

Modular QoS Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers

First Published: 2015-12-23

Last Modified: 2025-09-17

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface vii

Changes to This Document vii

Communications, Services, and Additional Information viii

CHAPTER 1

QoS Classification Commands 1

class (policy-map) 3

class-map 5

end-class-map 7

end-policy-map 8

hw-module profile mpls-ext-dscp-preserve 9

hw-module profile qos arp-isis-priority-enable 10

hw-module profile qos gre-exp-classification-enable 11

hw-module profile qos ingress-model peering 12

hw-module profile qos ipv6 short 13

hw-module profile qos ipv6 short-l2qos-enable 14

hw-module profile qos l2-match-dest-addr-v4v6 15

hw-module profile qos max-classmap-size 16

hw-module profile qos policer-scale 18

hw-module profile qos policer-scale l2-mode 20

hw-module profile qos qosg-dscp-mark-enable 21

hw-module profile stats egress-stats-scale 22

hw-module profile stats qos-enhanced 23

hw-module profile stats tx-scale-enhanced qos-enhanced 24

match access-group 25

match cos 27

match dei 29

match destination-address 30
match dscp 31
match mpls disposition class-map 34
match mpls experimental topmost 36
match precedence 38
match protocol 40
match qos-group 42
match traffic-class 43
random-detect discard-class 44
set cos 46
set dei 47
set discard-class 49
set dscp 51
set ip encapsulation 53
set mpls experimental imposition 55
set precedence 57
set qos-group 59
set traffic-class 60
shape average 61
show qos hw-module-status 63

CHAPTER 2 Congestion Management Commands 65
decapsulate gre 67
decapsulate gue 68
hw-module profile qos shared-policer-per-class-stats 69
hw-module profile qos etm-low-rate-connector 70
hw-module profile qos lag-scheduler 72
hw-module oversubscription 73
police rate 74
policy-map 77
priority (QoS) 79
vrf-policy 80
show qos interface 81
show policy-map interface 87

show policy-map targets 93

show policy-map type pbr 95

CHAPTER 3 Congestion Avoidance Commands 97

bandwidth (QoS) 99

bandwidth remaining 101

hw-module profile priority-flow-control 103

hw-module profile qos ecn-marking-stats 105

hw-module profile qos ingress-fadt-set 106

hw-module profile qos wred-stats-enable 107

pause 108

queue-limit 110

random-detect 113

service-policy (interface) 115

CHAPTER 4 Hierarchical Modular QoS Commands 117

hw-module profile qos conform-aware-policer 119

hw-module profile qos hqos-enable 120

hw-module profile qos hqos-enable-without-l2acl 121

hw-module profile qos max-trunks (hw-module profile bundle-scale) 123

hw-module profile qos physical-hqos-enable 124



Preface

This preface contains these sections:

- Changes to This Document, on page vii
- Communications, Services, and Additional Information, on page viii

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

Date	Summary
December 2015	Initial release of this document.
July 2016	Republished with documentation updates for Cisco IOS XR Release 6.0.2 features.
November 2016	Republished with documentation updates for Cisco IOS XR Release 6.1.x features
May 2017	Republished with documentation updates for Cisco IOS XR Release 6.1.31 features
March 2018	Republished for Release 6.3.2.
April 2019	Republished for Release 6.6.2
May 2019	Republished with documentation updates for Release 6.6.25 features
December 2019	Republished with documentation updates for Release 6.6.3 features
January 2020	Republished with documentation updates for Release 7.1.1 features
August 2020	Republished with documentation updates for Release 7.2.1 features

Date	Summary
August 2020	Republished with documentation updates for Release 7.1.2 features.
February 2021	Republished for Release 7.3.1
July 2021	Republished with documentation updates for Release 7.4.1 features.
November 2021	Republished with documentation updates for Release 7.5.1.
January 2022	Republished with documentation updates for Release 7.3.3.
September 2025	Republished with documentation updates for Release 25.3.1

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



QoS Classification Commands

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

This chapter describes the commands used for QoS packet classification.

- class (policy-map), on page 3

- class-map, on page 5
- end-class-map, on page 7
- end-policy-map, on page 8
- hw-module profile mpls-ext-dscp-preserve, on page 9
- hw-module profile qos arp-isis-priority-enable , on page 10
- hw-module profile qos gre-exp-classification-enable, on page 11
- hw-module profile qos ingress-model peering, on page 12
- hw-module profile qos ipv6 short, on page 13
- hw-module profile qos ipv6 short-l2qos-enable, on page 14
- hw-module profile qos l2-match-dest-addr-v4v6 , on page 15
- hw-module profile qos max-classmap-size, on page 16
- hw-module profile qos policer-scale, on page 18
- hw-module profile qos policer-scale l2-mode, on page 20
- hw-module profile qos qosg-dscp-mark-enable, on page 21
- hw-module profile stats egress-stats-scale, on page 22
- hw-module profile stats qos-enhanced, on page 23
- hw-module profile stats tx-scale-enhanced qos-enhanced, on page 24
- match access-group, on page 25
- match cos, on page 27
- match dei, on page 29
- match destination-address, on page 30
- match dscp, on page 31
- match mpls disposition class-map, on page 34
- match mpls experimental topmost, on page 36
- match precedence, on page 38
- match protocol, on page 40
- match qos-group, on page 42
- match traffic-class, on page 43
- random-detect discard-class, on page 44
- set cos , on page 46
- set dei, on page 47
- set discard-class, on page 49
- set dscp, on page 51
- set ip encapsulation, on page 53
- set mpls experimental imposition, on page 55
- set precedence, on page 57
- set qos-group, on page 59
- set traffic-class , on page 60
- shape average, on page 61
- show qos hw-module-status, on page 63

class (policy-map)

To specify the name of the class whose policy you want to create or change, use the **class** command in policy map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class [**type qos**] {*class-name* | **class-default**}
no class [**type qos**] {*class-name* | **class-default**}

Syntax Description

type qos	(Optional) Specifies a quality-of-service (QoS) class.
class-name	Name of the class for which you want to configure or modify policy.
class-default	Configures the default class.

Command Default

No class is specified.

Type is QoS when not specified.

Command Modes

Policy map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Within a policy map, the **class (policy-map)** command can be used to specify the name of the class whose policy you want to create or change. The policy map must be identified first.

To identify the policy map (and enter the required policy map configuration mode), use the **policy-map** command before you use the **class (policy-map)** command. After you specify a policy map, you can configure the policy for new classes or modify the policy for any existing classes in that policy map.

The class name that you specify in the policy map ties the characteristics for that class—that is, its policy—to the class map and its match criteria, as configured using the **class-map** command.

The **class-default** keyword is used for configuring default classes. It is a reserved name and cannot be used with user-defined classes. It is always added to the policy map (type qos) even if the class is not configured. For example, the following configuration shows that the class has not been configured, but the running configuration shows ‘class class-default’.

```
RP/0/RP0/CPU0:router(config)# class-map p2
RP/0/RP0/CPU0:router(config-cmap)# match precedence 2
RP/0/RP0/CPU0:router(config-cmap)# end-class-map
RP/0/RP0/CPU0:router(config)# commit

RP/0/RP0/CPU0:router(config)# policy-map pm2
RP/0/RP0/CPU0:router(config-pmap)# class p2
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence 3
RP/0/RP0/CPU0:router(config-pmap-c)# end-policy-map
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# end
```

```
RP/0/RP0/CPU0:router# show run policy-map pm2
policy-map pm2
class p2
set precedence 3
!
class class-default
!
end-policy-map
!
```

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to create a policy map called policy1, which is defined to shape class1 traffic at 30 percent and default class traffic at 20 percent.

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match precedence 3
RP/0/RP0/CPU0:router(config-cmap)#  exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:routerconfig-pmap-c)# shape average percent 30
RP/0/RP0/CPU0:router(config-pmap-c)# exit


RP/0/RP0/CPU0:router(config-pmap)# class class-default
RP/0/RP0/CPU0:router(config-pmap-c)# shape average percent 20
```

The default class is used for packets that do not satisfy configured match criteria for class1. Class1 must be defined before it can be used in policy1, but the default class can be directly used in a policy map, as the system defines it implicitly.

class-map

To define a traffic class and the associated rules that match packets to the class, use the **class-map** command in XR Config mode. To remove an existing class map from the router, use the **no** form of this command.

class-map [**type** **[traffic | qos]**] [**match-all**] [**match-any**] *class-map-name*
no **class-map** [**type** **[traffic | qos**]] [**match-all**] [**match-any**] *class-map-name*

Syntax Description

type qos	(Optional) Specifies a quality-of-service (QoS) class-map.
traffic	(Optional) Specifies traffic type class-map.
match-all	(Optional) Specifies a match on all of the match criteria.
match-any	(Optional) Specifies a match on any of the match criteria. This is the default.
class-map-name	Name of the class for the class map. The class name is used for the class map and to configure policy for the class in the policy map. The class name can be a maximum of 63 characters, must start with an alphanumeric character, and in addition to alphanumeric characters, can contain any of the following characters: . _ @ $ % + | # : ; - =

Command Default

Type is QoS when not specified.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **class-map** command specifies the name of the class for which you want to create or modify class map match criteria. Use of this command enables class map configuration mode in which you can enter any **match** command to configure the match criteria for this class. Packets arriving on the interface are checked against the match criteria configured for a class map to determine if the packet belongs to that class.

These commands can be used in a class map match criteria for the ingress direction:

- **match access-group**
- **match [not] dscp**
- **match [not] mpls experimental topmost**
- **match [not] precedence**
- **match [not] protocol**

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to specify class1 as the name of a class and defines a class map for this class. The packets that match the access list 1 are matched to class class1.

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 1
```

end-class-map

To end the configuration of match criteria for the class and to exit class map configuration mode, use the **end-class-map** command in class map configuration mode.

end-class-map

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to end the class map configuration and exit class map configuration mode:

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 1
RP/0/RP0/CPU0:router(config-cmap)# end-class-map
```

end-policy-map

To end the configuration of a policy map and to exit policy map configuration mode, use the **end-policy-map** command in policy map configuration mode.

end-policy-map

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Policy map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to end the policy map configuration and exit policy map configuration mode.

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# police rate 250
RP/0/RP0/CPU0:router(config-pmap)# end-policy-map
```

hw-module profile mpls-ext-dscp-preserve

To enable the QoS DSCP preservation at ingress for IPv4 or IPv6 SR-TE functionality, use the **hw profile mpls-ext-dscp-preserve** command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw profile mpls-ext-dscp-preserve { **v4uc-enable** | **v6uc-enable** }

Syntax Description

v4uc-enable	Allows you to preserve IP DSCP for IPv4 SR-TE traffic
v6uc-enable	Allows you to preserve IP DSCP for IPv6 SR-TE traffic

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.7.1	This command was introduced.
Release 7.10.1	The **v6uc-enable** keyword was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable QoS DSCP preservation for IPv4 SR-TE functionality at ingress.

```
Router#config
Router(config)#hw profile mpls-ext-dscp-preserve v4uc-enable
Router(config)#commit
Router(config)#exit
Router#reload location all
```

The following example shows how to enable QoS DSCP preservation for IPv6 SR-TE functionality at ingress.

```
Router#config
Router(config)#hw profile mpls-ext-dscp-preserve v6uc-enable
Router(config)#commit
Router(config)#exit
Router#reload location all
```

hw-module profile qos arp-isis-priority-enable

To enable the prioritization of IS-IS and ARP traffic in transit, use the **hw-module profile qos arp-isis-priority-enable** command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw-module profile qos arp-isis-priority-enable

no hw-module profile qos arp-isis-priority-enable

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

The line card must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the prioritization of IS-IS and ARP traffic in transit.

```
Router#config
Router(config)#hw-module profile qos arp-isis-priority-enable
Router(config)#commit
Router(config)#exit
Router#reload location 0/0/CPU0
```

hw-module profile qos gre-exp-classification-enable

To enable QoS classification on MPLS EXP labels in the inner MPLS header for MPLS over GRE single-pass scenarios, use the **hw-module profile qos gre-exp-classification-enable** command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw-module profile qos gre-exp-classification-enable

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.2	This command was introduced.

Usage Guidelines

The line card must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable QoS classification on MPLS EXP labels in the inner MPLS header for MPLS over GRE single-pass scenarios.

```
Router#config
Router(config)#hw-module profile qos gre-exp-classification-enable
Router(config)#commit
Router(config)#exit
Router#reload location 0/0/CPU0
```

hw-module profile qos ingress-model peering

To enable the peering QoS profile feature, use the hw-module profile qos ingress-model peering command in the XR Config mode. To disable this feature, use the no form of this command.

hw-module profile qos ingress-model peering [location*node-id***]**

Syntax Description

location *node-id*	Indicates the designated node. The *node-id* argument is entered in the rack/slot/module notation.

Command Default

The peering QoS profile feature is disabled by default, unless enabled by this command.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the hw-module command to be functional.

After enabling the QoS peering feature using the **hw-module profile qos ingress-model peering** command, you can set the Layer 2 class of service (CoS) or drop eligible indicator (DEI) values at the egress using the **set cos** or **set dei** commands, respectively. However, at the egress, ensure you don't set the MPLS experimental imposition (EXP) values (using the **set mpls experimental imposition** command). Otherwise, when committing the policy map with these configurations at the egress, you will encounter an error. This error occurs because the internal fields required for egress EXP marking are not available with peering enabled.

When you enable the peering mode (using the **hw-module profile qos ingress-model peering** command), the QPPB feature doesn't work.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the peering QoS profile feature.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos ingress-model peering
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos ipv6 short

To configure the IPv6 source short address TCAM lookup and enable QoS Policy Propagation via BGP (QPPB), run the **hw-module profile qos ipv6 short** command in the XR Config mode.

To disable this feature, use the no form of this command.

hw-module profile qos ipv6 short

Syntax Description

ipv6 short	Reduces the destination IP Address to 96 bits, thus making space in the key for QPPB

Command Default

The QPPB feature is disabled by default, unless enabled by this command.

Command Modes

XR Config

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module** command to be functional.

You must configure the **hw-module profile qos ipv6 short** command for QPPB to work with IPv6 address families and packets.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the QPPB feature.

```
Router#config
Router(config)#hw-module profile qos ipv6 short
Router(config)#commit
Router#reload
```

hw-module profile qos ipv6 short-l2qos-enable

To enable classification of IPv6 packets based on (CoS, DEI) on L3 sub-interfaces, run the hw-module profile qos ipv6 short-l2qos-enable command in the XR Config mode.

To disable this feature, use the no form of this command.

hw-module profile qos ipv6 short-l2qos-enable

Syntax Description

ipv6 short-l2qos-enable	Reduces the destination IP Address to 96 bits, thus making space in the key for (CoS, DEI).

Command Default

The peering QoS profile feature is disabled by default, unless enabled by this command.

Command Modes

XR Config

Command History

Release	Modification
Release 7.1.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the hw-module command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the peering QoS profile feature.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos ipv6 short-l2qos-enable
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos l2-match-dest-addr-v4v6

To enable matching class maps to IPv4 and IPv6 destination addresses on Layer 2 networks, run the hw-module profile qos l2-match-dest-addr-v4v6 command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw-module profile qos l2-match-dest-addr-v4v6

Syntax Description

This command has no keywords or arguments.

Command Default

This feature is disabled by default.

Command Modes

XR Config

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

Reload the router for the **hw-module**command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable matching class maps to IPv4 and IPv6 destination addresses on Layer 2 networks.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos l2-match-dest-addr-v4v6
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router(config)#exit
RP/0/RP0/CPU0:router#reload
```

hw-module profile qos max-classmap-size

To define the maximum number of class-maps per ingress traffic policy, use the hw-module profile qos max-classmap-size command in the Global Configuration Mode.

hw-module profile qos max-classmap-size *size*

Syntax Description

size	Indicates the maximum number of class-maps permitted per ingress traffic policy. Allowed values are 1, 2, 4, 8, 16, and 32.

Command Default

Default size is 32.

Command Modes

Global Configuration Mode

Command History

Release	Modification
Release 7.10.1	Introduced support for a maximum of 1 class-map per ingress traffic policy for the NCS 5500 Series Routers and Line Cards and the NCS 5700 Series Routers and Line Cards.
Release 7.9.1	Introduced support for a maximum of 2 class-maps per ingress traffic policy for the NCS 5500 Series Routers and Line Cards and the NCS 5700 Series Routers and Line Cards.
Release 7.5.1	Introduced support for 2 class-maps permitted per ingress traffic policy, in addition to existing support of 4, 8, 16, 32 for NCS 540 variants.
Release 6.0.0	This command was introduced.

Usage Guidelines

The router **must be reloaded** for the hw-module command to be functional. This command only applies to ingress traffic policies.

In releases prior to Cisco IOS XR 7.5.1 release, only 4, 8, 16, or 32 class-maps per ingress traffic policy are supported. Egress traffic policies can support up to 8 class-maps per traffic policy.

Starting Cisco IOS XR 7.5.1 release, the **hw-module profile qos max-classmap-size** command allows you to set the maximum number of class-map permitted per policy to 2 in addition to existing support of 4, 8, 16, 32 class-maps on N540-ACC-SYS, N540X-ACC-SYS, N540-24Z8Q2C-SYS, N540-28Z4C-SYS-A/D, N540X-16Z4G8Q2C-A/D, N540-12Z20G-SYS-A/D, N540X-12Z16G-SYS-A/D, N540X-6Z18G-SYS-A/D and N540X-8Z16G-SYS-A/D variants.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to change the maximum number of class-maps to 16.

```
Router#config
Router(config)#hw-module profile qos max-classmap-size 16
Router(config)#commit
```

```
Router(config)#exit
Router# reload
```

hw-module profile qos policer-scale

To allocate up to a maximum of 64000 QoS policers, use the **hw-module profile qos policer-scale** command in the XR Config mode. To disable this feature, use the **no** form of this command.

hw-module profile qos policer-scale *size*

Syntax Description

size Number of policers allocated for QoS.

The default value is 32000. You can increase the value to 48000 or 64000, and reduce it back to 32000. CLI snapshot:

```
RP/0/RP0/CPU0:ios(config)#hw-module profile qos policer-scale ?
  32000  Max 32000 policers
  48000  Max 48000 policers
  64000  Max 64000 policers
```

Command Default

The command is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

- The increase in QoS policer allocation is supported only on Cisco NCS 5700 series SE line cards.
- When more than 32000 policers are allocated for QoS, it reduces policers for BGP Flowspec. For example, if you allocate 48000 policers for QoS, the BGP Flowspec policer count reduces from 32000 to 16000.
- Since Enhanced QoS mode configuration does not support more than 32000 policers, you cannot enable the **hw-module profile qos policer-scale** and **hw-module profile stats qos-enhanced** commands at the same time.
- The QoS policer scale numbers are only applicable when the **hw-module profile mdb l3max-se** or **hw-module profile mdb l2max-se** command is enabled. For more information on hardware MDB profiles, see NCS5700 MDB Profile in the *NCS 5500 System Setup and Software Installation Guide*.
- After enabling this command, reload the router.

Some examples of increase in QoS policer allocation:

- If you allocate 48000 policers with 16 class-maps, then 2999 policers are allocated per core and 5998 policers per NPU.
- If you allocate 64000 policers with 16 class-maps, then 3999 policers are allocated per core and 7998 policers per NPU.

The following example shows how to allocate 48000 policers for QoS:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# hw-module profile qos policer-scale 48000
RP/0/RP0/CPU0:router(config)# commit
```



Note After you configure, reload the router to apply the profile. Use the **admin hw-module reload location all** command to reload the router.

hw-module profile qos policer-scale l2-mode

To enable the increase in number of ingress QoS policies supported on Layer 2, use the hw-module profile qos policer-scale l2-mode command in the global configuration mode. To disable this feature, use the **no** form of this command.

hw-module profile qos policer-scale l2-mode

Syntax Description

This command has no keywords or arguments.

Command Default

The command is disabled.

Command Modes

Global Configuration Mode

Command History

Release	Modification
Release 24.2.1	This command was introduced. Applicable only to N540X-6Z18G-SYS-A/D routers.

Usage Guidelines

This command applies only to Layer 2 ingress QoS policies.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable increase in number of ingress QoS policies on all the class-map sizes in Layer 2.

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# hw-module profile qos policer-scale l2-mode
RP/0/RP0/CPU0:router(config)# commit
```

hw-module profile qos qosg-dscp-mark-enable

To set the qos-group and DSCP values within the same QoS policy that is applied in the ingress direction, use the hw-module profile qos qosg-dscp-mark-enable command in the XR Config mode.

hw-module profile qos qosg-dscp-mark-enable *value*

Syntax Description

value	The DSCP or precedence values that can be used in any policy that have both **set qos-group** and **set dscp** configured. The range is from 0 through 63. To use precedence values (instead of DSCP), multiply the precedence value by 8 to get DSCP. For example, to enable precedence=2 and precedence=6 with the above configuration, use the values 16 and 48 in the hw-module configuration command.

Command Default

This feature is disabled by default, unless enabled by this command.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.1.2	This command was introduced.

Usage Guidelines

The router must be reloaded for the hw-module command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable setting both qos-group and DSCP values within the same QoS policy that is applied in the ingress direction.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos qosg-dscp-mark-enable 13 16
RP/0/RP0/CPU0:router(config)#commit
```

hw-module profile stats egress-stats-scale

To extend the MPLS scale from 8k to 20k, use the **hw-module profile stats egress-stats-scale** command in XR Config mode.

hw-module profile stats egress-stats-scale

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

- You must reload the router for the feature to be functional.
- The L2 counters/accounting will not work once this command is enabled.

Task ID

Task ID	Operation
configure-services	read, write
root-lr	read, write

The following example shows how to enable this command.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile stats egress-stats-scale
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile stats qos-enhanced

To enable the four counter mode in the system, use the hw-module profile stats qos-enhancedcommand in XR Config mode. To disable this mode, use the no form of the command. In the four counter mode, statistics for **conform**, **violate**, and **exceed** packets are collected in the hardware and displayed using the show policy-map command.

hw-module profile stats qos-enhanced

Syntax Description

This command has no keywords or arguments.

Command Default

The qos-enhanced mode is disabled by default, and therefore only the conform and violate statistics are available in the two counter mode.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the hw-module command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the four counter mode on the router.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile stats qos-enhanced
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile stats tx-scale-enhanced qos-enhanced

To enable the enhanced QOS statistics for increasing the Tx scale, use the **hw-module profile stats tx-scale-enhanced qos-enhanced** command in XR Config mode. To disable this mode, use the **no** form of the command.

hw-module profile stats tx-scale-enhanced qos-enhanced

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module** command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the enhanced QOS statistics for increasing the Tx scale.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile stats tx-scale-enhanced qos-enhanced
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

match access-group

To identify a specified access control list (ACL) number as the match criteria for a class map, use the **match access-group** command in class map configuration mode.

match access-group {**ipv4** | **ipv6**} *access-group-name*

Syntax Description

ipv4	Specifies the name of the IPv4 access group to be matched.
ipv6	Specifies the name of the IPv6 access group to be matched.
access-group-name	ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class.

Command Default

By default, if neither IPv6 nor IPv4 is specified as the match criteria for a class map, IPv4 addressing is used.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.7.1	QoS support was added for classifying ingress IPv6 and IPv4 traffic, based on its packet length.

Usage Guidelines

For class-based features (such as marking and policing), you define traffic classes based on match criteria, including ACLs and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match access-group** command specifies an ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **match access-group** command is supported only in the ingress direction. The maximum allowed entries: 8

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. You can specify up to eight IPv4 and IPv6 ACLs in a match statement.

QoS classification based on the packet length or TTL (time to live) field in the IPv4 and IPv6 headers is not supported. In Release 7.7.1, QoS support was added for classifying ingress IPv4 and IPv6 traffic, based on its packet length.

When an ACL list is used within a class-map, the deny action of the ACL is ignored and the traffic is classified based on the specified ACL match parameters.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to specify a class map called map1 and configures map1 to be used as the match criteria for this class:

```
RP/0/RP0/CPU0:router(config)# class-map map1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 map1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv6 map2
```

This example shows how to configure the QoS Classification Based on Packet Length feature.



Note This example enables traffic filtering for a specific packet length value by using **packet-length eq**. Instead of **eq**, you can also use one of these options:

- **gt** to filter packets with a greater value.
- **lt** to filter packets with a lesser value.
- **neq** to filter packets that do not contain the specified value.
- **range** to filter packets in the specified range of values.

```
/* Create an ACL that allows IPv4 traffic with the specified packet length */

Router# configure
Router(config)# ipv4 access-list aclv4_pktlen
Router(config-ipv4-acl)# 10 permit ipv4 any any packet-length eq 100
Router(config-ipv4-acl)# commit
```

Based on ACL **aclv4_pktlen**, create a QoS policy and apply it on the ingress IPv4 traffic.

```
/* QoS classification of ingress IPv4 traffic based on its packet length */

Router# configure
Router(config)# class-map match-any c_pktlen
Router(config-cmap)# match access-group ipv4 aclv4_pktlen
Router(config-cmap)# end-class-map
Router(config)# policy-map p_pktlen
Router(config-pmap)# class c_pktlen
Router(config-pmap-c)# set traffic-class 2
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# end-policy-map
Router(config-pmap-c)# commit
Router(config-pmap-c)# root
```

The policy-map **p_pktlen** is associated with interface HundredGigabitEthernet 0/0/0/0.

```
/* Apply the policy-map on the designated Ethernet interface */

Router(config)# interface hundredGigE 0/0/0/0
Router(config-if)# service-policy input p_pktlen
Router(config-if)# commit
```

match cos

To identify specified class of service (CoS) values as a match criteria in a class map, use the **match cos** command in class map configuration mode. To remove a specified CoS class value from the matching criteria for a class map, use the **no** form of this command.

match cos {*cos-value* [*cos-value1* **...** *cos-value7*]}
no match cos {*cos-value* [*cos-value1* **...** *cos-value7*]}

Syntax Description

cos-value	Identifier that specifies the exact value from 0 to 7. Up to eight CoS identifiers can be specified to match packets.

Command Default

No match criteria are specified.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **match cos** command is supported only in the ingress direction.

The **match cos** command specifies a class of service that is used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match cos** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. If you specify more than one **match cos** command in a class map, the values of subsequent match statements are added to the first **match cos** command.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure the service policy called policy-in and attach service policy policy-in to an interface HundredGigE 0/0/0/3. In this example, class map cos146 evaluates all packets of service values of 1, 4, or 6. If the incoming packet has been marked with any of these CoS values, the traffic is policed at 300 mbps.

```
RP/0/RP0/CPU0:router(config)# class-map cos146
RP/0/RP0/CPU0:router(config-cmap)# match cos 1 4 6
RP/0/RP0/CPU0:router(config-cmap)# exit
RP/0/RP0/CPU0:router(config)# policy-map policy-in
RP/0/RP0/CPU0:router(config-pmap)# class cos146
RP/0/RP0/CPU0:router(config-pmap-c)# police rate 300 mbps
RP/0/RP0/CPU0:router(config-pmap-police)#exit
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit
```

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-if)# service-policy input policy-in
```

match dei

To specify a drop eligible indicator (DEI) value as a match criteria in a class map, use the **match dei** command in class map configuration mode. To remove a specified DEI value from the matching criteria for a class map, use the **no** form of this command.

match dei *value*
no match dei

Syntax Description

value	Value of the DEI bit. Can be 0 or 1.

Command Default

There is no default DEI value; it must be specified.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **match dei** command specifies a DEI value that is used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

Task ID

Task ID	Operation
qos	read, write

Examples

In this example, DEI value is specified as the matching criteria in a class map.

```
RP/0/RP0/CPU0:router(config)# class-map match-any match-dei
RP/0/RP0/CPU0:router(config-cmap)# match dei 0
RP/0/RP0/CPU0:router(config-cmap)# exit
RP/0/RP0/CPU0:router(config)# policy-map p1
RP/0/RP0/CPU0:router(config-pmap)# class match-dei
RP/0/RP0/CPU0:router(config-pmap)# set dei 1
RP/0/RP0/CPU0:router(config-pmap-c)#exit
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/5/0/0.0 l2transport
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 1
RP/0/RP0/CPU0:router(config-subif)# rewrite ingress tag push dot1ad 5 symmetric
RP/0/RP0/CPU0:router(config-subif)# service-policy input p1
```

match destination-address

To identify a specified IP address as the match criteria for a class map, use the **match destination-address** command in class map configuration mode.

match destination-address { **ipv4** | **ipv6** } *ip-address*

Syntax Description

ipv4	Specifies the IPv4 address to be matched.
ipv6	Specifies the IPv6 address to be matched.
ip-address	IP address details.

Command Default

By default, if neither IPv6 nor IPv4 is specified as the match criteria for a class map, IPv4 addressing is used.

Command Modes

Class map configuration

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

The **match destination-address** command is supported only in the ingress direction. The maximum allowed entries (any combination of IPv4 and IPv6 addresses, with a maximum of 4 addresses for each): 8

To use the **match destination-address** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. You can specify up to a total of eight IPv4 and IPv6 addresses in a match statement.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to create a class-map and specify match-any criteria for IPv4 and IPv6 addresses:

```
RP/0/RP0/CPU0:router(config)# class-map match-any V4_V6_MATCH
RP/0/RP0/CPU0:router(config-cmap)# match destination-address ipv4 10.0.0.0 255.0.0.0
RP/0/RP0/CPU0:router(config-cmap)# match destination-address ipv6 201:1:1::1/32
```

match dscp

To identify specific IP differentiated services code point (DSCP) values as match criteria for a class map, use the **match dscp** command in class map configuration mode. To remove a DSCP value from a class map, use the **no** form of this command.

match [**not**] **dscp** {[**ipv4** | **ipv6**] *dscp-value* [*dscp-value1 . . . dscp-value7*] | [*min-value* – *max-value*]}
no match [**not**] **dscp** {[**ipv4** | **ipv6**] *dscp-value* [*dscp-value1 . . . dscp-value7*] | [*min-value* – *max-value*]}

Syntax Description

not	(Optional) Negates the specified match result.
ipv4	(Optional) Specifies the IPv4 DSCP value.
ipv6	(Optional) Specifies the IPv6 DSCP value.
dscp-value	IP DSCP value identifier that specifies the exact value or a range of values. Range is 0 - 63. Up to 64 IP DSCP values can be specified to match packets. Reserved keywords can be specified instead of numeric values. Table 2: IP DSCP Reserved Keywords, on page 32 describes the reserved keywords.
min-value	Lower limit of DSCP range to match. Value range is 0 - 63.
max-value	Upper limit of DSCP range to match. Value range is 0 - 63.

Command Default

Matching on IP Version 4 (IPv4) and IPv6 packets is the default.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **match dscp** command is supported only in the ingress direction. The minimum value is 0 and maximum value is 63. The maximum allowed entries: 64.

The **match dscp** command specifies a DSCP value that is used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match dscp** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish

The **match dscp** command examines the higher-order six bits in the type of service (ToS) byte of the IP header. If you specify more than one **match dscp** command in a class map, the new values are added to the existing statement.

The IP DSCP value is used as a matching criterion only. The value has no mathematical significance. For instance, the IP DSCP value 2 is not greater than 1. The value simply indicates that a packet marked with the IP DSCP value of 2 should be treated differently than a packet marked with an IP DSCP value of 1. The

treatment of these marked packets is defined by the user through the setting of policies in policy map class configuration mode.

Table 2: IP DSCP Reserved Keywords

DSCP Value	Reserved Keyword
0	default
10	AF11
12	AF12
14	AF13
18	AF21
20	AF22
22	AF23
26	AF31
28	AF32
30	AF33
34	AF41
36	AF42
38	AF43
46	EF
8	CS1
16	CS2
24	CS3
32	CS4
40	CS5
48	CS6
56	CS7
ipv4	ipv4 dscp
ipv6	ipv6 dscp

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure the service policy called policy1 and attach service policy policy1 to an interface HundredGigE 0/7/0/0 . In this example, class map dscp14 evaluates all packets entering for an IP DSCP value of 14. If the incoming packet has been marked with the IP DSCP value of 14, the packet is queued to the class queue with the bandwidth setting of 1000 mbps.

```
RP/0/RP0/CPU0:router(config)# class-map dscp14
RP/0/RP0/CPU0:router(config-cmap)# match dscp ipv4 14
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class dscp14
RP/0/RP0/CPU0:router(config-pmap-c)#bandwidth 1000 mbps
RP/0/RP0/CPU0:router(config-pmap-c)#exit
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/7/0/0
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
```

match mpls disposition class-map



Note This feature is not available on NC55-24DD and NC55-18DD-SE line cards for Cisco IOS XR Release 7.0.2.

To identify specific six-bit DSCP or three-bit precedence field values in the IPv4/IPv6 header in single MPLS labelled packet as match criteria for a class map, use the **match mpls disposition class-map <cmap-name>** command in class map configuration mode. The **<cmap-name>** is the child class-map name; the child class-map contains match statement for DSCP or precedence or both, and which must be configured before running this command. To remove **match mpls disposition class-map <cmap-name>**, use the **no** form of this command.

match mpls disposition {**class-map**} *c-map name*
no match mpls disposition {**class-map**} *c-map name*

Syntax Description

class-map *c-map name*	Name of the child class-map. The child class-map contains match statement for DSCP or precedence or both.

Command Default

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.6.25	This command was introduced.

Usage Guidelines

The **match mpls disposition class-map <cmap-name>** command is supported only in the ingress direction. It contains the child class-map name as argument which can have **match dscp <value>** or **match precedence <value>** statements. The minimum value for DSCP is 0 and the maximum value is 63. The maximum allowed entries are 8.

The class map uses this command to identify DSCP and/or precedence values matching on a packet.

To use this command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. If you specify more than one **match mpls disposition class-map <cmap-name>** command in a class map, the new values are added to the existing match statement.

This command examines the DSCP/precedence bits contained in the IPv4/IPv6 header.

Task ID

Task ID	Operations
qos	read, write

Examples

In this example, **class map mplsmap1** evaluates all packets entering the **HundredGigabit Ethernet interface 0/1/0/9** that has one MPLS label and for DSCP value ranging from 11-20 and a precedence value of 3. All types of marking are supported for this match.

```
RP/0/RP0/CPU0:router(config)# class-map child-class
RP/0/RP0/CPU0:router(config-cmap)# match dscp 11-20
RP/0/RP0/CPU0:router(config-cmap)# match precedence 3
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# class-map mplsmap1
RP/0/RP0/CPU0:router(config-cmap)# match mpls disposition class-map child-class
RP/0/RP0/CPU0:router(config-cmap# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class mplsmap1
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 3
RP/0/RP0/CPU0:router(config-pmap-c)# set dscp af31
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# interface HundredGigabitEthernet 0/1/0/9
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
```



Note The **set dscp** option is available from Release 7.1.1 onwards.

match mpls experimental topmost

To identify specific three-bit experimental (EXP) field values in the topmost Multiprotocol Label Switching (MPLS) label as match criteria for a class map, use the **match mpls experimental topmost** command in class map configuration mode. To remove experimental field values from the class map match criteria, use the **no** form of the command.

match [**not**] **mpls experimental topmost** *exp-value* [*exp-value1 . . .exp-value7*]
no match [**not**] **mpls experimental topmost** *exp-value* [*exp-value1 . . .exp-value7*]

Syntax Description

not	**not**
exp-value	Experimental value that specifies the exact value from 0 to 7. Up to eight experimental values can be specified to match MPLS headers.

Command Default

No default behavior or values

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **match mpls experimental topmost** command is supported only in the ingress direction. The minimum value is 0 and maximum value is 7. The maximum allowed entries: 8.

The **match mpls experimental topmost** command is used by the class map to identify MPLS experimental values matching on a packet.

To use the **match mpls experimental topmost** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. If you specify more than one **match mpls experimental topmost** command in a class map, the new values are added to the existing match statement.

This command examines the three experimental bits contained in the topmost label of an MPLS packet. Up to eight experimental values can be matched in one match statement. For example, match mpls experimental topmost 2 4 5 7 returns matches for experimental values of 2, 4, 5, and 7. Only one of the four values is needed to yield a match (OR operation).

The experimental values are used as a matching criterion only. The value has no mathematical significance. For instance, the experimental value 2 is not greater than 1. The value indicates that a packet marked with the experimental value of 2 should be treated differently than a packet marked with the EXP value of 1. The treatment of these different packets is defined by the user through the setting of QoS policies in policy map class configuration mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure the service policy called policy1 and attach service policy policy1 to an interface. In this example, class map mplsmap1 evaluates all packets entering HundredGigabit Ethernet interface 0/1/0/9 for an MPLS experimental value of 1. If the incoming packet has been marked with the MPLS experimental value of 1, the packet is queued to the class queue with the bandwidth setting of 1000 mbps.

```
RP/0/RP0/CPU0:router(config)# class-map mplsmap1
RP/0/RP0/CPU0:router(config-cmap)# match mpls experimental topmost 1
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class mplsmap1
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth 1000 mbps
RP/0/RP0/CPU0:router(config-pmap-c)#exit
RP/0/RP0/CPU0:router(config-pmap)#exit

RP/0/RP0/CPU0:router(config)# interface HundredGigabitEthernet  0/1/0/9
RP/0/RP0/CPU0:router(config-if)# service-policy input  policy1
```

match precedence

To identify IP precedence values as match criteria, use the **match precedence** command in class map configuration mode. To remove precedence values from a class map, use the **no** form of this command.

match [**not**] **precedence** [**ipv4** | **ipv6**] *precedence-value* [*precedence-value1* . . . *precedence-value7*]
no match [**not**] **precedence** [**ipv4** | **ipv6**] *precedence-value* [*precedence-value1* . . . *precedence-value7*]

Syntax Description

not	(Optional) Negates the specified match result.
ipv4	(Optional) Specifies the IPv4 precedence value.
ipv6	(Optional) Specifies the IPv6 precedence value.
precedence-value	An IP precedence value identifier that specifies the exact value. Reserved keywords can be specified instead of numeric values. Table 3: IP Precedence Values and Names, on page 39 describes the reserved keywords. Up to eight precedence values can be matched in one match statement.

Command Default

Matching on both IP Version 4 (IPv4) and IPv6 packets is the default.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **match precedence** command is supported only in the ingress direction. The minimum value is 0 and maximum value is 7. The maximum allowed entries: 8.

The **match precedence** command specifies a precedence value that is used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match precedence** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. If you specify more than one **match precedence** command in a class map, the new values are added to the existing statement.

The **match precedence** command examines the higher-order three bits in the type of service (ToS) byte of the IP header. Up to eight precedence values can be matched in one match statement. For example, **match precedence ipv4 0 1 2 3 4 5 6 7** returns matches for IP precedence values of 0, 1, 2, 3, 4, 5, 6, and 7. Only one of the eight values is needed to yield a match (OR operation).

The precedence values are used as a matching criterion only. The value has no mathematical significance. For instance, the precedence value 2 is not greater than 1. The value simply indicates that a packet marked with the precedence value of 2 is different than a packet marked with the precedence value of 1. The treatment of these different packets is defined by the user through the setting of QoS policies in policy map class configuration mode.

This table lists the IP precedence value number and associated name in descending order of importance.

Table 3: IP Precedence Values and Names

Value	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network
ipv4	ipv4 precedence
ipv6	ipv6 precedence

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure the service policy called policy1 and attach service policy policy1 to an interface. In this example, class map ipprec5 evaluates all packets entering HundredGigabit Ethernet interface 0/1/0/9 for a precedence value of 5. If the incoming packet has been marked with the precedence value of 5, the packet is queued to the class queue with the bandwidth setting of 1000 mbps.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# class-map ipprec5
RP/0/RP0/CPU0:router(config-cmap)# match precedence ipv4 5
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class ipprec5
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth 1000 mbps
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# interface HundredGigabitEthernet  0/1/0/9
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
```

match protocol

To identify a specific protocol as the match criterion for a class map, use the **match protocol** command in class map configuration mode. To remove protocol-based match criteria from a class map, use the **no** form of this command.

match [**not**] **protocol** {*protocol-value* [*protocol-value1* **. . .** *protocol-value7*] | [*min-value* – *max-value*]}
no match [**not**] **protocol** {*protocol-value* [*protocol-value1* **. . .** *protocol-value7*] | [*min-value* – *max-value*]}

Syntax Description

not	(Optional) Negates the specified match result.
protocol-value	A protocol identifier. A single value for *protocol-value* (any combination of numbers and names) can be matched in one match statement.
min-value	Lower limit of protocol range to match. Minimum value is 0.
max-value	Upper limit of protocol range to match. Maximum value is 255.

Command Default

No default behavior or values

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **match protocol** command is supported only in ingress direction. The maximum allowed entry is 1.

Definitions of traffic classes are based on match criteria, including protocols, access control lists (ACLs), input interfaces, QoS labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map. Available protocol names are listed in the table that follows.

The *protocol-value* argument supports a range of protocol numbers. After you identify the class, you may use the **match protocol** command to configure its match criteria.

Table 4: Protocol Names and Descriptions

Name	Description
ahp	Authentication Header Protocol
esp	Encapsulation Security Payload
gre	Cisco Generic Routing Encapsulation Tunneling

Name	Description
icmp	Internet Control Message Protocol
igmp	Internet Gateway Message Protocol
igrp	Cisco IGRP Routing protocol
ipinip	IP in IP tunneling
ipv4	Any IPv4 protocol
ipv6	Any IPv6 protocol
mpls	Any MPLS packet
nos	KA9Q NOS Compatible IP over IP Tunneling
ospf	Open Shortest Path First, Routing Protocol
pcp	Payload Compression Protocol
pim	Protocol Independent Multicast
sctp	Stream Control Transmission Protocol
tcp	Transport Control Protocol
udp	User Datagram Protocol

Task ID

Task ID	Operations
qos	read, write

Examples

In this example, all TCP packets belong to class class 1:

```
RP/0/RP0/CPU0:router(config)# class-map class 1
RP/0/RP0/CPU0:router(config-cmap)# match protocol tcp
```

match qos-group

To identify specific quality-of-service (QoS) group values as match criteria in a class map, use the **match qos-group** command in class map configuration mode. To remove a specific QoS group value from the matching criteria for a class map, use the **no** form of this command.

match qos-group [*qos-group-value*]
no match qos-group

Syntax Description

qos-group-value	QoS group value identifier that specifies the exact value from 1through 511 in peering profile, and 1 through 7 in all other cases. Range is not supported.

Command Default

No match criteria are specified.

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The egress default class will implicitly match qos-group 0. The minimum value is 1 and maximum value is 7, and 1 and 511 for peering profiles.

The **match qos-group** command sets the match criteria for examining QoS groups marked on the packet. One class map can match only one qos-group value from 1 through 7, and from 1 through 511 for peering profiles.

The QoS group value is used as a matching criterion only. The value has no mathematical significance. For instance, the QoS group value 2 is not greater than 1. The value simply indicates that a packet marked with the QoS group value of 2 should be treated differently than a packet marked with a QoS group value of 1. The treatment of these different packets is defined using the **service-policy** command in policy map class configuration mode.

The QoS group setting is limited in scope to the local router. Typically, the QoS group is set on the ingress on the local router to be used locally and the router to give differing levels of service based on the group identifier.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows that packets in qos-group 5 are matched.

```
RP/0/RP0/CPU0:router(config)# class-map qosgroup5
RP/0/RP0/CPU0:router(config-cmap)# match qos-group 5
RP/0/RP0/CPU0:router(config-cmap)# exit
```

match traffic-class

To identify specified traffic-class values as a match criteria in a class map, use the **match traffic-class** command in class map configuration mode. To remove a specified traffic-class value from the matching criteria for a class map, use the **no** form of this command.

match traffic-class *traffic-class-value*
no match traffic-class *traffic-class-value*

Syntax Description

traffic-class-value	Identifier that specifies the exact value from 1 through 7. The class-default in the egress policy maps to 0.

Command Default

None

Command Modes

Class map configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **match traffic-class** command is supported only in the egress direction.

The **match traffic-class** command specifies a traffic-class ID that is used as the match criteria against which packets are checked to determine if they belong to the queue set by an ingress policy-map.

To use the **match traffic-class** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Task ID

Task ID	Operations
qos	read, write

Examples

The following example shows that packets in traffic-class 2 are matched.

```
RP/0/RP0/CPU0:router(config)# class-map match-any rdb
RP/0/RP0/CPU0:router(config-cmap)# match traffic-class 2
RP/0/RP0/CPU0:router(config-cmap)# exit
```

random-detect discard-class

To configure the Weighted Random Early Detection (WRED) thresholds for packets with a specific discard class value, use the **random-detect discard-class** command in policy map class configuration mode. To return the thresholds to the default for the discard class, use the **no** form of this command.

random-detect discard-class *discard-value min-threshold* [*units*] *max-threshold* [*units*]
no random-detect discard-class *discard-value min-threshold* [*units*] *max-threshold* [*units*]

Syntax Description

discard-value	Discard class ID. Prior to IOS XR Release 7.1.1, an integer from 0 through 2, to be marked on the packet. From IOS XR Release 7.1.1, an integer from 0 through 3, to be marked on the packet. (See **Usage Guidelines** below.)
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 0 to 1073741823 in bytes.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 1073741823. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified discard class value.
units	(Optional) Units for the threshold values. Values can be: • **bytes**—bytes • **gbytes**—gigabytes • **kbytes**—kilobytes • **mbytes** —megabytes • **ms**—milliseconds • **packets**—packets (default) • **us**—microseconds

Command Default

Default unit for *max-threshold* and *min-threshold* is **packets**.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED is most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

If you set a discard-class of 3, the packet is dropped at ingress itself.

When you configure the **random-detect discard-class** command on an interface, packets are given preferential treatment based on the discard class of the packet.

When the value of the *units* argument is packets, packets are assumed to be 256 bytes in size.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the discard class values for discard class 1 to a minimum byte threshold of 1000000 and a maximum byte threshold of 2000000:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# random-detect discard-class 1 1000000 bytes 2000000
bytes
```

set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **set cos** command in policy map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos *cos-value*
no set cos *cos-value*

Syntax Description

cos-value	Specific IEEE 802.1Q CoS value from 0 to 7.

Command Default

No Layer 2 CoS value of an outgoing packet is set.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

Use the **set cos** command to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.

The **set cos** command is supported only in the ingress direction. Only unconditional COS marking in the ingress direction is supported.

Task ID

Task ID	Operations
qos	read, write

Examples

In this example, the policy map called cos-set is created to assign different CoS values for different service classes, and then is attached to the output interface HundredGigE 0/0/0/3.

```
RP/0/RP0/CPU0:router(config)# policy-map cos-set
RP/0/RP0/CPU0:router(config-pmap)# class class1...
RP/0/RP0/CPU0:router(config-pmap-c)# set cos 1
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# class class2...
RP/0/RP0/CPU0:router(config-pmap-c)#set cos 2
RP/0/RP0/CPU0:router(config-pmap-c)#exit
RP/0/RP0/CPU0:router(config-pmap)# interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-if)# service-policy input cos-set
```

set dei

To set the drop eligible indicator (DEI) value in a policy map class, use the **set dei** command in policy map class configuration mode. To remove a specified DEI value from a policy map class, use the **no** form of this command.

set dei *value*
no set dei

Syntax Description

value	Value of the DEI bit. Can be 0 or 1.

Command Default

There is no default DEI value; it must be specified.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

The **set dei** command specifies a DEI value in a policy map class. For example, traffic can be policed and the excess traffic can be marked with DEI value of 1, so that it can be preferentially dropped in the egress interface or further downstream, when there is congestion.

Note On NCS 5700 Series Routers, for L3 forwarded packets, the LSB ECN bit is copied to DEI when no egress marking policy with CoS is applied and CoS/DEI is not set from ingress. This is a limitation on ASIC.

Task ID

Task ID	Operation
qos	read, write

Examples

In this example, 802.1ad CoS plus DEI is derived from the incoming 802.1q CoS. Packets with a CoS value of 0 are remarked with a DEI value of 1.

```
RP/0/RP0/CPU0:router(config)# class-map match-any remark-cos
RP/0/RP0/CPU0:router(config-cmap)# match cos 0
RP/0/RP0/CPU0:router(config-cmap)# exit
RP/0/RP0/CPU0:router(config)# policy-map p1
RP/0/RP0/CPU0:router(config-pmap)# class remark-cos
RP/0/RP0/CPU0:router(config-pmap-c)# set dei 1
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/5/0/0.0 l2transport
RP/0/RP0/CPU0:router(config-subif)# encapsulation dot1q 1
```

```
RP/0/RP0/CPU0:router(config-subif)# rewrite ingress tag push dot1ad 5 symmetric
RP/0/RP0/CPU0:router(config-subif)# service-policy input p1
```

set discard-class

To set the discard class and Quality of Service (QoS) group identifiers on IP Version 4 (IPv4) or Multiprotocol Label Switching (MPLS) packets, use the **set discard-class** command in policy map class configuration mode. To leave the discard-class values unchanged, use the **no** form of this command.

set discard-class *discard-class-value*
no set discard-class *discard-class-value*

Syntax Description

discard-class-value	Discard class ID. Prior to IOS XR Release 7.1.1, an integer from 0 through 2, to be marked on the packet. From IOS XR Release 7.1.1, an integer from 0 through 3, to be marked on the packet. (See **Usage Guidelines** below.)

Command Default

No default behavior or values

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **set discard-class** command associates a discard class ID with a packet. After the discard class is set, other QoS services such as Weighted Random Early Detection (WRED) can operate on the bit settings.

If however, you set a discard-class of 3, the packet is dropped at ingress itself.

Discard-class indicates the discard portion of the per hop behavior (PHB). The **set discard-class** command is typically used in Pipe mode. Discard-class is required when the input PHB marking is used to classify packets on the output interface.

The **set discard-class** command is supported only in the ingress direction.Unconditional discard-class marking is supported.

The discard-class values can be used to specify the type of traffic that is dropped when there is congestion.



Note

1. Marking of the discard class has only local significance on a node.
2. Discard class cannot be associated with a QoS profile in peering mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the discard class value to 1 for packets that match the MPLS experimental bits 1:

```
RP/0/RP0/CPU0:router(config)# class-map cust1
RP/0/RP0/CPU0:router(config-cmap)# match mpls experimental topmost 1
RP/0/RP0/CPU0:router(config-cmap)# exit
RP/0/RP0/CPU0:router(config)# policy-map policy2
RP/0/RP0/CPU0:router(config-pmap)# class cust1
RP/0/RP0/CPU0:router(config-pmap-c)# set discard-class 1
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# service-policy input policy2
```

set dscp

To mark a packet by setting the IP differentiated services code point (DSCP) in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set dscp [**tunnel**] *dscp-value*
no set dscp [**tunnel**] *dscp-value*

Syntax Description

tunnel	(Optional) Sets the DSCP on the outer IP header. This command is available on Layer 3 interfaces in the ingress direction.
dscp-value	Number from 0 to 63 that sets the DSCP value. Reserved keywords can be specified instead of numeric values. Table 2: IP DSCP Reserved Keywords, on page 32 describes the reserved keywords.

Command Default

No default behavior or values

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

While marking a packet, ensure you don't set the IP DSCP (using the **set dscp** command) and the MPLS experimental imposition values (using the **set mpls experimental imposition** command) for the same class map. Else, neither the DSCP remarking nor the MPLS EXP values may take effect at the ingress. This will cause, per default QoS behavior, the IP precedence values to be copied to the EXP bits on the imposed packets. Such an action could lead to unintended packets marked as high-priority by your customer being forwarded as high-priority MPLS packets in the network.

After the DSCP bit is set, other quality-of-service (QoS) services can then operate on the bit settings. The **set dscp** is supported only in the ingress direction.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the DSCP value at the edge of the network (or administrative domain); data then is queued based on the DSCP value.

Task ID

Task ID	Operations
qos	read, write

Examples

In this example, the DSCP ToS byte is set to 6 in the policy map called policy-in. All packets that satisfy the match criteria of class1 are marked with the DSCP value of 6. The network configuration determines how packets are marked.

```
RP/0/RP0/CPU0:router (config)# policy-map policy-in
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set dscp 6
```

set ip encapsulation

To set traffic class imposition for SRv6 encapsulation, use the **set ip encapsulation** command in policy map class configuration mode.

set ip encapsulation class-of-service *cos-value*

Syntax Description

class-of-service	Specifies the class of service.
cos-value	Specifies the number that sets the SRv6 encapsulation in the IP header. The value ranges from 0 to 63.

Command Default

None

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 24.2.1	This command was introduced.

Usage Guidelines

- The **set ip encapsulation class-of-service** command is not allowed in egress QoS policies.
- The IP encapsulation marking (**set ip encapsulation class-of-service**) and the MPLS experimental imposition marking (**set mpls experimental**) features are mutually exclusive. Both the configurations are not allowed at the same time.
- On the NCS 5500 series routers, the **set ip encapsulation class-of-service** command is allowed only when the **policy-map-extend** oprion is enabled. On the NCS 5700series routers, the command is supported in native mode without enabling the **policy-map-extend**.
- The **policy-map-extend** option enables 6-bit DSCP marking for both L2 and L3 modes at the same time. It is not feasible to enable the **policy-map-extend** option exclusively for L2 and L3 modes due to the shared hardware resources for L2 and L3 SRv6 traffic-class.
- To support DSCP marking on the NCS 5700 series routers, the **propagate** option must be enabled in the SRv6 configurations.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the traffic class imposition for SRv6 encapsulations.

```
RP/0/RP0/CPU0:router(config)# class-map match-any class1
RP/0/RP0/CPU0:router(config-pmap)# match protocol ipv4
RP/0/RP0/CPU0:router(config-pmap-c)# match access-group ipv4 10
RP/0/RP0/CPU0:router(config-cmap-c)# class class-default
```

```
RP/0/RP0/CPU0:router(config-cmap-c)# end-class-map
RP/0/RP0/CPU0:router(config)# policy-map SRv6
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set ip encapsulation class-of-service 55
RP/0/RP0/CPU0:router(config-cmap-c)# class class-default
RP/0/RP0/CPU0:router(config-cmap-c)# end-policy-map
RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/0/0/24
RP/0/RP0/CPU0:router(config-if)# service-policy input SRv6
```

set mpls experimental imposition

To set the experimental (EXP) value of the Multiprotocol Label Switching (MPLS) packet topmost or imposition labels, use the **set mpls experimental** command in policy map configuration mode. To leave the EXP value unchanged, use the **no** form of this command.

set mpls experimental {**topmost**} *exp-value*
no set mpls experimental {**topmost**} *exp-value*

Syntax Description

topmost	Specifies to set the EXP value of the topmost label.
exp-value	Value of the MPLS packet label. Range is 0 to 7.

Command Default

No MPLS experimental value is set

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

After enabling the QoS peering feature using the **hw-module profile qos ingress-model peering** command, you can set the Layer 2 class of service (CoS) or drop eligible indicator (DEI) values at the egress using the **set cos** or **set dei** commands, respectively. However, at the egress, ensure you don't set the MPLS experimental imposition (EXP) values (using the **set mpls experimental imposition** command). Otherwise, when committing the policy map with these configurations at the egress, you will encounter an error. This error occurs because the internal fields required for egress EXP marking are not available with peering enabled.

While marking a packet, ensure you don't set the IP DSCP (using the **set dscp** command) and the MPLS experimental imposition values (using the **set mpls experimental imposition** command) for the same class map. Else, neither the DSCP remarking nor the MPLS EXP values may take effect at the ingress. This will cause, per default QoS behavior, the IP precedence values to be copied to the EXP bits on the imposed packets. Such an action could lead to unintended packets marked as high-priority by your customer being forwarded as high-priority MPLS packets in the network.

After the MPLS experimental bits are set, other QoS services can then operate on the bit settings.

This command is supported only in ingress direction. Unconditional MPLS experimental marking is supported.

The network gives priority (or some type of expedited handling) to the marked traffic. Typically, the MPLS experimental value is set at the edge of the network (or administrative domain) and queuing is acted on it thereafter.

While upgrading to Release 6.5.3 and above, if `set mpls experimental { topmost } exp-value` command is used in the egress PM of label imposition node, replace it with `set mpls experimental { imposition } exp-value` before the upgrade. Else, configuration fails after upgrade. This is because `set mpls experimental { topmost } exp-value` command does not work in egress.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the MPLS experimental to 5 for packets that match access list 101:

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 acl101
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set mpls experimental topmost 5
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/0
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
```

set precedence

To set the precedence value in the IP header, use the **set precedence** command in policy map class configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

set precedence [**tunnel**] *value*
no set precedence [**tunnel**] *value*

Syntax Description

tunnel	(Optional) Sets the IP precedence on the outer IP header.
value	Number or name that sets the precedence bits in the IP header. Range is from 0 to 7. Reserved keywords can be specified instead of numeric values. Table 3: IP Precedence Values and Names, on page 39 describes the reserved keywords.

Command Default

No default behavior or values

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Precedence can be set using a number or corresponding name. After IP Precedence bits are set, other QoS services can then operate on the bit settings.

The **set precedence** command is supported only in the ingress direction. Unconditional precedence marking is supported.

The network gives priority (or some type of expedited handling) to the marked traffic. IP precedence can be set at the edge of the network (or administrative domain) and have queueing act on it thereafter.

The mapping from keywords such as 0 (routine) and 1 (priority) to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of high-end Internet QoS, IP precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the IP precedence to 5 (critical) for packets that match the access control list named customer1:

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 customer1
RP/0/RP0/CPU0:router(config-cmap)# exit
```

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence 5
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# interface HundredGigE 0/1/0/9
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
```

set qos-group

To set the quality of service (QoS) group identifiers on packets, use the **set qos-group** command in policy map class configuration mode. To leave the QoS group values unchanged, use the **no** form of this command.

set qos-group *qos-group-value*
no set qos-group *qos-group-value*

Syntax Description

qos-group-value	QoS group ID. An integer from 1 to 7, to be marked on the packet. The *qos-group-value* is used to classify traffic and remark it on the egress interface policy.

Command Default

No group ID is specified.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **set qos-group** command is supported only in the ingress direction.

The **set qos-group** is used to group incoming traffic and then to classify and remark packets on the egress interface

Task ID

Task ID	Operations
qos	read, write

Examples

This example sets the **qos-group** value to 5:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set qos-group 5
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit
```

set traffic-class

To set the traffic-class of an ingress packet to allow for its subsequent classification into the correct egress queue in the egress QoS-policy, use the **set traffic-class** command in policy map class configuration mode. To remove a specific traffic-class value setting, use the **no** form of this command.

set traffic-class *traffic-class-value*
no set traffic-class *traffic-class-value*

Syntax Description

traffic-class-value	Value from 0 through 7.

Command Default

None

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

If you set a traffic class at the ingress policy and don’t have a matching class at egress for the corresponding traffic class value, then the traffic at ingress with this class isn't accounted for in the default class at the egress policy map.

The **set traffic-class** command is supported only on ingress policies.

If the ingress policy doesn't explicitly set the traffic-class value, it’s implicitly set to 0.

Task ID

Task ID	Operations
qos	read, write

Examples

In this example, traffic is set to the traffic-class value of 3.

```
RP/0/RP0/CPU0:router(config)# policy-map pm2
RP/0/RP0/CPU0:router(config-pmap)# class class-default
RP/0/RP0/CPU0:router(config-pmap-c)# set traffic-class 3
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit
```

shape average

To shape traffic to the indicated bit rate according to the algorithm specified, use the **shape average** command in policy map class configuration mode. To remove traffic shaping, use the **no** form of this command.

shape average { **percent** *percentage* *rate* [*units*] | | **per-thousand** *value* | | **per-million** *value* } { **peak burst size** *units* }
no shape average

Syntax Description

percent *percentage*	Specifies the interface bandwidth in percentage. Values can be from 1 to 100.
rate	Average shaping rate in the specified units. Values can be from 1 to 4294967295.
units	(Optional) Units for the bandwidth. Values can be: • **bps**—bits per second (default) • **gbps**—gigabits per second • **kbps**—kilobits per second • **mbps**—megabits per second
per-thousand *value*	Specifies shape rate as parts per thousand of the available bandwidth.
per-million *value*	Specifies shape rate as parts per million of the available bandwidth.
peak burst size	Specifies maximum burst size for the egress shaper. Values can be from 1 to 4294967295.
value	(Optional) Units for the bandwidth. Values can be: • **Bytes**—Bytes (default) • **Kbytes**—Kilobytes • **Ms**—Milliseconds • **packets**—Packets • **us**—Microseconds

Command Default

units: **bps**

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 6.6.25	Added absolute rate units for shaper on bundle and link aggregation (LAG) interfaces.

Release	Modification
Release 7.2.1	Added peak burst size for egress shaper.

Usage Guidelines

The **shape average** command is supported only in the egress direction.

When you use the **shape average** command, egress shaping is done at the Layer 1 level and includes the Layer 1 header in the rate calculation. If you have both shape and bandwidth configured for a class, ensure that the shape percent value is always greater than the percent value for bandwidth. For bundled interfaces, **shape average** can be configured only as a percentage.

The **priority** and **shape average** commands can be configured together in the same class.

The default burst size is bytes (when no unit is specified).

The per-class statistics for a shaper action do not reflect the Layer 1 header and the overhead bytes (if any configured) even though the shaper includes them in the rate calculation.

From Release 7.11.1, for Hierarchical QoS (H-QoS) and egress traffic management (ETM) models:

- Port shaper and burst on a particular physical interface are programmed when an egress policy map with only a **class-default** configuration and a configured shaper value is applied on that interface.
- The shaper rate on the default class is calculated as the port shaper and the burst as the port burst.

From Release 7.11.1, for non-H-QoS and non-ETM models:

- Port level burst on a particular interface is programmed when you configure it along with port shaper.
- You must attach an egress QoS parent policy map to the main interface.
- The shaper rate on the parent policy configured for the default class is considered as port shaper and the burst as port burst.

Task ID

Task ID	Operations
qos	read, write

Examples

This example sets traffic shaping to 50 percent of the parent shaper rate milliseconds and peak burst for egress shaping to 1000:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# shape average percent 50 1000
```

This example shows how to set traffic shaping to 100000 kbps and peak burst for egress shaping to 1000:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# shape average 100000 kbps 1000
```

show qos hw-module-status

To display all the QoS hardware module profile names on the router and to know if the profile is configured on the router, and whether it requires a reboot, use the **show qos hw-module-status** command in the XR EXEC mode.

show qos hw-module-status [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Displays detailed QoS hardware module profile information for the designated node. The *node-id* argument is entered in the *rack/slot/module/port* notation.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 25.3.1	Added **ingress-fadt-set** entry in the CLI output to display configuration and applied status of the fair adaptive drop threshold profile.
Release 7.8.1	This command was introduced. Applicable to NCS 540 variants only.

Usage Guidelines

The **show qos hw-module-status** command displays all QoS hardware module profile names on the router. The router must be reloaded for the **hw-module** profiles to be functional.

Task ID

Task ID	Operations
qos	read

Examples

This is the sample output of **show qos hw-module-status** command, displaying QoS hardware module profile names configured on the router. Following are the fields that are displayed:

- **hw-module profile**: Displays all the QoS hardware module profile names.
- **Configured**: Displays whether the profile is configured by the user, and if it's present in the router or not.
- **Applied**: Displays whether the configuration is applied on the router or not.
- **Action**: Displays whether the router needs a reboot or not.

```
RP/0/RP0/CPU0:router# show qos hw-module-status location 0/0/CPU0
-------------------------------------------------------------------------------------------
hw-module profile                    Configured          Applied            Action
-------------------------------------------------------------------------------------------
hqos-enable                           Yes                 Yes                None
```

physical-hqos-enable	Yes	Yes	None
wred-stats-enable	No	No	None
qos-stats-collection	No	No	None
arp-isis-priority-enable	No	No	None
conform-aware-policer	No	No	None
ecn_marking_stats	Yes	Yes	None
gre_exp_classification_enable	No	No	None
shared-policer-per-class-stats	No	No	None
ipv6_short	No	No	None
qos_ipv6_short_etm_profile	Yes	Yes	None
short_l2qos_enable	No	No	None
l2_match_dest_addr_v4v6	No	No	None
stats qos_enhanced	No	No	None
free-buffer-int-threshold	No	No	None
qosg-dscp-mark-enable	Yes	Yes	None
ingress_qos_model	No	Yes-DEFAULT	None
ingress_fadt_set	No	Yes-DEFAULT	None
max-classmap-size	No	Yes	None
etm_low_rate_connector	No	No	None



Congestion Management Commands

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

This chapter describes the commands used to manage congestion.

- decapsulate gre, on page 67

- decapsulate gue, on page 68
- hw-module profile qos shared-policer-per-class-stats, on page 69
- hw-module profile qos etm-low-rate-connector, on page 70
- hw-module profile qos lag-scheduler, on page 72
- hw-module oversubscription, on page 73
- police rate, on page 74
- policy-map, on page 77
- priority (QoS), on page 79
- vrf-policy, on page 80
- show qos interface , on page 81
- show policy-map interface, on page 87
- show policy-map targets, on page 93
- show policy-map type pbr, on page 95

decapsulate gre

To enable decapsulation of the Generic Routing Encapsulation (GRE) packets, use the **decapsulate gre** command in policy map class configuration mode. To remove a previously configured GRE decapsulation for a class, use the **no** form of this command.

decapsulate gre
no decapsulate gre

Command Default

No default action.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

This command applies only to the incoming IPv4 packets only.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure decapsulation of the GRE packets :

```
RP/0/RP0/CPU0:router(config)# policy-map type pbr gre-policy
RP/0/RP0/CPU0:router(config-pmap)# class type traffic gre-class
RP/0/RP0/CPU0:router(config-pmap-c)# decapsulate gre
```

decapsulate gue

To enable decapsulation of the Generic UDP Encapsulation (GUE) packets, use the **decapsulate gue** command in policy map class configuration mode. To remove a previously configured GUE decapsulation for a class, use the **no** form of this command.

decapsulate gue *version*
no decapsulate gue *version*

Syntax Description

version	Specifies the variant number that can indicate the version of the GUE protocol. Supports variant 1 only.

Command Default

No default action.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 7.1.2	This command was introduced.

Usage Guidelines

Supports Generic UDP Decapsulation for variant 1 only. This command is supported only in Cisco NCS 5500 Series Routers.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure decapsulation of the GUE packets:

```
Router# configure
Router(config)# policy-map type pbr gue-decap
Router(config-pmap)# class type traffic gue-class
Router(config-pmap-c)# decapsulate gue
```

hw-module profile qos shared-policer-per-class-stats

To view individual class statistics (also called per-class mode for the shared policer feature), use the

hw-module profile qos shared-policer-per-class-stats command in the XR Config mode. To disable this feature, use the no form of this command.

hw-module profile qos shared-policer-per-class-stats

Syntax Description

shared-policer-per-class-stats	Enables the ability to view per-class statistics (also called per-class mode for the shared policer feature).

Command Default

The per-class mode is disabled by default, unless enabled by this command.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Usage Guidelines

You must reload the affected line card to enable the per-class-stats mode.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the per-class-stats mode.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos shared-policer-per-class-stats
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos etm-low-rate-connector

To enable virtual flows and achieve precise shaper granularity at 0 kbps for shared shaper elements on the ETM-enabled interfaces, use the **hw-module profile qos etm-low-rate-connector** command in the XR Config mode to reserve system allocated low-rate connectors.

To disable this feature, use the **no** form of this command.

hw-module profile qos etm-low-rate-connector npu-id *npu-id* **reserve-conn-range** *range* **location** *node-location*

Syntax Description

npu-id	Specifies the NPU core for reserving low-rate connectors.
reserve-conn-range *range*	Specifies the number of low-rate connectors to reserve in the NPU core for virtual flows.
location *node-location*	Specifies the node location of the ETM-enabled interface. **Note** Use this keyword only if you have to reserve low-rate connectors for a specific line card or node in a modular router.

Command Default

By default, 2048 low-rate connectors are pre-allocated.

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.3.1	This command was introduced.

Usage Guidelines

- Supported Cisco NCS 5700 line cards must operate in the native mode only.
- By default, 2048 low-rate connectors are pre-allocated. However, you can configure to reserve the low-rate connectors based on specific QoS scale requirements.
- A virtual flow is allocated to a shared quad shaper if the shaper value of the parent policy applied on an ETM-enabled interface is less than 500 Mbps.
- Router must have an external TCAM.
- H-QoS mode must be disabled.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to reserve low-rate connectors for all line cards in a modular router.

```
router(config)#hw-module profile qos etm-low-rate-connector npu-id 0 reserve-conn-range 4
router(config)#commit
```

The following example shows how to reserve low-rate connectors for a specific line card or node in a modular router.

```
router(config)#hw-module profile qos etm-low-rate-connector npu-id 0 reserve-conn-range 1
location 0/1/CPU0
router(config)#commit
```

hw-module profile qos lag-scheduler

To enable LAG-level scheduling for egress queuing, use the **hw-module profile qos lag-scheduler** command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw-module profile qos lag-scheduler

Command Default

No default behavior or values.

Command Modes

XR Config mode

Command History

Release	Modification
Release 24.3.1	This command was introduced.

Usage Guidelines

For modular routers, you must verify the NCS 5700 line cards are operating in the native mode.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to enable the LAG-level scheduling mode on a bundle interface for egress queuing.

```
router#config
router(config)#hw-module profile qos lag-scheduler
router(config)#commit
router#reload location all
```

hw-module oversubscription

To configure traffic priorities on the interface during oversubscription, use the **hw-module oversubscription** command in the XR Config mode.

To disable this feature, use the **no** form of this command.

hw-module oversubscription [**prioritize untagged interface** *interface-name*] [**prioritize cos** *cos-value* **interface** *interface-name*]
no hw-module oversubscription [**prioritize untagged interface** *interface-name*] [**prioritize cos** *cos-value* **interface** *interface-name*]

Syntax Description

oversubscription	Enables prioritization of packets using Oversubscription Buffer Management (OBM).
prioritize untagged interface *interface-name*	Prioritizes all the traffic on this untagged interface with *interface-name*.
prioritize cos *cos-value***interface***interface-name*	Prioritizes all the traffic with the CoS *value* on the interface *interface-name*.

Command Default

By default, only CoS 6 and 7 is prioritized in case of oversubscription.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.7.1	This command was introduced.

The following example shows how to configure the traffic priorities on untagged interface.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#hw-module profile qos hqos-enable
RP/0/RP0/CPU0:router(config)#hw-module oversubscription
RP/0/RP0/CPU0:router(config-oversubscription)#prioritize untagged interface tenGigE 0/0/0/10
RP/0/RP0/CPU0:router(config-oversubscription)#commit
```

The following example shows how to configure the traffic priorities using CoS values on tagged interface.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#hw-module profile qos hqos-enable
RP/0/RP0/CPU0:router(config)#hw-module oversubscription
RP/0/RP0/CPU0:router(config-oversubscription)#prioritize cos 1 interface tenGigE 0/0/0/0
RP/0/RP0/CPU0:router(config-oversubscription)#commit
```

police rate

To configure traffic policing and enter policy map police configuration mode, use the **police rate** command in policy map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police rate {*value* [*units*] | **percent** *percentage* | *rate* [*units*] | **per-thousand** *value* | **per-million** *value* }[**burst** *burst-size* [*burst-units*]] [**peak-rate** {*value* [*units*] | **percent** *percentage*}] [**peak-burst** *peak-burst* [*burst-units*]]
no police rate {*value* [*units*] | **percent** *percentage* | *rate* [*units*] | **per-thousand** *value* | **per-million** *value* }[**burst** *burst-size* [*burst-units*]] [**peak-rate** {*value* [*units*] | **percent** *percentage*}] [**peak-burst** *peak-burst* [*burst-units*]]

Syntax Description

value	Committed information rate (CIR). Range is from 1 to 4294967295.
units	(Optional) Unit of measurement for the CIR. Values can be: • **bps** —bits per second (default) • **gbps** —gigabits per second • **kbps** —kilobits per second • **mbps** —megabits per second • **pps** —packets per second
percent *percentage*	Specifies the police rate as a percentage of the CIR. Range is from 1 to 100. See the Usage Guidelines for information on how to use this keyword.
per-thousand *value*	Specifies police rate as parts per thousand of the available bandwidth.
per-million *value*	Specifies police rate as parts per million of the available bandwidth.
burst *burst-size*	(Optional) Specifies the burst size in the specified *burst-units* . The default burst value is 10 milliseconds of the CIR. The maximum burst value allowed is 4194304 bytes.
burst-units	(Optional) Unit of measurement for the burst values. Values can be: • **bytes** —bytes (default) • **gbytes** —gigabytes • **kbytes** —kilobytes • **mbytes** —megabytes • **ms** —milliseconds • **us** —microseconds • **packets** —packets

peak-rate *value*	(Optional) Specifies the Peak Information Rate (PIR) in the specified *units*.
peak-burst *peak-burst*	(Optional) Specifies the peak burst size in the specified *burst-units*. The default peak burst value is 10 milliseconds of the PIR. The maximum peak-burst value allowed is 8388608 bytes. Also, the difference of the peak-burst value and burst value cannot be larger than 4194304 bytes.

Command Default

No restrictions on the flow of data are applied to any interface.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 6.6.25	Added absolute rate units for policer on bundle and link aggregation (LAG) interfaces.
Release 7.4.1	Added packets per second (pps) units for policer rate.

Usage Guidelines

Policer conditional set is unsupported.

Policing can be applied only in the ingress direction.

For **police rate** commands, interpret the **percent** keyword in this way:

- For a one-level policy, the **percent** keyword specifies the CIR as a percentage of the link rate. For example, the command **police rate percent 35** configures the CIR as 35% of the link rate.



Note Configured values take into account the Layer 2 encapsulation applied to traffic. This applies to ingress policing. For Ethernet transmission, the encapsulation is considered to be 14 bytes, whereas for IEEE 802.1Q, the encapsulation is 18 bytes.

For more information, see the Committed Bursts and Excess Bursts section in the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*.

Task ID

Task ID	Operations
qos	read, write

In this example for MPLS, traffic policing is configured with the average rate at 250 kbps, and the normal burst size at 50 bytes for all packets leaving HundredGigE interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match mpls experimental topmost 0
```

```
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# police rate 250 kbps burst 50
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# HundredGigE interface 0/1/0/0
RP/0/RP0/CPU0:router(config-if) service-policy input policy1
```

policy-map

To create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in XR Config mode. To delete a policy map, use the **no** form of this command.

policy-map [**type qos**] *policy-name*
no policy-map [**type qos**] *policy-name*

Syntax Description

type qos	(Optional) Specifies type of the service policy.
qos	(Optional) Specifies a quality-of-service (QoS) policy map.
policy-name	Name of the policy map.

Command Default

A policy map does not exist until one is configured. Because a policy map is applied to an interface, no restrictions on the flow of data are applied to any interface until a policy map is created.

Type is QoS when not specified.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you can configure policies for classes whose match criteria are defined in a class map. Entering the **policy-map** command enables policy map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure the match criteria for a class.

A single policy map can be attached to multiple interfaces concurrently.

The number of classes per policy-map supported in the egress direction is 8 and ingress direction is 32.

For egress classification, in order to see statistics on all 8 CoSQs, you are recommended to configure all 8 classes including class-default.

Task ID

Task ID	Operations
qos	read, write

Examples

These examples show how to create a policy map called policy1 and configures two class policies included in that policy map. The policy map is defined to contain policy specification for class1 and the default class (called class-default) to which packets that do not satisfy configured match criteria are directed. Class1 specifies policy for traffic that matches access control list 136.

```
RP/0/RP0/CPU0:router(config)# class-map class1
RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 136

RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence 3
RP/0/RP0/CPU0:router(config-pmap-c)# exit

RP/0/RP0/CPU0:router(config-pmap)# class class-default
RP/0/RP0/CPU0:router(config-pmap-c)# queue-limit  1000000 bytes
```

priority (QoS)

To assign priority to a traffic class based on the amount of available bandwidth within a traffic policy, use the **priority** command in policy map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [**level** *priority-level*]
no priority

Syntax Description

level *priority-level*	(Optional) Sets multiple levels of priority to a traffic class. Level 1 through 7. Default level is 1. Level 1 traffic has higher priority.

Command Default

No default action.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **priority** command configures low-latency queueing (LLQ), providing strict priority queueing (PQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued. The **priority** command is supported only in the egress direction. No policer is allowed with a priority class. To limit the priority traffic use the **shape average** command.

The **priority** command sets up classes based on a variety of criteria (not just User Datagram Protocol [UDP] ports) and assigns a priority to them.

The **bandwidth** and **priority** commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure priority queuing for the policy map named policy1 :

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# priority level 1
```

vrf-policy

To apply a policy on a per VPN routing and forwarding (VRF) basis, use the **vrf-policy** command in global configuration mode. To remove the association of the policy on a VRF, use the **no** form of this command.

vrf-policy vrf *vrf-name* **address-family** {**ipv4 | ipv6** } **policy type pbr input** *policy-name*
no vrf-policy vrf *vrf-name* **address-family** {**ipv4 | ipv6** } **policy type pbr input** *policy-name*

Syntax Description

vrf *vrf-name*	Sets the VRF name.
policy type pbr input *policy-name*	Sets the policy name.

Command Default

No default action.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

This command is supported with sub-mode. This command applies only to the incoming IPv4 packets only.

Use this command to apply a PBR policy on a per VRF basis during the classification and decapsulation of GRE packets.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to apply an already configured policy on a per VRF basis:

```
/* Configuring a VRF */
RP/0/RP0/CPU0:router(config)# vrf gre-vrf address-family ipv4 unicast
...
/* Configuring a policy */
RP/0/RP0/CPU0:router(config)# policy-map type pbr gre-policy
...
/* Applying the policy on the VRF */
RP/0/RP0/CPU0:router(config)# vrf-policy vrf gre-vrf address-family ipv4 policy type pbr
input gre-policy
```

show qos interface

To display QoS information for a specific interface, use the **show qos interface** command in the XR EXEC mode.

show qos interface *interface-name* {**input** | **output**}[**location** *node-id*]

Syntax Description

interface-name	Interface name. For more information about the syntax for the router, use the question mark (?) online help function. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
input	Attaches the specified policy map to the input interface.
output	Attaches the specified policy map to the output interface.
location *node-id*	(Optional) Displays detailed QoS information for the designated node. The *node-id* argument is entered in the rack/slot/module notation.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **show qos interface** command displays configuration for all classes in the service policy that is attached to an interface.

Use this command to check the actual values programmed in the hardware from the action keywords in the **police rate** command.

Task ID

Task ID	Operations
qos	read

Examples

This is the sample output shows the QoS information on a **interface hundredGigE 0/6/0/18** that are in the input direction:

```
RP/0/RP0/CPU0:router# show qos interface hundredGigE 0/6/0/18 input
```

```
Wed Dec  2 22:34:20.241 UTC
NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000210  -- input policy
NPU Id:                        3
Total number of classes:       28
Interface Bandwidth:           100000000 kbps
Accounting Type:               Layer1 (Include Layer 1 encapsulation and above)
------------------------------------------------------------------------------
Level1 Class                             =   exp-classifier-af1
New topmost exp                          =   7

Default Policer Bucket ID                =   0x102a0
Default Policer Stats Handle             =   0x8b304d98
Policer not configured for this class

Level1 Class                             =   exp-classifier-af2
New topmost exp                          =   6

Default Policer Bucket ID                =   0x102a1
Default Policer Stats Handle             =   0x8b304b48
Policer not configured for this class

Level1 Class                             =   exp-classifier-af3
New topmost exp                          =   5

Default Policer Bucket ID                =   0x102a2
Default Policer Stats Handle             =   0x8b3048f8
Policer not configured for this class

Level1 Class                             =   exp-classifier-af4
New topmost exp                          =   3

Default Policer Bucket ID                =   0x102a3
Default Policer Stats Handle             =   0x8b3046a8
Policer not configured for this class

Level1 Class                             =   exp-classifier-be1
New topmost exp                          =   4

Default Policer Bucket ID                =   0x102a4
Default Policer Stats Handle             =   0x8b304458
Policer not configured for this class

Level1 Class                             =   inet4-classifier-af1
New qos group                            =   1

Default Policer Bucket ID                =   0x102a5
Default Policer Stats Handle             =   0x8b304208
Policer not configured for this class

Level1 Class                             =   inet4-classifier-af2
New qos group                            =   2

Default Policer Bucket ID                =   0x102a6
Default Policer Stats Handle             =   0x8b303fb8
Policer not configured for this class

Level1 Class                             =   inet4-classifier-af3
New qos group                            =   3

Default Policer Bucket ID                =   0x102a7
Default Policer Stats Handle             =   0x8b303d68
Policer not configured for this class
```

```
Level1 Class                            =   inet4-classifier-af4
New qos group                           =   4

Default Policer Bucket ID               =   0x102a8
Default Policer Stats Handle            =   0x8b303b18
Policer not configured for this class

Level1 Class                            =   inet4-classifier-be1
New qos group                           =   5

Default Policer Bucket ID               =   0x102a9
Default Policer Stats Handle            =   0x8b3038c8
Policer not configured for this class

Level1 Class                            =   inet4-classifier-nc1
New qos group                           =   6

Default Policer Bucket ID               =   0x102aa
Default Policer Stats Handle            =   0x8b303678
Policer not configured for this class

Level1 Class                            =   inet6-classifier-af1
New qos group                           =   1

Default Policer Bucket ID               =   0x102ab
Default Policer Stats Handle            =   0x8b303428
Policer not configured for this class

Level1 Class                            =   inet6-classifier-af2
New qos group                           =   2

Default Policer Bucket ID               =   0x102ac
Default Policer Stats Handle            =   0x8b3031d8
Policer not configured for this class

Level1 Class                            =   inet6-classifier-af3
New qos group                           =   3

Default Policer Bucket ID               =   0x102ad
Default Policer Stats Handle            =   0x8b302f88
Policer not configured for this class

Level1 Class                            =   inet6-classifier-af4
New qos group                           =   4

Default Policer Bucket ID               =   0x102ae
Default Policer Stats Handle            =   0x8b302d38
Policer not configured for this class

Level1 Class                            =   inet6-classifier-be1
New qos group                           =   5

Default Policer Bucket ID               =   0x102af
Default Policer Stats Handle            =   0x8b302ae8
Policer not configured for this class

Level1 Class                            =   inet6-classifier-nc1
New qos group                           =   6

Default Policer Bucket ID               =   0x102b0
Default Policer Stats Handle            =   0x8b302898
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af1
```

```
New qos group                           =   1

Default Policer Bucket ID               =   0x102b1
Default Policer Stats Handle            =   0x8b302648
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af2
New qos group                           =   2

Default Policer Bucket ID               =   0x102b2
Default Policer Stats Handle            =   0x8b3023f8
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af3
New qos group                           =   3

Default Policer Bucket ID               =   0x102b3
Default Policer Stats Handle            =   0x8b3021a8
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af4
New qos group                           =   4

Default Policer Bucket ID               =   0x102b4
Default Policer Stats Handle            =   0x8b301f58
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af5
New qos group                           =   5

Default Policer Bucket ID               =   0x102b5
Default Policer Stats Handle            =   0x8b301d08
Policer not configured for this class

Level1 Class                            =   inet-classifier-ipv6-af6
New qos group                           =   6

Default Policer Bucket ID               =   0x102b6
Default Policer Stats Handle            =   0x8b301ab8
Policer not configured for this class

Level1 Class                            =   inet-management-classifier-af4
New qos group                           =   7

Default Policer Bucket ID               =   0x102b7
Default Policer Stats Handle            =   0x8b301868
Policer not configured for this class

Level1 Class                            =   exp-classifier-nc1
New qos group                           =   6
New topmost exp                         =   2

Default Policer Bucket ID               =   0x102b8
Default Policer Stats Handle            =   0x8b301618
Policer not configured for this class

Level1 Class                            =   inet-management-classifier-nc1
New prec                                =   6
New qos group                           =   5

Default Policer Bucket ID               =   0x102b9
Default Policer Stats Handle            =   0x8b3013c8
Policer not configured for this class
```

```
Level1 Class                              =   inet6-management-classifier-nc1
New qos group                             =   4

Default Policer Bucket ID                 =   0x102ba
Default Policer Stats Handle              =   0x8b301178
Policer not configured for this class

Level1 Class                              =   class-default

Default Policer Bucket ID                 =   0x102bb
Default Policer Stats Handle              =   0x8b3074e8
Policer not configured for this class
```

This is the sample output shows the QoS information on a **interface hundredGigE 0/6/0/18** that are in the output direction:

```
RP/0/RP0/CPU0:router# show qos interface hundredGigE 0/6/0/18 output
Wed Dec  2 22:34:25.476 UTC
NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/6/0/18 ifh 0x3000210  -- output policy
NPU Id:                        3
Total number of classes:       3
Interface Bandwidth:           100000000 kbps
VOQ Base:                      11176
VOQ Stats Handle:              0x887a6e18
Accounting Type:               Layer1 (Include Layer 1 encapsulation and above)
------------------------------------------------------------------------------
Level1 Class (HP7)                        =   qos-1
Egressq Queue ID                          =   11177 (HP7 queue)
Queue Max. BW.                            =   0 kbps (default)
TailDrop Threshold                        =   125304832 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class (HP6)                        =   qos-2
Egressq Queue ID                          =   11178 (HP6 queue)
Queue Max. BW.                            =   0 kbps (default)
TailDrop Threshold                        =   125304832 bytes / 10 ms (default)
WRED not configured for this class

Level1 Class                              =   class-default
Egressq Queue ID                          =   11176 (Default LP queue)
Queue Max. BW.                            =   101803495 kbps (default)
Queue Min. BW.                            =   0 kbps (default)
Inverse Weight / Weight                   =   1 / (BWR not configured)
TailDrop Threshold                        =   1253376 bytes / 10 ms (default)
WRED not configured for this class
```

This table describes the significant fields shown in the display.

Table 5: show QoS interface Field Descriptions

Field	Description
Level 1 class	Level 1 class identifier in decimal format.
Policer Bucket ID	Policer bucket identifier.
Policer Stats Handle	Policer statistics handle for this class.
Queue ID	VOQ number of the packet in this class.
Queue Max. BW	Maximum bandwidth of the queue.

Field	Description
Queue Min. BW	Minimum bandwidth of the queue.
Inverse Weight / Weight	Remaining bandwidth weight. **Note** The hardware weight is expressed in inverse value.
TailDrop Threshold	Number of bytes taildropped for this queue and the default/user-configured queue-limit expressed in milliseconds/user-configured unit.

The following example shows how to verify the virtual flow is configured and active.

```
router#show qos int hu0/0/0/25 output
Fri May 31 16:03:46.130 UTC
NOTE:- Configured values are displayed within parentheses
Interface HundredGigE0/0/0/25 ifh 0x228  -- output policy
NPU Id:                        0
Total number of classes:       6
Interface Bandwidth:           100000000 kbps
Policy Name:                   egr
SPI Id:                        0x0
VOQ Base:                      2048
PFC enabled:                   0
Accounting Type:               Layer1 (Include Layer 1 encapsulation and above)
------------------------------------------------------------------------------
Level1 Class                              =   qos-1
Queue Max. BW.                            =   453125 kbps (450 mbits/sec)
Queue Min. BW.                            =   453125 kbps (default)
Inverse Weight / Weight                   =   1 / (BWR not configured)
Virtual Flow ID                           =   98304

   Level2 Class (HP2)                        =   ETC2
   New traffic class                         =   2
   Egressq Queue ID                          =   2050 (HP2 queue)
   Queue Max. BW.                            =   no max (default)
   Peak burst                                =   36864 bytes (default)
   TailDrop Threshold                        =   562432 bytes / 10 ms (default)
```

show policy-map interface

To display policy information and statistics for all classes configured for all service policies on the specified interface, use the **show policy-map interface** command in XR EXEC mode.

show policy-map [**interface** {*interface type* | **all**} *interface-path-id*] [**input** | **output**]

Syntax Description

interface type	Interface type. For more information, use the question mark (?) online help function.
all	Specifies all interfaces.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
input	(Optional) Displays per class statistics on inbound traffic for the specified policy map and interface.
output	(Optional) Displays per class statistics on outbound traffic for the specified policy map and interface.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.1.1	The output for this command is enhanced to display the statistics for particular WRED profiles when Random Early Detection (RED) is configured on the policy-map for Cisco NCS 560 Series Routers.
Release 7.7.1	QoS support was added for classifying ingress IPv6 and IPv4 traffic based on its packet length. The command output is enhanced to display the corresponding configuration information.

Usage Guidelines

The **show policy-map interface** command displays the statistics for classes in the service policy attached to an interface.

The **show policy-map interface** command does not display the statistics and counters for the egress marking policy.

The per-class statistics for a shaper action do not reflect the Layer 1 header and the overhead bytes (if any configured) even though the shaper includes them in the rate calculation.

Task ID

Task ID	Operations
qos	read

Examples

This sample output shows how to display policy statistics information for all classes on the **interface hundredGigE 0/6/0/18** that are in the input direction:

```
RP/0/RP0/CPU0:router# show policy-map interface hundredGigE 0/6/0/18 input

Mon Nov 30 17:10:29.065 UTC

HundredGigE0/6/0/18 input: 32-classmaps

Class exp-classifier-af1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :              53186/54090162             3769
    Transmitted         :              53186/54090162             3769
    Total Dropped       :                  0/0                    0
Class exp-classifier-af2
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :              54279/55201743             7483
    Transmitted         :              54279/55201743             7483
    Total Dropped       :                  0/0                    0
Class exp-classifier-af3
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :              56710/57674070             7898
    Transmitted         :              56710/57674070             7898
    Total Dropped       :                  0/0                    0
Class exp-classifier-af4
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :             110405/112281885            11584
    Transmitted         :             110405/112281885            11584
    Total Dropped       :                  0/0                    0
Class exp-classifier-be1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :              52753/53649801             3756
    Transmitted         :              52753/53649801             3756
    Total Dropped       :                  0/0                    0
Class inet4-classifier-af1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :           38796901/14695393569          1580677
    Transmitted         :           38796901/14695393569          1580677
    Total Dropped       :                  0/0                    0
Class inet4-classifier-af2
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :           38850080/14715510334          1589124
    Transmitted         :           38850080/14715510334          1589124
    Total Dropped       :                  0/0                    0
Class inet4-classifier-af3
```

```
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            38757080/14679867944          1580632
    Transmitted         :            38757080/14679867944          1580632
    Total Dropped       :                   0/0                    0
Class inet4-classifier-af4
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            77228177/29251757855          3137985
    Transmitted         :            77228177/29251757855          3137985
    Total Dropped       :                   0/0                    0
Class inet4-classifier-be1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            38921394/14742645566          1588557
    Transmitted         :            38921394/14742645566          1588557
    Total Dropped       :                   0/0                    0
Class inet4-classifier-nc1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            77088116/29199136824          3144053
    Transmitted         :            77088116/29199136824          3144053
    Total Dropped       :                   0/0                    0
Class inet6-classifier-af1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            21953707/22326920019          1237979
    Transmitted         :            21953707/22326920019          1237979
    Total Dropped       :                   0/0                    0
Class inet6-classifier-af2
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            21701336/22070258712          1208262
    Transmitted         :            21701336/22070258712          1208262
    Total Dropped       :                   0/0                    0
Class inet6-classifier-af3
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            21715705/22084871985          1210060
    Transmitted         :            21715705/22084871985          1210060
    Total Dropped       :                   0/0                    0
Class inet6-classifier-af4
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            43418446/44156559582          2413245
    Transmitted         :            43418446/44156559582          2413245
    Total Dropped       :                   0/0                    0
Class inet6-classifier-be1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            21958845/22332119845          1236894
    Transmitted         :            21958845/22332119845          1236894
    Total Dropped       :                   0/0                    0
Class inet6-classifier-nc1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :            43428930/44167221810          2415137
    Transmitted         :            43428930/44167221810          2415137
    Total Dropped       :                   0/0                    0
Class inet-classifier-ipv6-af1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                   0/0                    0
    Transmitted         :                   0/0                    0
    Total Dropped       :                   0/0                    0
Class inet-classifier-ipv6-af2
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                   0/0                    0
    Transmitted         :                   0/0                    0
    Total Dropped       :                   0/0                    0
Class inet-classifier-ipv6-af3
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                   0/0                    0
    Transmitted         :                   0/0                    0
    Total Dropped       :                   0/0                    0
```

```
Class inet-classifier-ipv6-af4
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
Class inet-classifier-ipv6-af5
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
Class inet-classifier-ipv6-af6
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
Class inet-management-classifier-af4
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
Class exp-classifier-nc1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :              57115/58085955             7953
    Transmitted         :              57115/58085955             7953
    Total Dropped       :                  0/0                   0
  Policing statistics                (packets/bytes)     (rate - kbps)
    Policed(conform)    :              57115/58085955             7953
    Policed(exceed)     :                  0/0                   0
    Policed(violate)    :                  0/0                   0
    Policed and dropped :                  0/0
Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
```

This sample output shows how to display policy statistics information for all classes on the **interface hundredGigE 0/6/0/0** that are in the output direction:

```
RP/0/RP0/CPU0:router# show policy-map interface hundredGigE 0/6/0/0 output

Wed Dec  9 16:18:10.179 UTC
HundredGigE0/6/0/0 output: test-pol-out

Class tc2
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :          3080542734/394309469952         4808049
    Transmitted         :          3080542734/394309469952         4808049
    Total Dropped       :                  0/0                   0
  Queueing statistics
    Queue ID                            : 1026
    Taildropped(packets/bytes)          : 0/0
    RED random drops(packets/bytes)     : 0/0

    WRED profile for Discard Class 0
    RED Transmitted (packets/bytes)           : 1562482674/199997782272
    RED random drops(packets/bytes)           : 0/0
    RED maxthreshold drops(packets/bytes)     : N/A
    RED ecn marked & transmitted(packets/bytes): N/A
    WRED profile for Discard Class 1
    RED Transmitted (packets/bytes)           : 0/0
    RED random drops(packets/bytes)           : 0/0
    RED maxthreshold drops(packets/bytes)     : N/A
```

```
    RED ecn marked & transmitted(packets/bytes): N/A
    WRED profile for Discard Class 2
    RED Transmitted (packets/bytes)            : 1518060060/194311687680
    RED random drops(packets/bytes)            : 0/0
    RED maxthreshold drops(packets/bytes)      : N/A
    RED ecn marked & transmitted(packets/bytes): N/A
Class tc1
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :          1562482674/199997782272         2883014
    Transmitted         :          1434402692/183603544576         2646687
    Total Dropped       :           128079982/16394237696          236327
  Queueing statistics
    Queue ID                              : 1025
    Taildropped(packets/bytes)            : 128079982/16394237696
    RED random drops(packets/bytes)       : 0/0

    WRED profile for Discard Class 1
    RED Transmitted (packets/bytes)            : 1434402692/183603544576
    RED random drops(packets/bytes)            : 128079982/16394237696
    RED maxthreshold drops(packets/bytes)      : N/A
    RED ecn marked & transmitted(packets/bytes): N/A
Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                  0/0                   0
    Transmitted         :                  0/0                   0
    Total Dropped       :                  0/0                   0
  Queueing statistics
    Queue ID                              : 1024
    Taildropped(packets/bytes)            : 0/0
Policy Bag Stats time: 1557231345776  [Local Time: 05/07/19 12:15:45.776]
```



Note Statistics for WRED profiles are displayed when Random Early Detection (RED) is configured on the policy-map for Cisco NCS 560 Series Routers.

This table describes the significant fields shown in the display.

Table 6: show policy-map interface Field Descriptions

Field	Description
Classification statistics	
Matched	Number of packets or bytes that matched this class.
Transmitted	Number of packets or bytes transmitted for this class.
Total Dropped	Number of packets or bytes dropped for this class.
Policing statistics	
Policed(conform)	Number of packets or bytes that conformed to the police rate for this class.
Policed(exceed)	Number of packets or bytes that exceeded the police rate for this class.
Policed(violate)	Number of packets or bytes that violated the police rate for this class.
Policed and dropped	Number of packets or bytes dropped by the policer of this class.

Field	Description
Queuing statistics	
Queue ID	VOQ number of the packet in this class.
Taildropped (bytes)	Number of bytes taildropped for this queue.

This sample output displays policy information for the *QoS Classification Based on Packet Length* feature. With this feature, you can add an ingress QoS policy on an ACL that filters IPv6 and IPv4 traffic based on its packet length. The ACL specifies packet length criteria such as equal to, lesser than, greater than, and so on, and the QoS policy specifies the forwarding decision. The ACL provides an additional QoS match criteria for IP traffic, enhancing the overall network security.

```
Router# show policy-map interface hundredGigE 0/0/0/0 input

HundredGigE0/0/0/0 input: p_pktlen

Class c_pktlen
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :             53186/54090162          3769
    Transmitted         :             53186/54090162          3769
    Total Dropped       :                   0/0                   0

Class class-default
  Classification statistics          (packets/bytes)     (rate - kbps)
    Matched             :                   0/0                   0
    Transmitted         :                   0/0                   0
    Total Dropped       :                   0/0                   0

Policy Bag Stats time: 1657119549887  [Local Time: 07/06/22 14:59:09.887]
```

show policy-map targets

To display information about the interfaces on which policy maps are applied, use the **show policy-map targets** command in XR EXEC mode.

show policy-map targets [**location** *node-id* | **pmap-name** *name* | **type qos** [**location** *node-id* | **pmap-name** *name*]]

Syntax Description

location *node-id*	(Optional) Displays information about the interfaces on which policy maps are applied for the specified location. The *node-id* argument is entered in the *rack/slot/module* notation.
pmap-name *name*	(Optional) Displays information about the interfaces on which the specified policy map is applied.
type qos	(Optional) Displays information about the interfaces on which QoS policy maps are applied. This is the default type.

Command Default

The default QoS policy type is QoS.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

For a short period of time while a QoS policy is being modified, there might not be any policy in effect on the interfaces in which the modified policy is used. For this reason, modify QoS policies that affect the fewest number of interfaces at a time. Use the **show policy-map targets** command to identify the number of interfaces that will be affected during policy map modification.

Task ID

Task ID	Operations
qos	read

Examples

In this example, the TenGigabit Ethernet interface 4/0/10/0 has one policy map attached as a main policy. Outgoing traffic on this interface will be affected if the policy is modified:

```
RP/0/RP0/CPU0:router# show policy-map targets

Wed Dec  2 22:35:13.993 UTC
1) Policymap: test-qlimit    Type: qos
     Targets (applied as main policy):
       TenGigE0/4/0/10/0 output
       TenGigE0/6/0/30/1 output
     Total targets: 2

     Targets (applied as child policy):
     Total targets: 0
```

```
2) Policymap: test-priority    Type: qos
     Targets (applied as main policy):
       HundredGigE0/6/0/35 output
       HundredGigE0/6/0/34 output
       HundredGigE0/6/0/33 output
       HundredGigE0/6/0/32 output
       HundredGigE0/6/0/31 output
       HundredGigE0/6/0/29 output
       HundredGigE0/6/0/28 output
       HundredGigE0/6/0/27 output
       HundredGigE0/6/0/25 output
       HundredGigE0/6/0/24 output
       HundredGigE0/6/0/23 output
       HundredGigE0/6/0/22 output
       HundredGigE0/6/0/21 output
       HundredGigE0/6/0/20 output
       HundredGigE0/6/0/19 output
       HundredGigE0/6/0/1 output
       HundredGigE0/6/0/3 output
       HundredGigE0/6/0/4 output
       HundredGigE0/6/0/5 output
       HundredGigE0/6/0/6 output
       HundredGigE0/6/0/7 output
       HundredGigE0/6/0/8 output
       HundredGigE0/6/0/9 output
       HundredGigE0/6/0/10 output
       HundredGigE0/6/0/11 output
       HundredGigE0/6/0/13 output
       HundredGigE0/6/0/14 output
       HundredGigE0/6/0/15 output
       HundredGigE0/6/0/16 output
       HundredGigE0/6/0/17 output
     Total targets: 30

     Targets (applied as child policy):
     Total targets: 0
```

show policy-map type pbr

To view details of the configured PBR policy and related statistics, use the **show policy-map type pbr vrf** *vrf-name* **addr-family ipv4 statistics** command in XR EXEC mode.

show policy-map type pbr vrf *vrf-name* **addr-family** {**ipv4 | ipv6** } **statistics**

Syntax Description

vrf *vrf-name*	Sets the VRF name.

Command Default

No default action.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0.1	This command was introduced.

Usage Guidelines

This command applies only to the incoming IPv4 packets only.

Task ID

Task ID	Operations
qos	read

Examples

This example shows how to view details of the configured PBR policy and related statistics:

```
/* Configuring a VRF */
RP/0/RP0/CPU0:router(config)# vrf gre-vrf address-family ipv4 unicast
...
/* Configuring a policy */
RP/0/RP0/CPU0:router(config)# policy-map type pbr gre-policy
...
/* Applying the policy on the VRF */
RP/0/RP0/CPU0:router(config)# vrf-policy vrf gre-vrf address-family ipv4 policy type pbr
input gre-policy

/* Displaying policy details and statistics */
RP/0/RP0/CPU0:router# show policy-map type pbr vrf gre-vrf addr-family ipv4 policy type pbr
 input gre-policy
```



Congestion Avoidance Commands

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

This chapter describes commands used to avoid congestion.

Congestion avoidance is achieved through packet dropping.

- bandwidth (QoS), on page 99
- bandwidth remaining, on page 101
- hw-module profile priority-flow-control, on page 103
- **hw-module profile qos ecn-marking-stats**, on page 105
- hw-module profile qos ingress-fadt-set , on page 106
- **hw-module profile qos wred-stats-enable**, on page 107
- pause, on page 108
- queue-limit, on page 110
- random-detect, on page 113
- service-policy (interface), on page 115

bandwidth (QoS)

To specify the minimum bandwidth allocated to a class belonging to a policy map, use the **bandwidth** command in policy map class configuration mode. To remove the bandwidth specified for a class, use the **no** form of this command.

bandwidth {*rate* [*units*] | **percent** *percentage-value*}
no bandwidth {*rate* [*units*] | **percent** *percentage-value*}

Syntax Description

rate	Minimum bandwidth, in the units specified, to be assigned to the class. Range is from 1 to 4294967295.
units	Specifies the units for the bandwidth. Values can be: • **bps**—bits per second • **gbps**—gigabits per second • **kbps**—kilobits per second (default) • **mbps**—megabits per second
percent *percentage-value*	Specifies the amount of minimum guaranteed bandwidth, based on an absolute percentage of available bandwidth. Range is from 1 to 100.

Command Default

The default units is kbps.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **bandwidth** command is used to specify the minimum guaranteed bandwidth allocated for traffic matching a particular class. Bandwidth may be defined as a specific value or may be set as a percentage of the interface bandwidth.

If a percentage value is set, the accuracy that can be expected is 1 percent.

The **bandwidth** command is supported only in the egress direction.

A policy map can have a single bandwidth statement per class. Both percentage and actual value bandwidth configurations can be used within a policy map.

The **bandwidth** command does not specify how the bandwidth is to be shared. Instead it specifies how much bandwidth is guaranteed per class, by setting the number of tokens that are assigned to the token bucket of a particular class. For configured behavior to work correctly, you must ensure that the sum of the bandwidths plus any priority traffic is not greater than the bandwidth of the interface itself. If the interface is oversubscribed, unpredictable behavior results.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to guarantee 50 percent of the interface bandwidth to a class called class1 and 10 percent of the interface bandwidth to a class called class2:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth percent 50
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# class class2
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth percent 10
```

bandwidth remaining

To specify how to allocate leftover bandwidth to various classes, use the **bandwidth remaining** command in policy map class configuration mode. To return to the system defaults, use the **no** form of this command.

bandwidth remaining [**percent** *percentage-value* | **ratio** *ratio-value*]
no bandwidth remaining [**percent** *percentage-value* | **ratio** *ratio-value*]

Syntax Description

percent *percentage-value*	Specifies the amount of guaranteed bandwidth, based on an absolute percentage of the available bandwidth. Range is from 1 to 100.
ratio *ratio-value*	Specifies the amount of guaranteed bandwidth, based on a bandwidth ratio value. Range is 1 to 2000.

Command Default

No bandwidth is specified.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Bandwidth, bandwidth remaining, shaping, queue-limit and WRED commands can be configured together in the same class.

Note The **bandwidth remaining** command is supported only in the egress direction.

The available bandwidth is equally distributed among those queueing classes that do not have the remaining bandwidth explicitly configured.

The **bandwidth remaining** command is used to proportionally allocate bandwidth to the particular classes, but there is no reserved bandwidth capacity.

On egress, if the **bandwidth remaining** command is not present, then the bandwidth is shared equally among the configured queueing classes present in the policy-map.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how the remaining bandwidth is shared by classes class1 and class2 in a 20:80 ratio.

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
```

```
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 20
RP/0/RP0/CPU0:router(config-pmap-c)# exit
RP/0/RP0/CPU0:router(config-pmap)# class class2
RP/0/RP0/CPU0:router(config-pmap-c)# bandwidth remaining percent 80
```

hw-module profile priority-flow-control

To configure PFC threshold values per line card, use the **hw-module profile priority-flow-control** command in XR Config mode. To return to the system defaults, use the **no** form of this command.



Note For details on the show controller, set controller, clear controller and priority-flow-control watchdog commands, see the *Interface and Hardware Component Command Reference for Cisco NCS 5500 and NCS 540 and NCS 560 Series Routers*.

To disable this feature, use the no form of this command.

hw-module profile priority-flow-control { { | **location** <*lc*> } | { **traffic-class** *number* || | **pause-threshold** *x-off size units* | | **resume-threshold** *x-on size units* | **headroom** *value units* || } }

Syntax Description

location	<*lc*> —Line card location
traffic-class	Traffic class to configure PFC threshold values.
traffic class number	0—7 **Note** Reload the line card for all traffic-class addition and deletions. Parameters within an already configured traffic-class can be edited 'in place' without requiring a line card reload.
pause-threshold	Specifies the buffer limit at which the flow is paused.
x-off size	Buffer limit for pausing flow.
units	Unit of measurement for the x-off size in bytes.
resume-threshold	Specifies the buffer limit at which the flow is resumed.
x-on size	Buffer limit for resuming flow.
units	Unit of measurement for the x-on size in bytes.
headroom	Specifies the headroom.
value	Headroom value
units	Unit of measurement for the headroom value in bytes.

Command Default

No default behavior or values.

Command Modes

XR Config

Command History

Release	Modification
Release 6.6.4	This command was introduced and replaced the pause, on page 108 command.

Usage Guidelines

If you add a new traffic class and configure PFC threshold values for the first time on that traffic class, you must reload the line card.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to configure the PFC threshold values for traffic-class 3 and traffic-class 4.

```
RP/0/RP0/CPU0:router(config)#hw-module profile priority-flow-control location 0/0/CPU0
RP/0/RP0/CPU0:router(config-pfc-loc)#traffic-class 3 pause-threshold 403200 bytes
resume-threshold 40320 bytes headroom 441600 bytes
RP/0/RP0/CPU0:router(config-pfc-loc)#traffic-class 4 pause-threshold 403200 bytes
resume-threshold 40320 bytes headroom 441600 bytes
RP/0/RP0/CPU0:router(config-pfc-loc)#exit
RP/0/RP0/CPU0:router(config-pfc-loc)#commit
```

hw-module profile qos ecn-marking-stats

To enable the display of counters for ECN-marked and transmitted packets, configure the

hw-module profile qos ecn-marking-stats command in the XR Config mode. To disable this feature, use the no form of this command.

hw-module profile qos ecn-marking-stats

Syntax Description

This command has no keywords or arguments.

Command Default

The display of counters for ECN-marked and transmitted packets is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

You must reload the affected line card to enable the display of counters for ECN-marked and transmitted packets.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the display of counters for ECN-marked and transmitted packets.

```
Router#config
Router(config)#hw-module profile qos ecn-marking-stats
In order to activate this profile, you must manually reload the chassis/all line cards
Router(config)#commit
```

hw-module profile qos ingress-fadt-set

Use the **hw-module profile qos ingress-fadt-set** command in the XR Config configuration mode to configure fair adaptive limits for buffer descriptor usage per queue at ingress. To disable this feature, use the **no** form of the command.

hw-module profile qos ingress-fadt-set { **disable** | **high** | **low** | **medium** } [**location** *node-location*]

Syntax Description

disable	(Optional) Disables fair adaptive drop threshold. Not recommended.
high	(Optional) Sets the fair adaptive drop threshold to a high drop threshold.
low	(Optional) Sets the fair adaptive drop threshold to a low drop threshold.
medium	(Optional) Sets the fair adaptive drop threshold to a moderate drop threshold.
location *node-location*	(Optional) Applies the setting to a specific line card or node. If omitted, the command applies globally.

Command Default

medium fair adaptive drop threshold is specified.

Command Modes

XR Config.

Command History

Release	Modification
Release 25.3.1	This command was introduced.

Usage Guidelines

Avoid using the **disable** option, as this may impact system performance.

Select the appropriate threshold—**high**, **medium**, or **low**—based on the drop sensitivity required for ingress traffic.

If both global and per-location configurations are present for a line card, the per-location configuration takes precedence.

Reload the line card for the configured fair adaptive threshold value to take effect.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the ingress fair adaptive threshold option to **high**.

```
Router(config)#hw-module profile qos ingress-fadt-set high
Router(config)#commit
Router#reload location 0/0/CPU0
```

hw-module profile qos wred-stats-enable

To enable the display of Weighted Random Early Detection (WRED) statistics per class, use the

hw-module profile qos wred-stats command in the XR Config mode. To disable this feature, use the no form of this command.

This command has no keywords or arguments.

Command Default

The WRED statistics mode is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

You must reload the affected line card to enable the WRED statistics mode.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the wred-stats mode.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos wred-stats-enable
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router(config)#exit
RP/0/RP0/CPU0:router#reload
```

pause

This configuration allows you to configure nondefault Priority Flow Control (PFC) buffer thresholds per priority queue through an 8-priority egress queuing policy applied on a PFC-enabled interface.

Note From Release 6.6.4 onwards, the **pause** command is deprecated. To configure PFC thresholds, see hw-module profile priority-flow-control, on page 103.

The router ignores the **buffer-size parameter** , although the configuration is not optional. Hence, it is recommended that you keep the buffer-size on par with the queue-limit.

pause {**buffer-size***units* | | | **pause-threshold***x-off size units* | | **resume-threshold***x-on size units*}

Syntax Description

buffer-size	Buffer size for ingress traffic.
units	(Optional) Unit of measurement for the buffer size. Values can be: **bytes—bytes** (default) **gbytes—gigabytes** **kbytes—kilobytes** **mbytes—megabytes**
pause-threshold	Specifies the buffer limit at which the flow is paused.
x-off size	Buffer limit for pausing flow.
units	(Optional) Unit of measurement for the x-off size. Values can be: **bytes—bytes** (default) **gbytes—gigabytes** **kbytes—kilobytes** **mbytes—megabytes**
resume-threshold	Specifies the buffer limit at which the flow is resumed.
x-on size	Buffer limit for resuming flow.
units	(Optional) Unit of measurement for the x-off size. Values can be: **bytes—bytes** (default) **gbytes—gigabytes** **kbytes—kilobytes** **mbytes—megabytes**

Command Default

When you do not configure pause and resume thresholds for a priority queue, the pause threshold (*x-off size*) is set to 128 mbytes and the resume threshold (*x-on size*) is set to 8 kbytes.

Command Modes

Policy map class configuration.

Command History

Release	Modification
Release 6.6.3	This command was introduced.
Release 6.6.4	This command was deprecated and replaced by the hw-module profile priority-flow-control, on page 103 command.

Usage Guidelines

To configure PFC thresholds, see hw-module profile priority-flow-control, on page 103.

Task ID

Task ID	Operations
Qos	read, write

Examples

In this example, the policy map is configured with pause parameter.

```
RP/0/RP0/CPU0:router(config)# #policy-map pmap_out
RP/0/RP0/CPU0:router(config-pmap)# #class tc1
RP/0/RP0/CPU0:router(config-pmap-c)# #pause ?

 buffer-size  Configure buffer size

RP/0/RP0/CPU0:router(config-pmap-c)# pause buffer-size 100 kbytes ?

pause-threshold  Configure pause threshold

RP/0/RP0/CPU0:router(config-pmap-c)# )#$ pause-threshold 100?

  bytes             Bytes
  gbytes            Gigabytes
  kbytes            Kilobytes
  mbytes            Megabytes

RP/0/RP0/CPU0:router(config-pmap-c)# )#$ resume-threshold 90

  bytes             Bytes
  gbytes            Gigabytes
  kbytes            Kilobytes
  mbytes            Megabytes
```

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map for each port, use the **queue-limit** command in policy map class configuration mode. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *value* [*unit*] | *percent <1-100>*
no queue-limit

Syntax Description

value	Maximum threshold for tail drop in bytes. Range is from 1 to 4294967295.
unit	(Optional) Units for the queue limit value. Values can be: • **bytes** —bytes • **kbytes** —kilobytes • **mbytes** —megabytes • **ms** —milliseconds • **packets** —packets (default) • **us** —microseconds **Note** When the specified *units* is packets, packets are assumed to be 256 bytes in size.
percent	(Optional) Allows you to specify queue limit thresholds as a percentage of the total buffer limit for each port. This makes your provisioning model simpler and makes it easier for you to adjust the queue burst limit, irrespective of the queue's service rate. The calculation is based on the assumption that a port takes 40 milli-seconds of buffering at port-rate. This option was introduced in Release 6.1.2.

Command Default

The default value is 10 milliseconds for all queues including the high-priority queues.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When configuring the **queue-limit** command, you must configure one of the following commands: **priority**, **shape average**, **bandwidth** or **bandwidth remaining**, except for the default class. The default value is 10 milliseconds for all queues including the high-priority queues.

The **queue-limit** command is supported only in the egress direction.

Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are serviced by the scheduling mechanism. The **queue-limit** command defines the maximum threshold for a class. When that threshold is reached, enqueued packets to the class queue result in tail drop (packet drop).

Tail drop is a congestion avoidance technique that drops packets when an output queue is full, until congestion is eliminated.

Use the **show qos interface** command to display the queue limit and other QoS values.

Queue Limit Default Values

These default values are used when **queue-limit** is not configured in the class:

- If QoS is configured and Weighted Random Early Detection (WRED) is not configured:
  - Queue limit is 10 ms at the guaranteed service rate of the queue for non-priority queues.
  - Queue limit is 10 ms at the interface rate for priority classes
- If QoS is configured and WRED is configured:
  - Queue limit is two times the WRED maximum threshold. The maximum threshold can be an explicitly configured value or an implicit 10 ms.
  - If more than one WRED profile is configured in the class, the maximum threshold is the maximum for all profiles.
  - When the **queue-limit** is configured in time units, the guaranteed service rate (for the non-priority class) or the interface rate (for the priority class) is used to compute the queue-limit.

These restrictions apply to queue limits:

- For releases before Release 6.3.2, the queue limit should be at least the maximum MTU size, which is fixed at 9 * 1024 bytes = 9kb. From Release 6.3.2 onwards, the minimum queue limit is the interface MTU (which is dynamically configured).
- Queue limit should be 3 GB, which is the maximum packet buffer size in ingress and egress queuing ASICs.
- Only time-based units are allowed on bundle targets.

Guaranteed Service Rate

The guaranteed service rate is defined as the service rate of the queue when all queues are backlogged and derived as:

minimum_bandwidth + (bandwidth_remaining_percent * unallocated_bandwidth)

This example shows the guaranteed service rate calculation:

```
policy-map sample_policy
  class c1
    bandwidth percent 30
    bandwidth remaining percent 40
  class c2
    bandwidth percent 20
  class class-default
```

guaranteed service rate of c1 = 30 percent LR + (40 percent * 50 percent * LR)

guaranteed service rate of c2 = 20 percent LR + (30 percent * 50 percent * LR)

guaranteed service rate of class-default = 30 percent * 50 percent * LR

- Where LR is line rate of the target on which service policy "sample_policy" is attached.
- 50 percent is unallocated bandwidth.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to set the queue limit for a class to 1000000 packets for policy map policy1:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# queue-limit 1000000
```

random-detect

To enable random early detection (RED), use the **random-detect** command in policy map class configuration mode. To remove RED, use the **no** form of this command.

random-detect [**default** | [**discard-class** *value*] | [[**min-threshold** *value*] [**max-threshold** *value*] **probability** *percentage probability value*]]]

no random-detect

Syntax Description

default	Enables RED with default minimum and maximum thresholds.
discard-class *value*	Discard class ID. Prior to IOS XR Release 7.1.1, an integer from 0 through 2, to be marked on the packet. From IOS XR Release 7.1.1, an integer from 0 through 3, to be marked on the packet. (See **Usage Guidelines** below.)
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 0 to 1073741823 in packets.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 1073741823. When the queue length exceeds the maximum threshold, RED drops all packets with the specified discard class value.
units	(Optional) Units for the threshold values. Values can be: • **bytes**—bytes • **gbytes**—gigabytes • **kbytes**—kilobytes • **mbytes** —megabytes • **ms** —milliseconds • **packets** —packets (default) • **us** —microseconds
probability *percentage probability value*	Configure WRED mark probability in percent. The value range of this argument is from 1 through 100. **Note** • The default value is 10 • To see which line cards support this option, see *Configure ECN Maximum Marking Probability* in the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*

Command Default

Default unit for *max-threshold* and *min-threshold* is **packets**.

Command Modes

Policy map class configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.3.3	The functionality to configure ECN mark probability in percent was introduced.

Usage Guidelines

The RED congestion avoidance technique takes advantage of the congestion control mechanism of TCP. By randomly dropping packets before periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it decreases its transmission rate until all the packets reach their destination, indicating that the congestion is cleared. You can use RED as a way to cause TCP to slow transmission of packets. TCP not only pauses, but it also restarts quickly and adapts its transmission rate to the rate that the network can support.

RED distributes losses in time and maintains normally low queue depth while absorbing traffic bursts. When enabled on an interface, RED begins dropping packets when congestion occurs at a rate you select during configuration.

When time units are used, the guaranteed service rate is used to compute thresholds. The default minimum threshold is 6 ms and the maximum threshold is 10 ms.

When the value of the *units* argument is packets, packets are assumed to be 256 bytes in size.

If you set a discard-class of 3, the packet is dropped at ingress itself.

Weighted Random Early Detection

The following restriction applies to Weighted Random Early Detection (WRED):

- For thresholds in time units, the guaranteed service rate is used to calculate the thresholds in bytes.

For bundles, queue limit and WRED thresholds are supported in time units only.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows how to enable RED using a minimum threshold value of 1000000 and a maximum threshold value of 2000000:

```
RP/0/RP0/CPU0:router(config)# policy-map policy1
RP/0/RP0/CPU0:router(config-pmap)# class class1
RP/0/RP0/CPU0:router(config-pmap-c)# random-detect 1000000 2000000
```

service-policy (interface)

To attach a policy map to an input interface or output interface to be used as the service policy for that interface, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface, use the **no** form of the command.

service-policy {**input** | **output**} *policy-map*
no service-policy {**input** | **output**} *policy-map*

Syntax Description

input	Attaches the specified policy map to the input interface.
output	Attaches the specified policy map to the output interface.
policy-map	Name of a service policy map (created using the **policy-map** command) to be attached.

Command Default

No service policy is specified.

Command Modes

Interface configuration.

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

You can attach a single policy map to one or more interfaces to specify the service policy for those interfaces. The class policies composing the policy map are then applied to packets that satisfy the class map match criteria for the class. To apply a new policy to an interface, you must remove the previous policy. A new policy cannot replace an existing policy.

Task ID

Task ID	Operations
qos	read, write

Examples

This example shows policy map policy2 applied to HundredGigabitEthernet 0/0/0/1.

```
RP/0/RP0/CPU0:router(config)# class-map class2
RP/0/RP0/CPU0:router(config)# match precedence ipv4 2
RP/0/RP0/CPU0:router(config-cmap)# exit

RP/0/RP0/CPU0:router(config)# policy-map policy2
RP/0/RP0/CPU0:router(config-pmap)# class-map class2
RP/0/RP0/CPU0:router(config-pmap-c)# set precedence 3
RP/0/RP0/CPU0:router(config-pmap)# exit

RP/0/RP0/CPU0:router(config)# HundredGigabitEthernet 0/0/0/1
RP/0/RP0/CPU0:router(config-if)# service-policy input policy2
```

This example shows policy map policy 1 applied to Bundle-Ether interface.

```
RP/0/RP0/CPU0:router(config)# interface Bundle-Ether1
RP/0/RP0/CPU0:router(config-if)# service-policy input policy1
RP/0/RP0/CPU0:router(config-if)# exit
```



Hierarchical Modular QoS Commands

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D



Note If you try to configure a **hw-module** command in a hardware variant or line card that does not support it, an appropriate error message is logged.

This chapter describes the commands used to manage hierarchical modular QoS.

- hw-module profile qos conform-aware-policer , on page 119
- hw-module profile qos hqos-enable, on page 120
- hw-module profile qos hqos-enable-without-l2acl, on page 121
- hw-module profile qos max-trunks (hw-module profile bundle-scale), on page 123
- hw-module profile qos physical-hqos-enable, on page 124

hw-module profile qos conform-aware-policer

To enable the conform-aware hierarchical policy feature, use the **hw-module profile qos conform-aware-policer** command in the XR Config mode. To disable this feature, use the no form of this command.

This configuration allows conform traffic from the child level policy to prioritize exceed or violate traffic at the parent level policy. There was no way for the conform traffic belonging to a child policy to get priority over the parent level policy in earlier releases. When this profile is enabled, the entire system is in color-aware mode compared to the default color-blind mode. There is no effect on other features or resources.

hw-module profile qos conform-aware-policer

Syntax Description

conform-aware-policer	Enables conform traffic from the child level policy to prioritize exceed or violate traffic at the parent level policy.

Command Default

The conform-aware hierarchical policy feature is disabled by default, unless enabled by this command.

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Usage Guidelines

- You must reload the affected line card to enable the conform-aware hierarchical policy feature.
- On your router with dual-rate three-color (2R3C) policer:
  - committed information rate (CIR) value is marked as GREEN, with discard-class=0 and drop precedence=0
  - excess information rate (EIR) is marked as YELLOW, with discard-class=1 and drop precedence=1

  This is the default hardware behavior that allows the color-aware parent policer to differentiate between CIR and EIR. It's not possible to modify this behavior.
- For details on this feature, see Conform Aware Hierarchical Policy Overview.

Task ID

Task ID	Operation
qos	read, write

Example

The following example shows how to enable the conform-aware hierarchical policy feature.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)#hw-module profile qos conform-aware-policer
RP/0/RP0/CPU0:router(config)#commit
RP/0/RP0/CPU0:router#reload
```

hw-module profile qos hqos-enable

To enable H-QoS profile with ingress Layer 2 Access Control List (L2 ACL) functionality, but without egress bridging service EVPN ethernet LAN (ELAN) QoS functionality, use the hw-module profile qos hqos-enable command in XR Config mode. To remove the H-QoS profile, use the no form of the command.

hw-module profile qos hqos-enable

no hw-module profile qos hqos-enable

Syntax Description

This command has no keywords or arguments.

Command Default

H-QoS is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

- H-QoS on EVPN ELAN and L2 ACL cannot be enabled simultaneously on an interface. You can either use the hw-module profile qos hqos-enable-without-l2acl command to enable H-QoS on EVPN ELAN or the hw-module profile qos hqos-enable command to enable H-QoS on L2 ACL.
- After enabling H-QoS profile, the router must be reloaded.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the H-QoS profile on the router.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)# hw-module profile qos hqos-enable
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos hqos-enable-without-l2acl

To enable H-QoS profile with egress bridging service EVPN ethernet LAN (ELAN) QoS functionality, but without ingress Layer 2 Access Control List (L2 ACL) functionality, use the hw-module profile qos hqos-enable-without-l2acl command in XR Config mode. To remove the H-QoS profile, use the no form of the command.

Note This command is applicable for Release 6.5.2.

hw-module profile qos hqos-enable-without-l2acl

no hw-module profile qos hqos-enable-without-l2acl

Syntax Description

This command has no keywords or arguments.

Command Default

H-QoS is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.5.2	This command was introduced.

Usage Guidelines

- H-QoS on EVPN ELAN and L2 ACL cannot be enabled simultaneously on an interface. You can either use the hw-module profile qos hqos-enable-without-l2acl command to enable H-QoS on EVPN ELAN or the hw-module profile qos hqos-enable command to enable H-QoS on L2 ACL.
- Even though L2 ACL functionality is not supported if you create an H-QoS profile using the hw-module profile qos hqos-enable-without-l2acl command, L2 ACL user profiles are not explicitly blocked in this profile.
- Bridged Virtual Interface (BVI) and Integrated Routing and Bridging (IRB) are not supported in this profile.
- Ensure that you remove the hw-module profile qos hqos-enable command before using this command.
- After enabling H-QoS profile, the router must be reloaded.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the H-QoS profile on the router.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)# hw-module profile qos hqos-enable-without-l2acl
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos max-trunks (hw-module profile bundle-scale)

To control the scale of bundle sub-interfaces and the number of members per bundle, use the **hw-module profile qos max-trunks** or **hw-module profile bundle-scale** (only from Release 6.5.1) command in XR Config mode.

hw-module profile qos max-trunks {256|512|1024}

hw-module profile bundle-scale {256|512|1024}

Syntax Description

256	Permits up to 128 bundle sub-interfaces, each containing up to 64 member-links
512	Permits up to 384 bundle sub-interfaces, each containing up to 32 member-links.
1024	Permits up to 896 bundle sub-interfaces, each containing up to 16 member-links.

Command Default

hw-module profile qos max-trunks 256, that is, permits up to 128 bundle sub-interfaces, each containing up to 64 member-links.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.
Release 6.5.1	The **hw-module profile qos max-trunks <256/512/1024>** command is replaced with the **hw-module profile bundle-scale <256/512/1024>** command

Usage Guidelines

The router must be reloaded for the hw-module command to be functional.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to change the scale of bundle interfaces to 256.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)# hw-module profile qos hqos-enable
RP/0/RP0/CPU0:router(config)#hw-module profile qos max-trunks 256
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# reload
```

hw-module profile qos physical-hqos-enable

To enable hierarchical egress policies on the physical or on the virtual main interfaces, use the hw-module profile qos physical-hqos-enable command in XR Config mode. To remove the H-QoS profile, use the no form of the command.

hw-module profile qos physical-hqos-enable

no hw-module profile qos physical-hqos-enable

Syntax Description

This command has no keywords or arguments.

Command Default

Physical-H-QoS is disabled by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.2.2	This command was introduced.

Usage Guidelines

- H-QoS enable and physical H-QoS enable profiles are mutually exclusive, so both cannot be applied together. You can either use the hw-module profile qos hqos-enable command to enable H-QoS on virtual interface or the hw-module profile qos physical-hqos-enable command to enable H-QoS on physical interface. If you apply both, then the configuration is rejected.
- No egress policy-map is supported on any type of sub-interface.
- The parent traffic policy, only supports the traffic class of type class-default.
- The parent traffic policy, only supports the class-action shape and no other queuing action can be configured in it.
- A maximum of only 4-priority levels are supported in this mode, unlike the default mode where up to 7-priority levels are supported.
- Bandwidth and bandwidth remaining configurations are not supported simultaneously within the same policy-map. If a class has bandwidth (CIR), other classes must also have only bandwidth configuration. If a class-map has bandwidth remaining percent or ratio (EIR), other classes must also have only the bandwidth remaining configuration. Shaping is applied on any class.
- The granularity of bandwidth or bandwidth remaining ration (BRR) is 1:64 as compared to 1:4096 for non-hqos mode.

Task ID

Task ID	Operation
qos	read, write

The following example shows how to enable the physical H-QoS profile on the router.

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router(config)# hw-module profile qos physical-hqos-enable
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# reload
```