |     1         |      0         |
------------------------------------------------------------
Channel based measurement supported: TRUE
```

### Displaying detailed status: Hub site

Use **show domain iwan master status** at a hub site to display the detailed status of channel-based-measurement. ("…" indicates abbreviated output)

```
Device-MC1#show domain iwan master status
*** Domain MC Status ***

Master VRF: Global

  Instance Type:    Hub
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 10.8.10.10
  Global Config Last Publish status: Peering Success
…
 Channel Based Measurement:
    State: Enabled
    Parameters:
      Sampled Packets for Normal Monitor: 10 pps
      Sampled Packets for Quick Monitor: 10 pps
      Maximum packet size for sampling: 1200 bytes(Default)
      Clock frequency for timestamp: 4000 Hz
…
```

### Displaying detailed status: Border router

Use **show domain iwan border status** on a border router to display the status of channel-based-measurement. ("…" indicates abbreviated output)

```
Device-BR1#show domain iwan border status
**** Border Status ****

Instance Status: UP
Present status last updated: 1d23h ago
Loopback: Configured Loopback0 UP (10.8.1.1)
Master: 10.8.10.10
Master version: 2
Connection Status with Master: UP
MC connection info: CONNECTION SUCCESSFUL
Connected for: 00:05:31
Branch bandwidth check percentage: 0%
Route-Control: Enabled
…
Channel Based Measurement:
  State: Enabled
  Parameters:
    Sampled Packets for Normal Monitor: 10 pps
    Sampled Packets for Quick Monitor: 10 pps
    Maximum packet size for sampling: 1200 bytes(Default)
    Clock frequency for timestamp: 4000 Hz
…
```

# class (master controller configuration)

To enter policy class configuration mode and configure domain class, use the **class** command in master controller configuration mode. To remove the domain class configuration, use the **no** form of this command.

**class** *domain-name* **sequence** *number*
**no class** *domain-name* **sequence** *number*

## Syntax Description

| | |
|---|---|
| *domain-name* | Specifies the domain class name. |
| **sequence** | Specifies the sequence for the class. |
| *number* | Specifies the sequence number for the class. The range is from 1 to 65535. |

## Command Default

Domain class is not configured.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command for hub master controller configuration.

### Example

The following example shows how to configure class:

```
Device(config-domain-vrf-mc)# class policy sequence 100
```

# collector

To configure IP address of the Network Management System (NMS) or external v9 collector, use the **collector** command in master controller configuration mode. To remove the NMS/externalv9 collector, use the **no** form of this command.

**collector** *ip-address*
**no collector** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Specifies the IP address of NMS/v9 collector. |

## Command Default

NMS/ external v9 collector is not configured.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

### Example

The below example shows how to configure collector IP address:

```
Device(config-domain-vrf-mc)# collector 10.10.10.10
```

# debug platform hardware qfp active feature pfrv3

To enable Performance Routing Version 3 (PfRv3) Cisco Quantum Flow Processor (QFP) debug logging, use the **debug platform hardware qfp active feature pfrv3** command in privileged EXEC mode.

**debug platform hardware qfp active feature pfrv3**{**client**|**datapath**|**pal**}

## Syntax Description

| | |
|---|---|
| **client** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) client debug logging. |
| **datapath** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) data path debug logging. |
| **pal** | Enables debug logging for PfRv3 in the Cisco Quantum Flow Processor (QFP). |

## Command Default

Cisco Quantum Flow Processor (QFP) debug logging on PfRv3 is not enabled

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to enable debug logging for PfRv3 Cisco Quantum Flow Processor (QFP).

# debug platform software pfrv3

To enable debugging of Performance Routing Version 3 (PfRv3) configuration, use the **debug platform software pfrv3** command in privileged EXEC mode.

**debug platform software pfrv3**[{**auto-tunnel |channel|route-control|site-prefix|smart-probe**}]

## Syntax Description

| | |
|---|---|
| **auto-tunnel** | Enables debugging of PfRv3 auto-tunnels. |
| **channel** | Enables debugging of PfRv3 channels. |
| **route-control** | Enables debugging of PfRv3 route control. |
| **site-prefix** | Enables debugging of PfRv3 site prefixes. |
| **smart-probe** | Enables debugging of PfRv3 smart probes. |

## Command Default

Debugging of PfRv3 configuration is not enabled.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use the debug platform software pfrv3 command to enable debugging of PfRv3 configurations for troubleshooting purposes.

### Example

The following example enables debugging traffic probe configuration in PfRv3.

```
Device# debug platform software pfrv3 smart-probe
PfRv3 smart-probe debug debugging is on
```

# description (interface configuration)

To add a description to an interface configuration, use the **description** command in interface configuration mode. To remove the description, use the **no**form of this command.

**description** *string*
**no description**

## Syntax Description

| | |
|---|---|
| *string* | Comment or a description to help you remember what is attached to this interface. This string is limited to 238 characters. |

## Command Default

No description is added.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 9.21 | This command was introduced. |

## Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain interfaces are used for. The description appears in the output of the following EXEC commands:**morenvram:startup-config**, **showinterfaces**, and**moresystem:running-config**

## Examples

The following example shows how to add a description for a T1 interface:

```
interface serial 0
 description Fractional T1 line to remote office -- 128 kbps
```

## Related Commands

| Command | Description |
|---|---|
| **more nvram:startup-config** | Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable. |
| **more system:running-config** | Displays the running configuration. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |

# domain (interface configuration)

To configure the Internet Service Provider (ISP) for a hub border router in a Performance Routing Version 3 (PfRv3) configuration, use the **domain** command in interface configuration mode. To remove the configured ISP, use the **no** form of the command.

**domain** *domain-name*{**path** *path-name*}[{**path-id** *number*}][{**internet-bound**|**path-last-resort**|**zero-sla**}]
**no domain** *domain-name*{**path** *path-name*}[{**path-id** *number*}][{**internet-bound**|**zero-sla**|**path-last-resort**}]

## Syntax Description

| | |
|---|---|
| *domain-name* | The domain name. |
| **path** *path-name* | Associates a path to the ISP.<br>**Note** The value for the *path-name* argument is restricted to seven characters. |
| **path-id** *number* | Specifies a unique path ID for the interface in the domain. The values for the *number* argument are from 1 to 255. |
| **internet-bound** | Configures Internet bound interface. |
| **zero-sla** | Configures zero SLA for interface. |

## Command Default

ISP is not configured.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |
| Cisco IOS XE Release 3.14S | This command was modified. The **zero-sla** keyword was added. |
| Cisco IOS XE Release 3.16S | This command was modified. The **path-last-resort** keyword was added. |

## Usage Guidelines

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. The domain command configures the Internet Service Provider (ISP). 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. Internet-bound external interface is configured only on the hub site for the internet edge deployment and cannot be discovered by any branch site. It is recommended that you use 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_abc, you must specify the same domain name for configuring ISP paths.

You must assign a unique path ID for all paths that are connected from hub-border routers to the same ISP domain.

## Example

The following example shows the **domain** command configured on a hub border router with MPLS as the domain path, with a path ID of 30, and zero SLA.

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

# domain (global configuration)

To configure a top level domain for Performance Routing version 3 (PfRv3) configuration, use the **domain** command in global configuration mode. To remove the domain configuration, use the **no** form of this command.

**domain** {*domain-name*|**default**}
**no domain** {*domain-name*|**default**}

## Syntax Description

| | |
|---|---|
| *domain-name* | Name of the domain for PfRv3 configuration. |
| **default** | Default domain for PfRv3 configuration. |

## Command Default

Domain is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

The **domain** command is entered on a master controller or border router on both hub and branch to configure the domain. You can then configure Virtual Routing and Forwarding (VRF) on a domain for PfRv3 configuration.

You can either configure a default domain or define a specific domain for Master Controller (MC) configuration. If you are defining the specific domain, for example “domain-cisco”, you must configure the same domain for all devices for PfRv3 configuration.

The following example shows how to configure domain:

```
Device> enable
Device# configure terminal
Device(config)# domain default
Device(config)# domain domain-cisco
```

# enterprise-prefix

To configure an enterprise prefix-list with static site targets, use the **enterprise-prefix** command in master controller configuration mode. To remove the enterprise-prefix, use the **no** form of this command.

**enterprise-prefix prefix-list** *site-list*
**no enterprise-prefix prefix-list** *site-list*

## Syntax Description

| | |
|---|---|
| **prefix-list** | Specifies prefix-list with static site targets. |
| *site-list* | Specifies prefix-list with list of site targets. |

## Command Default

Prefix-list is not configured for hub master controller configuration.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command with the **ip prefix-list** command. Match conditions specified in the **ip prefix-list** command are only supported.

### Example

The following example shows how to configure enterprise prefix-list:

```
Device(config-domain-vrf-mc)# enterprise-prefix prefix-list site_prefixes
```

## Related Commands

| Command | Description |
|---|---|
| **ip prefix-list** | Creates a prefix list or adds a prefix-list entry. |

# fallback-timer

To specify the time interval for re-evaluating a primary path after traffic has changed to a backup path, use the **fallback-timer** command in domain class configuration mode.

**fallback-timer** *time-in-minutes*[{**dampening** {**enable**|**disable**}}]

**fallback-timer off**

## Syntax Description

| | |
|---|---|
| *time-in-minutes* | Evaluation period (called timeout) for re-evaluating the performance of the primary path, to determine whether to switch a traffic class from a backup path back to the primary path. If the primary path meets the performance requirements specified for the traffic class again, PfRv3 switches the traffic class to the primary path.<br>Increasing the time causes PfRv3 to evaluate the primary path over a longer time. In some situations, this can prevent excessive switching between the primary and backup paths.<br>Applicable to:<br>Global (per VRF)<br>Traffic class<br>Possible values: 1 to 1440 minutes<br>Default: 3 minutes |
| **dampening** | (Optional) When enabled, dampening reduces excessive switching between primary and backup paths by dynamically adjusting the evaluation period for re-evaluating the performance of the primary path.<br>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<br>Applicable to:<br>Traffic class<br>Possible values: enable, disable<br>Default: enable (if fallback-timer is configured) |
| **off** | 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. |

## Command Default

Default interval: 3 minutes

## Command Modes

Domain class configuration (config-domain-vrf-mc-class)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

### Example

Set the evaluation period to 10 minutes.

```
fallback-timer 10
```

### Example

Set the evaluation period to 10 minutes, and disable dampening.

```
fallback-timer 10 dampening enable
```

On a traffic class, set the fallback timer to 5 minutes, dampening enabled by default.

```
domain iwan
vrf default
master hub
class VOICE sequence 10
match app audio policy voice
path-preference MPLS1 fallback INET1
fallback-timer 5
```

On a traffic class, set the fallback timer to 10 minutes, disable dampening.

```
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
```

On a traffic class, turn the fallback timer off.

This disables 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 MPLS1fallback-timer off
```

Globally, configure the fallback timer to 4 minutes.

```
domain iwan
vrf default
master hub
```

```
advanced
fallback-timer 4
```

Globally, disable the fallback timer.

Disables 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.

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

**Related Commands**

| Command | Description |
|---|---|
| **show domain vrf master policy** | Shows fallback-timer status. |
| **show domain vrf master traffic-classes detail** | Shows fallback-timer status. |

# hub

To configure the IP address of the hub master controller, use the **hub** command in master controller configuration mode. To remove the IP address, use the **no** form of this command.

**hub** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Specifies the IP address of regional-hub master controller. |

## Command Default

IP address of regional-hub master controller is not configured.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

Use this command for the branch master controller configuration.

### Example

The following example shows how to configure IP address of the regional-hub master controller when configuring branch master controller:

```
Device(config-domain-vrf-mc)# hub 10.1.1.1
```

# interface tunnel (global configuration)

To enter interface configuration mode and configures tunnel name, use the **interface tunnel** command in global configuration mode.

**interface tunnel** *tunnel-name*

## Syntax Description

| | |
|---|---|
| *tunnel-name* | Specifies tunnel interface number. The range is from 0 to 2147483647. |

## Command Default

Tunnel interfaces are not configured.

## Command Modes

Global configuration (config)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

### Example

The following example shows how to enter interface configuration mode:

```
Device(config)# interface Tunnel100
```

# ip prefix-list

To create a prefix list or to add a prefix-list entry, use the **ip prefix-list** command in global configuration mode. To delete a prefix-list entry, use the **no** form of this command.

**ip prefix-list** {*list-name* [**seq** *number*] {**deny**|**permit**} *network*/*length* [**ge** *ge-length*] [**le** *le-length*]|**description** *description*|**sequence-number**}
**no ip prefix-list** {*list-name* [**seq** *number*] [{**deny**|**permit**} *network*/*length* [**ge** *ge-length*] [**le** *le-length*]]|**description** *description*|**sequence-number**}

## Syntax Description

| | |
|---|---|
| *list-name* | Configures a name to identify the prefix list. Do not use the word "detail" or "summary" as a list name because they are keywords in the **show ip prefix-list** command. |
| **seq** | (Optional) Applies a sequence number to a prefix-list entry. |
| *number* | (Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5. |
| **deny** | Denies access for a matching condition. |
| **permit** | Permits access for a matching condition. |
| *network* / *length* | Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32. |
| **ge** | (Optional) Specifies the lesser value of a range (the "from" portion of the range description) by applying the *ge-length* argument to the range specified.<br>**Note** The **ge** keyword represents the greater than or equal to operator. |
| *ge-length* | (Optional) Represents the minimum prefix length to be matched. |
| **le** | (Optional) Specifies the greater value of a range (the "to" portion of the range description) by applying the *le-length* argument to the range specified.<br>**Note** The **le** keyword represents the less than or equal to operator. |
| *le-length* | (Optional) Represents the maximum prefix length to be matched. |
| **description** | (Optional) Configures a descriptive name for the prefix list. |
| *description* | (Optional) Descriptive name of the prefix list, from 1 to 80 characters in length. |
| **sequence-number** | (Optional) Enables or disables the use of sequence numbers for prefix lists. |

## Command Default

No prefix lists or prefix-list entries are created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. Prefix lists are configured with **permit** or **deny** keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the **ge** and **le** keywords are used. The **ge** and **le** keywords are used to specify a range of prefix lengths and provide more flexible configuration than using only the *network*/*length* argument. A prefix list is processed using an exact match when neither the **ge** nor **le** keyword is specified. If only the **ge** value is specified, the range is the value entered for the **ge** *ge-length* argument to a full 32-bit length. If only the **le** value is specified, the range is from the value entered for the *network*/*length argument* to the **le** *le-length* argument. If both the **ge** *ge-length* and **le** *le-length* keywords and arguments are entered, the range is between the values used for the *ge-length* and *le-length* arguments.

The following formula shows this behavior:

*length* <**ge** *ge-length* <**le** *le-length* <= 32

If the **seq** keyword is configured without a sequence number, the default sequence number is 5. In this scenario, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5. For example, the next two entries would have sequence numbers 10 and 15. If a sequence number is entered for the first prefix list entry but not for subsequent entries, the subsequent entry numbers increment by 5. For example, if the first configured sequence number is 3, subsequent entries will be 8, 13, and 18. Default sequence numbers can be suppressed by entering the **no ip prefix-list** command with the **seq** keyword.

Evaluation of a prefix list starts with the lowest sequence number and continues down the list until a match is found. When an IP address match is found, the permit or deny statement is applied to that network and the remainder of the list is not evaluated.

**Tip** For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The **seq** *number* keyword and argument can be used for resequencing.

A prefix list is applied to inbound or outbound updates for a specific peer by entering the **neighbor prefix-list** command. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

## Examples

In the following example, a prefix list is configured to deny the default route 0.0.0.0/0:

```
Router(config)# ip prefix-list RED deny 0.0.0.0/0
```

In the following example, a prefix list is configured to permit traffic from the 172.16.1.0/24 subnet:

```
Router(config)# ip prefix-list BLUE permit 172.16.1.0/24
```

In the following example, a prefix list is configured to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

```
Router(config)# ip prefix-list YELLOW permit 10.0.0.0/8 le 24
```

In the following example, a prefix list is configured to deny routes from the 10.0.0.0/8 network that have a mask length that is greater than or equal to 25 bits:

```
Router(config)# ip prefix-list PINK deny 10.0.0.0/8 ge 25
```

In the following example, a prefix list is configured to permit routes from any network that have a mask length from 8 to 24 bits:

```
Router(config)# ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24
```

In the following example, a prefix list is configured to deny any route with any mask length from the 10.0.0.0/8 network:

```
Router(config)# ip prefix-list ORANGE deny 10.0.0.0/8 le 32
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip prefix-list** | Resets the prefix list entry counters. |
| **ip prefix-list description** | Adds a text description of a prefix list. |
| **ip prefix-list sequence** | Enables or disables default prefix-list sequencing. |
| **match ip address** | Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets. |
| **neighbor prefix-list** | Filters routes from the specified neighbor using a prefix list. |
| **show ip prefix-list** | Displays information about a prefix list or prefix list entries. |

# load-balance

To configure load balancing for non-policy traffic, use the **load-balance** command in master controller configuration mode. To remove the load-balancing, use the **no** form of this command.

**load-balance**
**no load-balance**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Load balancing is not configured for hub master controller configuration.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

### Example

The following example shows how to configure load-balancing:

```
Device(config-domain-vrf-mc)# load-balance
```

# logging (domain configuration)

To enable syslog event logging for Performance Routing Version 3(PfRv3), use the **logging** command in domain configuration mode. To disable PfRv3 event logging, use the **no** form of this command.

**logging**[{**ime**}][{**path**}][{**tc**}][{**tca**}][{**version**{**v1**|**v2**}}]
**no logging**

## Syntax Description

| | |
|---|---|
| **ime** | Enables syslog for inimitigable events. |
| **path** | Enables syslog for path changes. |
| **tc** | Enables syslog for traffic control. |
| **tca** | Enables syslog for threshold crossing alert. |
| **version** {**v1** \| **v2**} | Enables choosing the syslog format version, which could be version 1 (v1) or version 2 (v2). |

## Command Default

Syslog event logging is not enabled.

## Command Modes

Domain configuration (config-domain)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

The logging command is entered on a hub and distributed to master controllers.

## Examples

The following example shows a sample output of the **logging imc**command on a master controller:

```
Router(config)# domain one
Router(config-domain)# logging ime
May 26 10:44:05.316 PDT: %DOMAIN-2-IME: Immitigable event occured. IME-ID=1804: Details:
Instance=1: VRF=green:
Source Site ID=100.10.1.1: Destination Site ID=100.30.1.1: Reason=No Alternate Exit: TCA-ID=0:
 Policy Violated=None:
Current Exit=[CHAN-ID=54, BR-IP=100.10.1.1, DSCP=ef[46], Interface=Tunnel30,
Path=ISP3[label=0:0 | 0:7 [0x7]]]:
Out Of BW Alt Exits=0: Out Of Policy Alt Exits=4
```

## Related Commands

| Command | Description |
|---|---|
| **domain** | Configures a top level domain for PfRv3 configuration. |

# master (border router configuration)

To specify the IP address of a branch-master controller and branch border router, use the **master** command in border router configuration mode. To remove the IP address, use the **no** form of this command.

**master** {*ip-address*|**local**}
**no master** {*ip-address*|**local**}

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the branch-master controller. |
| **local** | Local IP address of the branch-master controller. |

## Command Default

No IP address is specified.

## Command Modes

Border router configuration (config-domain-vfr-br)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

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.

## Examples

The following example shows how to Configure the device as branch master controller .

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

The following example shows how to configure a device as border router.

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

## Related Commands

| Command | Description |
|---|---|
| **border (PfRv3)** | Configures border devices for Performance Routing v3 configuration. |

# master (domain vrf configuration)

To define a master type for the device in the Performance Routing Version 3 (PfRv3) configuration, use the **master** command in domain VRF configuration mode. To remove the master type configuration, use the **no** form of this command.

**master**{**branch**|**hub**|**transit** *pop-id*}
**no master**{**branch**|**hub**|**transit**}

## Syntax Description

| | |
|---|---|
| **branch** | Sets master type as branch hub. |
| **hub** | Sets master type as hub. |
| **transit** | Sets master type as transit. |
| *pop-id* | Specifies the POP ID. |

## Command Default

The master type is not defined.

## Command Modes

Domain VRF configuration (config-domain-vrf)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

### Example

The following example shows how to set up master type for a device:

```
Device> enable
Device# configure terminal
Device(config)# domain default
Device(config-domain)# vrf cisco
Device(config-domain-vrf)# master branch
Device(config-domain-vrf)# master hub
Device(config-domain-vrf)# master regional-hub
```

# match

To specify the application or DSCP policies for class, use the **match** command in domain class configuration mode. To remove the class policies, use the **no** of this command.

**match**
{**application** {*application-name* | **default** | **policy** {**best-effort** | **bulk-data** | **custom** | **low-latency-data** | **real-time-video** | **scavenger** | **voice**}} | **dscp** {*codepoint-value* | **af** | **cs** | **default** | **ef** | **policy** {**best-effort** | **bulk-data** | **custom** | **low-latency-data** | **real-time-video** | **scavenger** | **voice**}}}
**no match**
{**application** {*application-name* | **default** | **policy** {**best-effort** | **bulk-data** | **custom** | **low-latency-data** | **real-time-video** | **scavenger** | **voice**}} | **dscp** {*codepoint-value* | **af** | **cs** | **default** | **ef** | **policy** {**best-effort** | **bulk-data** | **custom** | **low-latency-data** | **real-time-video** | **scavenger** | **voice**}}}

## Syntax Description

| | |
|---|---|
| **application** | Specifies the application. |
| **dscp** | Specifies the DSCP. |
| *codepoint-value* | Specifies the differentiated services code-point value. The range is from 0 to 63. |
| **af** | Specifies the match packets with AF DSCP. |
| **cs** | Specifies the match packets with CS DSCP. |
| **default** | Specifies the match packets with default DSCP. |
| **ef** | Specifies the match packets with EF DSCP. |
| **policy** | Specifies the user-defined or pre-defined policy type. |
| **best-effort** | Specifies the domain policy type as best effort. |
| **bulk-data** | Specifies the domain policy type as bulk data. |
| **custom** | Specifies the domain policy type as custom. |
| **low-latency-data** | Specifies the domain policy type as low latency data. |
| **real-time-video** | Specifies the domain policy type as real time video. |
| **scavenger** | Specifies the domain policy type as scavenger. |
| **voice** | Specifies the domain policy type as voice. |

## Command Default

User-defined or pre-defined policies are not defined.

## Command Modes

Domain class configuration (config-domain-vrf-mc-class)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to configure domain policies on a master hub controller. 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 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.

### Example

The following example shows how to configure DSCP policies:

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

# minimum-mask-length

To configure minimum mask length value to be applied on egress flows, use the **minimum-mask-length** command in advanced configuration mode. To remove the mask length value, use the **no** form of this command.

**minimum-mask-length**{*value*|**enterprise**|**internet**}
**no minimum-mask-length**[{**enterprise**|**internet**}]

## Syntax Description

| | |
|---|---|
| *value* | Specifies the minimum mask length. The range is from 1 to 32. |
| **enteprise** | Specifies the enterprise minimum mask length. |
| **internet** | Specifies the internet minimum mask length. |

## Command Default

Default minimum mask length is used for hub master controller configuration.

## Command Modes

Advanced configuration mode (config-domain-vrf-mc-advanced)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |
| Cisco IOS XE Denali 16.3.1 | This command was modifed. The keywords **enterprise** and **internet** were added. |

## Usage Guidelines

Minimum mask value is applied on IP addresses to generate a prefix to be used on egress flows

### Example

The following example shows how to configure minimum mask length value for hub master controller configuration:

```
Device(config-domain-vrf-mc-advanced)# minimum-mask-length 28
```

# mitigation-mode

To configure mitigation mode for hub master controller configuration, use the **mitigation-mode** command in advanced configuration mode.

**mitigation-mode aggressive**
**no mitigation-mode aggressive**

## Syntax Description

| | |
|---|---|
| **aggressive** | Specifies the aggressive brownout. |

## Command Default

Brownout mitigation is not configured.

## Command Modes

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

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

### Example

The below example shows how to configure brownout mitigation mode:

```
Device(config-domain-vrf-mc-advanced)# mitigation-mode aggressive
```

# monitor-interval

To configure interval time that defines monitoring interval on ingress monitors, use the **monitor-interval** command in master controller configuration mode. To remove the monitoring interval time, use the **no** form of this command.

**monitor-interval** *seconds*
**dscp**{*dscp-value*|**af11**|**af12**|**af13**|**af21**|**af22**|**af23**|**af31**|**af32**|**af33**|**af41**|**af42**|**af43**|**cs1**|**cs2**|**cs3**|**cs4**|**cs5**|**cs6**|**cs7**|**default**|**ef**}
**no monitor-interval**

## Syntax Description

| | |
|---|---|
| *seconds* | Specifies the monitoring interval in seconds. The range is from 1 to 300. |
| **dscp** | Specifies the Differentiated Services Code Point (DSCP). |
| *dscp-value* | Specifies the DSCP value codes. The range is from 0 to 63. |
| **af11** | Match packets with AF11 dscp (001010). |
| **af12** | Match packets with AF12 dscp (001100). |
| **af13** | Match packets with AF13 dscp (001110). |
| **af21** | Match packets with AF21 dscp (010010). |
| **af22** | Match packets with AF22 dscp (010100). |
| **af23** | Match packets with AF23 dscp (010110). |
| **af31** | Match packets with AF31 dscp (011010). |
| **af32** | Match packets with AF32 dscp (011100). |
| **af33** | Match packets with AF33 dscp (011110). |
| **af41** | Match packets with AF41 dscp (100010). |
| **af42** | Match packets with AF42 dscp (100100). |

| | |
|---|---|
| **af43** | Match packets with AF43 dscp (100110). |
| **cs1** | Match packets with CS1(precedence 1) dscp (001000). |
| **cs2** | Match packets with CS2(precedence 2) dscp (010000). |
| **cs3** | Match packets with CS3(precedence 3) dscp (011000). |
| **cs4** | Match packets with CS4(precedence 4) dscp (100000). |
| **cs5** | Match packets with CS5(precedence 5) dscp (101000). |
| **cs6** | Match packets with CS6(precedence 6) dscp (110000). |
| **cs7** | Match packets with CS7(precedence 7) dscp (111000). |
| **default** | Match packets with default dscp (000000). |
| **ef** | Match packets with EF dscp (101110). |

**Command Default**

Monitor interval time is not configured.

**Command Modes**

Master controller configuration mode (config-domain-vrf-mc)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

**Usage Guidelines**

Use this command on the hub device for the master controller configuration to configure monitor interval on ingress monitors.

### Example

The following example shows how to configure monitor interval time:

```
Device(config-domain-vrf-mc)# monitor-interval 1 dscp ef
```

# password

To specify a password for enabling secure connection, use the **password** command in domain border configuration mode. To remove the password, use the **no** form of this command.

**password** {**0**|**7**|**LINE**}
**no password**

## Syntax Description

| | |
|---|---|
| **0** | Specifies an unencrypted password. |
| **7** | Specifies a hidden password. |
| **LINE** | Specifies an unencrypted clear text line password. |

## Command Default

The password for secure connection is not specified.

## Command Modes

Domain border configuration mode (config-domain-vrf-br)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

### Example

The following example shows how to specify the password:

```
Device (config-domain-vrf-br)# password 7 13061E010803
```

# path-last-resort

To specify the path of the last service provider, use the **path-last-resort** command in domain class configuration mode. To remove the path, use the **no** form of this command.

**path-last-resort** *service-provider-name*

## Syntax Description

| | |
|---|---|
| *service-provider-name* | Specifies the last service provider name. |

## Command Default

Last service provider is not specified.

## Command Modes

Domain class configuration (config-domain-vrf-mc-class)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

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). Use this command to specify a last service provider on a network.

### Example

The following example shows how to specify a last service provider on a network:

```
Router(config)# domain default
Router(config-domain)# vrf default
Router(config-domain-vrf)# master hub
Router(config-domain-vrf-mc)# class VOICE sequence 10
Router(config-domain-vrf-mc-class)# path-last-resort MPLS1
```

## Related Commands

| Command | Description |
|---|---|
| **domain (pfrv3)** | Configures top level domain for PfRv3. |

# path-preference

To set a preferred path for a traffic class policy, use the **path-preference** command in domain-class configuration mode. To remove the path preference, use the **no** form of this command.

**path-preference** *path1*{*path 2*|[{*pathn*}]|**fallback** *fallback-path1*|[{*fallback-path2*|[{*fallback-pathn*}]|**next-fallback**}]|{*next-fallback-path1*[{*next-fallback-pathn*}]|{**blackhole**|**routing**}}}

**no path-preference** *path1*{*path 2*|[{*pathn*}]|**fallback** *fallback-path1*|[{*fallback-path2*|[{*fallback-pathn*}]|**next-fallback**}]|{*next-fallback-path1*[{*next-fallback-pathn*}]|{**blackhole**|**routing**}}}

## Syntax Description

| | |
|---|---|
| *path-name* | Specifies the path preference name.<br>**Note** You can specify up to five primary paths and four fallback paths. |
| **fallback** | Specifies the fallback path(s) preference to used when the primary path(s) are out of policy. |
| **blackhole** | Specifies the blackhole fallback action. If the primary path is out of policy, then the packets are dropped. |
| **routing** | Specifies the routing fallback action. If the primary path is out of policy, then the routing table is used to forward the traffic. |
| *fallback-path* | Specifies the fallback path preferences.<br>**Note** You can specify multiple fallback paths. |
| **next-fallback** | Specify the next-fallback path preferences. |

## Command Default

Path preference is not defined.

## Command Modes

Domain class configuration mode (config-domain-vrf-mc-class)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |
| Cisco IOS XE Denali 16.3.1 | This command was modified. The **next-fallback** keyword was added. |

## Usage Guidelines

The **path-preference** command is configured on the hub-master controller to configure the WAN paths.

### Example

The following example shows how to set up the path preference for an ISP:

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

```
Device(config-domain-vrf)# master hub
Device(config-domain-vrf-mc)# class VOICE sequence 10
Device(config-domain-vrf-mc-class)# path-preference MPLS1 MPLS2 fallback ISP3 ISP4
```

# priority

To specify thresholds for user-defined policy, use the **priority** command in master controller class type configuration mode. To remove the specifications, use the **no** form of this command.

**priority** *number* {**jitter**|**loss**|**one-way-delay**}**threshold** *threshold-value*
**no priority** *number* {**jitter**|**loss**|**one-way-delay**}**threshold** *threshold-value*

## Syntax Description

| | |
|---|---|
| *number* | Specifies the priority number. The range is from 1 to 65535, 1 being the highest priority. |
| **jitter** | Specifies the jitter threshold value. |
| **loss** | Specifies the loss threshold value. |
| **one-way-delay** | Specifies the one-way-delay threshold value. |

## Command Default

Threshold values for the user-defined policy is not specified.

## Command Modes

Master controller class type mode (config-domain-vrf-mc-class-type)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

The **priority** command is entered in the hub master controller to specify the threshold for user-defined policies. You can specify the jitter, loss rate, and one-way-delay.

### Example

The following example shows how to specify threshold values:

```
Device(config-domain-vrf-mc-class-type)# priority 1 loss threshold 10
```

# show derived-config

To display the composite results of all the configuration commands that apply to an interface, including commands that come from sources such as static templates, dynamic templates, dialer interfaces, and authentication, authorization, and accounting (AAA) per-user attributes, use the **show derived-config** command in privileged EXEC mode.

**show derived-config** [**interface** *type number*]

## Syntax Description

| | |
|---|---|
| **interface** *type number* | (Optional) Displays the derived configuration for a specific interface. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, interface ethernet 0). |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.1(2)S | This command was modified. The output was extended to include information about service instances and xconnects that are downloaded and provisioned. |

## Usage Guidelines

Configuration commands can be applied to an interface from sources such as static templates, dynamic templates bound by resource pooling, dialer interfaces, AAA per-user attributes and the configuration of the physical interface. The **show derived-config** command displays all the commands that apply to an interface.

The output for the **show derived-config**command is nearly identical to that of the **show running-config** command. It differs when the configuration for an interface is derived from a template, a dialer interface, or some per-user configuration. In those cases, the commands derived from the template, dialer interface, and so on, will be displayed for the affected interface.

If the same command is configured differently in two different sources that apply to the same interface, the command coming from the source that has the highest precedence will appear in the display.

On Performance Routing Version 3 (PfRv3) configured device, this command is used to display automatically configured components.

## Examples

The following examples show sample output for the **show running-config** and **show derived-config** commands for serial interface 0:23 and dialer interface 0. The output of the **show running-config** and **show derived-config** commands is the same for dialer interface 0 because none of the commands that apply to that interface are derived from any sources other than the configuration of the dialer interface. The output for the **show running-config** and **show derived-config** commands for serial interface 0:23 differs because some of the commands that apply to serial interface 0:23 come from dialer interface 0.

```
Router# show running-config interface Serial0:23
Building configuration...
Current configuration :296 bytes
!
```

```
interface Serial0:23
 description PRI to ADTRAN (#4444150)
 ip unnumbered Loopback0
 encapsulation ppp
 dialer rotary-group 0
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 isdn calling-number 4444150
 peer default ip address pool old_pool
end
Router# show running-config interface Dialer0
Building configuration...
Current configuration :257 bytes
!
interface Dialer0
 description Dialin Users
 ip unnumbered Loopback0
 no ip proxy-arp
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 30
 dialer-group 1
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end
Router# show derived-config interface Serial0:23
Building configuration...
Derived configuration :332 bytes
!
interface Serial0:23
 description PRI to ADTRAN (#4444150)
 ip unnumbered Loopback0
 encapsulation ppp
 dialer rotary-group 0
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 isdn calling-number 4444150
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end
Router# show derived-config interface Dialer0
Building configuration...
Derived configuration :257 bytes
!
interface Dialer0
 description Dialin Users
 ip unnumbered Loopback0
 no ip proxy-arp
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 30
 dialer-group 1
 peer default ip address pool new_pool
 ppp authentication pap chap callin
end
```

The following sample output from the **show running-config** and **show derived-config** commands show service instance and xconnect configurations.

```
Router# show running-config interface ethernet 0/0

Building configuration...

Current configuration : 201 bytes
```

```
!
interface Ethernet0/0
 no ip address
 service-policy type control mypolicy
 service instance dynamic 1 ethernet
  encapsulation dot1q 2-99
  ethernet subscriber
  initiator unclassified vlan
 !
end

Router# show derived-config interface ethernet 0/0

Building configuration...

Derived configuration : 306 bytes
!
interface Ethernet0/0
 no ip address
 service-policy type control mypolicy
 service instance dynamic 1 ethernet
  encapsulation dot1q 2-99
  ethernet subscriber
  initiator unclassified vlan
 !
 service instance 2 ethernet
  encapsulation dot1q 22
  xconnect 33.33.33.34 12346 encapsulation mpls
 !
end
```

This following is a sample output of the **show derived-config | section eigrp** command displaying that 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

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the contents of the currently running configuration file or the configuration for a specific interface. |

# show domain

To display the status of the PfRv3 configuration, use the **show domain** command in user EXEC or privileged EXEC mode.

**show domain**{*domain-name*|**default**}{**border**|**master**|**vrf**}
**show domain**{**default**{**border**|{**all**|**channels**|{**dscp**}|**exporter**| **neighbor-channels**|
**parent-route**}|**master**|**vrf**}}

## Syntax Description

| | |
|---|---|
| *domain-name* | Displays specific domain information. |
| **default** | Displays default domain information. |
| **border** | Displays domain border information. |
| **master** | Displays domain master information. |
| **vrf** | Displays specific vrf information for domain. |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

### Example

# show eigrp address-family neighbors

To display neighbors that are discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp address-family neighbors** command in user EXEC or privileged EXEC mode.

**show eigrp address-family** {**ipv4**|**ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] **[multicast] neighbors [static] [detail]** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| **ipv4** | Selects the IPv4 protocol address family. |
| **ipv6** | Selects the IPv6 protocol address family. |
| **vrf** *vrf-name* | (Optional) Displays information about the specified VPN routing and forwarding (VRF). |
| *autonomous-system- number* | (Optional) Autonomous system number. |
| **multicast** | (Optional) Displays information about multicast instances. |
| **static** | (Optional) Displays static neighbors. |
| **detail** | (Optional) Displays detailed EIGRP neighbor information. |
| *interface-type interface-number* | (Optional) Interface type and number. If an interface is not specified, all enabled interfaces are displayed. |

## Command Default

Information about all neighbors discovered by EIGRP is displayed.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |
| 15.2(2)S | This command was modified. The output of the command was enhanced to display information for the Bidirectional Forwarding Detection (BFD) sessions. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |
| 15.2(1)E | This command was integrated into Cisco IOS Release 15.2(1)E. |

## Usage Guidelines

Use the **show eigrp address-family neighbors** command to determine when neighbors become active and inactive. The command is also useful for debugging certain types of transport problems.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous system configurations.

This command displays the same information as the **show ip eigrp neighbors** command. We recommend that you use the **show eigrp address-family neighbors** command.

## Examples

The following sample output from the **show eigrp address-family ipv4 4453 neighbors** command shows how to display neighbors that are discovered by EIGRP:

```
Device# show eigrp address-family ipv4 4453 neighbors

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Address Interface Hold Uptime SRTT RTO Q Seq
                                  (sec)          (ms)   (ms)    Cnt   Num
172.16.81.28            Ethernet1     13   0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14   0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12   0:02:02  0      4    5     20
```

The following sample output from the **show eigrp address-family ipv4 neighbors detail** command shows how to display detailed information about neighbors that are discovered by EIGRP, including whether a neighbor has been restarted:

```
Device# show eigrp address-family ipv4 neighbors detail

EIGRP-IPv4 VR(test) Address-family Neighbors for AS(3)
H Address Interface Hold Uptime SRTT RTO Q Seq
                                  (sec)          (ms)   (ms)    Cnt   Num
172.16.81.28            Ethernet1     13   0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14   0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12   0:02:02  0      4    5     20


EIGRP-IPv4 VR(test) Address-Family Neighbors for AS(3)
H Address Interface Hold Uptime SRTT RTO Q Seq
                   (sec)       (ms) Cnt   Num
172.16.81.28 Et1/1 11 01:11:08 10 200 0 8
Time since Restart 00:00:05
Version 5.0/3.0, Retrans: 2, Retries: 0, Prefixes: 2
Topology-ids from peer - 0
```

The following sample output from the **show eigrp address-family ipv6 neighbors detail** command shows how to display detailed information about the neighbors that are discovered by EIGRP with BFD enabled on an interface:

```
Device# show eigrp address-family ipv6 neighbors detail

EIGRP-IPv6 Neighbors for AS(1)
H Address           Interface Hold Uptime SRTT RTO Q Seq
                              (sec)       (ms) Cnt   Num
0 Link-Local address: Et1/0 13 00:00:24 1592 5000 0  3
FE80::A8BB:CCFF:FE00:C901
Version 6.0/3.0, Retrans: 1, Retries: 0, Prefixes: 32
Topology-ids from peer - 0

BFD Sessions
NeighAddr Interface
FE80: :A8BB:CCFF:FE00:C901 Ethernet1/0
```

The table below describes the significant fields shown in the sample displays:

*Table 1: show eigrp address-family neighbors Field Descriptions*

| Field | Description |
|---|---|
| AS(4453) | Autonomous system number specified in the configuration command, for example 4453. |
| Address | IP address of the peer. |
| Interface | Interface on which the device is receiving hello packets from the peer. |
| Hold | Duration (seconds) for which the device will wait to hear from the peer before declaring it down. If the default hold time is specified, the hold time value will be less than 15. If a nondefault hold time is specified, the hold time value is displayed. |
| Uptime | Elapsed time (in seconds) since the local device first heard from this neighbor. |
| SRTT | Smooth round-trip time (SRTT). Duration (milliseconds) for which an EIGRP packet requires to be sent to its neighbor and for the local device to receive an acknowledgment of that packet. |
| RTO | Retransmission timeout (RTO). Duration (milliseconds) for which EIGRP waits before retransmitting a packet from the retransmission queue to a neighbor. |
| Q Cnt | Number of packets (update, query, and reply) that the software is waiting to send. |
| Seq Num | Sequence number of the last update, query, or reply packet that was received from this neighbor. |
| Time since Restart | Time elapsed since a neighbor has been restarted. |

## Related Commands

| Command | Description |
|---|---|
| **show eigrp address-family accounting** | Displays prefix accounting information for EIGRP processes. |
| **show eigrp address-family events** | Displays information about EIGRP events. |
| **show eigrp address-family interfaces** | Displays information about interfaces configured for EIGRP. |
| **show eigrp address-family sia-event** | Displays information about EIGRP SIA events. |
| **show eigrp address-family sia-statistics** | Displays information about EIGRP SIA statistics. |
| **show eigrp address-family timers** | Displays information about EIGRP timers and expiration times. |
| **show eigrp address-family topology** | Displays entries in the EIGRP topology table. |
| **show eigrp address-family traffic** | Displays the number of EIGRP packets sent and received. |

# show flow monitor type performance-monitor

To display the flow monitor information for passive-performance monitoring on the egress interface of WAN, use the **show flow monitor type performance-monitor** command in privileged EXEC mode.

**show flow monitor type type performance-monitor**

## Syntax Description

This commands has no keywords or arguments.

## Command Default

The flow monitor type is not displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use the **show flow monitor type performance-monitor** command to display 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

## Examples

The following is a sample output from the **show flow monitor type mace performance-monitor** command:

```
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 table below describes the significant fields shown in the display.

***Table 2: show flow record type performance-monitor Field Descriptions***

| Field | Description |
|---|---|
| Description | Displays the description provided for a flow monitor. |
| Flow Record | Displays the flow record that is included in the flow monitor. |
| Flow Exporter | Displays the flow exporter that is included in the flow monitor. |
| Cache Type | Displays flow monitor cache type. |
| entries | Displays the number of entries available for a flow monitor. |
| interval | Displays the time duration between two flow monitor. |
| history size | Displays the time duration between two flow monitors. |
| timeout | Current value for the timeout in seconds. |
| export spreading | Displays the export spreading status, where the flow export is spread out over a time interval, which is automatically set by MMA or specified by the user. |
| Interface applied | Number interfaces applied with flow monitor. |

# show platform hardware qfp active feature pfrv3

To display the platform hardware information on a Cisco ASR 1000 Series Aggregation Services Routers for Performance Routing Version 3 (PfRv3) configuration, use the show platform hardware qfp active feature pfrv3 command in privileged EXEC mode.

**show platform hardware qfp active feature pfrv3**{**client**|**datapath**|**pal**}

## Syntax Description

| | |
|---|---|
| **client** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) client debug logging. |
| **datapath** | Enables PfRv3 Cisco Quantum Flow Processor (QFP) data path debug logging. |
| **pal** | Enables debug logging for PfRv3 in the Cisco Quantum Flow Processor (QFP). |

## Command Default

Platform informtion for PfRv3 configuration is not displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to display PfRv3 configuration information.

# show platform software interface

To display the interface information for Performance Routing Version 3 (PfRv3) configuration, use the **show platform software interface** command in privileged EXEC mode.

**show platform software interface** {**fp**|**rp**}{**active**|[{**name***interface-name*}]}

## Syntax Description

| | |
|---|---|
| **fp** | Specifies the Embedded Service Processor (ESP). |
| **rp** | Specifies the Route Processor (RP). |
| **active** | Specifies the active instance. |
| **name** *interface-name* | Specifies the interface. |

## Command Default

PfRv3 configuration information is not displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to display the interface information for PfRv3 configuration on devices running Cisco IOS XE software.

### Example

The following is a sample output from the **show platform software interface** command.

```
Device# show platform software interface rp active

Name: Null0, ID: 1, QFP ID: 0, Schedules: 0
Type: LOOPBACK/NULL0, State: enabled, SNMP ID: 0, MTU: 1500
IP Address:
IPV6 Address:
Flags: unknown
ICMP Flags: unknown, no-unreachables, no-redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unknown, no-unreachables, no-redirects
SMI enabled on protocol(s): UNKNOWN
Authenticated-user:
FRR linkdown ID:
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
QOS trust type: Unknown

Name: GigabitEthernet1, ID: 7, QFP ID: 0, Schedules: 4096
Type: PORT, State: disabled, SNMP ID: 1, MTU: 1500
Flow control ID: 65535
bandwidth: 1000000, encap: ARPA
IP Address: 0.0.0.0
IPV6 Address:
Flags: unknown
ICMP Flags: unknown, no-unreachables, no-redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unknown, no-unreachables, no-redirects
```

```
SMI enabled on protocol(s): UNKNOWN
Authenticated-user:
FRR linkdown ID:
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
QOS trust type: Unknown

Name: GigabitEthernet2, ID: 8, QFP ID: 0, Schedules: 4096
Type: PORT, State: enabled, SNMP ID: 2, MTU: 1500
Flow control ID: 65535
bandwidth: 1000000, encap: ARPA
IP Address: 9.45.6.172
IPV6 Address:
Flags: ipv4
ICMP Flags: unknown, no-unreachables, no-redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unknown, no-unreachables, no-redirects
SMI enabled on protocol(s): UNKNOWN
Authenticated-user:
FRR linkdown ID:
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
QOS trust type: Unknown
```

# site-prefixes

To create new site-prefix list, use the **site-prefixes** command in master controller configuration mode. To remove the site-prefixes, use the **no** form of this command.

**site-prefixes prefix-list** *list-name*
**no site-prefixes prefix-list** *list-name*

## Syntax Description

| | |
|---|---|
| **prefix-list** | Specifies the prefix-list with static site prefixes. |
| *list-name* | Specifies the prefix-list containing list of site prefixes. |

## Command Default

The site-prefixes are not created.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

Use this command on the hub device for the master controller configuration to configure site-prefixes. Use this command with the **ip prefix-list** command. Match conditions specified in the **ip prefix-list** command are only supported.

### Example

The following example shows how to configure site-prefixes:

```
Device(config-domain-vrf-mc)# site-prefixes prefix-list hub_site_prefixes
```

## Related Commands

| Command | Description |
|---|---|
| **ip prefix-list** | Creates a prefix list or adds a prefix-list entry. |

# source-interface

To configure a loopback used as a source for peering with other sites and master controller (MC), use the **source-interface** command in master controller configuration mode or border configuration mode.

**source-interface loopback** *interface-number*

## Syntax Description

| | |
|---|---|
| **loopback** | Specifies the loopback interface. |
| *interface-number* | Specifies the loopback interface number. The range is from 0 to 2147483647. |

## Command Default

The loopback interface is not configured.

## Command Modes

Master controller configuration mode (config-domain-vrf-mc)#

Border configuration mode (config-domain-vrf-br)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to configure the loopback used as a source for peering with other sites or master controller.

### Example

The following example shows how to configure source-interface for hub MC:

```
Device> enable
Device# configure terminal
Device(config)# domain default
Device(config-domain)# vrf default
Device(config-domain-vrf)# master hub
Device(config-domain-vrf-mc)# source-interface loopback 2
```

The following example shows how to configure source-interface for border devices:

```
Device> enable
Device# configure terminal
Device(config)# domain default
Device(config-domain)# vrf default
Device(config-domain-vrf)# border
Device(config-domain-vrf-br)# source-interface loopback 0
```

# smart-probes

To configure smart-probes ports, use the **smart-probes** command in advanced configuration mode. To remove the ports, use the **no** form of this command.

**smart-probes** {**destination-port**|**source-port**|{*port-number*}}
**smart-probes** {**destination-port**|**source-port**}

## Syntax Description

| | |
|---|---|
| **destination-port** | Specifies smart-probes destination port. |
| **source-port** | Specifies smart-probes source port. |
| *port-number* | Specifies port number of the destination and source. The range is from 1 to 65535. |

## Command Default

Predefined smart-probes ports are used in hub master controller configuration.

## Command Modes

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

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to specify user-defined source and destination smart-probes port numbers.

The following examples shows how to configure smart-probes ports:

```
Device(config-domain-vrf-mc-advanced)# smart-probes destination-port 20
Device(config-domain-vrf-mc-advanced)# smart-probes source-port 25
```

# smart-probes burst

To configure burst probing on a master or branch device, use the **smart-probes burst** command in domain master controller advanced configuration mode. To remove the burst probing configuration, use the **no** form of this command.

**smart-probes burst** {*packet-number*|**quick**} {**packets every** *interval* **seconds**}
**no smart-probes burst** [{**quick**}]

## Syntax Description

| | |
|---|---|
| *packet-number* | Specifies the number of packets in one burst. |
| **quick** | Specifies smart probe burst profile for channels monitored by quick monitor. |
| **packets** | Specifies the number of packets in every burst. |
| **every** | Specifies each burst interval. |
| *interval* | Specifies the interval between adjacent bursts. |
| **seconds** | Specifies the interval length in seconds. |

## Command Default

Burst probing is not configured.

## Command Modes

Domain master controller advanced configuration (config-domain-mc-advanced)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

## Usage Guidelines

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 don't 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.

The following examples shows how to configure burst probing on a master controller:

```
Device(config)# domain default
Device(config-domain)# master hub
Device(config-domain-mc)# advanced
Device(config-domain-mc-advanced)# smart-probes burst quick 10 packets every 20 seconds
```

# threshold-variance

To configure threshold tolerance for hub master controller configuration, use the **threshold-variance** command in advanced configuration mode. To remove the threshold tolerance, use the **no** form of this command.

**threshold-variance** *tolerance-percentage*
**no threshold-variance** *tolerance-percentage*

## Syntax Description

| | |
|---|---|
| *tolerance-percenatge* | Specifies the percentage of tolerance. The range is from 0 to 100. |

## Command Default

Default threshold tolerance is used for hub master controller configuration.

## Command Modes

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

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

Use this command to specify the threshold with respect to jitter, loss, and one-way-delay that can be tolerated across two links.

### Example

The following examples shows how to configure threshold variance percentage:

```
Device(config-domain-vrf-mc-advanced)# threshold-variance 20
```

# vrf (domain configuration)

To configure a Virtual Rouitng and Forwarding (VRF) instance for a domain, use the **vrf** command in domain configuration mode. To remove VRF instance, use the **no** form of this command.

**vrf** {*vrf-name*|**default**}
**no vrf** {*vrf-name*|**default**}

## Syntax Description

| | |
|---|---|
| *vrf-name* | Name of the VRF instance. |
| **default** | Default VRF. |

## Command Default

VRF instance is not configured for a domain.

## Command Modes

Domain configuration (config-domain)#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.13S | This command was introduced. |

## Usage Guidelines

Use the **vrf** command to configure user-defined VRFs for PfRv3 configuration. You can either configure default VRF or specific VRF definitions for master controller and border devices.

### Example

The following example shows how to configure VRF:

```
Device> enable
Device# configure terminal
Device(config)# domain default
Device(config-domain)# vrf default
Device(config-domain)# vrf vrf-cisco
```