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 ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In

particular, QoS features provide improved and more predictable network service by implementing the following services:

Note ATM and SONET are *not* supported on the Cisco ASR 900 RSP3 Module.

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

For more information about Quality of Service, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html

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 1: QoS Feature Overview

Feature	Main	Service Instance	Trunk EFP
Dynamic policy modification	3.16	3.16	3.16
EFP QoS Support	3.16	3.16	3.16
Classification			
Ingress	3.16	3.16	3.16
Egress	3.16	3.16	3.16
Match any	3.16	3.16	3.16
Marking			
Ingress	3.16	3.16	3.16
Egress	3.16	3.16	3.16
Policing			
Ingress	3.16	3.16	3.16
Shaping			
Port Shaping	3.16	3.16	3.16

Feature	Main	Service Instance	Trunk EFP
Congestion Avoidance			
WRED	3.16	3.16	3.16
Multiple Priority Queues	3.16	3.16	3.16
Congestion Management			
Strict Priority	3.16	3.16	3.16
Scheduling			
Egress	3.16	3.16	3.16
QoS ACLs			
Ingress	3.16	3.16	3.16

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 2: 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 3: 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

Ternary content-addressable memory (TCAM) resources are commonly used for PHB policies that use match DSCP or IP precedence, multi match PHB policies, or parent match EFP policies with child PHB. Starting with Cisco IOS XE Fuji 16.7.1 release, the supported TCAM scale limit per network processor (NPU) for ingress QoS policy maps is increased from 1024 entries to 2048.

Since TCAM resources are shared between multiple features, increasing the scale limit for one feature may not be supported by other features. For example, QoS, IPv4 ACL, and IPv6 multicast features share the common TCAM resources. When you increase the TCAM scale limit for QoS, then the other two features might not be able to support these increased scale limits.

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
```

Table 4: Feature History

Feature Name	Release	Description
Increase QoS Service-Policy Scale	Cisco IOS XE Bengaluru 17.5.1	Starting with Cisco IOS XE Bengaluru 17.5.1 release, you can further increase the TCAM scale limit per NPU from 2048 entries to 3072 entries for ingress QoS policy maps. This feature is supported on the Cisco RSP3 module.

Starting with Cisco IOS XE Bengaluru 17.5.1 release, you can further increase the TCAM scale limit per NPU from 2048 entries to 3072 entries for ingress QoS policy maps. This increased scale limit is to support certain use cases that may require higher TCAM resources.

Use the following SDM template to set the TCAM scale limit.

- **enable_qos_scale** – Enable this template to achieve 3072 QoS TCAM entries.
- **disable_qos_scale** – Disable this template to get back to 2048 QoS TCAM entries.

Note If the system is configured with SDM template enable_qos_scale, then the scale limits of IPv6 multicast and IPv4 ACLs behave as follows:

- No TCAM entries are consumed for IPv6 multicast
- TCAM limit is reduced to 700 for IPv4 ACL

You can perform the following sample configuration across multiple EFPs to increse the scale value.

```
Class-map:
========
class-map match-any cos4
match cos 4
match dscp ef
class-map match-any cos3
match cos 3
match dscp cs3
class-map match-any cos2
match cos 2
match dscp cs2
class-map match-any cos1
match cos 1
match dscp cs1

Policy-map:
=========
policy-map cos
class cos1
police cir 10000000
set qos-group 1
class cos2
police cir 20000000
set qos-group 2
```

```
class cos3
police cir 30000000
set qos-group 3
class cos4
police cir 40000000
set qos-group 4

Interface config (policy-map attachment):
==========
interface HundredGigE0/5/0
no ip address
cdp enable
service instance 1 ethernet
encapsulation dot1q 1
rewrite ingress tag pop 1 symmetric
service-policy input cos
bridge-domain 1
!
service instance 2 ethernet
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
service-policy input cos
bridge-domain 2
!
service instance 3 ethernet
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
service-policy input cos
bridge-domain 3
!
.
.
.
.
.
.
service instance 341 ethernet
encapsulation dot1q 341
rewrite ingress tag pop 1 symmetric
service-policy input cos
bridge-domain 341
!
```

Use the following **show platform hardware pp active feature qos resource-summary** command to display the increased scale values for QoS:

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

Type                                        Total       Used        Free
-------------------------------------------------------------------------------
QoS TCAM                                    3072        3069        3
VOQs                                        49152       648         48504
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

- The DSCP field (TAG to IP) value does not change in both the uniform mode and in pipe mode. This is applicable to both the Unicast and Multicast traffic scenario.
- 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.
- Ingress queuing is not supported on Cisco ASR 900 routers.
- 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.

Following are the restrictions for QoS on Serial or MLPPP interfaces:

- For the Class-based weighted fair queueing (CBWFQ) and priority on multilink interface, the QoS policy moves to the suspend state if the configured value is greater than that of the interface bandwidth.

  For the CBWFQ and priority on serial interfaces, the QoS policy is not attached to the serial interface, if the configured value is greater than that of the interface bandwidth.
- For SHAPE on multilink interface, the QOS policy move to suspend state ,iff the configured shape rate of each class is greater than that of the interface bandwidth.
- For SHAPE on serial interfaces, the policies are not attached to the interface, if the configured rate of each shape class is greater than that of the interface bandwidth.

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 5: 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

[1] 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 XE Release 3.18:

- 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.
- High latency for priority traffic is observed during congestion for egress QoS over 1G link.

Priority Queues

Table 6: Feature History

Feature Name	Release	Description
4x Priority Queue support on RSP3 modules	Cisco IOS XE Dublin 17.10.1	In certain networks, more than two priority levels are required as traffic with more than two priorities need to be scheduled on priority basis and in certain condition you need to have more than one priority queue per level. Now the priority level is enhanced 2–4. You can now configure up to four priority levels and apply the same priority levels on more than one class-map by enabling **enable_4x_priority** template. This feature is supported on the Cisco RSP3 module.

The router employs priority queuing to manage the flow of traffic within the network and to achieve throughput and latency targets. You can assign these priority queue levels to traffic classes (class maps) to manage the sequencing of packets to yield a consistent flow of traffic within the network.

On the RSP3 interface modules, you can configure only up to two priority levels on the Ethernet Flow Point (EFP) policy map. Hence, only traffic up to 2 priorities are scheduled. Starting from release Cisco IOS XE Dublin 17.10.1, the RSP3 interface modules support 4 priority queue settings for QoS levels, 1–4, where 1 is the highest priority and 4 is the lowest.

For example, the router forwards all outgoing traffic with a priority queue level of 1, the highest priority setting, before forwarding any outgoing traffic with a priority queue level of 2. Similarly, the router forwards all traffic with a priority queue level of 2 before traffic with a priority queue level of 3. This pattern continues until the router forwards traffic from the lowest priority queue of 4. When the queue buffer overloads, the router drops the packets.

If you need, more than 2 priority levels and more than one priority queue per level, then you must enable **sdm prefer enable_4x_priority** command template. After you enable this template, the router may reboot, and is

ready to configure different levels on priority. Templates allow you to dynamically change QoS parameters without defining a new QoS policy on the CLI. You can change QoS policy when a session begins or anytime after the session is established.

Restrictions

- You can configure only a maximum of upto four priority levels.
- The EFP policy map scale is reduced to half. These scale numbers may vary based on number of class-maps under policy-maps.
- The enhanced priority queue is supported only when **sdm prefer enable_4x_priority** template is configured.

Enabling Priority Queue Template

You must enable the priority queue template using the **sdm prefer enable_4x_priority** command template on the router.

```
Router(config)#sdm prefer enable_4x_priority
 4X priority template change.
 Current template = disable_4x_priority
 Updated template = enable_4x_priority
 Standby is reloaded, it will come up with init required for new template
 once standby comes up Please trigger SSO

*Aug  1 16:23:25.543 IST: Changes to 4X priority template stored
```

Example: Priority Level on Policy-Map

The sample configuration shows the priority level 1–4. The priority packets are scheduled first compared to non-priority packets. The priority order is from 1 -4 and if there's any bandwidth left, the remaining will be shared across **class nni_data_3_2** and **class-default** based on the remaining bandwidth percent.

```
Router#show running-config policy-map egress_child_level1-4
Building configuration...
Current configuration : 316 bytes
!
policy-map egress_child_level1-4
 class nni_connection_7
  priority level 1
 class nni_control_6
  priority level 2
 class nni_realtime_5
  priority level 3
 class nni_premium_4
  priority level 4
 class nni_data_3_2
  bandwidth remaining percent 50
 class class-default
  bandwidth remaining percent 50
!
end
```

Example: Same Priority Level on Multiple Class

The sample configuration shows the same priority level on multiple classes. The **class nni_control_6** and **class nni_connection_7** are assigned the same priority level as 1. The priority order is from 1 and 2 and if

there's any bandwidth left, the remaining will be shared across **class nni_premium_4**, **class nni_data_3_2**, and **class nni_basic_1_0** based on the remaining bandwidth ratio.

```
Router#show running-config policy-map egress_child
Building configuration...
Current configuration : 385 bytes
!
policy-map egress_child
 class nni_control_6
  priority level 1
 class nni_connection_7
  priority level 1
 class nni_realtime_5
  priority level 2
 class nni_premium_4
  bandwidth remaining ratio 30
 class nni_data_3_2
  bandwidth remaining ratio 40
 class nni_basic_1_0
  bandwidth remaining ratio 20
!
end
```

Disabling Priority Queue Template

You can disable the priority queue template using the **sdm prefer disable_4x_priority** command.

```
Router(config)#sdm prefer disable_4x_priority
 4X priority template change.
 Current template = enable_4x_priority
 Updated template = disable_4x_priority
 Standby is reloaded, it will come up with init required for new template
 once standby comes up Please trigger SSO

*Aug  1 16:23:25.543 IST: Changes to 4X priority template stored
```

Verifying Priority Queue Template

You can verify the priority queue template using the **show sdm prefer current** command.

```
Router#show sdm prefer current
The current sdm template is "default"
The current efp template is "enable_8k_efp"
The current portchannel template is "enable_portchannel_qos_multiple_active"
The current qos scale template is "enable_qos_scale"
The current 4x priority template is "enable_4x_priority"
```

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

- With the **enable_8k_efp** SDM template, shut or noshut on Port-channel (PoCH) is blocked. To make the PoCH as UP or DOWN, all the port channel member links must be either shut or noshut.
- 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#
```

Ingress QoS Support on EFPs under a Port Channel

Table 7: Feature History

Feature Name	Release Information	Feature Description
Ingress QoS Support on EFPs under a Port Channel	Cisco IOS XE Dublin 17.10.1	You can now configure 8K ingress policy maps on 8K Ethernet Flow Points (EFPs) or service instances under a port channel (8K EFPs are supported for each ASIC). There should be a one-to-one mapping between an ingress QoS policy and an EFP.

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 32 individual active links into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. You can configure Ethernet flow Points (EFPs) or service instances under a port channel and apply QoS policies on each EFP by using the Switch Database Management (SDM) template. The following are the prerequisite SDM templates used to configure ingress QoS policies on EFPs under a port channel:

- sdm prefer enable_8k_efp
- enable_portchannel_qos_multiple_active

From Cisco IOS XE Dublin 17.10.1, you can map up to 8K ingress policy maps with 8K EFPs under a port channel. Ensure that the mapped 8k policy maps and 8K EFPs belong to the same ASIC, for example ASIC1.

Configuring Ingress Policy Maps on EFPs under a Port Channel

The process of enabling ingress policy maps on EFPs under a port channel includes the following configurations.

The first step includes the following substeps:

1. Enable the SDM template.
2. Register the required port channel as multiactive.
3. Assign the port channel to an ASIC.
4. Initiate QoS.

Example

This example shows that port channel 10 is registered as multiactive and is assigned to ASIC ID 1.

At the ingress PE router:

```
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
```

Thereafter, apply a policy map on an EFP under the configured port channel.

Example

This example shows that the policy map, VPN_POLICY is mapped to an EFP or service instance 34 under port channel 10. Similarly, you can map up to 8k policy maps to 8k EFPs under port channel 10.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface port-channel 10
Router(config-if)#service instance 34 ethernet
Router(config-if-srv)#service-policy input VPN_POLICY
Router(config-if-srv)#end
```

Verification

Enter the following command to verify that the VPN_POLICY map is applied to EFP 34 under port channel 10:

```
Router#show policy-map interface port-channel 10 service instance 34 input
Port-channel10: EFP 34
Service-policy input: VPN_POLICY
Class-map: cos0123 (match-any)
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: cos 0 1 2 3
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: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
cir 3200000 bps, bc 100000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps
```

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.
- While adding member links to port channels with 3K to 8K EFPs, the router sends CPUHOG messages to the console output to inform that this process has consumed CPU memory. The number of messages increases with the increase in the scale of the EFPs. Such messages do not impact any functionality. They ensure that the system does not become unresponsive or locked up due to the total consumption of the CPU.

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
```

Hierarchical Policy Design

In Cisco IOS XE Release 3.16, 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 8: 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 9: 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 10: 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
```

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 11: 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	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 12: 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 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, Cisco IOS XE Release 3S (ASR 900 Series) .

Configuring Multiple Match Statements

The router supports a single **match** or **match-any** command in a given QoS class-map in IOS XE Release 3.16, 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
```

IOS XE Release 3.16 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 3.16 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 13: Marking QoS Limitations

Features	**Main Interface**		**EFP Interface**		**Trunk EFP**	
set	I	E	I	E	I	E
cos	3.16	3.16	3.16	3.16	3.16	3.
cos inner	X	X	X	X	X	X
discard-class	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 prece-dence (IPv4)	3.16	X	3.16	X	3.16	X

Features	Main Interface		EFP Interface		Trunk EFP
ip precedence (IPv6)	16.5.1	X	16.5.1	X	16.5.1
mpls experimental imposition	3.16	X	3.16	X	3.16
mpls experimental topmost	3.16	X	3.16	X	3.16
precedence	3.16	X	3.16	X	3.16
qos-group	3.16	X	3.16	X	3.16

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

Starting with Cisco IOS Release 3.18, egress marking based on color of traffic is introduced on the RSP3 module. 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 14: 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.

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 10.0.0.1 255.255.255.255

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

router ospf 10
network 10.0.0.1 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 10.0.0.2 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 10.0.0.2 255.255.255.255

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 10.0.0.2 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 10.0.0.1 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
```

CoS Conditional Marking

Table 15: Feature History

Feature Name	Release	Description
CoS Conditional Marking	Cisco IOS XE Amsterdam 17.3.1	This feature lets you implement the CoS marking on the basis of the Traffic class and the Drop precedence. This feature is supported on the Cisco RSP3 module.

The CoS Conditional Marking implements the CoS marking on the basis of the Traffic class and the Drop precedence.

Restrictions for CoS Conditional Marking

- The Four-level policy is not supported.
- The modification of policy with unsupported or a combination of COS and EXP is not supported.
- The COS conditional marking is not supported when the EFP is configured with encapsulation **default**.
- The COS conditional marking is not supported when the rewrite ingress tag push rule is configured on the EFPs.
- The policies attached to the EFPs stop COS conditional marking. This happens because of the two-level conditional marking policy attached to the individual EFPs and a class-default shaper on the port. When attaching a two-level child policy to the class-default on port-shaper, results in unexpected conditional

COS marking change and corrupt policy-map counters. However, detaching the port-shaper, results in COS conditional marking failure.

- The conditional marking policy displays the Profile Exhaustion error. This error occurs due to a limitation of the profile creation or modification logic in the system and the marker profile 15 is changed or detached from the parent policy.
- The CoS marking is supported on EFP interface when the SR PFP Template is configured.
- The conditional marking does not work when an egress policy with class-default is attached, as a profile is not created. However, when a non default class is attached to the egress policy, the Conditional Marking on class-default works as a profile gets created.

How to Configure CoS Conditional Marking

Configuring Egress Policy Map

To configure egress policy map, enter the following commands:

```
class-map match-all dp0
match discard-class 0
class-map match-all dp1
match discard-class 1

class-map qos1
match qos-group 1

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

policy-map egress_child
class qos1
bandwidth 4000
service-policy sub-child
class class-default

policy-map sub-child
class dp0
set cos 4
class dp1
set cos 5
```

Configuring Ingress 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-any cos012
 match cos 0 1 2

policy-map ingress
class cos012
```

```
set qos-group 1
police cir 256000 pir 556000
```

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 and received on an interface. Traffic policing also allows partition of 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) (default is color-aware mode)
- Two-rate policer with three color marker (2R3C) (default is color-aware mode)

Table 16: Feature History

Feature Name	Release	Description
Inter-cos bursting support	Cisco IOS XE Bengaluru 17.6.2, Cisco IOS XE Cupertino 17.7.1	This feature introduces color-blind mode of policer operation support on routers with single-rate policer (1R2C) and two-rate policer (2R3C) policing types. With this feature, all policers support color-blind mode with the new template.

Starting with 17.6.2 and 17.7.1 releases, policer modes support the RSP3 module with the following approach:

- Color-aware mode (default mode) – All policers support color-aware mode with the existing template.
- Color-blind mode – All policers support color-blind mode with the new template.

When you configure a child with a two-rate policer with three color marker (2R3C) policy, then the packets with green, yellow, and red is marked accordingly. Even if the parent policy single-rate policer with two color marker (1R2C) is configured with higher policer rate (CIR or PIR), the yellow and red packets marked by the child policer is not allowed.

With the color-blind mode of policer operation, parent policer configured with higher policer rate allows the packets marked with yellow and red.

The conditional CoS or EXP marking of packets perform based on the color result of the child policer.

Use the following SDM template to set the color-blind mode:

- **enable_color_blind_policer** – Enable this template to set policers to work in color-blind mode.
- **disable_color_blind_policer** – Disable this template to set policers to work in color-aware mode (default mode).

Note Ensure to remove the color-blind mode configured template before you downgrade the image.

The following table summarizes the QoS policing limitations for the router. In the table, I represent Ingress and E represents Egress.

Table 17: 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
Two rates and three actions	3.16	X	3.16	X	3.16	X
Drop	3.16	X	3.16	X	3.16	X

Features	Main Interface		EFP Interface		Trunk EFP	
Transmit	3.16	X	3.16	X	3.16	X

Table 18: 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** *level<1/2>*] {**percent** *percentage*}

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

Note The **police** (policy map) command is supported only on the ingress interface and not supported on an egress interface in the 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 19: 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
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

IOS XE 3.16 Release for the 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 3.16:

- The 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.
- Maximum queue-limit that can be configured in bytes is 4 MB.

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 20: 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:

- http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conavd/configuration/xe-3s/qos-conavd-diffserv-wred.html
- http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_wred.html
- http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00805b9497.html

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 the following documents:

- http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conavd/configuration/xe-3s/qos-conavd-diffserv-wred.html
- http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_wred.html

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.

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 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
```

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.

QoS Support on Ether Channel LACP Active Standby (1:1)

Link Aggregation Control Protocol (LACP) supports the automatic creation of ether channels by exchanging LACP packets between LAN ports. Effective Cisco IOS-XE 3.18 SP release, LACP packets are exchanged only between ports in standby and active modes. LACP "learns" the capabilities of LAN port groups dynamically and informs the other LAN ports. After LACP identifies correctly matched links, it facilitates grouping the

links. Both the passive and active modes allow LACP to negotiate between LAN ports to determine if they can form an ether channel, based on port speed and trunking state.

Effective Cisco IOS-XE 3.18 SP release, the Aggregate QoS method with single member link is also supported.

On ports configured to use LACP, configuration of the maximum number of compatible ports happens, up to the maximum allowed by the hardware. To use the hot standby or active standby or 1:1 feature in the event an ether channel fails, both ends of the LACP bundle must support the **lacp max-bundle** command.

Use the **platform qos-port-channel-aggregator** *port-channel-number* **enable** command to apply QoS policy on the ether channel. Create an ether channel using the **interface port-channel** *1* command, configure **lacp max-bundle** *1* command, and add the member links. This configures LACP max bundle on the port-channel.

LACP port priority can be configured automatically or through the **lacp max-bundle** *1* command,. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

In releases before Cisco IOS-XE 3.18 SP, egress QoS policy was achieved by applying the policy-map on the member links instead of on the ether channel.

But, it has the following restrictions:

- No match EFP policy is supported on the member links.
- Only port-based policies are supported.

Effective Cisco IOS-XE 3.18 SP release, the configuration of QoS egress policies on ether channel is supported on the Cisco RSP3 Module.

Carrier delay of 25 ms is recommended on member links for better convergence. Member links of ether channel active or standby should be in the same ASIC to apply QoS.

Policy map based on matching a certain service instance is also supported. The features such as QoS marking, QoS policing, QoS shaping, QoS bandwidth, LLQ, and WRED are also supported on this policy type.

Restrictions for LACP Active Standby

- If you perform a double SSO, LDP neighborship is not coming up on port-channel Active/Standby.
- First use the **platform qos-port-channel_aggregator** *1* **enable** command to apply QoS policy on the port channel and then create a port channel using the **interface port-channel** *1* command. Configure **lacp max-bundle** *1* command and then add the member links.
- To disable the **platform qos-port-channel_aggregator** *1* **enable** command, delete the port-channel.
- All member links should be present on the same ASIC.

Support of QoS Classification

Classifying network traffic allows you to organize packets into traffic classes or categories on the basis of whether the traffic matches specific criteria. The support of QoS classification is based on PREC, EXP, VLAN, COS, COS-inner, DISCARD-class, and QoS-group fields.

Traffic classification, marking, and policing can be configured in ingress service policy and traffic classification, queuing, marking, and scheduling can be configured in egress service policy.

Support of QoS Marking

QoS marking is supported on ingress and egress policies.

Marking is supported on COS, PREC, DSCP, EXP, QoS-group, and DISCARD-class fields.

On ingress policies:

- For Layer 2 Flows: Classification on COS and marking on COS are supported.
- For Layer 3 Flows: Classification on PREC or DSCP fields and marking on PREC or DCSP fields are supported.

Support of QoS Policing

Class-based policing allows you to control the maximum rate of traffic that is transmitted or received on an interface. The chassis supports the following policing types:

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

Committed Information Rate (CIR) and Peak Information Rate (PIR) can be configured from 64Kbps to 10Gbps. Bc and Be can be configured from 8Kbytes to 16Mbytes.

Support of QoS Shaping

QoS shaping is supported on egress policies only.

The default PIR value of a class equals to the PIR value of the parent entity. If the parent entity is not configured, the default PIR value of a class equals to the link rate.

Shape Average

The rate of shape average is calculated in units of bps. The rate of shape average can be configured from 384kbps to 100Gbps.

Shape Average Percent

The rate of shape average percent is calculated in units of percent. The absolute rate is calculated as a percent of the PIR of the parent entity.

Tc, Bc, and Be are not configurable.

Support of QoS Bandwidth

QoS Bandwidth remaining percent and Bandwidth remaining ratio set the EIR of the queue.

Bandwidth calculated in kbps and bandwidth percent calculated in units of percent set the CIR of the queue. The CIR value can be configured from 100Kbps to 10Gbps.

Note Different bandwidth types cannot be configured in the same policy. For example, you cannot configure BRR in one class and BRP in another class of the same policy.

The configurable BRR ratio ranges from 1 to 63.

Support of LLQ

This feature allows you to configure bandwidth as a percentage within Low Latency Queueing (LLQ). Strict priority and priority shaper rate configurations are supported.

Overhead that is considered for LLQ is L2+L3+Frame Checksum.

The **priority** [**level** *level<1/2>*] {**percent** *percentage*} works like a priority shaper. Traffic exceeding the given rate in the **priority** command is dropped as exceed drop.

Support of WRED

DiffServ Compliant WRED extends the functionality of Weighted Random Early Detection (WRED) to enable support for DiffServ and Assured Forwarding (AF) per hop behavior (PHB). This feature enables customers to implement AF PHB by coloring packets according to Differentiated Services Code Point (DSCP) values and then assigning preferential drop probabilities to those packets.

WRED based on discard-class is only supported. The supported match condition of class-map is QoS-group. The queuing features like shape or bandwidth support WRED in a class.

The minimum and maximum thresholds are specified in bytes or microseconds only.

The following shows 3 WRED profiles per class:

- 2 WRED Profiles
- 1 Tail Drop Profile

Configuring Hierarchical Policy Maps

Use the following commands to configure hierarchal policy maps:

```
enable
configure terminal
policy-map child-llq
qos-group 1
set cos 5
bandwidth percent 20
exit
qos-group 2
bandwidth percent 80
exit
policy-map parent-llq
class class-default
service-policy child-llq
```

Configuring Class-default Port-Shaper Policy Maps

```
enable
configure terminal
policy-map policy-map child-llq
class class-default
shape-average 200000000
exit
```

Configuring Port-Shaper Policy Maps

```
enable
configure terminal
policy-map policy-map def
```

```
class class-default
shape-average 200000000
service-policy child-llq
```

Configuring an LLQ Policy Map

```
enable
configure terminal
policy-map llq-flat
class dscp-af1
priority
exit
qos-group 1
shape average 200000000
exit
qos-group 2
bandwidth 4000000
exit
```

Configuring Port Level Shaping on the Main Interface with Ethernet Flow Points

```
enable
configure terminal
interface port-channel 1
no ip address
negotiation auto
lacp max-bundle 1
service-policy output parent-llq
service instance 1 ethernet
encapsulation dot1q 100
bridge-domain 100
exit
service instance 2 ethernet
encapsulation dot1q 101
bridge-domain 101
exit
```

Configuring Match EFP-based Policy

Use the following commands to configure match EFP-based policy:

```
enable
configure terminal
class-map match-any efp123
match service instance ethernet 1
match service instance ethernet 2
match service instance ethernet 3
policy-map efp_based
class efp123
shape average 10m
class class-default
shape average 20m
end
```

Configuring policy on EFP

Use the following commands to configure policy on EFP.

```
enable
configure terminal
interface port-channel 1
```

```
service instance 1 ethernet
encapsulation dot1q 100
bridge-domain 100
service-policy output child-llq
end
```

Verification of Policy Map Configuration

Use the **show policy-map interface** command to verify the policy map configuration:

```
Router#show policy-map interface po1
Port-channel1

  Service-policy output: egress

    Class-map: qos1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 1

    Class-map: qos2 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 2

    Class-map: qos3 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 3

    Class-map: qos4 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 4

    Class-map: qos5 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 5

    Class-map: qos6 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 6

    Class-map: qos7 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps
      Match: qos-group 7

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

Use the **show policy-map interface port-channel** *1* **service instance** *1* **output** / **input** command to verify the policy map configuration for an EFP:

```
Router#show policy-map int po2 service instance 1 output
Port-channel2: EFP 1

Service-policy output: l1c

Class-map: qos4 (match-all)
```

```
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 74472 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 11% (110000 kbps)

Class-map: qos1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 1
Queueing
queue limit 68266 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 12% (120000 kbps)

Class-map: qos2 (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 43115 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 19% (190000 kbps)

Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 54613 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 15% (150000 kbps)
```

Associated Commands

The following commands are used to configure LACP Active/Standby mode:

Commands	Links
platform qos-port-channel_aggregator	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-n1.html
lacp max-bundle	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-i2.html
show policy-map interface port-channel	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s4.html

QoS Support on Port Channel LACP Active Active

Link Aggregation Control Protocol (LACP) supports the automatic creation of ether channels by exchanging LACP packets between LAN ports. Cisco IOS XE Everest 16.6.1 release introduces the support of QoS on port channel LACP active active mode. A maximum of eight member links form a port channel and thus the traffic is transported through the port channel. This feature is supported on Cisco RSP3 Module.

Benefits of QoS Support on Port Channel LACP Active Active

- This feature facilitates increased bandwidth.
- The feature supports load balancing.
- This features allows support on QoS on Port Channel with one or more active member links.

Restrictions for QoS Support on Port Channel Active Active

- Policy-map on member links is not supported.
- 100G ports and 40G ports cannot be a part of the port channel.
- Total number of port channel bandwidth supported on a given ASIC should not exceed 80G.
- This feature is not supported on multicast traffic.
- Only 3k service instance (EFP) scale is supported on port channel active active.
- Ensure that 2-3 seconds of delay is maintained before and after unconfiguring and re-configuring the port channel with the **platform qos-port-channel_multiple_active** command.

Note This delay increases when you have scaled EVC configurations on the port channel.

Configuring QoS Support on Port Channel Active Active

Enabling Port Channel Active/Active

Use the following commands to enable port channel active active:

```
enable
configure terminal
sdm prefer enable_portchannel_qos_multiple_active
end
```

Note The device restarts after enabling the **sdm prefer enable_portchannel_qos_multiple_active** command. After a successful reboot, verify the configuration using the command **show sdm prefer current**

Disabling Port Channel Active/Active

Use the following commands to disable port channel active active:

```
enable
configure terminal
sdm prefer disable_portchannel_qos_multiple_active
end
```

Configuring Active Active Port Channel per bundle

Use the following commands to configure active active port channel per bundle:

```
enable
configure terminal
platform qos-port-channel_multiple_active 10
end
```

Creating Port Channel Interface

Use the following commands to configure the port channel interface:

```
enable
configure terminal
interface port-channel 10
no shutdown
end
```

Attaching member link to port channel

Use the following commands to attach a member link to the port channel:

```
enable
configure terminal
interface Te0/4/0
channel-group 10 mode active
end
```

Configuring QoS Class Map and Policy Map

Use the following commands to configure QoS class map and policy map:

```
enable
configure terminal
class-map match-any qos1
match qos-group 1
class-map match-any qos2
match qos-group 2
policy-map policymapqos
class qos1
shape average 10000 k
class qos2
shape average 20000 k
end
```

Attaching Configured Policy Map (policymapqos) on Port Channel Interface on Egress Direction

Use the following commands to attach the configured policy map (policymapqos) on the port channel interface on egress direction:

```
enable
configure terminal
interface port-channel 10
service-policy output policymapqos
end
```

Verification of QoS Support on Port Channel LACP Active Active

Use the commands below to verify the port channel summary details:

```
Device#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     Te0/4/0(bndl)
```

Use the commands below to verify the attached policy map on the port channel interface:

```
Device#show policy-map interface brief
Service-policy input: ingress
TenGigabitEthernet0/4/0
Service-policy output: policymapqos
Port-channel10

      Device#show policy-map interface po10
  Port-channel10

     Service-policy output: policymapqos

     Class-map: qos1 (match-any)
       1027951 packets, 1564541422 bytes
       30 second offered rate 50063000 bps, drop rate 40020000 bps
       Match: qos-group 1
       Queueing
       queue limit 819200 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/821727/0
       (pkts output/bytes output) 206224/313872928
       shape (average) cir 10000000, bc 40000, be 40000
       target shape rate 10000000

     Class-map: qos2 (match-any)
       852818 packets, 1297988996 bytes
       30 second offered rate 41534000 bps, drop rate 21447000 bps
       Match: qos-group 2
       Queueing
       queue limit 409600 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/440370/0
       (pkts output/bytes output) 412448/627745856
       shape (average) cir 20000000, bc 80000, be 80000
       target shape rate 20000000

     Class-map: class-default (match-any)
       1565 packets, 118342 bytes
       30 second offered rate 3000 bps, drop rate 0000 bps
       Match: any

       queue limit 102 us/ 1024000 bytes
       (queue depth/total drops/no-buffer drops) 0/0/0
       (pkts output/bytes output) 1565/118342
```

Use the commands below to verify the configuration after enabling port channel active/active mode:

```
#show sdm prefer current
The current sdm template is "default"
The current portchannel template is "enable_portchannel_qos_multiple_active"
```

Associated Commands

Commands	Links
platform qos-port-channel_multiple_active	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-n1.html
sdm prefer enable_portchannel_qos_multiple_active	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s1.html
sdm prefer disable_portchannel_qos_multiple_active	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s1.html
show sdm prefer current	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book/qos-s4.html