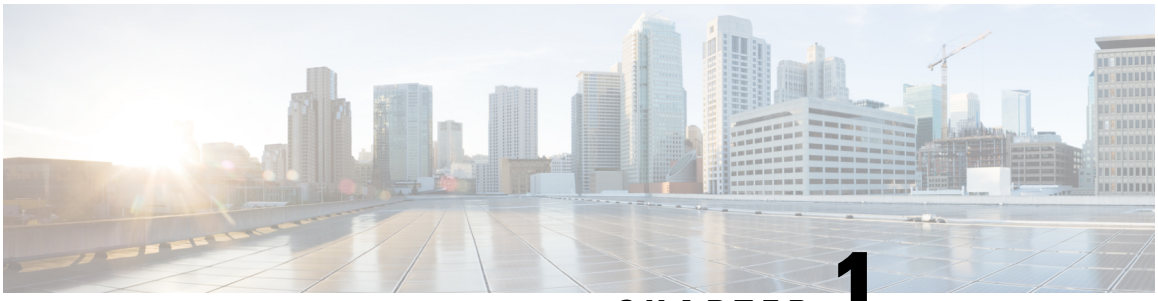
Quality of Service Configuration Guidelines, Cisco IOS XE 16 (Cisco NCS 4200 Series)

First Published: 2019-07-31

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

CONTENTS



CHAPTER 1

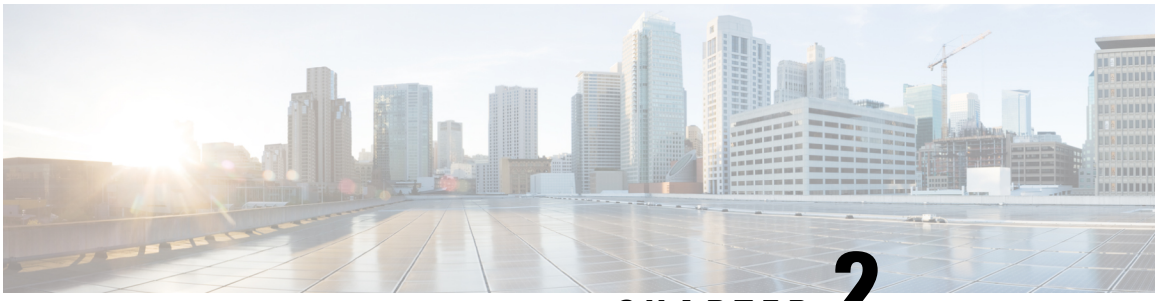
Feature History

The following table lists the new and modified features that are supported in the Quality of Service Configuration Guidelines in Cisco IOS XE 16 releases, on Cisco NCS 4201 and Cisco NCS 4202 routers.

Feature Name	Cisco IOS XE Release
CoS Marking for Local Traffic	16.11.1
Egress QoS for IPSLA	16.8.1

The following table lists the new and modified features that are supported in the Quality of Service Configuration Guidelines in Cisco IOS XE 16 releases, on Cisco NCS 4206 and Cisco NCS 4216 routers.

Feature Name	Cisco IOS XE Release
MPLS Layer 3 VPN Conditional Marking	16.12.1
QoS Short-pipe Mode	16.12.1
CoS Marking for Local Traffic on the RSP2 Module	16.11.1
Global Table Map	16.11.1
16K EFP Support on Port Channel	16.8.1
16K EFP QoS Support	16.6.1
IPv6 QoS	16.5.1
Table Map MDT Index Optimization	16.5.1



CHAPTER 2

Quality of Service Configuration Guidelines for RSP1, RSP2 Module

This document outlines Quality of Service features and limitations available on the Cisco ASR 903 Series Router and contains the following sections:

Quality of Service

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Ethernet and 802.1 networks, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by implementing the following services:

- Supporting guaranteed bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

Quality of Service Configuration

This document provides details on the platform-dependent implementation of QoS on the router.

QoS Support Overview

Table below provides an overview of QoS feature support on the router. For more detail about the support for each feature, see s Global QoS Limitations.

Table 1: QoS Feature Overview

Feature	Main	Service Instance	Trunk EFP	Port- Channel	Member Link
Dynamic policy modification	3.6	3.6	3.6		3.6
EFP QoS Support	3.6	3.6	3.6		
Classification					
Ingress		3.5	3.5.1		3.5
Egress		3.5	3.5.1		3.5
IPv6 [1]	3.6	3.6	3.6		3.6
Match any	3.6	3.6	3.6		3.6
Marking					
Ingress	3.5	3.5	3.5.1		3.5

Feature	Main	Service Instance	Trunk EFP	Port- Channel	Member Link
Egress	3.6	3.6	3.6		3.6
Policing					
Ingress	3.5	3.5	3.5.1		3.5
Egress	3.6	3.6	3.6		3.6
Priority policing	3.6	3.6	3.6		3.6
Shaping					
Port Shaping	3.6.1	3.6.1	3.6.1		
Congestion Avoidance					
WRED	3.6	3.6	3.6		3.6
Multiple Priority Queues	3.7	3.7	3.7		3.7
Congestion Management					
Strict Priority	3.5	3.5	3.5.1		3.5
Scheduling					
Ingress					
Egress	3.5	3.5	3.5.1		3.5
QoS ACLs					
Ingress	3.5.1	3.5.1	3.5.1		3.5.1
Egress					

[1] IPv6 based ACLs are not supported for TDM interfaces.

Table 2: QoS Support for TDM Features

Feature	Release	Interface Module	Ingress	Egress
HDLC	3.9	T1/E1	No	Yes
	3.13	OC-3	Yes	Yes
MLPPP	3.7	T1/E1	No	Yes
	3.8	OC-3	No	Yes
	3.13	T1/E1 and OC-3	Yes	Yes

Feature	Release	Interface Module	Ingress	Egress
POS	3.8	T1/E1	NA	NA
	3.8	OC-3	No	Yes
	3.9	OC-12	No	Yes
	3.13	OC-3	Yes	Yes
ATM QoS L2 for ATM PW	3.7	T1/E1 and OC-3	Yes	NA
QoS for CEM/ATM/IMA PW	3.9	T1/E1 and OC-3	Yes	NA

Global QoS Limitations

The following limitations apply to multiple QoS features on the router:

- When EVCs under a physical interface have a QoS policy attached, the following limitations apply:
  - The port-level policy is limited to the class-default class.
  - Only the **shape** command is supported in the port-level policy.
- The router supports up to 64 unique QoS classification service instances in a given bridge domain. QoS service instances refer to ports, VLAN classes, EFPs associated with a QoS classification policy.
- Modification of class-map definitions while applied to an interface or Ethernet Flow Point is *not* supported.
- Effective with Cisco IOS XE Everest 16.5.1, if the same table-mapping is applied on multiple interfaces, the MDT index is shared across these interfaces. Thus increased scaling of table-map is possible if table-mapping is reused.
- Policy validation—Some QoS policy configurations are not validated until you apply the policy-map to an interface or EFP. If a QoS configuration is invalid, the router rejects the configuration when you apply it to an interface. In some cases, a QoS configuration may be rejected due to hardware resource exhaustion or limitations. If you receive such an error message, detach the policy and adjust your QoS configuration.
- After TCAM resource exhaustion (tcam resource reaches 4000 tcams), the QoS policy applied on the EFP may *not* function as expected. The QoS policy must be re-applied on the EFP.
- The **match-all** keyword is supported only for QinQ classification.
- Only one **match access-group** match is supported on the same class map.
- SAToP and CESoPSN pseudowire traffic has a default MPLS Exp priority setting of 5 (high).
- QoS is supported on POS interfaces on optical interface module.
- Three-level QoS policies are not supported on the OC-3/OC-12 serial, MLPPP, and PoS interfaces. You can only apply QoS policies on two levels on these interfaces.

- QoS does not account for CRC values on an interface and assumes that the value is 2 bytes. CRC differences can cause accuracy issues for 2 to 3% of the 128-byte traffic.
- The router supports a maximum of 128 internal and reserved labels that represent PHB (cos/dscp/exp/prec) values on a QoS policy. A label exhaustion message is displayed if a policy exceeds the maximum number of labels.
- QoS does not support WRED counters for all the match conditions.
- Configuring **set mpls exp topmost** in edge router does not copy the exp value to MPLS label. At Ingress interface, only VC label is supported as topmost label. At Egress interface, the topmost label is supported which takes MPLS label based on LDP. The outer MPLS label exp value is same as inner MPLS label. When the VC label exp value is zero, the outer MPLS label exp value becomes zero. At Ingress, when the VLAN is pushed, the MPLS exp value also becomes VLAN pushed tag.
- The ICMPv4 packets classification based on ACL attached on the interface is not supported.
- EXP-based classification at the egress of PE routers is not supported by default. To achieve this, the EXP bits are required to be imposed over the cross connect at the ingress of the same PE router using an input policy.
- When a class-map and policy-map are created with match-and-set action(s) and attached to an interface, an internal value called label is allocated for each PHB value used in the class-map. These label values are consumed only when the class-maps and policy-maps are attached to an interface.

  The platform has only a handful of available labels, and usage of class and policy-maps leads to exhaustion of labels at some point. As the number of PHB matches at egress policy-maps increases, the label consumption also increases.

  When you attach class and policy-maps to interfaces after the labels are exhausted, the platform can no longer process the class and policy-maps. As the number of PHB matches at egress policy-maps increases so does the label consumption.

  To avoid this condition, a convention is followed wherein, at the ingress interface for a traffic flow the classes match the PHB values such as CoS, PREC, and so on, and set the internal QoS-Group values. At the egress interface, the classes match the traffic based on the QoS groups that are set at the ingress.
- Match on DSCP classification or policing or QoS group marking is not supported for IPv6 traffic on the disposition node when MPLS is configured for both per-prefix and per-VRF modes.
- In case of a PE router,
  - For an egress policy-map to work at the access interface, it is mandatory to configure an ingress policy-map at the core interface of the same router.
  - If an ingress policy-map on core port has a marking option along with a egress policy-map on the same router, then egress policy-map must be configured at the corresponding access port for the marking to be preserved.

QoS Features Using MQC Limitations

Table below lists the QoS MQC scaling limitations on router per release.

Table 3: Qos on MQC Limitations

Supported on Cisco ASR 903	Cisco IOS XE 3.5S	Cisco IOS XE 3.6S	Cisco IOS XE 3.7S	Cisco IOS XE 3.8S	Cisco IOS XE 3.9S	Cisco IOS XE 3.10S
No. of unique policy-maps	1024					
No. of unique class-maps	4096					
No. of classes per policy-map	512					256
No. of filters per class-map	16					

[2] For releases which are not listed, refer to the most recent previous release limit.

Restrictions for Ingress QoS

Restrictions for Ingress QoS in the Cisco IOS Release 3.9 and later:

- EC main interface
  - Only policing and marking are supported.
  - A class-map can have any type of filter, including the **match vlan** and **match service instance** commands.
- EC EVC/TEFP
  - Only policing and marking are supported.
  - Match service instance is *not* supported.
- Member links
  - Only policing and marking are supported.
  - Policy-map on a member link is *not* supported with EVC configured at the port-channel level.
- Policy-map application is allowed only on the EC main interface, EC member link, or EC EVC.

Note Ingress policer on port-channel across cylon works at twice the policer rate.

Restrictions for Egress QoS

- The maximum number of classes supported on the policy map is 8, which includes class class-default; 7 user-defined classes and class class-default is supported.

- The maximum number of port-channel interfaces that can be created and supported for QoS on the router is 16.

Restrictions for Egress QoS in the Cisco IOS XE Release 3.9 and later:

- EC main interface
  - Classification statistics for the policy-map on a port-channel main interface are *not* supported as no queues are allocated for a port-channel main interface.
  - Policing and marking actions are only allowed in the policy-map on a port-channel main interface.
  - Queuing actions are *not* supported.
  - Egress TCAM entries are used even in the absence of member links.
- EC EVC/TEFP
  - Classification statistics for the policy-map on port-channel EVC/TEFP are *not* supported as no queues are allocated for port-channel EVC/TEFP.
  - Policing and marking actions are only allowed in the policy-map on port-channel EVC/TEFP.
  - Queuing actions are *not* supported.
  - Egress TCAM entries are used even if there are no member links present.
- EC Member links
  - For egress match service-instance policy-map on EC member links, the same policy must be present on all other EC member links.
  - Match service-instance policy-map is replicated automatically for all the member links when the first policy is applied on any of the member links.
  - For non-match service-instance policy-map, the same policy-map can be applied for all member-links.
  - Dynamic modification of match service-instance policy-map actions is *not* allowed.
  - Deleting a global match service instance policy-map is *not* allowed if it applied to the member links.
  - Policing, marking and queuing action are supported on port-channel member links.
  - The running configuration displays the first member link on the first policy applied in a service-policy configuration.
  - The s**how policy-map interface brief** command only displays the policy-map applied on the running configuration.
  - Applying a same policy again on other member links where a policy-map was already applied will not display any error. A differently named policy if applied again will display an error.
  - For match service instance policy-map on egress member links, the policy-map statistics information is reset, when a member link is added or deleted from a port-channel either by configuration or by LACP port-bundling/unbundling action.
  - There is no difference in behavior for non-match service instance policies on the member links. They continue to work in the legacy mode. There is no conservation of TCAM entries in this mode, even if the same policy is applied on all member links.

- Policy-map application is allowed only on either EC main interface, or EC member link, or EC EVC.

Restrictions of Ether Channel QoS

This section lists the various restrictions/limitations of the QoS-specific port-channel.

- Egress QoS policy-map is supported only on a member-link interface and not on a port-channel, port-channel EVC and port-channel TEFP.
- Effective Cisco IOS XE Everest 16.5.1 release, the egress policy-map can be configured on port-channel interface, which is in active/standby mode.
- Egress Match efp policy is not supported on PC member-links.
- Egress Match vlan policy is not supported on PC member-links.
- A maximum of 8 member-links will be bundled into a port-channel.
- All the other restrictions that are applicable to a regular port interface on the Cisco RSP3 module are applicable to a port-channel interface and port-channel EVC.
- Egress policy-map with marking action is not supported on port-channel member links.

8K EFP (4 Queue Model)

In Cisco IOS XE Release 3.18SP, the 8K EFP (4 Queue Model) support allows up to 8000 EFPs at the system level. EFP scale implementation follows the static model, that is, eight queues are created per EFP by default.

Information About 8000 (8K) EFP

- In default model, 5000 EFPs can be configured on Cisco ASR 903 RSP3 module.
- The Switch Database Management (SDM) template feature can be used to configure 8000 EFPs across ASIC(4000 EFPs per ASIC interfaces).
- In 8K EFP model, each EFP consumes four Egress queues. If 8K EFP SDM template is not enabled, each EFP consumes eight Egress queues.
- Ingress policy map can specify more than eight traffic classes based on PHB matches, which remains the same. However, Egress policy map can have three user defined class and class-default class.
- Each Egress class-maps can be mapped to a single or multiple traffic classes and each class-map mapped to a single queue.
- Maximum of two queues are set to Priority according to policy configuration.
- All the existing QOS restrictions that apply in default model are also applicable to 8K EFP model.

Prerequisites for 8000 (8K) EFP

- Activate the Metro Aggregation Services license on the device.
- To configure 8000 EFPs, enable the SDM template using CLI **sdm prefer enable_8k_efp**.
- Reset the SDM template using the CLI **sdm prefer disable_8k_efp** .

Restrictions for 8000 (8K) EFP

- Traffic class to Queue mapping is done per interface and not per EVC.
- Four traffic classes including class-default can be supported in Egress policy.
- Same three traffic classes or subset of three traffic classes match is supported on EVCs of an interface.
- Traffic classes to queue mapping profiles are limited to four in global, hence excluding class-default, only three mode unique combinations can be supported across interfaces.
- TRTCM always operates with conform-action transmit, exceed-action transmit and violate-action drop.
- By default, 1R2C Policer will behave as 1R3C Policer in 4 Queue model.
- All the QOS restrictions that is applicable in default mode is also applicable in 8k EFP mode

Configuring 8K Model

Configuring 8K EFP Template

Below is the sample configuration to enable 8K EFP or 4 Queue mode template. On enabling **sdm prefer enable_8k_efp**, the router reloads and boots up with 8K EFP template.

```
RSP3-903(config)#sdm prefer enable_8k_efp

Template configuration has been modified. Save config and Reload? [yes/no]: yes
Building configuration...

Jul 22 05:58:30.774 IST: Changes to the EFP template preferences have been stored[OK]
Proceeding with system reload...
Reload scheduled for 06:00:38 IST Fri Jul 22 2016 (in 2 minutes) by console
Reload reason: EFP template change
```

Verifying 8K EFP Template

You can verify the current template as below.

```
Device#sh sdm prefer current

The current sdm template is "default" template and efp template is "enable_8k_efp" template
```

Configuring QOS in 8K EFP Model

Below is sample configuration to configure egress policy map when 4Q mode is enabled.

```
Device#enable
Device#configure terminal
```

```
Device(config)#interface GigabitEthernet0/3/0
Device(config-if)#service instance 10 e
Device(config-if-srv)#service-policy output egress


Current configuration : 193 bytes
!
policy-map egress
class qos2
  shape average 2000000
 class qos3
  shape average 3000000
 class qos4
  shape average 4000000
 class class-default
  shape average 5000000
!
end
```

```
Device#sh run class-map qos2
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos2
match qos-group 2
!
end


Device#sh run class-map qos3
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos3
match qos-group 3
!
end


Device#sh run class-map qos4
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos4
match qos-group 4
!
end
```

Verifying QOS in 8K EFP Model

You need to verify the interface and policy-map details to check 8K model queue is working.

```
Device# show run interface g0/3/0
Building configuration...

Current configuration : 217 bytes
!
interface GigabitEthernet0/3/0
no ip address
negotiation auto
```

```
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  service-policy output egress
  bridge-domain 10
!
end
```

```
Router#show running-config policy-map egress
Building configuration...

Current configuration : 193 bytes
!
policy-map egress
class qos2
shape average 2000000
class qos3
shape average 3000000
class qos4
shape average 4000000
class class-default
shape average 5000000
!
end
```

```
Device#sh policy-map int g0/3/0 serv inst 10
Port-channel10: EFP 10

Service-policy output: egress

Class-map: qos2 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 4096000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/119746/0
(pkts output/bytes output) 2820/2882040
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000

Class-map: qos3 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 3
Queueing
queue limit 2730666 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/118806/0
(pkts output/bytes output) 3760/3842720
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Class-map: qos4 (match-all)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 2048000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 4000000, bc 16000, be 16000
target shape rate 4000000

Class-map: class-default (match-any)
245131 packets, 250523882 bytes
```

```
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 1638400 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 5000000, bc 20000, be 20000
target shape rate 5000000
Device#
```

16K EFP Support

Starting Cisco IOS Release 16.6.1, 16K EFPs are supported on the RSP3 module. The key features with this enhancement are:

- 16000 EFPs are supported on the RSP3 module (8K EFPs are supported per ASIC). Each port can have maximum of 8K EFPs configured.
- 8K bridge-domains are supported.
- Maximum of 16000 EVCs can be configured on the physical interface.
- Maximum of 8K Local-connect configurations are supported.
- Maximum of 1K bridge domain interface (BDI) can be configured upto BDI 4096.

Note In scenarios where VLAN range is greater than 5, VLAN compression is enabled.

Restrictions for 16K EFP

- 16k EFP scale is *not* supported if sdm template is enabled for split horizon scale.
- Egress policy-map is *not* supported on interfaces with 8K EFP configuration.
- The EVC/BD scale is *not* supported for port-channel.
- Minute traffic outage (few milliseconds) may be observed when applying or removing a policy-map.
- MAC security configuration must be reconfigured after every policy is attaced or detached.
- G8032, CFM and other Layer2 configurations are *not* supported if bridge-domains configured exceeds 4096.
- EVC MAC flush is triggered after attaching or detaching an egress policy map on the EVC.
- In a full scale setup, the EFP statistics update takes more than 1min to complete.

Configuring QoS with 16K EFP

Sample configurtion on how to configure 16K EFP

```
enable
Configure terminal
interface gigbaitethernet interface 0/0/1
service instance 8001 ethernet
encapsulation dot1q 20
bridge-domain 20
```

Verifying QoS Using 16k EFP

Following are verfication examples to verify QoS configurations using 16K EFP.

show ethernet service instance summary

```
Router# show ethernet ser instance summary
System summary
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain     16000    16000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all         16000    16000        0        0        0        0        0        0
Associated interface: GigabitEthernet0/6/1
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
Associated interface: TenGigabitEthernet0/7/7
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
```

show ethernet service instance id interface stats

```
Router# show ethernet service instance id 12000 interface te0/7/7 stats
Port maximum number of service instances: 16000
Service Instance 12000, Interface TenGigabitEthernet0/7/7
   Pkts In   Bytes In   Pkts Out  Bytes Out
       252     359352        252     359352
```

show platform hardware pp active interface all

```
Router# show platform hardware pp active interface all
Interface manager platform keys
-------------------------------------------------

Name: TenGigabitEthernet0/7/7, Asic: 0, hwidx: 62
lpn: 0, ppn: 62, gid: 62, mac: 7426.acf6.5685
InLportId: 0, ELportId: 0, dpidx: 22, l3ID: 19
port_flags: 0, port_speed: 10000 Mbps, efp_count: 8000, destIndex: 62, intType: 1
etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 1, l3PhyIf: 0, l3TDM: 0, loopBack: 0
tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 65535, protocols: 0
v4_netsmask: 0, v4_tableid: 0, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
vrfid: 0, enctype: 0, admin_state: 1, admin_state_oir: 0
```

show platform hardware pp active feature qos resource-summary

```
Rouer# show platform hardware pp active feature qos resource-summary 0
RSP3 QoS Resource Summary

Type Total Used Free
-------------------------------------------------------------------------------
QoS TCAM 1024 0 1024
VOQs 49152 784 48368
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 32000 32768

Router# show platform hardware pp active feature qos resource-summary 1
RSP3 QoS Resource Summary

Type Total Used Free
-------------------------------------------------------------------------------
QoS TCAM 1024 0 1024
VOQs 49152 784 48368
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
```

show interface

```
Router# show interface gig0/1/6 | in pack
  30 second input rate 43604000 bits/sec, 43955 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     1521946 packets input, 188721304 bytes, 0 no buffer
     0 packets output, 0 bytes, 0 underruns

Router# show interface gig0/1/7 | in pack
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 43131000 bits/sec, 43482 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     1523724 packets output, 188941776 bytes, 0 underruns
```

Routed Port-Channel

Routed Port-channel Interface

The following features are supported for the ingress policy-map on a routed port-channel interface:

- Marking
- Policing
- Conditional marking
- Marking and policing
- Classification criteria is prec, dscp or ip acl.

Example for Routed Port-channel Interface

```
policy-map routed_pc_ingress
class prec1
set prec 2
class prec2
police cir 100m
class prec3
police cir 150m conform-action set-prec-transmit 4 exceed-action drop
class prec4
police cir 200m
set prec 0
!
end
```

The following features are supported for egress policy-map on routed port-channel interface:

- Marking
- Policing
- Classification criteria is prec or dscp.

Example for egress policy-map on routed port-channel interface

```
policy-map pc_egress
class dscp0
set dscp 16
class dscp48
police cir 1m
!
end
```

Member-links on Routed Port-channel Interface

The following features are supported for ingress policy-map on member links on the routed port-channel interface:

- Marking
- Policing
- Conditional marking
- marking and policing
- Classification criteria is prec, dscp or ip acl.

The following features are supported for egress policy-map on member links on the routed port-channel interface:

- Shaping
- Queue-limit
- Bandwidth (kbps, percent)
- Bandwidth remaining (ratio, percent)
- WRED
- Port Shaper
- Low Latency Queue (LLQ or priority queue)

Example for egress policy-map on member links on the routed port-channel interface

```
policy-map mem_link_egress
class qos-group0
bandwidth percent 90
class qos-group67
police cir 1m
priority
class class-default
shape average 64k
!
end
```

Port-channel with EFP

The following features are supported for ingress policy-map on port-channel on EFP:

- Marking
- Policing
- Conditional marking
- marking and policing
- The classification criteria is VLAN or EFP, Cos in child.

Example for Port-channel with EFP

```
policy-map cos_child
class cos0
set cos1
!
policy-map efp_pc_ingress
class vlan100
police cir 10m
service-policy cos_child
!
end
```

The following features are supported for egress policy-map on port-channel on EFP:

- Marking
- Policing
- Conditional marking
- marking and policing
- The classification criteria is VLAN or EFP, Cos in child

Example for egress policy-map on port-channel on EFP

```
policy-map cos_child
class cos0
set cos1
!
policy-map efp_pc_ingress
class vlan100
```

```
police cir 10ms
service-policy cos_child
!
end
```

EFP of Port-channel with EFP Configuration

- The following features are supported for ingress and egress policy-map on EFP of port-channel on EFP:
  - Marking
  - Policing
  - Conditional marking
  - marking and policing
  - The classification criteria is VLAN or EFP, Cos in child.

Note Match EFP is cannot be configured.

Member Links of Port-channel with EFP Configuration

- The following features are supported for ingress and egress policy-map on member links of port-channel on EFP:
  - Marking
  - Policing
  - Conditional marking
  - marking and policing
  - The classification criteria is VLAN or EFP, Match VLAN and Cos in child.

Restrictions for Hierarchical Policies

The Cisco ASR 903 Router supports hierarchical QoS policies with up to three levels, allowing for a high degree of granularity in traffic management.

There are limitations on the supported classification criteria at each level in the policy-map hierarchy. The following limitations apply when configuring hierarchical policy-map classification:

- The topmost policy-map in a three-level hierarchy only supports classification using class-default.

Sample Hierarchical Policy Designs

The following are examples of supported policy-map configurations:

- Three-Level Policy—You can only apply a three-level policy to a physical port on the router. A three-level policy consists of:

- Topmost policy: class-default
- Middle policy: match vlan
- Lowest policy: match qos-group/match prec/match cos/match dscp

  The following sample policy uses a flat class-default policy on the port and VLAN policies on EFP interfaces to unique QoS behavior to each EFP.

Sample Policy

```
Policy-map port-shaper
Class class-default
Shape average percent 70
Service-policy Vlan_set

Policy-map Vlan_set
Class vlan100
Bandwidth percent 20
Shape average 200m
Service-policy child1
Class vlan200_300
Bandwidth percent 75
Service-policy child2

Policy-map child1
Class prec2
Shape average percent 40

Policy-map child2
Class prec4
Police cir percent 50
```

- Two-Level Policy
  - Topmost policy: match vlan
  - Lowest policy: match qos-group/match prec/match cos/match dscp
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match vlan
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match mpls experimental topmost
- Flat policy: match ip dscp
- Flat policy: match vlan inner
- Flat policy: class-default

Ingress and Egress Hierarchical Policing

In releases before Cisco IOS XE Release 3.9, policing was supported only at one level in the ingress and egress policy. It was only at the PHB or class level.

Effective with Cisco IOS XE Release 3.9, policing is supported at two levels of the policy-map.

- Ingress policing
  - Port and EFP level
  - EFP and Class level
  - Port and Class level
- Egress policing
  - EFP and Class level
  - Port and Class level

Note Egress hierarchical policing is supported on two levels but one of the levels must be Class level.

If an Ingress hierarchal policy is configured on the interface, the **show Ethernet service instance interface** command does not display the service instance statistics.

The class-level in an Egress hierarchal policy is configured internally as shaper.

Dissimilar PHB Support for MPLS and VPLS Interfaces

Effective with Cisco IOS XE Release 3.11S, dissimilar per-hop behavior (PHB) **match** on exp is supported for Ingress and Egress on MPLS and VPLS interfaces.

In earlier releases prior to Cisco IOS XE Release 3.11S, when **qos-group** or **discard-class** based on exp classification was configured, Egress based classification was *not* allowed on any other classification except Ingress **set qos-group** or **discard-class**. This was due to the PHB security model.

With Cisco IOS Release 3.11, only EVC based tunnel type configuration with either Layer2 VPN or Layer3 VPN is supported.

As pipe mode and uniform mode are supported, when **qos-group** or **discard class** (pipe-mode) is matched again on the Egress interface, all **qos-groups** in tunnel types (such as Layer2 VPN, Layer3 VPN, and MPLS VPN) are supported only if the tunnel type exists on the EFP. The **qos-group** entries in the TCAM are matched on the tunnel type. Thus, dissimilar PHB match at the egress is supported for both Ingress and Egress simultaneously on the router.

For example, the qos-group configured at Layer2 terminating Egress interface is matched against the Layer2 VPN tunnel type. This enables the **dscp** (uniform-mode) on the Layer3 VPN terminating Egress interface to **match** with the Layer3 VPN Egress interface.

Restrictions for Dissimilar PHB Support for MPLS and VPLS Interfaces

- Supported for **qos-group** or **discard-class** and **dscp** dissimilar matches for Egress PE (VPN terminating) and *not* for regular EVCs.
- If match **discard-class** policy is applied at the interface level (the policy is applied to the Layer3 interface), the match **dscp** policies on the other Layer3 VPN interfaces *cannot* be applied.

  We recommend that the policy is applied at the EVC level on individual Layer2 or Layer3 interfaces instead of at port-level. Alternatively, configuring a match EFP policy to match **qos-group** or **discard-class** classification on the EFP for Layer 2 VPN, and match **dscp** on the EFP for Layer3 VPN is recommended.
- If both Layer2 VPN and Layer3 VPN configurations exists on an interface, and the port-based policy has **match qos-group** or **discard-class**, then two match dscp classifications are *not* supported on the **match dscp**.

MPLS VPN QoS Mapping

Table below summarizes the default MPLS mappings for the Cisco ASR 903 Series Router.

Table 4: Default MPLS QoS Mapping

Feature	Imposition	Disposition
L3VPN, MPLS	IP Prec bit copied to MPLS Exp bit.	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.
L2VPN (EoMPLS, VPLS)	MPLS Exp bit is set to 0	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.
MPLS-TP		
CESoPN	MPLS Exp bit is set to 5	IP Prec bit is unchanged.
SAToP	MPLS Exp bit is set to 5	IP Prec bit is unchanged.
6VPE, 6PE	Prec bit value is copied to the MPLS Exp bit	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.

Note You can modify the default mapping behaviors using explicit marking policies.

QoS on Ether Channels

The following three types of ether channels are supported

- Legacy Port Channel
- Port Channel LACP Active Standby (1:1)
- Port Channel LACP Active Active

Restrictions of Ether Channel QoS

This section lists the various restrictions/limitations of the QoS-specific port-channel.

- Egress QoS policy-map is supported only on a member-link interface and not on a port-channel, port-channel EVC and port-channel TEFP.
- Effective Cisco IOS XE Everest 16.5.1 release, the egress policy-map can be configured on port-channel interface, which is in active/standby mode.
- Egress Match efp policy is not supported on PC member-links.
- Egress Match vlan policy is not supported on PC member-links.
- A maximum of 8 member-links will be bundled into a port-channel.
- All the other restrictions that are applicable to a regular port interface on the Cisco RSP3 module are applicable to a port-channel interface and port-channel EVC.
- Egress policy-map with marking action is not supported on port-channel member links.

Example for Configuring QoS on an Ether Channel

Ingress Policy Map

The below example shows how to configure an ingress QoS policy-map.

```
do sh policy-map cos
  Policy Map cos
    Class cos1
     police cir 1000000 bc 31250
       conform-action transmit
       exceed-action drop
```

Member Link Policy-Map

The below example shows how to apply an ingress QoS policy-map onto a member-link.

```
interface GigabitEthernet0/2/1
    no ip address
       negotiation auto
         service-policy input cos
         channel-group 1
```

Port-Channel Interface Level

The below example shows how to apply an ingress QoS policy-map onto a port-channel interface.

```
interface Port-channel1
no ip address
 negotiation auto
  service-policy input cos
  service instance 1 ethernet
   encapsulation dot1q 10
   rewrite ingress tag pop 1 symmetric
   bridge-domain 10
!
```

Port-Channel EVC Level

The below example shows how to apply an ingress QoS policy-map onto a port-channel EVC.

```
interface Port-channel1
no ip address
 negotiation auto
  service instance 1 ethernet
   encapsulation dot1q 10
   rewrite ingress tag pop 1 symmetric
   service-policy input cos
   bridge-domain 10
```

Egress Policy-Map

The below example shows how to configure an egress QoS policy-map

```
sh policy-map qos
  Policy Map qos
    Class qos-1
      Average Rate Traffic Shaping
      cir 1000000 (bps)
```

Member-Link Policy Map

The below example shows how to apply an egress QoS policy-map on a member-link.

```
interface GigabitEthernet0/2/1
          no ip address
           negotiation auto
            service-policy output qos
            channel-group 1
```

Support of Egress QoS on Ether Channel

The following are the different modes of egress QoS on ether channel:

- Aggregate QoS
- Replication on the member links by Actual values
- Replication on the member links by Division

Replication on the Member Links by Actual Values

Policy map is replicated on all the active member links. The QoS parameters are copied or replicated in actual values on the individual member links. For example, if the policy map has a class with shaper value 10 Mbps, each member link has 10Mbps shaper value for that class. This helps in easier management of the hardware support as QoS physical ports are supported on majority of the ASICs natively.

But, this mode has the following disadvantages:

- Match EFP or VLAN policies (subscriber aggregate) cannot be configured unless it is per EFP based hashing.
- Port Level aggregate policies cannot be configured as the traffic is distributed on the member links.
- EFP based policies cannot be configured unless it is per EFP based hashing.

Replication onto the member links by Division

In this mode, the QoS parameters are divided equally or are in proportion with the member bandwidth or speed. It has the same disadvantages as that of the "Replication on the Member Links by Actual Values" mode.

Aggregate QoS

In this mode, the QoS parameters are applied to the aggregated traffic on the ether channel.

This mode has the following disadvantages:

- The members span across different NPUs and ASICs.
- Aggregate QoS allows the traffic, but the hashing overloads one of the single member links and hence drops the traffic.

But, this mode has the following advantages:

- Port level aggregate policies can be configured.
- Match EFP or VLAN policies (subscriber aggregate) can be configured.
- EFP policies can be configured.

MPLS VPN QoS Mapping

Table below summarizes the default MPLS mappings for the Cisco ASR 903 Series Router.

Table 5: Default MPLS QoS Mapping

Feature	Imposition	Disposition
L3VPN, MPLS	IP Prec bit copied to MPLS Exp bit.	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.
L2VPN (EoMPLS, VPLS)	MPLS Exp bit is set to 0	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.
MPLS-TP		
CESoPN	MPLS Exp bit is set to 5	IP Prec bit is unchanged.
SAToP	MPLS Exp bit is set to 5	IP Prec bit is unchanged.

Feature	Imposition	Disposition
6VPE, 6PE	Prec bit value is copied to the MPLS Exp bit	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.

Note You can modify the default mapping behaviors using explicit marking policies.

QoS Policer and Shaper Calculation

Table below summarizes the packet accounting information used to make policer and shaper calculations on the Cisco ASR 903 Series Router.

Table 6: QoS Accounting Calculation

Feature	Direction	Traffic Type	Values Counted
Policing	Ingress	IPv4/L3VPN	L2 overhead, VLAN tag, CRC
Shaping	Egress	IPv4/L3VPN	L2 Ethernet overhead, VLAN tag, CRC, preamble, IPG
Policing	Egress	IPv4/L3VPN	Layer 2 Ethernet overhead, VLAN
Policing	Ingress	L2VPN	Layer 2 Ethernet overhead, VLAN tag, CRC
Shaping	Egress	L2VPN	Layer 2 Ethernet overhead, VLAN tag, CRC, preamble, IPG
Policing	Egress	L2VPN	Layer 3 payload (without CRC)

The following considerations also apply when understanding QoS policer and shaper calculations:

- Egress shaping is applied at layer 1.
- Ingress packet length accounting is performed at egress.
- Egress shaping and policing do not account for newly pushed VLAN tags and MPLS labels.
- If two policers are configured at egress, the statistics on the child PHB or PQ level are *not* displayed.

Service Groups

The Service Group feature (aggregate policing) introduced in Cisco IOS XE Release 3.11 allows you create service groups, add service instances to those service groups, and apply service policies to the newly created groups. The service policies contain the aggregate features such as traffic policing that can applied to the groups.

A service group can be configured with certain match conditions and police traffic can flow via multiple targets at PHB level, EFP level or multiple ports.

The following features are supported in Cisco IOS XE Release 3.11:

- Policing is only supported for service groups. Both Ingress and Egress policies are supported.
- Service groups are supported on EFPs and Trunk EFPs.
- Service groups are supported at both Ingress and Egress.
- A service group policy can be configured as hierarchical policy of user-defined classes.
- EFPs support both regular and service group policies.
- At Ingress, only two level policer is allowed on the service group policy.
- At Egress, only one level policer is allowed on the service group policy.

Restrictions for Service Groups

- Service groups is *not* supported on port and port-channels.
- Queuing and Marking on service group policy is *not* supported in Cisco IOS XE Release 3.11.
- Classification based on **match input vlan**, **match input interface**, and **match service instance** is *not* supported.
- Service group policies is **not** supported on EFPs configured on port channel.
- The same EFP *cannot* be configured as members of multiple service groups.
- If an EFP is a member of service group with a policy-map present in service group, the same policy-map *cannot* be applied on that EFP. The same policy-map applied on an EFP cannot be used in a service group.
- Limited support for statistics counters is provided.
- The **no policy-map** command cannot be executed for policies attached to service groups or to the policies attached to service instance which are configured as member of service groups.
- Policer percentage policy-maps are *not* supported on service groups.
- If dynamic modification is performed on the service-group policy or policy attached to EFP that is part of service-group, you have to exit of the policy-map sub-mode for the changes to take effect
- Service-group can have EFP members present across ports. If these ports are present across the ASIC in the router, then aggregate policing cannot work. For aggregate policing to work correctly, ports has to be present on same ASIC.

- QoS service groups for port channel sub-interface (BDI) is *not* supported.

Merging Service Groups and EFP Policies

- If an EFP is a member of a service group without any policy configuration, and a service group policy is configured, then the service group policy is internally attached to the EFP.
- If an EFP which is member of service-group has a policy configured, then the service-group policy and EFP policy are merged to form a new internal policy that is attached to the EFP.
- The **show policy-map interface** *interface_num* **service instance** *id* command displays the statistics for the policy configured on the service instance. This command output deviates when service groups are configured.
  - If the service instance is a member of a service group *without* a policy configured, it displays statistics for the service group policy.

Example

```
policy-map ex
class phb
police cir 50000000
class class-default
!
service-group 1
service-policy input ex
end
interface GigabitEthernet0/0/1
no ip address
negotiation auto
service instance 1 ethernet
encapsulation dot1q 100
group 1
bridge-domain 100
!
End
```

Router(config)# **show policy-map interface gigabitEthernet 0/0/1 service instance**

```
GigabitEthernet0/0/1: EFP 1
Service-policy input: ex
Class-map: phb (match-all)
2210042 packets, 3315063000 bytes
5 minute offered rate 82024000 bps, drop rate 77782000 bps
Match: cos 1
police:
cir 50000000 bps, bc 1562500 bytes
conformed 112980 packets, 169470000 bytes; actions:
transmit
exceeded 2097062 packets, 3145593000 bytes; actions:
drop
conformed 4191000 bps, exceeded 77782000 bps
Class-map: class-default (match-any)
```

```
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

- If the service instance is configured with a policy, it displays statistics for the merged policy.

Example

```
policy-map efpp
class efpc
set dscp 2
!
end
interface GigabitEthernet0/0/1
no ip address
negotiation auto
service instance 1 ethernet
encapsulation dot1q 100
group 1
service-policy input efpp
bridge-domain 100
!
End
```

Router(config)# **show policy-map interface gigabitEthernet 0/0/1 service instance**

```
GigabitEthernet0/0/1: EFP 1
Service-policy input: ex+efpp
Class-map: phb (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: cos 1
police:
cir 50000000 bps, bc 1562500 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps
Class-map: efpc (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: dscp 1
QoS Set
dscp 2
Marker statistics: Disabled
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

Restrictions for Merging Service Groups and EFP Policies

- If the physical port of a member EFP has a policy, the policy *cannot* be attached to a service group.

- If the physical port of a member EFP has an egress policy, attaching the egress policy on the service group or adding a member after attaching a policy is *not* supported on the service group.
- If EFP has rewrite push configured, the EFP *cannot* be a member to a service group with any policy configured.
- Internally created (merged) policies cannot be used for configuring of interfaces. Modifications to these policies is *not* supported.
- Policer actions with similar class names on both policies is *not* allowed.
- Conditional and non-conditional marking simultaneously in same class *not* allowed.
- Marking at more than one level is *not* supported.
- Only single level policer is supported at Egress.
- 3 level Ingress policer is *not* supported.
- Attach queuing-based child policy to a non-queuing based class is *not* supported.
- Match EXP and, match L4 port type is *not* supported in a single policy-map.
- The maximum number of PHB level classes *cannot* exceed 8 in an Egress policy.
- The following commands are not supported:
  - **show policymap interface** *interface_name* **service group** *service_group_id*
  - **show policy-map target service-group**
  - **show service-group traffic-stats**

Creating a Service Group

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **service-group** *service-group-identifier*

Example:

```
Device(config)# service-group 20
```

Creates a service group and enters service-group configuration mode.

- *service-group-identifier*—Service group number.

Step 4 **description** *descriptive-text*

Example:

```
Device(config-service-group)# description subscriber account number 105AB1
```

(Optional) Creates a description of the service group.

- *descriptive-text*— Additional information about the service group. Descriptions can be a maximum of 240 characters.

Step 5 **service-policy** (**input** | **output**) *policy-map-name*

Example:

```
Device(config-service-group)# service-policy input policy1
```

(Optional) Attaches a policy map to the service group, in either the ingress (input) or egress (output) direction.

- *policy-map-name*—previously created policy map.

Step 6 **end**

Example:

```
Device(config-service-group)# end
```

(Optional) Returns to privileged EXEC mode.

Adding Service Instance Members to the Service Group

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface gigabitethernet** *slot/subslot/port*

Example:

```
Device(config)# interface gigabitEthernet 0/1/5
```

Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:

- *slot/subslot/port*—The location of the interface.
  - *slot*—The chassis slot number where the interface module is installed.

    Note The interface module slot number is always 0.

  - *subslot*—The subslot where the interface module is installed. Interface module subslots are numbered from 0 to 5, from bottom to top.
  - *port*—The number of the individual interface port on an interface module.

Step 4 **service instance** *number* **ethernet** [*name*]

Example:

```
Device(config-if)# service instance 200 ethernet
```

Configure an EFP (service instance) and enter service instance configuration) mode.

- The number is the EFP identifier, an integer from 1 to 4000.
- (Optional) ethernet name is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.

Step 5 **group** *service-group-identifier*

Example:

```
Device(config-if-srv)# group 20
```

Creates a service group.

- *service-group-identifier*—Service group number.

Step 6 **exit**

Example:

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

(Optional) Returns to interface configuration mode.

Step 7 **end**

Example:

```
Device(config-if-srv)# end
```

(Optional) Returns to privileged EXEC mode.

Deleting a Service Group

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **no service-group** *service-group-identifier*

Example:

```
Device(config)# service-group 20
```

Deletes a service group and deletes all members from the service group.

- *service-group-identifier*—Service group number.

Note When you delete a service group, all members of the service group are automatically removed from the service group.

Step 4 **end**

Example:

```
Device(config)# end
```

(Optional) Returns to privileged EXEC mode.

Configuration Examples

- This example shows policing action on the service group:

```
policy-map qos-group-in
class cos1
police cir 64000
policy-map qos-group-out
class cos2
```

```
police cir 64000
policy-map qos-member-out1
class cos3
police cir 64000
policy-map qos-member-out2
class cos4
police cir 64000
```

- This example shows both Ingress and Egress policies supported on the service group:

```
service-group 1
service-policy in qos-group-in
service-policy out qos-group-out
int gigabitEthernet1/0/0
service instance 101 ethernet
group 1
service-policy out qos-member-out1
service instance 102 ethernet
group1
service-policy out qos-member-out2
int gigabitEthernet1/0/1
service instance 200 ethernet
group 1
service-policy out qos-member-out1
service instance 300 ethernet
service-policy out qos-member-out2
```

Verifying the Service Group

- Use the **show running-config service group** command to verify the service groups configuration:

  Router# **show running-config service-group 1**

```
Building configuration...
Current configuration:
service-group 1
service-policy input co1
end
```

- Use the **show platform software uea-qos service-group stats** command to verify the statistics of service groups:

  Router# **show platform software uea-qos service-group 1 stats**

```
Service Group 1
Service-policy input: co1
class-map: co1:
policy name co1, parent class , parent policy
conformed 54645 packets, 3497280 bytes
exceeded 3705853 packets, 237174592 bytes
violated 0 packets, 0 bytes
conformed 93000 bps, exceeded 6300000 bps
```

MPLS Diffserv Tunneling Modes Implementation

The MPLS specification defines three Diffserv operation modes:

- Uniform—There is only one DiffServ marking that is relevant for a packet when traversing the MPLS network.
- Pipe—The network uses two markings for traffic: the original marking value, which is used once the packets leave the MPLS network, and a separate marking value that is used while the traffic crosses intermediate nodes on the LSP span. The second marking value is dropped when traffic exits the MPLS network.
- Short-Pipe—the egress LSR uses the original packet marking instead of using the marking used by the intermediate LSRs.

The following sections describe how to implement these modes on the Cisco ASR 903 Series Router using QoS policies.

Implementing Uniform Mode

Use the following guidelines to implement uniform mode on the Cisco ASR 903 Series Router:

Imposition

To copy the diffserv value to the MPLS Exp bit, create a QoS configuration as follows:

- Option 1
  - Classify based on Prec bit or DSCP bit at ingress.
  - Set the qos-group.
  - Classify on qos-group.
  - Set the MPLS exp value.
- Option 2
  - Classify based on Prec bit or DSCP bit at ingress.
  - Set the mpls Exp bit at imposition.

Tag-to-tag Transfer

To ensure that outer tag values are copied to inner tags, explicitly mark the outer Exp value on the inner Exp bit.

Disposition

To copy the MPLS Exp bit to the diffserv/IP prec bit, create a QoS configuration as follows:

- Classify based on MPLS Exp bit on the ingress interface.
- Set the qos-group value.
- Classify based on qos-group on the egress interface.

- Mark the IP prec or DSCP bit.

Implementing Pipe Mode

Use the following guidelines to implement pipe mode on the Cisco ASR 903 Series Router:

Imposition

To set the MPLS Exp bit by policy, create a QoS configuration as follows:

- Option 1
  - Set the qos-group on the egress interface.
  - Classify based on qos-group on the egress interface.
  - Set the MPLS Exp value.
- Option 2
  - Apply the set mpls exp imposition command at ingress.

  Disposition

To preserve the original IP Prec or diffserv value so that egress queuing is based on MPLS exp value, create a QoS configuration as follows:

- Classify on MPLS Exp value on the ingress interface.
- Set the qos-group on the egress interface.
- Classify based on qos-group value on the egress interface.

Implementing Short-Pipe Mode

Use the following guidelines to implement short-pipe mode on the Cisco ASR 903 Series Router:

Disposition

To preserve the original IP Prec or diffserv value so that egress queuing is based on MPLS Prec or diffserv value, create a QoS configuration as follows:

- Classify based on IP prec or DSCP value on the egress interface.
- Mark the IP prec or DSCP bit.

Classification

Classifying network traffic allows you to organize packets into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic (used in conjunction with marking network traffic) is the foundation for enabling many quality of service (QoS) features on your network.

Table below summarizes the QoS Classification limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 7: QoS Classification Limitations

Match	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
Features	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
Match fragment control	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
access-group	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
all	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
any	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
class-map	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
cos	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
cos inner	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
destination address	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
destination ip	X	3.5	X	3.5	X	3.5	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
dscp (IPv4)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
dscp (IPv6)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
flow pdp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
fr de	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
fr dlci	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ip dscp	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1

Match	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
ip precedence (IPv4)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
ip precedence (IPv6)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
ip rtp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
mpls experimental topmost	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
not	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
packet-length	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
precedence (IPv4)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
precedence (IPv6)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
protocol	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
qos-group	X	3.5	X	3.5	X	3.5	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
service-instance ID	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
source address	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
vlan	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
vlan inner	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X

Ingress Classification Limitations

The following limitations apply to QoS classification on the router:

- If you configure egress classification for a class of traffic affected by an input policy-map, you must use the same classification criteria on the ingress and egress policy-maps.

Egress Classification Limitations

- Egress policy-map with police action is supported on port-channel interface(LAG).
- When applying a QoS policy to a link aggregation group (LAG) bundle, you must assign the policy to a physical link within the bundle; you cannot apply the policy to the LAG bundle or the port channel interface associated with the bundle.
- MPLS Pipe Mode Limitations—When you configure pipe mode for Time to Live (TTL), the router enables pipe mode for QoS as well. When pipe mode is enabled, you cannot enable egress classification based on the header on an egress interface. For example, you cannot classify based on egress DSCP value for MPLS IP packets when the router is in pipe mode.
- MPLS classification using EXP values in an egress policy are applied to normal IP packets in an MPLS core network. When Egress classification for EXP values are converted to equivalent IP precedence values, the first 5 bits in the DSCP values will be used to classify the MPLS packets. However, normal IP packets will be classified as well.

  It is recommended to move the EXP classification to ingress policy and egress classification to be moved to the QoS group set from ingress policy to avoid classification of normal IP packets.

Traffic Classifying on MLPPP Interfaces

Release 3.7(1) introduces support for egress QoS on MLPPP interfaces. The router supports the following **match** commands in a QoS class-map applied to an egress MLPPP interface.

- **match discard-class**
- **match dscp**
- **match precedence**
- **match qos-group**

The router supports the following **match** commands in a QoS class-map applied to a ingress MLPPP interface.

- **match access-group**
- **match dscp**
- **match precedence**

The Cisco router supports **service-policy input** *policy-name* command on the ingress and egress QoS interface.

Classifying Traffic using an Access Control List

You can classify inbound packet based on an IP standard or IP extended access control list (ACL). By default, TCAM optimization or expansion method is used. Both Security ACL and QoS ACL can be configured on the same interface. Follow these steps to classify traffic based on an ACL:

1. Create an access list using the **access-list** or ip **access-list** commands
2. Reference the ACL within a QoS class map using the **match access-group** configuration command
3. Attach the class map to a policy map

Limitations and Usage Guidelines

The following limitations and usage guidelines apply when classifying traffic using an ACL:

- QoS ACLs are supported only for IPv4 and IPv6 traffic
- IPv6 QoS ACLs are supported on the Cisco RSP1 Module starting from Release 3.16
- QoS ACLs are supported only for ingress traffic
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
  - TCP source and destination
  - UDP source and destination
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:
  - 1-99—IP standard access list
  - 100-199—IP extended access list
  - 1300-1999—IP standard access list (expanded range)
  - 2000-2699—IP extended access list (expanded range)
- You must create an ACL before referencing it within a QoS policy.
- Deny statements within an ACL are ignored for the purposes of classification.
- Classifying traffic based on TCP flags using an ACL is not supported.
- Classifying traffic using multiple mutually exclusive ACLs within a **match-all** class-map is not supported.
- Classifying traffic on a logical/physical level using an ACL is not supported.
- Applying QoS ACLs to MAC addresses is not supported.
- Port matching with the **neq** keyword is only supported for a single port.

- A given command can consume multiple matching operations if you specify a source and destination port, as shown in the following examples:
  - **permit tcp any lt 1000 any**—Uses one port matching operation
  - **permit tcp any lt 1000 any gt 2000**—Uses two port matching operations
  - **permit tcp any range 1000 2000 any 400 500**—Uses two port matching operations
- Only the following combination of matches are currently supported for Ingress policies:
  - Combination A: DSCP, Outer COS, UDP/TCP Source and Destination port number, IP SA/DA
  - Combination B: IP SA/DA, Outer COS, Inner COS, DSCP, MPLS EXP
  - Combination C: MAC DA, Outer COS, Inner COS, DSCP, MPLS Exp

Note Policy with match on L4 ACL and MPLS EXP together is currently not supported.

For more information about configuring QoS, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html. For more information about configuring access control lists, see the *Security Configuration Guide: Access Control Lists for Cisco NCS 4200 Series*.

Additional Classification Limitations

- The topmost policy-map in a three-level hierarchy only supports classification using class-default.

Configuring Multiple Match Statements

In IOS XE Release 3.5, the Cisco ASR 903 Series Router supported a single **match** or **match-any** command in a given QoS class-map, as shown in the following example:

Exampe for IOS XE 3.5 Class Map

```
class-map match-any my-restrict-class_00
   match ip prec

class-map match-any my-restrict-class_01
   match qos-group 2

class-map match-any my-restrict-class_03
```

match cos 3

IOS XE Release 3.6 introduces support for multiple **match** or **match-any** commands in a given QoS class-map, as shown in the following example:

Example for IOS XE 3.6 Class Map

```
class-map match-any my-class
```

```
match ip prec 1
match qos-group 2
match cos 3
```

The router treats the statements as a logical OR operation and classifies traffic that matches any **match** statement in the class map.

Traffic Classification Using Match EFP Service Instance Feature

Service Provider configurations have various service instances on the PE. QoS policy-maps are applied on these service instances or group of service instances. Cisco IOS XE Release 3.9S introduces the Match EFP Service Instance feature. The benefits of this feature are:

- Identify the various types of service-instances like EFP, Trunk EFPs
- Apply policies on these service instances at the port
- Manage bandwidth and priority across the service instances on the port and across classes within the service instance
- Apply policies on a group of transport service instances such as applying similar policies to a group of EFPs.

Restrictions for Configuring Match Service Instances

- Ethernet service instances configured under the interface can be classified in a class of a policy-map. The class can match on a group or set of match service instance statements.

```
class-map match-any policeServiceInstance
    match service instance ethernet  100
    match service instance ethernet 200
```

- Match service instance supported at both Ingress and Egress level.
- match service instance and match PHB per flows classification are defined at respective levels in the policy hierarchy under the port.
- The number of EFPs supported per group is 256. Only 256 match statements are supported per class.
- Match EFP policy-map can be configured only on the port and *not* under the service instance.

Example for Configuring Match Service Instances

```
interface GigabitEthernet0/3/4
 no ip address
 negotiation auto
 service-policy output BTS_Total
 service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance trunk 20 ethernet
  encapsulation dot1q 20-29
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
 service instance 30 ethernet
```

```
  encapsulation dot1q 30
  xconnect 192.44.32.21 101 encapsulation mpls


class-map match-any service-instance-group-with-BMG
match service instance ethernet 10
match service instance ethernet 20

class-map service-instance-30
match service instance ethernet 30

class-map service-instance-20
match service instance ethernet 20

class-map VOICE
match qos-group 0

class-map SIGNALING
match qos-group 1

class-map match-any DATA
match qos-group 2
match qos-group 4

policy-map child-X
class VOICE
priority level 1
police cir 20m
class SIGNALING
priority level 2
police cir 30m
class DATA
shape average 90m
random-detect cos-based


policy-map BTS_OUT_Bi
class service-instance-group-with-BMG
shape average 100m
service-policy child-X
class service-instance-30
shape average 200m
service-policy child-X

policy-map BTS_Total
class class-default
shape average 250m
service-policy BTS_OUT_Bi
```

QoS Marking

QoS marking allows you to set a desired value on network traffic to make it easy for core devices to classify the packet.

Table below summarizes the QoS Marking limitations for the Cisco ASR 903 Series Router. In the table, I represents Ingress and E represents Egress.

Table 8: Marking QoS Limitations

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
set	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
atm-clp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
cos	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
cos inner	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
discard-class	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.9	3.13	3.7.1
dscp	3.6	3.6	3.6	3.6	3.6	3.6	3.9	3.9	3.9	3.9	3.6	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.7.1
dscp-tunnel	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	X	X
ip dscp	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.7.1
ip precedence	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.7.1
mpls experimental																						
mpls experimental imposition	3.5	X	3.5	X	3.9	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.9	X	3.9	X

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
mpls experimental imposition qos-group	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
mpls experimental topmost	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.9
precedence	3.6	3.6	3.6	3.6	3.6	3.6	3.9	3.9	3.9	3.9	3.6	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.7.1
precedence transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	X	X
qos-group	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1	3.13

Overview of Marking

The Cisco ASR 903 Series Router supports the following parameters with the **set** command:

- **set cos**
- **set discard-class**
- **set dscp**
- **set precedence**
- **set ip dscp**
- **set ip precedence**
- **set mpls experimental imposition** (ingress marking)
- **set mpls experimental topmost**

- **set qos-group**

CoS Marking Limitations

The following limitations apply when configuring CoS marking:

- **set cos**—This set action has no effect unless there is a egress push action to add an additional header at egress. The COS value set by this action will be used in the newly added header as a result of the push rewrite. If there are no push rewrite on the packet, the new COS value will have no effect.
- The **set cos inner** command is not supported.

Ingress Marking Limitations

The following limitations apply to QoS marking on the router:

- The router does *not* support hierarchical marking.
- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.
- In the flow of the packet, if both ingress and egress markings are needed, you must classify the packet with the ingress marked phb class at egress and remark it to preserve the ingress marking. Marking in class-default of the ingress marked packets will not preserve the ingress markings.

Egress Marking Limitations

IOS XE Release 3.6 introduces support for egress marking. The following limitations apply when configuring marking on egress interfaces:

- The **set cos inner** command is not supported.
- The **set mpls experimental imposition** command is supported.
- The **set mpls experimental topmost** command is supported for marking MPLS Exp bits; other commands for marking MPLS Exp bits are not supported.

CoS Marking for Pseudowires

The Outer-CoS set in the transport VLAN of the MPLS PW packet, egressing the NNI based on the incoming CoS of the packet coming in on the UNI. With the existing support, a per-EFP or interface QoS policy is applied on the pseudowire originating on the cross-connect on the incoming UNI, to mark the MPLS EXP imposition using the per-EFP or interface policy. By supporting a default EXP to CoS mapping for all pseudowire (L2VPN), the traffic in the transport L2 ring gets the same priority as the ingress policy in the MPLS network.

- The default marking of COS from EXP imposition impacts all the pseudowires initiating from the router which are configured with EXP marking policy, that is, the policy to mark imposition EXP marks COS as well.
- Egress set cos using egress policy overwrites the S-COS.

- If the topmost EXP is changed through ingress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.
- If the topmost EXP is changed through egress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.
- The implicit mapping of this EXP to MPLS transport VLAN COS is *not*supported. This is applicable only for L2VPN traffic for which the EXP value is derived from the user configured policy.

Example

In the following configuration example, the SVI MPLS is configured between PE1 and P routers. MPLS in physical interfaces is configured between P and PE 2 routers. The EFP X-connect is configured on the Access side.

Topology

ixia---(g0/0/1)PE1(teng0/0/2)---(teng0/2)P(g0/7)---(g0/7)PE2(g0/1)---ixia

PE1 Router

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255

vlan 2
interface vlan2
no shut
ip address 20.0.0.1 255.255.255.0
mpls ip
mpls label protocol ldp

router ospf 10
network 1.1.1.1 0.0.0.0 area 0
network 20.0.0.1 0.0.0.0 area 0

policy-map ingress
class class-default
set mpls experimental imposition 4

interface GigabitEthernet 0/0/1
load-interval 30
media-type rj45
service-policy input ingress
service instance 2 ethernet
encapsulation dot1q 2
xconnect 2.2.2.2 10 encapsulation mpls

class-map match-all cos4
match cos 4

policy-map egress
class cos4

interface TenGigabitEthernet 0/0/2
load-interval 30
service-policy output egress
service instance 2 ethernet
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
bridge-domain2
```

Verifying PE 1 Router

```
show policy-map interface gig0/1 input GigabitEthernet 0/0/1

Service-policy input: ingress
Target association type: DEFAULT
Class-map: class-default (match-any)
2000 packets, 128000 bytes
30 second offered rate 4000 bps, drop rate 0000 bps
Match: any
set mpls exp imposition 4

show policy-map interface teng0/2 output TenGigabitEthernet 0/0/2
Service-policy output: egress
Target association type: DEFAULT
Class-map: cos4 (match-all)
2000 packets, 128000 bytes
30 second offered rate 4000 bps
Match: cos 4

Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
```

P router

```
class-map match-all cos4
match cos 4

policy-map ingress
class cos4

interface TenGigabitEthernet 0/2
load-interval 30
service-policy input ingress

interface Vlan2
ip address 20.0.0.2 255.255.255.0
mpls ip
mpls label protocol ldp

router ospf 10
network 20.0.0.2 0.0.0.0 area 0
network 30.0.0.2 0.0.0.0 area 0

class-map match-all exp4
match mpls experimental topmost 4

policy-map egress
class exp4

interface GigabitEthernet 0/7
ip address 30.0.0.2 255.255.255.0
media-type rj45
mpls ip
mpls label protocol ldp
service-policy output egress
```

Verifying P Router

```
Router# show policy-map interface teng0/2 input TenGigabitEthernet0/2

Service-policy input: ingress
Target association type: DEFAULT
Class-map: cos4 (match-all)
2000 packets, 188000 bytes
```

```
30 second offered rate 6000 bps
Match: cos 4
Class-map: class-default (match-any)
181 packets, 13992 bytes
30 second offered rate 1000 bps, drop rate 0000 bps
Match: any

Router# show policy-map interface gig0/1 output GigabitEthernet 0/7
Service-policy output: egress
Target association type: DEFAULT
Class-map: exp4 (match-all)
2000 packets, 144000 bytes
5 minute offered rate 0000 bps
Match: mpls experimental topmost 4
Class-map: class-default (match-any)
4 packets, 216 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

PE 2 Router

```
class-map match-all cos3
match cos 3

class-map match-all exp4
match mpls experimental topmost 4

policy-map ingress
class exp4

policy-map egress
class cos3

interface Loopback0
ip address 2.2.2.2 255.255.255.255

interface GigabitEthernet 0/7
no switchport
ip address 30.0.0.1 255.255.255.0
media-type rj45
mpls ip
mpls label protocol ldp
service-policy input ingress

router ospf 10
network 2.2.2.2 0.0.0.0 area 0
network 30.0.0.1 0.0.0.0 area 0

interface GigabitEthernet 0/1
load-interval 30
media-type rj45
service-policy output egress
service instance 2 ethernet
encapsulation dot1q 2
xconnect 1.1.1.1 10 encapsulation mpls
```

Verifying PE2 Route

```
show policy-map interface gig0/7 input GigabitEthernet 0/7

Service-policy input: ingress
Target association type: DEFAULT
Class-map: exp4 (match-all)
2000 packets, 172000 bytes
5 minute offered rate 0000 bps
```

```
Match: mpls experimental topmost 4
Class-map: class-default (match-any)
47 packets, 4222 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

show policy-map interface gig0/1 output GigabitEthernet0/0/1
Service-policy output: egress
Target association type: DEFAULT
Class-map: cos3 (match-all)
2000 packets, 128000 bytes
30 second offered rate 4000 bps
Match: cos 3
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
```

CoS Marking for CPU generated Traffic

You can use QoS marking to set or modify the cos values of traffic from the CPU. The QoS marking action can cause the cos packets to be rewritten . QoS uses packet markings to identify certain traffic types. The locally generated traffic is marked with a cos value based on the source IP address and Vlan ID.

Use the **platform qos-mark cos <1-7> vlanid <2-4094> ipaddress <IPADDR>** command to specify and mark CPU-generated traffic.

Limitation of CoS marking for CPU generated traffic

- Maximum of 8 configuration lines can be supported. Beyond that you need to delete any configuration and apply the new configuration
- The command can be used for classifying multiple IP addresses under a single VLAN ID.
- 8 qos entries will be reserved for use during bootup.
- DEI region for dropping the packet is first 8 entries and after that cos marking entries are programmed in the qos region of TCAM. If CoS marking entries are conflicting with the dei entries, then the packets will be dropped as dei entries have higher priority.
- The packets will go through the high priority queue of the interface
- For double tagged packets, only the outer CoS will be marked in case of ICMP echo reply packets.
- If other control protocols have the same IP and vlanId as is configured for the cos marking scenario, then those packets will also be marked. So you need to be aware of the IP address and VLAN ID while configuring cos marking.
- Initial TFTP/FTP packets can only be cos-marked having RRQ/WRQ with TFTP destination port.
- Use **platform acl drop-dei-1-packets** command to filter DOT1Q and DOT1AD packets marked with CFI/DEI bits. The feature only matches the outermost tag and the matching on the inner tag is not supported.

Supported Protocols

Following are the protocols supported on CoS Marking for CPU generated Traffic:

- Telnet
- SSH
- ICMP
- Syslog
- SNMP
- RADIUS/TACACS
- NTP
- FTP/TFTP
- OSPF, BFD

Configuration Example

The following example shows how to configure COS marking for CPU generated traffic:

```
interface GigabitEthernet0/4/4
mtu 9212
no ip address
carrier-delay msec 10
shutdown
negotiation auto
spanning-tree mst 0 cost 20000
service instance 1 ethernet
encapsulation untagged
l2protocol peer
bridge-domain 1

service instance 483 ethernet
encapsulation dot1q 4083
rewrite ingress tag pop 1 symmetric
bridge-domain 4083

interface BDI4083
ip address 172.24.244.37 255.255.255.224

platform qos-mark cos 5 vlanid 4083 ip address 172.24.244.37
```

Traffic Marking on MLPPP Interfaces

Release 3.7(1) introduces support for egress QoS on MLPPP interfaces. The Cisco ASR 903 Series Router supports the following parameters with the **set** command on egress MLPPP interfaces:

- **set ip dscp**
- **set ip precedence**

Release 3.13 introduces support for ingress QoS on MLPPP interfaces. The Cisco ASR 903 Series Router supports the following parameters with the **set** command on the ingress MLPPP interfaces:

- **set dscp**

- **set precedence**
- **set ip dscp**
- **set ip precedence**
- **set mpls exp imposition**
- **set mpls exp topmost**
- **set qos-group**
- **set discard-class**

IPv6 Traffic Marking

The Cisco ASR 903 supports the following commands for marking both IPv4 and IPv6 packets:

- **set dscp**
- **set precedence**

For more information about IPv6 QoS, see:

- http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-qos_xe.html
- http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-qos.html

Additional Marking Limitations

The following additional marking usage guidelines apply in Release 3.9:

- Release 3.9 introduces support for ingress MPLS Exp marking on pseudowire CEM and ATM interfaces, including SAToP, CESoPSN, ATM IMA, and ATMoMPLS.
- Marking is supported on Etherchannel interfaces and individual member links; however, you cannot configure marking on both interface levels at once.

CoS Marking for Local Traffic

The injected control packets that are generated from CPU, are marked to a specific CoS value for the list of supported protocols based on the user configuration. The remaining unsupported protocols carry CoS marking as per the existing platform behavior.

Note The following list of protocols is marked as COS-0 for packets that are generated from RSP2 devices, by default.

- The default marking value for NTP is 7.
- The default marking value for the other supported protocols is 0.

Following are the supported protocols:

- ARP
- ISIS
- SNMP
- NTP
- TELNET
- SSH
- TFTP
- Syslog
- FTP
- DNS
- TACACS
- ICMP

Example

The following example shows how to enable CoS marking on protocols.

platform cos-mark protocol *protocol* **cos-value** *cos-value*

```
platform cos-mark protocol snmp cos-value 7 mark
```

Note In CoS_mark double tagged packets, if the values remain same then the outer tag CoS value is also copied to inner tag. For the supported protocols, user configured CoS value is marked in outer tag and inner tag.

Limitations

Following are the CoS marking limitations for protocols:

- Marking a higher or lower CoS value does not modify egressing queuing decisions on the device where CoS marking is enabled. Locally generated packets exhibit default behavior of egressing on a high-priority queue or a low-priority queue. The CoS value is only marked again on a user configured packet.
- For control packets on a class-default queue, if the class-default has set action, then class-default marking overrides the configured protocol marking.

Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or class of service (CoS). This section describes the policing limitations and configuration guidelines for the Cisco ASR 903 Series Router.

The Cisco ASR 903 Series Router supports the following policing types:

- Single-rate policer with two color marker (1R2C) (color-blind mode)
- Two-rate policer with three color marker (2R3C) (color-blind mode)

Table below summarizes the QoS policing limitations for the Cisco ASR 903 Series Router. In the table, I represents Ingress and E represents Egress.

Policing QoS Limitations

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
Rate limiting																						
One rate	3.5	3.6	3.5	3.6	3.6	3.6	3.9	3.9	3.9	3.9	3.5	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
One rate and two rates	3.5	3.6	3.5	3.6	3.6	3.6	3.9	3.9	3.9	3.9	3.5	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
Two rates and three actions	3.5	X	3.5	X	3.6	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	X	X
Color Aware policing																						

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
Ingress																						
bandwidth	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
bandwidth remaining ratio	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
bandwidth percent	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
police (aggr)	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.9	X	3.7.1
police (only map)	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.9	X	3.7.1
police (only map class)	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.9	X	3.7.1
police (two rates)	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.9	X	3.7.1
priority	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.9	X	3.7.1
Set Actions																						
dscp	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	3.9	X	3.9	X	3.9	X	3.7.1
set-qos-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-cos-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
set-dscp-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-prec-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-dscp-class-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-mpls-experimental-topmost-transmit	3.5	3.6	3.5	3.6	3.5.1	3.6	3.9	3.9	3.9	3.9	3.5	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.9
set-mpls-experimental-imposition-transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
transmit	3.5	X	3.5	X	3.5.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	3.9	X	3.9	X	3.9	3.13	X

Supported Commands

The router supports the following policing commands on ingress interfaces:

- **police** (percent)—**police cir percent** *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **police** (policy map)—**police cir** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **police** (two rates)—**police cir** *cir* [**bc** *conform-burst*] [**pir** *pir*] [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

The router supports the following queuing commands:

- **bandwidth** (policy-map class)—bandwidth {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*} [**account** {**qinq** | **dot1q**} **aal5 subscriber-encapsulation**]
- **bandwidth remaining ratio**—**bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**] {*subscriber-encapsulation* | **user-define**d *offset*}]
- **police** (policy map)—**police cir** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **priority—priority** {**percent** *percentage*} [*burst*]
- **priority level 1/2—priority level 1/2** {**percent** *percentage*} [*burst*]

Several restrictions apply when using egress policing; see the *Egress policing Limitations* section for more information.

Note **police** (policy map) command on egress interface is not supported in Cisco RSP3 module.

Supported Actions

The Cisco ASR 903 Series Router supports the following policing actions on ingress interfaces:

- **transmit**
- **drop**
- **set-qos-transmit**
- **set-cos-transmit**
- **set-dscp-transmit**
- **set-prec-transmit**
- **set-discard-class-transmit**
- **set-mpls-experimental-topmost-transmit**
- **set-mpls-experimental-imposition-transmit**

Percentage Policing Configuration

The router calculates percentage policing rates based on the maximum port PIR rate. The PIR rate is determined as follows:

- Default—Port line rate
- Speed command applied—Operational rate
- Port shaping applied to port—Shaped rate

Ingress Policing Limitations

The following limitations apply to QoS policing on the Cisco ASR 903 Series Router:

- If you configure a policer rate or burst-size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.
- If you configure marking using the **set** command, you can only configure policing on that level using the transmit and drop command.
- If you configure a policer using a **set** command, you cannot use the **set** command at other levels of the hierarchical policy-map.

Egress Policing Limitations

The router supports the **bandwidth** and **bandwidth-remaining** commands on egress interfaces under the following conditions:

- Mixed bandwidth types are not supported in the same policy. For example, you cannot configure a policy containing both the **bandwidth remaining percent** command and **bandwidth remaining ratio** command.
- In egress, 1R2C means confirm-action transmit and exceed-action drop. By configuring exceed-action transmit on egress will drop those packets.
- The **bandwidth** and **bandwidth-remaining** commands are *not* supported in a class containing the **priority** command. The **bandwidth** and **bandwidth-remaining** commands must be configured on classes of the same level.
- If you want to create a configuration that uses the **bandwidth** or **bandwidth-remaining** commands and the priority command, you must include a **police** statement in the QoS class.

  The following is a sample supported configuration:

```
Router# show policy-map
  Policy Map PHB
    Class cos1
     police cir 200000 bc 8000
       conform-action transmit
       exceed-action drop
```

```
    priority
  Class cos2
    bandwidth 100
    bandwidth remaining percent 40
  Class cos3
    bandwidth 200
    bandwidth remaining percent 50
```

- The **priority** and **police** commands must be applied on a single class.

  The following is a sample supported configuration:

```
Router# show policy-map
  Policy Map PHB
    Class cos1
     police cir 200000 bc 8000
       conform-action transmit
       exceed-action drop
      priority
    Class cos2
      bandwidth 100
    Class cos3
      bandwidth 200
```

- Egress MLPPP interfaces support a single-rate policer with two color marker (1R2C) (color-blind mode) at the LLQ level.
- Egress port-level policing is supported with ingress EFP policy on the router.

  The following is a sample supported configuration:

```
Policy-map ingress_policy
  Class cos3
    Set cos 5
Policy-map egress policy
  Class cos5
    Shape average 30m

###Ingress
interface GigabitEthernet0/4/0
no ip address
negotiation auto
service instance 100 ethernet
  encapsulation dot1q 100
  service-policy input ingress_policy  >>>> Ingress policy in EFP
  bridge-domain 100

###Egress
interface GigabitEthernet0/4/0
no ip address
negotiation auto
service-policy output egress_policy   >>>>>Egress policy on Port
service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
```

- Release 3.7(1) introduces support for QoS features on egress policing on MLPPP interfaces using the **police** command. Egress MLPPP interfaces support a single-rate policer with two color marker (1R2C) (color-blind mode) at the LLQ level.
- **Police and Set in same policy class-map**

Effective 3.10 and later, **police** and **set** commands can be configured together in the egress policy class-map. In prior releases, a error message was displayed when both **police** and **set** commands were configured.

Sample example displaying the error message:

```
Router(config)#policy-map egress
Router(config-pmap)#class p1
Router(config-pmap-c)#police cir 200m
Router(config-pmap-c-police)#set prec 2
Qos:Configuration failed - Set and police not allowed in same class p1 of policy egress
QoS: Configuration failed. Invalid set
```

- **Egress Policing on Non Priority Queue**

  Starting Cisco IOS XE Release 3.6 and later, policing is supported at the egress on non priority queues.

Sample configuration:

```
Router#sh policy-map testp
  Policy Map testp
    Class cos1
      priority
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
    Class cos2
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
    Class cos4
     police cir 50000000 bc 1562500
       conform-action transmit
       exceed-action drop
```

Traffic Policing on MLPPP Interfaces

1R2C color-blind policer is supported for egress QoS on MLPPP interfaces.

The router supports the following parameters with the **set** command on the ingress MLPPP interfaces:

- **set dscp transmit**
- **set prec transmit**
- **set mpls exp imposition transmit**
- **set mpls exp topmost transmit**
- **set qos transmit**
- **set discard-class transmit**

1R2C color-blind policer and 2R3C color-blind policer is supported for ingress QoS on MLPPP interfaces.

Traffic Shaping

Traffic shaping allows you to control the speed of traffic that is leaving an interface in order to match the flow of traffic to the speed of the receiving interface. Percentage-based policing allows you to configure traffic shaping based on a percentage of the available bandwidth of an interface.Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

This section describes the shaping limitations and configuration guidelines for the Cisco ASR 903 Series Router.

Table below summarizes the QoS shaping limitations for the Cisco ASR 903 Series Router.; an X indicates support.

Table 9: Shaping Limitations by Interface

	GigE		10 GigE		EFP		Trunk EFP		Port Channel		Member Link		OC-3		OC-12		T1/E1		Serial		MLPPP		ACL	
	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
Ide																								
Cla Pa																								
Di bu																								
Fra																								
Co																								
Sh		X		X																				
ad																								
av		X				X		X			X											X		
fra ad		X				X		X			X													
ma bu		X				X		X			X													
pa		X				X		X			X													

Additional Shaping Limitations

The following additional shaping usage guidelines apply in Release 3.9:

- Policies using shaping are supported only on individual member links of an etherchannel. Applying a shaping policy directly on an etherchannel interface is not supported.
- Class-based shaping is supported at all levels.

Configuring Egress Shaping on EFP Interfaces

Configuring an EFP port shaper allows you to shape all EFPs on a port using a port policy with a class-default shaper configuration, as in the following partial sample configuration:

```
policy-map port-policy
  class class-default
    shape average percent 50
policy-map efp-policy
  class class-default
    shape average percent 25
    service-policy child-policy
policy-map child-policy
  class phb-class
    <class-map actions>
```

The following configuration guidelines apply when configuring an EFP port shaping policy:

- When the configuration specifies a shaper rate using a percentage, the router calculates the value based on the operational speed of a port. The operational speed of a port can be the line rate of the port or the speed specified by the **speed** command.
- The rates for **bandwidth percent** and **police percent** commands configured under a port-shaper are based on the absolute rate of the port-shaper policy.
- You can combine a port shaper policy (a flat shaper policy with no user-defined classes) with an egress EFP QoS shaping policy.
- Configure the port shaper policy before configuring other egress QoS policies on EFP interfaces; when removing EFP QoS configurations, remove other egress EFP QoS policies before removing the port shaper policy.

Congestion Management

Congestion management features allow you to control congestion by determining the order in which packets are sent out an interface based on priorities assigned to those packets. Congestion management entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

This section describes the classification limitations and configuration guidelines for the Cisco ASR 903 Series Router.

Table below summarizes the QoS congestion management and queuing limitations for the Cisco ASR 903 Series Router. In the table, I represents Ingress and E represents Egress.

Table 10: Congestion Management QoS Limitations

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
CBWFQ	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.8	X	3.9	X	3.9	X	3.7.1
CBWFQ																						
IP RTP priority	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Frame Relay IP RTP	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Frame Relay PVC Interface Priority Queueing	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ILQ	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.8	X	3.9	X	3.9	X	3.7.1
IBQ																						
IQR																						
Generic queueing																						
Priority Queueing																						
Shaping																						
Bandwidth (kbps)	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
Bandwidth percent	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
[illegible]	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
[illegible]	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
[illegible]	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
[illegible]																						
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
[illegible]	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
[illegible]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Ingress Queuing Limitations

The router does not support queuing on ingress interfaces.

Egress Queuing Limitations

The Cisco ASR 903 Series Router supports tail drop queuing on egress interfaces using the **queue-limit** command. The following limitations apply to egress queuing:

- If you configure a queue size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- Egress policy-map with queuing action is *not* supported on port-channel interface(LAG). The policy must be applied to the policy-maps on the member links.
- Release 3.8 extends the maximum **bytes** value of the **queue-limit** *number-of-packets* [*bytes* | *ms* | *packets*] command. The previous maximum value was 491520 bytes; the new value is 2 MB.
- Release 3.8 enhances the **show policy-map interface** command to display the default queue-limit.
- Release 3.8 introduces support for the **queue-limit** *percent* command.

Support for Queuing Features on MLPPP Interfaces

Release 3.7(1) introduces support for QoS features on egress MLPPP interfaces. The following queuing features are supported on egress MLPPP interfaces:

- Tail drop queuing uses the **queue-limit** command.
- Hierarchical QoS (2 level) is supported on MLPPP.
- 3-level policies are *not* supported on MLPPP interfaces.

Support for Low Latency Queuing on Multiple EFPs

IOS XE 3.6 Release for the Cisco ASR 903 router introduces support for QoS policies that allow for low-latency queuing (LLQ) across multiple EFPs. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-ehqos-pshape.html.

Additional Queuing Limitations

The following additional queuing usage guidelines apply in Release 3.9:

- The Cisco ASR 903 router supports QoS policies that allow for low-latency queuing (LLQ) across multiple EFPs. For more information about this feature, see http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-ehqos-pshape.html.
- CBWFQ is supported on 2nd and 3rd level classes.

Congestion Avoidance

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS QoS includes an implementation of RED that, when configured, controls when the router drops packets. If you do not configure Weighted Random Early Detection (WRED), the router uses the cruder default packet drop mechanism called tail drop.

Table below summarizes the QoS congestion avoidance limitations for the Cisco ASR 903 Series Router. In the table, I represents Ingress and E represents Egress.

Table 11: Congestion Avoidance QoS Limitations

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
Tail Drop (default)																						
RED	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
auto-detect	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
WRED	not supported on ingress ifcs																					
auto-detect default-class																						
auto-detect default-class-based	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
auto-detect exponential-weighting-constant	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
fair-queue	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
precedence																						
auto-detect cos-based	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
auto-detect dscp-based	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
auto-detect precedence based	X	3.6	X	3.6	X	3.6	X	X	X	X	X	3.6	X	3.9	X	3.9	X	3.9	X	3.9	X	3.7.1
shape																						
WRED																						
Hw-based WRED																						
Dist WRED																						

Congestion Avoidance Configuration

The following sections describe the supported congestion avoidance features on the router:

Supported Commands

The router supports the following commands for WRED:

- **random-detect cos-based**—Outer CoS
- **random-detect discard-class-based**— Outerr CoS
- **random-detect dscp-based**— IPv4 DSCP
- **random-detect precedence-based**— IPv4 Precedence bit

Supported Interfaces

WRED is supported at the PHB level but not on logical or physical interfaces. You can apply WRED policies on the following interface types:

- Main Layer 3 interface
- Port-channel Layer 3 member-links
- Service instances
- Trunk EFPs

Verifying the Configuration

You can use the **show policy-map interface** command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see the following documents:

- *QoS: Congestion Avoidance Configuration Guide for Cisco NCS 4200 Series*

Ingress Congestion Avoidance Limitations

WRED is not supported on ingress interfaces.

Egress Congestion Avoidance Limitations

The following limitations apply when configuring congestion avoidance on the Cisco ASR 903 Series Router:

- Queuing feature to support WRED in a class such as shape or bandwidth are supported.
- You must apply WRED within a policy map.
- WRED is only supported on egress interfaces.
- WRED is *not* supported in priority queues.
- WRED is supported in the class-default class if there are no other user-defined classes in the policy-map.
- You can configure a maximum of 2 WRED curves per class.
- Fair-queue is *not* supported. You can configure WRED with either the **shape** or the **fair-queue** (CBWFQ) commands.

- The default value for **exponential-weighting-constant** is 9.
- The default value for **mark-probability** is 10.
- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.

Egress Congestion Avoidance on MLPPP Interfaces

Release 3.7(1) introduces support for the following egress congestion features on MLPPP interfaces:

- RED queuing using the **random-detect** command
- WRED queuing using the **random-detect** command. You can apply WRED to:
  - DSCP
  - Precedence
  - Discard-class

MLPPP egress queuing is supported only on the 3rd level classes (bottom-most).

- Class-based Weighted Fair Queuing (CBWFQ) using the **bandwidth** and **bandwidth percent** commands. CBWFQ is supported on 2nd and 3rd level classes.
- Class-based Shaping using the **shape average** and **shape average percent** commands. Class-based shaping is supported at all levels.
- Class-based excess bandwidth scheduling using the **bandwidth remaining percent** and **bandwidth remaining ratio** commands. Class-based excess bandwidth scheduling is supported on 2nd and 3rd level QoS classes.

Additional Congestion Avoidance Limitations

- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.
- Policies using Class-based Weighted Fair Queuing (CBWFQ) and WRED are supported only on individual member links of an etherchannel. Applying a CBWFQ policy directly on an etherchannel interface is not supported.
- Aggregate-WRED is *not* supported. However, multiple random-detect statements with the same curve are supported in the same class.

Verifying the Configuration

You can use the **show policy-map interface** command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see *QoS: Congestion Avoidance Configuration Guide*.

Scheduling

This section describes the scheduling limitations and configuration guidelines for the router.

Ingress Scheduling Limitations

The router does not support scheduling on ingress interfaces.

Egress Scheduling Limitations

- If you configure a CIR, PIR, or EIR rate that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- You can only configure one **priority** value on each parent class applied to a QoS class or logical interface.
- You can only configure priority on one class in a QoS policy.
- You can not configure **priority** value and a policer in the same class.

The following limitations apply when configuring a 3-level scheduling policy on an egress interface configured as an EFP:

- Only two of the three levels can contain scheduling actions such as **bandwidth**, **shape**, or **priority**.
- Class-based excess bandwidth scheduling is supported on 2nd and 3rd level QoS classes.
- One of the levels containing scheduling actions must be the class (bottom) level.

Egress Scheduling on MLPPP Interfaces

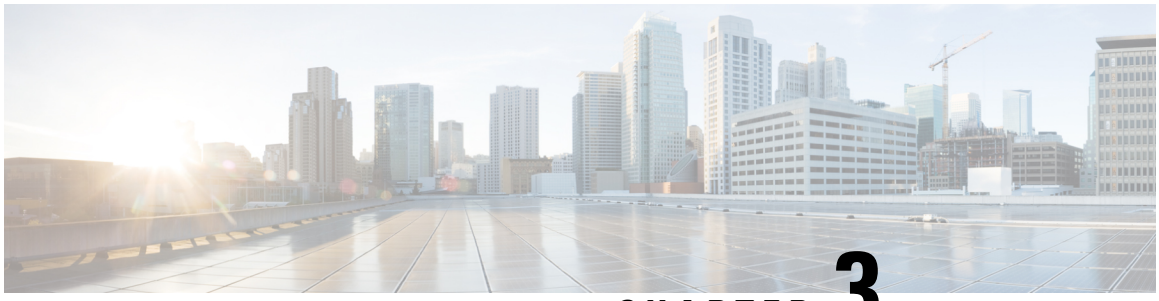
Release 3.7(1) introduces support for QoS features on egress MLPPP interfaces including scheduling. The following scheduling features are supported:

- Strict priority using the **priority** command; strict priority is supported on 2nd and 3rd level classes.
- Multi-level priority using the **priority level** command. You can configure two priority levels; the feature is supported on 3rd level classes. The following is the sample configuration of multi-level priority.

```
policy-map eg_pri_queuing
class eg_mul1_prec1
  set precedence 6
  priority level 1 percent 20
class eg_mul1_prec2
  set precedence 5
  priority level 2 percent 18
class eg_mul1_prec3
  set precedence 4
  shape average 4000000
class class-default
  set precedence 3
  shape average 2000000
!
```

The following limitations apply when configuring a 3-level scheduling policy on an egress interface configured as an EFP:

- Only two of the three levels can contain scheduling actions such as **bandwidth**, **shape**, or **priority**.
- QoS policies using the **priority** command are supported only on individual member links.
- MLPPP is *not* supported on port-channel (etherchannel).



CHAPTER 3

Quality of Service Configuration Guidelines for RSP3 Module

This document outlines Quality of Service features and limitations available on the Cisco RSP3 module and contains the following sections:

Quality of Service

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Ethernet and 802.1 networks, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by implementing the following services:

- Supporting guaranteed bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

Quality of Service Configuration

This document provides details on the platform-dependent implementation of QoS on the router.

QoS Support Overview

Table below provides an overview of QoS feature support on the router. For more detail about the support for each feature, see *Global QoS Limitations* section.

Table 12: QoS Feature Overview

Feature	Main	Service Instance	Trunk EFP	Member Link	Port Channel Interface
Dynamic policy modification	3.16	3.16	3.16	3.18	3.18 SP and later
EFP QoS Support	3.16	3.16	3.16	Not supported in 3.18	3.18 SP and later
Classification					
Ingress	3.16	3.16	3.16	3.18	3.18 SP and later
Egress	3.16	3.16	3.16	3.18	3.18 SP and later
Match any	3.16	3.16	3.16	3.18	3.18 SP and later
Marking					
Ingress	3.16	3.16	3.16	3.18	3.18 SP and later
Egress	3.16	3.16	3.16	Not supported in 3.18	3.18 SP and later

Feature	Main	Service Instance	Trunk EFP	Member Link	Port Channel Interface
Policing					
Ingress	3.16	3.16	3.16	3.18	3.18 SP and later
Shaping					
Port Shaping	3.16	3.16	3.16	3.18	3.18 SP and later
Congestion Avoidance					
WRED	3.16	3.16	3.16	3.18	3.18 SP and later
Multiple Priority Queues	3.16	3.16	3.16	3.18	3.18 SP and later
Congestion Management					
Strict Priority	3.16	3.16	3.16	3.18	3.18 SP and later
Scheduling					
Egress	3.16	3.16	3.16	3.18	3.18 SP and later
QoS ACLs					
Ingress	3.16	3.16	3.16	3.18	3.18 SP and later

Cisco RSP3 Module QoS Capabilities

- RSP3 module has 4 GB external packet buffers per NPU.
- RSP3 module supports 48000 queues.
- By default, RSP3 module supports upto 1 MB queue-limit per queue.
- Queue limit percentage is considered out of 1 GB of the total buffers.
- Usage of Traffic Classes (TC) in RSP3 module:
  - TC is used to map packets into appropriate queue (Priority, default and so on).
  - TC can be used to remark packet on egress interface.
  - Upto 8 TCs are supported on RSP3 module.
  - Based on packet forwarding type, NPU picks specific PHB from a packet.
- Default mapping of traffic classes:

Table 13: Default Mapping of Packet Fields to Traffic Classes

Flow Type	From	To
Layer2 Flow	COS Bits (0-7)	TC (0-7)
Layer3 (L3/BDI) Flow	IP PREC (0-7)	TC (0-7)
MPLS Flow	EXP (0-7)	TC (0-7)

Table 14: Default Queue priority for respective Traffic Classes

Traffic Class	Default Priority
TC0 – TC6	Fair Queue
TC7	Strict Priority

Note Effective Cisco IOS XE Everest 16.6.1, the inner DSCP preservation is supported.

TCAM Scale Support for Ingress QoS

Starting with Cisco IOS XE Fuji 16.7.1 release, the TCAM scale increases to 2048 TCAM entries per NPU for the ingress QoS policy maps. The TCAM resources are shared between multiple features, and if one feature increases the scale limit, then the other features might not be able to scale up.

For example, the QoS, IPv4 ACL, and IPv6 multicast features share the common TCAM resources. When you increase the scale limit for QoS, then the other two features might not be able to scale upto the supported numbers.

The supported TCAM scale limit for IPv4 ACL is 1000 and IPv6 multicast is 2000 TCAM entries. These supported scale numbers cannot be achieved with the QoS TCAM scale of 2048.

The following **show platform hardware pp active feature qos resource-summary** command displays the increased scale support for QoS:

```
router#show platform hardware pp active feature qos resource-summary 0
RSP3 QoS Resource Summary

Type Total Used Free
------------------------------------------------------------------------------
QoS TCAM 2048 0 2048
VOQs 49152 816 48336
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
```

```
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768


router#show platform hardware pp active feature qos resource-summary 1
RSP3 QoS Resource Summary

Type Total Used Free
--------------------------------------------------------------------------------
QoS TCAM 2048 0 2048
VOQs 49152 816 48336
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
```

Cisco RSP3 Module Marking Capabilities

- Time to Live (TTL) value does not decrement on the imposition node in IP to MPLS LABEL case with L3VPN Conditional Marking.
- By default, tunnel mode in RSP3 module is in Uniform mode.
- For MPLS L3VPN:
  1. PREC/DSCP values are automatically copied to the EXP bit on imposition.
  2. EXP topmost values are automatically copied to PREC/DSCP bits on disposition.
  3. For marking MPLS EXP, **set mpls exp imposition** on imposition and **set mpls exp topmost** on swap cases.
- For MPLS L2VPN:
  1. COS values are automatically copied to the EXP bit on imposition.
  2. EXP topmost values are automatically copied to COS bits on disposition.
  3. For marking MPLS EXP, **set qos-group** on imposition and **set mpls exp topmost** on swap cases.

Note Starting from:

- Cisco IOS XE Everest 16.7.1 and later, conditional marking is supported in Pipe mode.
- Cisco IOS XE Fuji 16.8.x and later, conditional marking for L2VPN is supported on BDI.

Configuring Short-Pipe Mode on QoS

Short-pipe mode on QoS RSP3 module can be activated using an SDM template. You can identify the egress traffic on an interface or EVC and classify based on DSCP, mark qos-group, and color using the platform

table-map command. You can perform WFQ/WRED based on qos-group and color on egress interface using egress policy-map.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **sdm prefer enable_egr_l3vpn_cm**

Example:

```
Device(config)# sdm prefer enable_egr_l3vpn_cm
```

Enables the SDM template.

Step 4 **platform qos-table-map**

Example:

```
Device(config-table-map)# platform qos-table-map Customer#6
    from dscp 10 to qos-group 0 discard-class 0
    from dscp 63 to qos-group 0 discard-class 1

    qos-table-map Customer#6 interface GigabitEthernet0/4/0
```

Creates platform table-map and applying it on an interface.

Step 5 **Class-map match-any qos0**

Example:

```
Device(config-table-map)# Class-map match-any qos0
    match qos-group 0
Policy-map short-pipe-qos
    class qos0
        bandwidth 30000
        random-detect discard-class-based
        random-detect discard-class 0 25000 bytes 75000 bytes 1
        random-detect discard-class 1 95000 bytes 300000 bytes 1
        queue-limit 375000 bytes
```

Creates egress class map and policy map.

Example

Configuration Example

```
sdm prefer enable_egr_l3vpn_cm

platform qos-table-map Customer#6
    from dscp 10 to qos-group 0 discard-class 0
    from dscp 63 to qos-group 0 discard-class 1

qos-table-map Customer#6 interface GigabitEthernet0/4/0

interface Gig 0/5/0
    service-policy output short-pipe-qos

Class-map match-any qos0
    match qos-group 0

Policy-map short-pipe-qos
    class qos0
        bandwidth 30000
        random-detect discard-class-based
        random-detect discard-class 0 25000 bytes 75000 bytes 1
        random-detect discard-class 1 95000 bytes 300000 bytes 1
        queue-limit 375000 bytes
```

Restrictions on Short-Pipe Mode

- The **enable_egr_l3vpn_cm** SDM template command cannot co-exist with other templates such as **sdm prefer enable_copp** and **sdm prefer enable_match_inner_dscp** commands.
- Short-pipe mode on QoS RSP3 module is applicable only for conditional marking, which is not supported for multicast L3VPN traffic flows (TAG to IP).
- Short-pipe mode on QoS RSP3 module is not applicable for IPv6 traffic.
- You can configure only up to 7 table-maps.
- Following QoS classifications does not work after you enable the **sdm template** to activate short-pipe mode QoS feature:
    - DstMac
    - InnerVlanPri
    - InnerVlan
    - SrcIp
    - DstIp
- Before deleting the corresponding BDI interface, ensure to detach or unconfigure the table-map, if the table-map is applied on the BDI interface.
- Each table-map entry (classify on DSCP, mark to Qos-Group and DC) consumes up to 3 TCAM entries.
- Egress table-map matched traffic does not hit core interface policy-map.
- Core interface policy-map stats do not count egress table-map hit packets.

- Platform table-map stats are not supported.
- All backup paths (LB/FRR case) should be mapped with same table-map profile.

Global QoS Limitations

The following limitations apply to multiple QoS features for the router:

- Ingress policer rate does not display the configured value when member links of a port channel are configured from different ASIC boards.
- 16K QoS policers are supported per ASIC on the RSP3 module, hence 32K policers are supported per chassis (dual ASIC board).
- Both ingress MAC (L2) ACL and ingress QoS policy map are not supported on the same EFP.
- The configurable committed burst (bc) value, under the QoS policy-map must only be between 8000 and 4161500 bytes in RSP3 module.
- RSP3 module supports 2 discard-class based WRED profiles per class.
- IPv6 QoS is *not* supported on port channel and port channel member links on the RSP3 module.
- With L3VPN, Ingress QoS match on DSCP or PREC and set EXP marking, overwrites the DSCP value with EXP at imposition resulting in loss of the DSCP value.
- When EVCs under a physical interface have a QoS policy attached, the following limitations apply:
  - The port-level policy is limited to the class-default class.
  - Only the **shape** command is supported in the port-level policy.
- The router supports up to 64 unique QoS classification service instances in a given bridge domain. QoS service instances refer to ports, VLAN classes (for ingress), EFPs associated with a QoS classification policy.
- Modification of class-map definitions while applied to an interface or Ethernet Flow Point is *not* supported.
- Policy validation—Some QoS policy configurations are not validated until you apply the policy-map to an interface or Ethernet Flow Point. If a QoS configuration is invalid, the router rejects the configuration when you apply it to an interface. In some cases, a QoS configuration may be rejected due to hardware resource exhaustion or limitations. If you receive such an error message, detach the policy and adjust your QoS configuration.
- The **match-all** keyword is supported only for QinQ classification. The following matches are allowed in a match class-map.
  - Vlan and vlan-inner classification
  - Cos and cos-inner classification
- Only one **match access-group** match is supported on the same class-map.
- COS to PREC marking does not work for L2 flows.
- PREC to COS marking does not work on L3 flows.

- VLAN classification policy is not supported on EFP with cross connect configured.
- Match VLAN egress classification is not supported.
- Egress policy-map can have match QoS-group.
- Egress policing is not supported.
- Egress queuing is supported.
- CPU generated traffic is not subjected to QoS on the egress interface. So, no QoS policy is required to treat CPU generated traffic on the egress interface.
- QoS does not account for CRC values on an interface and assumes that the value is 2 bytes. CRC differences can cause accuracy issues for 2 to 3 percent of the traffic.
- QoS does not support WRED counters for all the match conditions.
- Match on DSCP classification or policing or QoS group marking is *not* supported for IPv6 traffic on the disposition node when MPLS is configured for both per-prefix and per-VRF modes.
- When the ingress interface has both the MPLS tunnel terminated packets and transit tunnel packets, and the ingress policy is applied on the interface for exp marking, then the DSCP value is not preserved for tunnel terminated packets.
- Queuing support at physical, logical, and queue levels:
  - Queuing action supported at physical level: Shaper
  - Queuing action supported at logical level: Shaper
  - Queuing action supported at queue level: Bandwidth, Shaper, WRED, Queue Limit
- Traffic drops are observed for minimum-sized MPLS pseudowire packets.
- RSP3 does not support policy-based routing.
- Match Inner DSCP feature is supported only on the L3 interface and not on the Bridge Domain Interface.
- The **hw-module subslot** *0/<bay>* **default** command for interface module or **default interface** *<ethernet_interface_type> <0/bay/port>* command for interface to remove the QoS overhead accounting configuration from a particular interface module or interface at a global configuration level, does not remove the QoS overhead accounting configuration set. To disable the QoS overhead accounting configuration from a particular interface, enter the **no** form of the **qos-overhead-accounting** command manually.
- DSCP bits are not retained for Multicast traffic at the disposition node in uniform mode.
- Starting with Cisco IOS-XE Release 16.6.1, multi active port-channel templates are used to apply a QoS policy for a port-channel interface.

Difference in WRED Behavior

As WRED is enforced at the VoQs, it is independently enforced on each ingress ASIC, when the ingress traffic is from interfaces belonging to different ASICs. This results in per ASIC VoQ build up and drop decision. The drops may be fair as long as the ingress traffic rate is similar across different ASICs.

This behavior is also applicable, if multiple filters exist in the egress policy-map class.

QoS Features Using MQC Limitations

Table below lists the QoS MQC scaling limitations on router per release.

Table 15: Qos on MQC Limitations

Supported on Router	Cisco IOS XE 3.16
No. of unique policy-maps	1024
No. of unique class-maps	4096
No. of classes per policy-map	512
No. of filters per class-map	16

[3] For releases which are not listed, refer to the most recent previous release limit.

Restrictions for Ingress QoS

- QoS ACL inbound policy-map is only supported.
- QoS ACLs based to classification are not supported for:
  - TCP source and destination
  - UDP source and destination
- Apply QoS ACL only to the third level class (bottom-most). This means that you cannot configure ACL classifications in a parent class.
- Deny statements within ACL are ignored for the purpose of classification.
- Classifying traffic using multiple mutually exclusive ACLs within a match-all class-map is not supported.
- MAC-based QoS ACLs are supported on destination MAC ACLs only.
- Match EFP policy is not supported on member-links.
- Match VLAN policy is not supported on member-links.
- Ingres COS marking is not supported when the service-instance is configured with encapsulation “untagged” and rewrite rule is “rewrite ingress tag push dot1g <*vlan*> symmetric.

The following restrictions apply to the Cisco IOS XE Everest 16.5.1 release:

- IPv6 QoS is not supported on port channel and member-link.
- In case of multi-match policy IPv6 traffic is not classified to any class, that is, QoS is not supported for IPv6 traffic.

- By default, set of eight DSCP values are mapped to one traffic class.
- Switched Layer 2 packets with IPv6 payload are not subjected to DSCP based QoS at the ingress.
- IPv6 QoS ACL is not supported.
- Match-VLAN is not supported for routed IPv6 streams.
- If set dscp policy is applied, all other DSCPs belonging to the traffic class which are being matched get classified, but set-dscp action only works for the DSCP which is being matched.

Restrictions for Egress QoS

- The maximum number of PHB classes supported on the policy map is 8, which includes one class class-default; 7 user-defined classes and class class-default is supported.
- Match EFP policy is not supported on member-links.

8K EFP (4 Queue Model)

In Cisco IOS XE Release 3.18SP, the 8K EFP (4 Queue Model) support allows up to 8000 EFPs at the system level. EFP scale implementation follows the static model, that is, eight queues are created per EFP by default.

Information About 8000 (8K) EFP

- In default model, 5000 EFPs can be configured on Cisco ASR 903 RSP3 module.
- The Switch Database Management (SDM) template feature can be used to configure 8000 EFPs across ASIC(4000 EFPs per ASIC interfaces).
- In 8K EFP model, each EFP consumes four Egress queues. If 8K EFP SDM template is not enabled, each EFP consumes eight Egress queues.
- Ingress policy map can specify more than eight traffic classes based on PHB matches, which remains the same. However, Egress policy map can have three user defined class and class-default class.
- Each Egress class-maps can be mapped to a single or multiple traffic classes and each class-map mapped to a single queue.
- Maximum of two queues are set to Priority according to policy configuration.
- All the existing QOS restrictions that apply in default model are also applicable to 8K EFP model.

Prerequisites for 8000 (8K) EFP

- Activate the Metro Aggregation Services license on the device.
- To configure 8000 EFPs, enable the SDM template using CLI **sdm prefer enable_8k_efp**.
- Reset the SDM template using the CLI **sdm prefer disable_8k_efp** .

Restrictions for 8000 (8K) EFP

- Traffic class to Queue mapping is done per interface and not per EVC.
- Four traffic classes including class-default can be supported in Egress policy.
- Same three traffic classes or subset of three traffic classes match is supported on EVCs of an interface.
- Traffic classes to queue mapping profiles are limited to four in global, hence excluding class-default, only three mode unique combinations can be supported across interfaces.
- TRTCM always operates with conform-action transmit, exceed-action transmit and violate-action drop.
- By default, 1R2C Policer will behave as 1R3C Policer in 4 Queue model.
- All the QOS restrictions that is applicable in default mode is also applicable in 8k EFP mode

Configuring 8K Model

Configuring 8K EFP Template

Below is the sample configuration to enable 8K EFP or 4 Queue mode template. On enabling **sdm prefer enable_8k_efp**, the router reloads and boots up with 8K EFP template.

```
RSP3-903(config)#sdm prefer enable_8k_efp

Template configuration has been modified. Save config and Reload? [yes/no]: yes
Building configuration...

Jul 22 05:58:30.774 IST: Changes to the EFP template preferences have been stored[OK]
Proceeding with system reload...
Reload scheduled for 06:00:38 IST Fri Jul 22 2016 (in 2 minutes) by console
Reload reason: EFP template change
```

Verifying 8K EFP Template

You can verify the current template as below.

```
Device#sh sdm prefer current

The current sdm template is "default" template and efp template is "enable_8k_efp" template
```

Configuring QOS in 8K EFP Model

Below is sample configuration to configure egress policy map when 4Q mode is enabled.

```
Device#enable
Device#configure terminal
Device(config)#interface GigabitEthernet0/3/0
Device(config-if)#service instance 10 e
Device(config-if-srv)#service-policy output egress



Current configuration : 193 bytes
!
policy-map egress
class qos2
  shape average 2000000
```

```
 class qos3
  shape average 3000000
 class qos4
  shape average 4000000
 class class-default
  shape average 5000000
!
end
```

```
Device#sh run class-map qos2
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos2
match qos-group 2
!
end
```

```
Device#sh run class-map qos3
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos3
match qos-group 3
!
end
```

```
Device#sh run class-map qos4
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos4
match qos-group 4
!
end
```

Verifying QOS in 8K EFP Model

You need to verify the interface and policy-map details to check 8K model queue is working.

```
Device# show run interface g0/3/0
Building configuration...

Current configuration : 217 bytes
!
interface GigabitEthernet0/3/0
no ip address
negotiation auto
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  service-policy output egress
  bridge-domain 10
!
end
```

```
Router#show running-config policy-map egress
Building configuration...
```

```
Current configuration : 193 bytes
!
policy-map egress
class qos2
shape average 2000000
class qos3
shape average 3000000
class qos4
shape average 4000000
class class-default
shape average 5000000
!
end
```

```
Device#sh policy-map int g0/3/0 serv inst 10
Port-channel10: EFP 10

Service-policy output: egress

Class-map: qos2 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 4096000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/119746/0
(pkts output/bytes output) 2820/2882040
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000

Class-map: qos3 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 3
Queueing
queue limit 2730666 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/118806/0
(pkts output/bytes output) 3760/3842720
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Class-map: qos4 (match-all)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 2048000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 4000000, bc 16000, be 16000
target shape rate 4000000

Class-map: class-default (match-any)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 1638400 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 5000000, bc 20000, be 20000
target shape rate 5000000
Device#
```

16K EFP Support

Starting Cisco IOS Release 16.6.1, 16K EFPs are supported on the RSP3 module. The key features with this enhancement are:

- 16000 EFPs are supported on the RSP3 module (8K EFPs are supported per ASIC). Each port can have maximum of 8K EFPs configured.
- 8K bridge-domains are supported.
- Maximum of 16000 EVCs can be configured on the physical interface.
- Maximum of 8K Local-connect configurations are supported.
- Maximum of 1K bridge domain interface (BDI) can be configured upto BDI 4096.

Note In scenarios where VLAN range is greater than 5, VLAN compression is enabled.

Restrictions for 16K EFP

- 16k EFP scale is *not* supported if sdm template is enabled for split horizon scale.
- Egress policy-map is *not* supported on interfaces with 8K EFP configuration.
- The EVC/BD scale is *not* supported for port-channel.
- Minute traffic outage (few milliseconds) may be observed when applying or removing a policy-map.
- MAC security configuration must be reconfigured after every policy is attaced or detached.
- G8032, CFM and other Layer2 configurations are *not* supported if bridge-domains configured exceeds 4096.
- EVC MAC flush is triggered after attaching or detaching an egress policy map on the EVC.
- In a full scale setup, the EFP statistics update takes more than 1min to complete.

Configuring QoS with 16K EFP

Sample configurtion on how to configure 16K EFP

```
enable
Configure terminal
interface gigbaitethernet interface 0/0/1
service instance 8001 ethernet
encapsulation dot1q 20
bridge-domain 20
```

Verifying QoS Using 16k EFP

Following are verfication examples to verify QoS configurations using 16K EFP.

show ethernet service instance summary

```
Router# show ethernet ser instance summary
System summary
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain     16000    16000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all         16000    16000        0        0        0        0        0        0
Associated interface: GigabitEthernet0/6/1
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
Associated interface: TenGigabitEthernet0/7/7
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
```

show ethernet service instance id interface stats

```
Router# show ethernet service instance id 12000 interface te0/7/7 stats
Port maximum number of service instances: 16000
Service Instance 12000, Interface TenGigabitEthernet0/7/7
   Pkts In   Bytes In   Pkts Out  Bytes Out
       252     359352        252     359352
```

show platform hardware pp active interface all

```
Router# show platform hardware pp active interface all
Interface manager platform keys
-------------------------------------------------

Name: TenGigabitEthernet0/7/7, Asic: 0, hwidx: 62
lpn: 0, ppn: 62, gid: 62, mac: 7426.acf6.5685
InLportId: 0, ELportId: 0, dpidx: 22, l3ID: 19
port_flags: 0, port_speed: 10000 Mbps, efp_count: 8000, destIndex: 62, intType: 1
etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 1, l3PhyIf: 0, l3TDM: 0, loopBack: 0
tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 65535, protocols: 0
v4_netsmask: 0, v4_tableid: 0, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
vrfid: 0, enctype: 0, admin_state: 1, admin_state_oir: 0
```

show platform hardware pp active feature qos resource-summary

```
Rouer# show platform hardware pp active feature qos resource-summary 0
RSP3 QoS Resource Summary

Type Total Used Free
--------------------------------------------------------------------------------
QoS TCAM 1024 0 1024
VOQs 49152 784 48368
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 32000 32768
```

```
Router# show platform hardware pp active feature qos resource-summary 1
RSP3 QoS Resource Summary

Type Total Used Free
------------------------------------------------------------------------------
QoS TCAM 1024 0 1024
VOQs 49152 784 48368
QoS Policers 32768 0 32768
QoS Policer Profiles 1023 0 1023
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
```

show interface

```
Router# show interface gig0/1/6 | in pack
  30 second input rate 43604000 bits/sec, 43955 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     1521946 packets input, 188721304 bytes, 0 no buffer
     0 packets output, 0 bytes, 0 underruns

Router# show interface gig0/1/7 | in pack
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 43131000 bits/sec, 43482 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     1523724 packets output, 188941776 bytes, 0 underruns
```

16K EFP Support on Port Channel

Starting with Cisco IOS XE 16.8.1 release, 16K EFPs on port channel are supported on the RSP3 module.

The following are the key features supported:

- In order to enable 16K EFP over a port channel, you need to enable the following template:

  enable_portchannel_qos_multiple_active

- 16000 EFPs are supported on the RSP3 module (8K EFPs are supported per ASIC). Each port can have a maximum of 8K EFPs configured.
- 8K bridge domains are supported.
- On the RSP3 module, 1024 BDI interfaces that include physical interface, port channel interface, and BDI are available, and these interfaces can be configured upto 4096 BDI interfaces.

Note If a port channel is configured on an application-specific integrated circuit (ASIC), for example ASIC 0 , then ensure that physical members to be added to port channel also should be in the same ASIC.

Restrictions for 16K EFP on Port Channel

- G.8032, SADT, CFM, and TEFP are not supported on the port channel.

- 16k EFP scale is not supported if SDM template is enabled for split horizon scale.
- Minimal traffic outage (for example, in milliseconds) is observed, when a policy map is applied or removed.
- In a complete scale environment, the EFP statistics update requires more than 1 minute to complete.

Configuring 16K EFP on Port Channel

To configure 16K EFP on port channel, use the following commands:

```
router>enable
router#configure terminal
router(config)#sdm prefer enable_portchannel_qos_multiple_active
router(config)#platform port-channel 10 members-asic-id 1
router(config)#platform qos-port-channel_multiple_active port-channel 10
router(config)#interface port-channel 10
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter *yes* to save the configuration.

Verifying 16k EFP on Port Channel

The following are examples to verify for 16K EFP configuration on port channel.

show etherchannel summary

```
Router# show etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10      Po10(RU)                LACP     Te0/5/0(bndl) Te0/5/1(bndl)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show ethernet service instance id interface stats

```
Router# show ethernet service instance id 12000 interface port-channel 10 stats
Port maximum number of service instances: 16000
Service Instance 12000, Interface port-channel 10
   Pkts In   Bytes In   Pkts Out  Bytes Out
       252     359352        252     359352
```

show ethernet service instance summary

```
Router# show ethernet service instance summary
System summary
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain     16000    16000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all         16000    16000        0        0        0        0        0        0
Associated interface: port-channel 10
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
Associated interface: port-channel 11
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
```

QoS on Ether Channels

Restrictions of Legacy Ether Channel QoS

This section lists the various restrictions/limitations of the QoS-specific port-channel.

- Egress QoS policy-map is supported only on a member-link interface and not on a port-channel, port-channel EVC and port-channel TEFP.
- Effective Cisco IOS XE Everest 16.5.1 release, the egress policy-map can be configured on port-channel interface, which is in active/standby mode.
- Egress Match efp policy is not supported on PC member-links.
- Egress Match vlan policy is not supported on PC member-links.
- A maximum of 8 member-links will be bundled into a port-channel.
- All the other restrictions that are applicable to a regular port interface on the Cisco RSP3 Module are applicable to a port-channel interface and port-channel EVC.
- Egress policy-map with marking action is not supported on port-channel member links.

Example for Configuring QoS on an Ether Channel

Ingress Policy Map

The below example shows how to configure an ingress QoS policy-map.

```
do sh policy-map cos
         Policy Map cos
         Class cos1
         police cir 1000000 bc 31250
```

```
         conform-action transmit
         exceed-action drop
```

Member Link Policy-Map

The below example shows how to apply an ingress QoS policy-map onto a member-link.

```
interface GigabitEthernet0/2/1
         no ip address
         negotiation auto
         service-policy input cos
         channel-group 1
```

Port-Channel Interface Level

The below example shows how to apply an ingress QoS policy-map onto a port-channel interface.

```
interface Port-channel1
         no ip address
         negotiation auto
         service-policy input cos
         service instance 1 ethernet
         encapsulation dot1q 10
         rewrite ingress tag pop 1 symmetric
         bridge-domain 10
!
```

Port-Channel EVC Level

The below example shows how to apply an ingress QoS policy-map onto a port-channel EVC.

```
interface Port-channel1
         no ip address
         negotiation auto
         service instance 1 ethernet
         encapsulation dot1q 10
         rewrite ingress tag pop 1 symmetric
         service-policy input cos
         bridge-domain 10
```

Egress Policy-Map

The below example shows how to configure an egress QoS policy-map

```
sh policy-map qos
        Policy Map qos
        Class qos-1
        Average Rate Traffic Shaping
        cir 1000000 (bps)
```

Member-Link Policy Map

The below example shows how to apply an egress QoS policy-map on a member-link.

```
interface GigabitEthernet0/2/1
         no ip address
         negotiation auto
         service-policy output qos
         channel-group 1
```

Hierarchical Policy Design

Policing at two levels for the policy map is supported.

Ingress Hierarchical Policy Support

Three-Level Policy: You can only apply a three-level policy to a physical port on the router. A three-level policy consists of:

- Topmost policy: class-default
- Middle policy: match vlan/match efp
- Lowest policy: match prec/match cos/match dscp/match mpls exp topmost/match acl

The following sample policy uses a flat class-default policy on the port and VLAN policies on EFP interfaces to unique QoS behavior to each EFP.

Sample Policy

```
Policy-map port-policer
Class class-default
police cir 7m
Service-policy Vlan_set
Policy-map Vlan_set
Class vlan100
police cir 3m

Policy-map child1
Class prec2
police cir 3m

Service-policy port-policer-1
Class vlan200_300
police cir 4m
Service-policy child1
```

- Two-Level Policy
  - Topmost policy: match vlan/match efp
  - Lowest policy: match prec/match cos/match dscp
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match vlan
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match mpls experimental topmost
- Flat policy: match ip dscp
- Flat policy: class-default

Egress Hierarchical Policy Support

The following are examples of supported policy-map configurations:

- Three-Level Policy—You can only apply a three-level policy to a physical port on the router. A three-level policy consists of:
  - Topmost policy: class-default
  - Middle policy: match efp
  - Lowest policy: match qos-group

  The following sample policy uses a flat class-default policy on the port and class-default or PHB policy on the EFP interfaces to unique QoS behavior to each EFP.

Sample Policy

```
Policy-map port-shaper
Class class-default
Shape average percent 70
Service-policy child2
Service-policy Efp_set

Service-policy child1
Policy-map Efp_set
Class efp100
Shape average 200m
Class efp200_300
Shape average 200m


Policy-map child1
Class qos2
Shape average percent 40

Policy-map child2
Class qos4
Shape average percent 50
```

- Two-Level Policy
  - Topmost policy: match efp
  - Lowest policy: match qos-group
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match efp
- Two-Level Policy
  - Topmost policy: class-default
  - Lowest policy: match qos-group
- Flat policy: match qos-group

- Flat policy: class-default
- Flat policy: match efp

MPLS VPN QoS Mapping

Tables below summarize the default MPLS propagation and MPLS QoS mapping for the router.

Table 16: Default Propagation

Feature	IP to TAG	TAG to TAG	TAG to IP	Comments
L3VPN Uniform mode	Copy IP Prec/DiffServ into MPLS EXP by default	When the outer label is displayed, copy the exp of the . tag to the inner tag	MPLS EXP copied to IP Prec/DiffServ	
		When outer tag is swapped out, copy the exp to newly added tag		
L2VPN Uniform mode	Copy the outer COS to MPLS Exp by default	When the outer tag is popped out, copy the exp of the . tag to the inner tag	MPLS EXP is copied to COS by default.	
		When outer tag is swapped out, copy the exp to newly added tag		

Table 17: MPLS QoS Mapping

Feature	IP to TAG	TAG to TAG	TAG to IP	Comments
L3VPN Uniform mode	Match on PREC/DSCP and mark to MPLS EXP imposition	Match on MPLS EXP topmost and mark to MPLS EXP topmost	EXP to PREC marking is supported at ingress.	With L3VPN, Ingress QoS match on DSCP or PREC and set EXP marking, overwrites the DSCP value with EXP at imposition resulting in loss of the DSCP value.

Feature	IP to TAG	TAG to TAG	TAG to IP	Comments
L2VPN Uniform mode	With the policy-map with match on COS and set QoS_Group (which marks internally to EXP)	Match on MPLS EXP topmost and mark to MPLS EXP topmost	Use policy-map with match on EXP and mark to qos-group, which maps to COS. Egress COS can be marked by match on qos-group and set cos at access interface on PE2.	Sample configuration `policy-map P class exp1 set qos-group 1 policy-map P1 class qos2 set cos 2`

Note You can modify the default mapping behaviors using explicit marking policies.

QoS Policer and Shaper Calculation

Table below summarizes the packet accounting information used to make policer and shaper calculations on the router.

Table 18: QoS Accounting Calculation

Feature	Direction	Traffic Type	Values Counted
Policing	Ingress	IPv4/L3VPN	L2 overhead, VLAN tag, CRC
Shaping	Egress	IPv4/L3VPN	L2 Ethernet overhead, VLAN tag, CRC, preamble, IPG
Policing	Ingress	L2VPN	Layer 2 Ethernet overhead, VLAN tag, CRC
Shaping	Egress	L2VPN	Layer 2 Ethernet overhead, VLAN tag, CRC, preamble, IPG

The following considerations also apply when understanding QoS policer and shaper calculations:

- Egress shaping is applied at layer 1.
- Ingress packet length accounting is performed at egress.
- Egress shaping is supported and accounts for newly pushed VLAN tags and MPLS labels.

Simultaneous Policy support on Port/EFP

This feature provides the flexibility to apply EFP based classification on port and PHB based classification on EFP simultaneously.

At egress, it supports 4 level egress scheduling hierarchy and at ingress it supports simultaneous port and EFP policies.

Information about Simultaneous Policy Support on Port/EFP

In the Cisco RSP3 Module, this feature enables you to group EFP's and share policy (shaper/policer) for the range of EFP's simultaneously. This is designed to achieve the aggregate policer /shaper in ingress/egress respectively.

In RSP1/RSP2, this feature is implemented by the name "Service Group".

Benefits of simultaneous policy support on Port/EFP

This section provides the benefit/s of implementing simultaneous policy support on Port/EFP.

- Enables nested shaper up to fourth level.
- Enables EFP based classification on port and PHB based classification on EFP simultaneously.

Restrictions for simultaneous policy support on Port/EFP

- This feature is not supported on port channel, member-link and T-EFP.
- Policy-map should be applied on Port before applying on EFP, but in case of detaching, policy-map on EFP should be removed before removing from the port.
- BW/ BRR /BRP / WRED is supported only at PHB at egress.
- 2 level policy-map on port and marking policy on EVC, simultaneously is not supported.
- Only Match cos policy on EVC and match-efp policy on port is supported.
- Limited support is provided for statistics counters.

How to configure simultaneous policy support on Port/EFP

This feature is configured through qos policy on port (matching EFP range with policing/shaping action) and policy on EFP(matching PHB) simultaneously.

The configuration includes the following steps:

1. Create a class-map with efp range based classification.
2. Create a policy based on the class-map defined in step1.
3. Apply the efp classification based policy on the main interface.
4. Create a PHB policy to be applied on service instance.

5. Apply PHB based policy on service instance.

Configuring simultaneous policy support on Port/EFP

You can configure this feature in order to limit the traffic across all the instances where it is applied.

Before you begin

Ensure you add policy on interface first and then on the service instance.

Procedure

Ingress Configuration

```
1. Create a class-map with efp range based classification:
enable
configure terminal
class-map match-any efp_range
match service instance ethernet  1-100

2. Create a policy based on the class-map defined in step1:
policy-map ing_efp_range
class efp_range
police cir 40m

3. Apply the efp classification based policy on the main interface:
interface Gigabitethernet 0/14/0
service-policy input ing_efp_range


4. Create a PHB policy to be applied on service instance:
policy-map cos1
class cos1
police cir 10m

5. Apply PHB based policy on service instance:
interface Gigabitethernet 0/14/0
service instance 1 ethernet
service-policy input cos1
```

Egress configuration

```
1. Create a class-map with efp range based classification:
enable
configure terminal
class-map match-any efp_range
match service instance ethernet  1-100

2. Create a policy based on the class-map defined in step1:
policy-map egress_efp_range
class efp_range
shape average 500m

3. Apply the efp classification based policy on the main interface:
interface Gigabitethernet 0/14/0
service-policy output egress_efp_range

4. Create a PHB policy:
policy-map qos1
class qos1
```

```
shape average 300000000

5. Create a policy based on class-default:
policy-map egress_efp
 class class-default
   shape average 500000000
    service-policy qos1

6. Apply class-default policy-map on Service Instance:
Interface gigabitethernet 0/14/0
 service instance 1 ethernet
   service-policy output egress_efp
```

Result

You will be able to apply policy-maps on interface & EFP simultaneously.

Verification of the simultaneous policy support on Port/EFP configuration

To verify the configuration, use the **show policy-map** command in privileged EXEC mode to display summary configuration information.

```
Router#show policy-map interface brief
Service-policy input: ing_efp_range
GigabitEthernet0/14/0
Service-policy input: cos1
GigabitEthernet0/14/0: EFP 1

Router#show policy-map interface gig 0/14/0
GigabitEthernet0/14/0

Service-policy input: ing_efp_range

Class-map: efp_range (match-any
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: service instance ethernet  1-100
police:
cir 40000000 bps, bc 1250000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps

Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any

Router#show policy-map interface gig 0/14/0 service instance 1
GigabitEthernet0/0/5: EFP 1

Service-policy input: cos1

Class-map: cos1 (match-any)
48828201 packets, 49023513804 bytes
30 second offered rate 490218000 bps, drop rate 480258000 bps
Match: cos  1
QoS Set
qos-group 1
Marker statistics: Disabled
police:
```

```
cir 10000000 bps, bc 312500 bytes
conformed 992125 packets, 996093500 bytes; actions:
transmit
exceeded 47836076 packets, 48027420304 bytes; actions:
drop
conformed 9961000 bps, exceeded 480258000 bps
```

Configuring simultaneous policy support on Port/EFP: Example

The following example shows how to configure simultaneous policy support on Port/EFP:

```
interface GigabitEthernet0/14/0
no ip address
negotiation auto
service-policy input p1
service-policy output q1
service instance 1 ethernet
encapsulation dot1q 1
rewrite ingress tag pop 1 symmetric
service-policy input cos1
service-policy output qos1
bridge-domain 1
!
```

MPLS Diffserv Tunneling Modes Implementation

The MPLS specification defines Diffserv operation mode.

Uniform Mode—There is only one DiffServ marking that is relevant for a packet when traversing the MPLS network.

The following section describe how to implement uniform mode on the router using QoS policies.

Implementing Uniform Mode

Table 19: Default Propagation

Feature	IP to TAG	TAG to TAG	TAG to IP	Comments
L3VPN Uniform mode	Copy IP Prec/DiffServ into MPLS EXP by default	When the outer label is displayed, copy the exp of the . tag to the inner tag	MPLS EXP copied to IP Prec/DiffServ	
		When outer tag is swapped out, copy the exp to newly added tag		

Feature	IP to TAG	TAG to TAG	TAG to IP	Comments
L2VPN Uniform mode	COS is not copied to EXP by default, explicit policy-map is required to set qos-group which marks the EXP automatically.	When the outer tag is popped out, copy the exp of the . tag to the inner tag	MPLS EXP copied to COS by default	
		When outer tag is swapped out, copy the exp to newly added tag		

Use the following guidelines to implement uniform mode on the router:

MPLS EXP Imposition/Topmost Marking:

For L3 VPN

- Classify based on Prec bit or DSCP bit at ingress
- Set the mpls exp imposition

Tag-to-tag Transfer

- Classify based on mpls exp topmost
- Set the mpls exp topmost

For L2 VPN

- Classify based on COS bit at ingress
- Set the qos-group (which marks the mpls exp imposition)

Tag-to-tag Transfer

- Classify based on mpls exp topmost
- Set the mpls exp topmost

Classification

Classifying network traffic allows you to organize packets into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic (used in conjunction with marking network traffic) is the foundation for enabling many quality of service (QoS) features on your network.

Table below summarizes the QoS Classification limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 20: QoS Classification Limitations

Match	Main Interface		EFP Interface		Trunk EFP	
Features	I	E	I	E	I	E
Multiple match statements	3.16	3.16	3.16	3.16	3.16	3.16
access-group	3.16	X	3.16	X	3.16	X
all	3.16	3.16	3.16	3.16	3.16	3.16
any	3.16	3.16	3.16	3.16	3.16	3.16
cos	3.16	X	3.16	X	3.16	X
cos inner	3.16	X	3.16	X	3.16	X
dscp (IPv4)	3.16	X	3.16	X	3.16	X
dscp (IPv6)	16.5.1	X	16.5.1	X	16.5.1	X
ip dscp	3.16	X	3.16	X	3.16	X
ip precedence (IPv4)	3.16	X	3.16	X	3.16	X
ip precedence (IPv6)	16.5.1	X	16.5.1	X	16.5.1	X
mpls experimental topmost	3.16	X	3.16	X	3.16	X
precedence (IPv4)	3.16	X	3.16	X	3.16	X
qos-group	X	3.16	X	3.16	X	3.16
service instance ethernet	3.16	3.16	3.16	3.16	3.16	3.16
vlan	3.16	X	3.16	X	3.16	X
vlan inner	3.16	X	3.16	X	3.16	X

Ingress Classification Limitations

The following limitations apply to QoS classification on the router:

- QoS ACLs are supported only for ingress traffic.
- QoS ACLs are not supported for L4 traffic match criteria.

Egress Classification Limitations

- Egress classification can have only match qos-group.

Classifying Traffic using an Access Control List

You can classify inbound packet based on an IP standard or IP extended access control list (ACL). By default, TCAM optimization or expansion method is used. Both Security ACL and QoS ACL can be configured on the same interface. Follow these steps to classify traffic based on an ACL:

1. Create an access list using the **access-list** or ip **access-list** commands
2. Reference the ACL within a QoS class map using the **match access-group** configuration command
3. Attach the class map to a policy map

Limitations and Usage Guidelines

The following limitations and usage guidelines apply when classifying traffic using an ACL:

- QoS ACLs are supported only for IPv4 traffic.
- QoS ACLs are supported only for ingress traffic.
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:
  - 1-99—IP standard access list
  - 100-199—IP extended access list
  - 1300-1999—IP standard access list (expanded range)
  - 2000-2699—IP extended access list (expanded range)
- You must create an ACL before referencing it within a QoS policy.
- Deny statements within an ACL are ignored for the purposes of classification.
- Classifying traffic based on TCP flags using an ACL is not supported.
- Classifying traffic using multiple mutually exclusive ACLs within a **match-all** class-map is not supported.
- Classifying traffic on a logical/physical level using an ACL is not supported.

- Applying QoS ACLs to MAC addresses is supported for L2 flows only destination MAC.

For more information about configuring access control lists, see the *Security Configuration Guide: Access Control Lists for NCS 4200 Series*.

Configuring Multiple Match Statements

The router supports a single **match** or **match-any** command in a given QoS class-map, as shown in the following example:

Exampe for IOS XE 3.16 Class Map

```
class-map match-any my-restrict-class_00
   match ip precedence 0

class-map match-any my-restrict-class_01
   match qos-group 2

class-map match-any my-restrict-class_03
   match cos 3
```

Support for multiple **match** or **match-any** commands in a given QoS class-map, as shown in the following example:

Example for IOS XE 3.16 Class Map

```
class-map match-any my-class
match ip prec 1
match ip prec 2
match ip prec 3
```

The router treats the statements as a logical OR operation and classifies traffic that matches any **match** statement in the class map.

Traffic Classification Using Match EFP Service Instance Feature

Service Provider configurations have various service instances on the PE. QoS policy-maps are applied on these service instances or group of service instances. The benefits of the Match EFP Service Instance feature are:

- Identify the various types of service-instances like EFP, Trunk EFPs.
- Apply policies on these service instances at the port.
- Apply policies on a group of transport service instances such as applying similar policies to a group of EFPs.

Restrictions for Configuring Match Service Instances

- Ethernet service instances configured under the interface can be classified in a class of a policy-map. The class can match on a group or set of match service instance statements.

```
class-map match-any policeServiceInstance
    match service instance ethernet  100
    match service instance ethernet 200
```

- Match service instance supported at both Ingress and Egress level.

- match service instance and match PHB per flows classification are defined at respective levels in the policy hierarchy under the port.
- The number of EFPs supported per group is 256. Only 256 match statements are supported per class.
- Match EFP policy-map can be configured only on the port and *not* under the service instance.

Example for Configuring Match Service Instances

```
interface GigabitEthernet0/3/4
 no ip address
 negotiation auto
 service-policy output BTS_Total
 service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance trunk 20 ethernet
  encapsulation dot1q 20-29
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
 service instance 30 ethernet
  encapsulation dot1q 30
  xconnect 192.44.32.21 101 encapsulation mpls


class-map match-any service-instance-group-with-BMG
match service instance ethernet 10
match service instance ethernet 20

class-map service-instance-30
match service instance ethernet 30

class-map service-instance-20
match service instance ethernet 20

class-map VOICE
match qos-group 0

class-map SIGNALING
match qos-group 1

class-map match-any DATA
match qos-group 2
match qos-group 4

policy-map child-X
class VOICE
priority level 1 30000
class SIGNALING
priority level 2 30000
class DATA
shape average 90m


policy-map BTS_OUT_Bi
class service-instance-group-with-BMG
shape average 100m
service-policy child-X
class service-instance-30
```

```
shape average 200m
service-policy child-X

policy-map BTS_Total
class class-default
shape average 250m
service-policy BTS_OUT_Bi
```

QoS Marking

QoS marking allows you to set a desired value on network traffic to make it easy for core devices to classify the packet.

Table below summarizes the QoS Marking limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 21: Marking QoS Limitations

Features	Main Interface		EFP Interface		Trunk EFP		Port-channel Active Standby		Port-channel Active Active		Port-Channel Member Link		OC-3		OC-12		T1/E1		MLPPP	
set	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
cos	3.16	3.16	3.16	3.16	3.16	3.16	3.18 SP	3.18 SP	3.18.1 SP	3.18.1 SP	X	X	X	X	X	X	X	X	X	X
cos inner	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
discard-class	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X
dscp (IPv4)	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X
dscp (IPv6)	16.5.1	X	16.5.1	X	16.5.1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ip dscp	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X
ip precedence (IPv4)	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X

Features	Main Interface		EFP Interface		Trunk EFP		Port-channel Active Standby		Port-channel Active Active		Port-Channel Member Link		OC-3		OC-12		T1/E1		MLPPP	
ip precedence (IPv6)	16.5.1	X	16.5.1	X	16.5.1	X	16.5.1	X	16.5.1	X	X	X	X	X	X	X	X	X	X	X
mpls experimental imposition	3.16	X	3.16	X	3.16	X	X	X	X	X	3.18 SP	X	X	X	X	X	X	X	X	X
mpls experimental topmost	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X
precedence	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X
qos-group	3.16	X	3.16	X	3.16	X	3.18 SP	X	3.18.1 SP	X	X	X	X	X	X	X	X	X	X	X

Overview of Marking

The router supports the following parameters with the **set** command:

- **set cos**
- **set discard-class**
- **set dscp**
- **set precedence**
- **set ip dscp**
- **set ip precedence**
- **set mpls experimental imposition**
- **set mpls experimental topmost**

- **set qos-group**

Ingress Marking Limitations

The following limitations apply to QoS marking on the router:

- The router does *not* support hierarchical marking.
- COS to PREC/DSCP marking does not work for L2 flows.
- PREC/DSCP to COS marking does not work on L3 flows.
- **set mpls experimental imposition** command is not supported for L2VPN. Mark to qos-group, which internally marks to EXP value as qos-group marked.
- **set cos inner** command is not supported on the router.
- Ingress COS marking is supported only with no rewrite type EFPs and rewrite PUSH cases.
- Ingress COS marking is not supported for all remaining POP rewrite types.
- Ingress marking to qos-group, mark the egress COS based on qos-group marked value.
- With L3VPN, Ingress marking to mpls experimental imposition, mark the egress PREC based on mpls exp imposition value.
- With L3VPN, BDI based configuration; classification based on COS is supported only for marking.
- **set cos** command has no effect unless there is a egress push action to add an additional header at egress. The COS value set by this action will be used in the newly added header as a result of the push rewrite. If there are no push rewrite on the packet, the new COS value will have no effect.

Egress Marking Limitations

The following limitations apply when configuring marking on egress interfaces:

- Egress COS marking is supported. Match on qos-group and **set cos** command is supported.
- For Egress L3 BDI, match on qos-group and mark to COS is supported.
- Egress MPLS EXP and PREC/DSCP marking are not supported.

Egress Marking based on Color of Traffic

Egress marking is based on color of traffic. The RSP3 supports TRTCM and SRTCM policing algorithms. This results in different colors such as green, yellow, and red. The policer drops the red packets at ingress. With this feature, the packets are marked such that the policer passes or drops the packets accordingly. However the RSP3 policer has the following limitations:

- Direct marking or update to the MPLS EXP or DSCP packets based on policer result is not supported; only drop precedence packets are updated. To achieve marking, the drop precedence values from policer are used to mark the packet. The drops precedence packet values are 0 and 1 for green and yellow packets respectively.
- WRED has only 2 curves for drop precedence values 0 and 1.

- Marking is applicable to all traffic going out at the egress interface.

Note Egress marking policy-map is supported only at the interface level, and only on the imposition nodes (core interfaces). Egress marking *cannot* be done on Provider (P) routers in the network.

As the RSP3 module *does not* support the direct marking of the PHB, to achieve egress marking based on color, another child policy level must be added to the existing queue class level policy as in the below example.

```
class-map match-all dp0
match discard-class 0
class-map match-all dp1
match discard-class 1
class-map match-all qos5
match qos-group 5
class-map match-all qos4
match qos-group 4
class-map match-all qos1
match qos-group 1

policy-map egress_evc186_norm_parent
class class-default
  shape average 31250000
   service-policy egress_evc186_norm_child

policy-map egress_evc186_norm_child
class qos1
  bandwidth 4000
class qos4
  bandwidth 9000
   service-policy sub-child
class qos5
  bandwidth 18000
class class-default
policy-map sub-child
class dp0
  set mpls experimental topmost 4
class dp1
  set mpls experimental topmost 4
!
```

Restrictions for Egress MPLS EXP Marking based on Color of Traffic

- Green and yellow packets are only marked.

Note The packet marking actions are as:

- Confirm color is green
- Exceed color is yellow
- Violate color is red

Red packets are dropped by default.

- Egress MPLS EXP marking based on color of traffic is supported only for L2VPN and VPLS EFPs (xconnect and EFPs) services.
- Marking occurs only at egress interface. Hence, all traffic (from multiple policers and non-policed policers) going out through this interface is marked.
- Mapping from color to PHB value occurs only at the egress interface. Ingress policer marks the incoming packet to green and yellow. Use the **set discard-class** command to mark the color of the packets explicitly.
- Marking statistics is *not* supported.
- WRED based on DSCP is *not* supported. WRED based on discard class is supported.

Example: Configuring Egress MPLS EXP Marking

```
class-map match-all dp0
match discard-class 0

class-map match-all dp1
match discard-class 1

class-map match-all qos4
 match qos-group 4
class-map match-all qos5
match qos-group 5
class-map match-all qos4
match qos-group 4
class-map match-all qos1
match qos-group 1
!

policy-map cond-marking
class dp0
  set mpls experimental topmost 4
class dp1
  set mpls experimental topmost 4

policy-map egress_child
class qos1
  bandwidth 4000
class qos4
  bandwidth 9000
  queue-limit 300000 bytes
  random-detect discard-class-based
  random-detect discard-class 0 160000 bytes 256000 bytes 1
  random-detect discard-class 1 16000 bytes 256000 bytes 1
  service-policy cond-marking
class qos5
  bandwidth 18000
class class-default
  shape average 1000000

policy-map egress_parent
class class-default
  shape average 31250000
   service-policy egress_child

interface tenGigabitEthernet 0/8/6
service-policy output egress_parent
```

Example: Configuring Color based Marking At Ingress

```
class-map match-any cos012
    match cos 0 1 2

policy-map police_policy
class cos012
  police cir 256000 bc 9216 pir 512000 be 9216
  set qos-group 4
```

CoS Marking

Table 22: CoS Marking with Policy Map

Incoming Tag	Ingress Rewrite	Egress Rewrite			
		NO-RW	Pop-1(push 1 tag)	POP-2(push 2 tag)	PUSH-1(pop 1 tag)
One	NO-RW	Ingress COS marking supported	Outer COS copied to inner COS	N/A	N/A
	POP-1	N/A	Ingress COS marking not supported	Ingress COS marking not supported	N/A
	POP-2	N/A	N/A	N/A	N/A
	PUSH-1	Outer COS only marked and inner COS retained	N/A	N/A	Results in inner COS marking
Two	NO-RW	Cos marked as configured	N/A	N/A	Results in inner COS marking
	POP-1	Ingress COS marking not supported	Ingress COS marking not supported	N/A	N/A
	POP-2	N/A	Ingress COS marking not supported	Ingress COS marking not supported	N/A
	PUSH-1	N/A	N/A	N/A	N/A

CoS Marking Limitations

The following limitations apply when configuring CoS marking:

- The **set cos inner** command is not supported.

Configuring Short-Pipe Mode on QoS

Short-pipe mode on QoS RSP3 module can be activated using an SDM template. You can identify the egress traffic on an interface or EVC and classify based on DSCP, mark qos-group, and color using the platform table-map command. You can perform WFQ/WRED based on qos-group and color on egress interface using egress policy-map.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **sdm prefer enable_egr_l3vpn_cm**

Example:

```
Device(config)# sdm prefer enable_egr_l3vpn_cm
```

Enables the SDM template.

Step 4 **platform qos-table-map**

Example:

```
Device(config-table-map)# platform qos-table-map Customer#6
    from dscp 10 to qos-group 0 discard-class 0
    from dscp 63 to qos-group 0 discard-class 1

    qos-table-map Customer#6 interface GigabitEthernet0/4/0
```

Creates platform table-map and applying it on an interface.

Step 5 **Class-map match-any qos0**

Example:

```
Device(config-table-map)# Class-map match-any qos0
    match qos-group 0
Policy-map short-pipe-qos
    class qos0
        bandwidth 30000
        random-detect discard-class-based
        random-detect discard-class 0 25000 bytes 75000 bytes 1
```

```
        random-detect discard-class 1 95000 bytes 300000 bytes 1
        queue-limit 375000 bytes
```

Creates egress class map and policy map.

Example

Configuration Example

```
sdm prefer enable_egr_l3vpn_cm

platform qos-table-map Customer#6
    from dscp 10 to qos-group 0 discard-class 0
    from dscp 63 to qos-group 0 discard-class 1

qos-table-map Customer#6 interface GigabitEthernet0/4/0

interface Gig 0/5/0
    service-policy output short-pipe-qos

Class-map match-any qos0
    match qos-group 0

Policy-map short-pipe-qos
    class qos0
        bandwidth 30000
        random-detect discard-class-based
        random-detect discard-class 0 25000 bytes 75000 bytes 1
        random-detect discard-class 1 95000 bytes 300000 bytes 1
        queue-limit 375000 bytes
```

Restrictions on Short-Pipe Mode

- The **enable_egr_l3vpn_cm** SDM template command cannot co-exist with other templates such as **sdm prefer enable_copp** and **sdm prefer enable_match_inner_dscp** commands.
- Short-pipe mode on QoS RSP3 module is applicable only for conditional marking, which is not supported for multicast L3VPN traffic flows (TAG to IP).
- Short-pipe mode on QoS RSP3 module is not applicable for IPv6 traffic.
- You can configure only up to 7 table-maps.
- Following QoS classifications does not work after you enable the **sdm template** to activate short-pipe mode QoS feature:
    - DstMac
    - InnerVlanPri
    - InnerVlan
    - SrcIp
    - DstIp

- Before deleting the corresponding BDI interface, ensure to detach or unconfigure the table-map, if the table-map is applied on the BDI interface.
- Each table-map entry (classify on DSCP, mark to Qos-Group and DC) consumes up to 3 TCAM entries.
- Egress table-map matched traffic does not hit core interface policy-map.
- Core interface policy-map stats do not count egress table-map hit packets.
- Platform table-map stats are not supported.
- All backup paths (LB/FRR case) should be mapped with same table-map profile.

CoS Marking for Pseudowires

The packet when enters the pseudowire, COS is mapped to EXP by default. The policy-map on interface level is applicable for all xconnects. The policy-map attached at xconnect efp is specific to the xconnect.

- Egress set cos using egress policy overwrites the S-COS.
- If the topmost EXP is changed through ingress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.
- If the topmost EXP is changed through egress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.

Example

In the following configuration example, the MPLS is configured between PE1 and P routers. MPLS in physical interfaces is configured between P and PE 2 routers. The EFP X-connect is configured on the Access side.

Topology

ixia---(g0/0/1)PE1(teng0/0/2)---(teng0/2)P(g0/7)---(g0/7)PE2(g0/1)---ixia

PE1 Router

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255

interface BDI2
no shut
ip address 20.0.0.1 255.255.255.0
mpls ip
mpls label protocol ldp

router ospf 10
network 1.1.1.1 0.0.0.0 area 0
network 20.0.0.1 0.0.0.0 area 0

policy-map ingress
class class-default
set qos-group 4
interface GigabitEthernet 0/0/1
load-interval 30
service-policy input ingress
service instance 2 ethernet
```

```
encapsulation dot1q 2
xconnect 2.2.2.2 10 encapsulation mpls
```

Note The default mapping of EXP from COS is *not* supported on the Cisco RSP3 Module. But the mapping is done via COS to QoS group and QoS group to EXP. An explicit policy-map with match on COS and set qos-group is also used to mark the EXP.

Verifying PE 1 Router

```
 show policy-map interface GigabitEthernet 0/9/7
GigabitEthernet0/9/7

Service-policy input: ingress

Class-map: class-default (match-any)
13602943 packets, 13602943000 bytes
30 second offered rate 98040000 bps, drop rate 0000 bps
Match: any
QoS Set
qos-group 4
Marker statistics: Disabled
```

P router

```
class-map match-all exp4
match mpls exp topmost 4

policy-map ingress
class exp4

interface TenGigabitEthernet 0/2
load-interval 30
service-policy input ingress

interface BDI2
ip address 20.0.0.2 255.255.255.0
mpls ip
mpls label protocol ldp

router ospf 10
network 20.0.0.2 0.0.0.0 area 0
network 30.0.0.2 0.0.0.0 area 0
```

Verifying P Router

```
Router# show policy-map interface TenGigabitEthernet 0/2
TenGigabitEthernet0/2

Service-policy input: ingress

Class-map: exp4 (match-all)
560284 packets, 574851384 bytes
30 second offered rate 78284000 bps
Match: mpls experimental topmost 4

Class-map: class-default (match-any)
94 packets, 8224 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
```

PE 2 Router

```
class-map match-all exp4
match mpls experimental topmost 4

policy-map ingress
class exp4

interface Loopback0
ip address 2.2.2.2 255.255.255.255

interface GigabitEthernet 0/7
no switchport
ip address 30.0.0.1 255.255.255.0
media-type rj45
mpls ip
mpls label protocol ldp
service-policy input ingress 10:39 AM

router ospf 10
network 2.2.2.2 0.0.0.0 area 0
network 30.0.0.1 0.0.0.0 area 0 10:40 AM

interface GigabitEthernet 0/1
load-interval 30
service instance 2 ethernet
encapsulation dot1q 2
xconnect 1.1.1.1 10 encapsulation mpls
```

Verifying PE2 Route

```
show policy-map interface GigabitEthernet 0/7
GigabitEthernet0/7

Service-policy input: ingress

Class-map: exp4 (match-all)
133436 packets, 136905336 bytes
30 second offered rate 2956000 bps
Match: mpls experimental topmost 4

Class-map: class-default (match-any)
7 packets, 562 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
```

Global Table Map

A table-map helps you to define a mapping from an integer to an integer. In the RSP3 platform, by default global table-map configuration is used to map DSCP to EXP for L3 VPN services. Usage of ingress policy-map for marking the EXP is not recommended as it also modifies the DSCP. Hence, the global table-map allow you to configure a global level mapping of fields in the packet, without configuring a policy and keeps the DSCP value transparent.

The table-map is applicable to all L3 VPN MPLS packets, which sets the EXP field that is based on the incoming packet DSCP field. This mapping is also applicable to all L3 VPN IPv4/IPV6 traffic on the router.

The global table-map supports L2 VPN and L3 VPN traffic. L2 VPN conditional marking policy-map is supported and conditional marking policy is applicable to L2 VPN traffic.

The following sample table-map configuration enables a mapping at the router-level and it supports modification and deletion of table-map.

```
Router(config)# table-map DSCPTOEXP
Router(config-tablemap)# map from 10 to 1
Router(config-tablemap)# map from 22 to 2
Router(config-tablemap)# default copy


Router# show table-map
table-map DSCPTOEXP
      map from 10 to 1
      map from 22 to 2
      default copy
```

Restrictions

Following limitations are applicable to global table-map:

- Only one table-map configuration is supported globally.
- Table-map configuration is limited to DSCP to EXP mapping of L3 VPN traffic.
- Ingress policy-map to mark EXP on ingress interface is not recommended when you have global table-map configured for L3 VPN traffic.

MPLS Layer 3 VPN Conditional Marking QoS for RSP3 Module

The MPLS Layer 3 conditional marking feature enables you to mark the traffic with appropriate QoS group and sets policer to mark the color (discard class) based on Committed Information Rate (CIR) and Peak Information Rate (PIR) values. You can use the QoS group to create ingress policy map. It is mandatory to set the QoS group as a part of ingress policy-map to support Layer 3 VPN conditional marking.

At the egress side, you can classify the packets based on qos-group and discard class and set the EXP bits. Before configuring the ingress and egress policy maps, you need to activate an SDM template **enable_egr_l3vpn_cm** on the router.

After configuring the ingress and egress policy maps, you need to attach service policy to to the ingress interface and QoS policy to the egress interface.

You can verify the configuration using the **show policy-map interface** command.

Restrictions for MPLS Layer 3 VPN Conditional Marking

- The MPLS layer 3 conditional marking for QoS can be enabled only using an SDM tempate: **enable_egr_l3vpn_cm**.
- LB and Fast Reroute (FRR) cases should have marking policies applied on data paths.
- The MPLS layer 3 conditional marking for QoS is not supported for the IPv6 and multicast traffic.
- Discard-class statistics is not supported.
- Control Plane Policing (COPP) and match-inner-dscp templates are not supported.
- It is mandatory that you need to set QoS-group as a part of ingress policy-map.

- The number of egress conditional marking policy-maps is limited to 2.
- The following QOS qualifiers are not supported for the **enable_egr_l3vpn_cm** SDM template:
  - Match inner VLAN
  - Match inner QoS
  - Source (SRC) IP
  - Destination (DST) IP
- TCAM utilization for Layer 3 VPN conditional marking template:
  - Service policy under an interface for COS based classification takes 1 entry
  - Service policy under an EFP for COS based classification takes 2 entries on LPM
  - Service policy under an EFP for COS/DSCP based classification occurs on LPM

How to Configure MPLS Layer 3 Conditional Marking

Enabling SDM Tempalte

Before configuring ingress and egress policy map, you need to enable the SDM template on router.

```
router(config)#sdm prefer enable_egr_l3vpn_cm
```

Configuring Ingress Policy Map

After enabling the SDM template, you can match the class map and DSCP for ingress traffic, and apply class map to the policy map. You can set CIR and PIR values for police action and apply transmit actions to ingress traffic. You can set QoS group to the policy map applied.

To configure ingress traffic using policy map, enter the following commands:

```
class-map match-all AF41
 match dscp af41
 policy-map INGRESS
 class AF41
  police cir 200000000 pir 300000000 conform-action
  transmit exceed-action transmit violate-action drop
  set qos-group 2
```

Configuring Egress Policy Map

To configure egress policy map, enter the following commands:

```
class-map match-any qos-group2
 match qos-group 2
 policy-map Conditional_Marking_Leaf
 class DC0
  set mpls experimental topmost 2
 class DC1
  set mpls experimental topmost 1
 policy-map Conditional_Marking_Child
```

```
 class qos-group2
    bandwidth percent 20
   service-policy Conditional_Marking_Leaf
policy-map EGRESS_PARENT
 class class-default
  shape average 150000000
   service-policy Conditional_Marking_Child
```

Attaching Service Policy to Ingress

To attach service policy to the ingress direction, enter the following commands:

```
service-policy input INGRESS
```

Attaching QoS Policy Map on Egress Interface

To attach QoS policy map on egress direction, enter the following commands:

```
service-policy output EGRESS_PARENT
```

Verifying MPLS Layer 3 Conditional Marking

To verify the MPLS Layer 3 conditional marking configuration, use the **show policy-map interface *interface-name*** command.

```
router#show policy-map interface gi 0/15/2
 GigabitEthernet0/15/2

  Service-policy output: EGRESS_PARENT

    Class-map: class-default (match-any)
      2749290 packets, 23705425676 bytes
      5 minute offered rate 362014000 bps, drop rate 250204000 bps
      Match: any
      Queueing
      queue limit 54613 us/ 1024000 bytes
      (queue depth/total drops/no-buffer drops) 0/1844419/0
      (pkts output/bytes output) 904871/7105654676
      shape (average) cir 150000000, bc 600000, be 600000
      target shape rate 150000000

      Service-policy : Conditional_Marking_Child

        queue stats for all priority classes:
          Queueing
          priority level 2
          queue limit 109226 us/ 1024000 bytes
          (queue depth/total drops/no-buffer drops) 1037760/131743/0
          (pkts output/bytes output) 394863/3553767000

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 2730666 us/ 1024000 bytes
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0

         Class-map: qos-group0 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
```

```
    Match: qos-group 0
    Queueing
    queue limit 54613 us/ 1024000 bytes
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining 10%

  Class-map: qos-group1 (match-any)
    526606 packets, 4739454000 bytes
    5 minute offered rate 72387000 bps, drop rate 54345000 bps
    Match: qos-group 1
    Queueing
    queue limit 54613 us/ 1024000 bytes
    (queue depth/total drops/no-buffer drops) 1037760/395342/0
    (pkts output/bytes output) 131264/1181376000
    bandwidth remaining 20%

  Class-map: qos-group2 (match-any)
    526606 packets, 4739454000 bytes
    5 minute offered rate 72387000 bps, drop rate 63373000 bps
    Match: qos-group 2
    Queueing
    queue limit 54613 us/ 1024000 bytes
    (queue depth/total drops/no-buffer drops) 1037760/461018/0
    (pkts output/bytes output) 65588/590292000
    bandwidth remaining 10%

   Class-map: qos-group3 (match-any)
    526606 packets, 4739454000 bytes
    5 minute offered rate 72387000 bps, drop rate 63365000 bps
    Match: qos-group 3
    Queueing
    queue limit 54613 us/ 1024000 bytes
    (queue depth/total drops/no-buffer drops) 1037760/460973/0
    (pkts output/bytes output) 65633/590697000
    bandwidth remaining 10%

  Class-map: qos-group5 (match-any)
    526607 packets, 4739463000 bytes
    5 minute offered rate 72387000 bps, drop rate 54346000 bps
    Match: qos-group 5
    Queueing
    queue limit 54613 us/ 1024000 bytes
    (queue depth/total drops/no-buffer drops) 1037760/395343/0
    (pkts output/bytes output) 131264/1181376000
    bandwidth remaining 20%

  Class-map: qos-group4 (match-any)
    526606 packets, 4739454000 bytes
    5 minute offered rate 72387000 bps, drop rate 18118000 bps
    Match: qos-group 4
    Priority: 50% (75000 kbps), burst bytes 1875000, b/w exceed drops: 131743

    Priority Level: 2
 Service-policy : Conditional_Marking_Leaf

      Class-map: DC0 (match-any)
        0 packets, 0 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: discard-class 0
        QoS Set
          mpls experimental topmost 2
            Marker statistics: Disabled
```

```
    Class-map: DC1 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: discard-class 1
      QoS Set
        mpls experimental topmost 1
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

Class-map: qos-group6 (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: qos-group 6
  Priority: 2% (3000 kbps), burst bytes 75000, b/w exceed drops: 0

  Priority Level: 1

Class-map: class-default (match-any)
  116259 packets, 8146676 bytes
  5 minute offered rate 134000 bps, drop rate 0000 bps
  Match: any

  queue limit 54613 us/ 1024000 bytes
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 116259/8146676
```

Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or class of service (CoS). This section describes the policing limitations and configuration guidelines for the router.

The router supports the following policing types:

- Single-rate policer with two color marker (1R2C) (color-aware mode)
- Two-rate policer with three color marker (2R3C) (color-aware mode)

Table below summarizes the QoS policing limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 23: Policing Feature Support

Features	**Main Interface**		**EFP Interface**		**Trunk EFP**	
	I	E	I	E	I	E
One rate	3.16	X	3.16	X	3.16	X
One rate and two marking	3.16	X	3.16	X	3.16	X

Features	Main Interface		EFP Interface		Trunk EFP	
Two rates and three actions	3.16	X	3.16	X	3.16	X
drop	3.16	X	3.16	X	3.16	X
transmit	3.16	X	3.16	X	3.16	X

Table 24: Traffic Queuing Support

Features	Main Interface		EFP Interface		Trunk EFP	
	I	E	I	E	I	E
bandwidth	X	3.16	X	3.16	X	3.16
bandwidth remaining ratio	X	3.16	X	3.16	X	3.16
bandwidth percent	X	3.16	X 3.16	3.16	X	3.16
priority	X	3.16	X	3.16	X	3.16
priority level 1/2	X	3.16	X	3.16	X	3.16

Supported Commands

The router supports the following policing commands on ingress interfaces:

- **police** (percent)—**police cir percent** *percentage* [*burst-in-msec*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **police** (policy map)—**police cir** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **police** (two rates)—**police cir** *cir* [**bc** *conform-burst*] [**pir** *pir*] [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

The router supports the following queuing commands:

- **bandwidth** (policy-map class)—bandwidth {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*} [**account** {**qinq** | **dot1q**} **aal5 subscriber-encapsulation**]
- **bandwidth remaining ratio**—**bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**] {*subscriber-encapsulation* | **user-define**d *offset*}]

- **police** (policy map)—**police cir** *bps* [[**bc**] *normal-burst-bytes* [*maximum-burst-bytes* | [**be**] [*burst-bytes*]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]
- **priority—priority** {**percent** *percentage*} [*burst*]
- **priority level 1/2—priority level 1/2** {**percent** *percentage*} [*burst*]

Several restrictions apply when using egress policing; see the *Egress policing Limitations* section for more information.

Note **police** (policy map) command on egress interface is not supported in Cisco RSP3 module.

Percentage Policing Configuration

The router calculates percentage policing rates based on the maximum port PIR rate. The PIR rate is determined as follows:

- Default—Port line rate
- Speed command applied—Operational rate
- Port shaping applied to port—Shaped rate

Ingress Policing Limitations

The following limitations apply to QoS policing on the router:

- If you configure a policer rate or burst-size that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.
- If you configure a policer using a **set** command, you cannot use the **set** command at other levels of the hierarchical policy-map.
- If you configure a SRTCM policer at parent level, you cannot use the TRTCM on any other level (child level) in case of hierarchical policy-map. Similarly, if TRTCM is configured at parent level, SRTCM cannot be configured at child level. To resolve this problem, configure parent TRTCM with exceed and violate-action as drop and TRTCM at child level policy-map hierarchy.

Example for HQOS Ingress Interface

```
Policy-map parent
Class class-default
Police cir 100m conform-action transmit exceed-action drop violate-action drop
Service-policy child

Policy-map child
Class prec2
```

```
Police cir 100000 pir 200000 conform-action transmit exceed-action transmit violate-action
 drop
```

Policing at ingress also colors the traffic. You can use ingress policer to set discard-class 0 and 1, which can be used at egress for WRED. Green (confirm-action) is discard-class 0. Yellow/Red (exceed/violate action) is discard-class 1.

Traffic Shaping

Traffic shaping allows you to control the speed of traffic that is leaving an interface in order to match the flow of traffic to the speed of the receiving interface. Percentage-based shaping allows you to configure traffic shaping based on a percentage of the available bandwidth of an interface. Configuring traffic shaping in this manner enables you to use the same policy map for multiple interfaces with differing amounts of bandwidth.

This section describes the configuration guidelines for the router.

Additional Shaping Limitations

The following are the shaping usage guidelines:

- Shaping is supported at all levels in the policy-map hierarchy.
- 3-level hierarchical shaping is supported.
- Port-level shaping is supported.

Configuring Egress Shaping on EFP Interfaces

Configuring an EFP port shaper allows you to shape all EFPs on a port using a port policy with a class-default shaper configuration, as in the following partial sample configuration:

```
policy-map port-policy
  class class-default
    shape average percent 50
policy-map efp-policy
  class EFP100
    shape average percent 25
    service-policy child-policy
policy-map child-policy
  class qos-group1
    shape average percent 20
```

The following configuration guidelines apply when configuring an EFP port shaping policy:

- You can combine a port shaper policy (a flat shaper policy with no user-defined classes) with an egress EFP QoS shaping policy.
- Configure the port shaper policy before configuring other egress QoS policies on EFP interfaces; when removing EFP QoS configurations, remove other egress EFP QoS policies before removing the port shaper policy.
- When the configuration specifies a shaper rate using a percentage, the router calculates the value based on the operational speed of a port. The operational speed of a port can be the line rate of the port or the speed specified by the **speed** command.

- The rates for **bandwidth percent** and **shape percent** commands configured under a port-shaper are based on the absolute rate of the port-shaper policy.

Congestion Management

Congestion management features allow you to control congestion by determining the order in which packets are sent out an interface based on priorities assigned to those packets. Congestion management entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

This section describes the classification limitations and configuration guidelines for the router.

Table below summarizes the QoS congestion management and queuing limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 25: Congestion Management QoS Limitations

Features	**Main Interface**		**EFP Interface**		**Trunk EFP**	
	I	E	I	E	I	E
CBWFQ	X	3.16	X	3.16	X	3.16
LLQ	X	3.16	X	3.16	X	3.16
bandwidth (kbps)	X	3.16	X	3.16	X	3.16
bandwidth percent	X	3.16	X	3.16	X	3.16
bandwidth remaining percent	X	3.16	X	3.16	X	3.16
bandwidth remaining ratio	X	3.16	X	3.16	X	3.16
fair-queue	X	X	X	X	X	X
priority	X	3.16	X	3.16	X	3.16
priority (kbps)	X	3.16	X	3.16	X	3.16
priority percent	X	3.16	X	3.16	X	3.16
queue-limit (bytes)	X	3.16	X	3.16	X	3.16

Features	Main Interface		EFP Interface		Trunk EFP	
queue-limit (packets)	X	X	X	X	X	X
queue-limit (msec)	X	3.16	X	3.16	X	3.16

Ingress Queuing Limitations

The router does not support queuing on ingress interfaces.

Egress Queuing Limitations

The router supports tail drop queuing on egress interfaces using the **queue-limit** command. The following limitations apply to egress queuing:

- Queue allocation is per EFP/TEFP per TC(qos-group) for L2 interfaces with egress policy map applied.
- Queue allocation is per Port per TC(qos-group) for L3 interfaces.
- If class is matching multiple TC(qos-group) then multiple queues are generated for this class. For L2 interface, queues belonging to all EFP with the same TC comes under same class.
- Configuring shaping using committed burst (bc) is supported and excess burst (be) is not supported on the router.
- Granularity at lower rates is 384Kbps and at higher rates is 1.5 percent.
- **Priority Level** command and **Priority** command are not supported in the same policy.
- Strict **Priority** and **bandwidth** command cannot be configured in the same policy-map.
- Mixed bandwidth types are not supported in the same policy. For example, if you use **bandwidth remaining percent** command in one class, you cannot use **bandwidth percent** or **bandwidth remaining ratio** command in the same policy.
- The **bandwidth** and **bandwidth-remaining** commands are *not* supported on class containing the **Priority** command.
- Priority propagation is not supported.

Support for Low Latency Queuing on Multiple EFPs

The router supports the QoS policies that allow for low-latency queuing (LLQ) across multiple EFPs. For more information about this feature, see *QoS Policing and Shaping Configuration Guide for NCS 4200 Series*.

Additional Queuing Limitations

The additional queuing usage guidelines are the following:

- The router supports QoS policies that allow for low-latency queuing (LLQ) across multiple EFPs. For more information about this feature, see *QoS: Policing and Shaping Configuration for Cisco NCS 4200 Series.*

Congestion Avoidance

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS QoS includes an implementation of RED that, when configured, controls when the router drops packets. If you do not configure Weighted Random Early Detection (WRED), the router uses the cruder default packet drop mechanism called tail drop.

Table below summarizes the QoS congestion avoidance limitations for the router. In the table, I represents Ingress and E represents Egress.

Table 26: Congestion Avoidance QoS Limitations

Features	**Main** **Layer 3** **Interface**		**EFP** **Interface**		**Trunk** **EFP**	
	I	E	I	E	I	E
random-detect discard- class-based	X	3.16	X	3.16	X	3.16

Congestion Avoidance Configuration

The following sections describe the supported congestion avoidance features on the router:

Supported Commands

The router supports the following commands for WRED:

- **random-detect discard-class-based**

Supported Interfaces

WRED is supported at the PHB level but not on logical or physical interfaces. You can apply WRED policies on the following interface types:

- Main interface
- Service instances
- Trunk EFPs

Verifying the Configuration

You can use the **show policy-map interface** command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see the following documents:

- *QoS: Congestion Avoidance Configuration Guide for Cisco NCS 4200 Series*

Ingress Congestion Avoidance Limitations

WRED is not supported on ingress interfaces.

Egress Congestion Avoidance Limitations

The following limitations apply when configuring congestion avoidance on the router:

- WRED is only supported on egress interfaces.
- WRED based on discard-class only supported.
- Class-map match condition must be qos-group and WRED based on discard-class.
- Queuing feature to support WRED in a class such as shape or bandwidth are supported.
- You must apply WRED within a policy-map.
- WRED is *not* supported in priority queues.
- You can configure a maximum of 2 WRED curves per class.
- You can configure WRED with either the **shape** or the **fair-queue** (CBWFQ) commands.
- WRED is supported in the class-default class if there are no other user-defined classes in the policy-map.
- The default value for **exponential-weighting-constant** is 9.
- The default value for **mark-probability** is 10.
- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.
- Aggregate-WRED is not supported.

Additional Congestion Avoidance Limitations

- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.

Verifying the Configuration

You can use the **show policy-map interface** command to display the number of WRED drops and tail drops.

For more information about configuring congestion avoidance, see *QoS: Congestion Avoidance Configuration Guide*.

Scheduling

This section describes the scheduling limitations and configuration guidelines for the router.

Ingress Scheduling Limitations

The router does not support scheduling on ingress interfaces.

Egress Scheduling Limitations

- If you configure a CIR, PIR, or EIR rate that the router cannot achieve within 1% accuracy, the configuration is rejected. The command output presents recommendations for the closest possible lower and higher configuration value.
- You can only configure one **priority** value on each parent class applied to a QoS class or logical interface.
- You can only configure priority on one class in a QoS policy.

The following limitations apply when configuring a 3-level scheduling policy on an egress interface configured as an EFP:

- Only two of the three levels can contain scheduling actions such as **bandwidth**, **shape**, or **priority**.
- Class-based excess bandwidth scheduling is supported on 2nd and 3rd level QoS classes.
- One of the levels containing scheduling actions must be the class (bottom) level.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Other QoS Guides	*QoS: Classification Configuration Guide* *QoS: Congestion Avoidance Configuration Guide* *QoS: Congestion Management Configuration Guide* *QoS: Modular QoS Command-Line Interface Configuration Guide* *QoS: Policing and Shaping Configuration Guide*

Standards

Standard	Title
The supported standards applicable to the MPLS applications appear in the respective feature module for the application.	--

MIBs

MIB	MIBs Link
The supported MIBs applicable to the MPLS applications appear in the respective feature module for the application.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
The supported RFCs applicable to the MPLS applications appear in the respective feature module for the application.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html