Quality of Service Configuration Guidelines for RSP1, RSP2 Module

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

- New and Changed Information, on page 2
- Quality of Service, on page 4
- Quality of Service Configuration, on page 5
- QoS Support Overview, on page 5
- Global QoS Limitations, on page 7
- Routed Port-Channel, on page 11
- Sample Hierarchical Policy Designs, on page 14
- Ingress and Egress Hierarchical Policing, on page 15
- Dissimilar PHB Support for MPLS and VPLS Interfaces, on page 16
- MPLS VPN QoS Mapping, on page 17
- Example for Configuring QoS on an Ether Channel, on page 17
- MPLS VPN QoS Mapping, on page 18
- QoS Policer and Shaper Calculation, on page 19
- Service Groups, on page 20
- MPLS Diffserv Tunneling Modes Implementation, on page 28
- Classification, on page 30
- QoS Marking, on page 37
- Traffic Policing, on page 46
- Traffic Shaping, on page 53
- Congestion Management, on page 54
- Congestion Avoidance, on page 57
- Scheduling, on page 62

New and Changed Information

Table 1: New and Changed Information

Feature	Description	ASR 903 RSP1	ASR 903 RSP2	ASR 902	Where Documented
Support for MLPPP on Serial Interfaces	Ingress and Egress QoS on MLPPP is supported on serial interfaces	Cisco IOS XE Release 3.13	Cisco IOS XE Release 3.15	Cisco IOS XE Release 3.12	QoS Support Overview, on page 5
Service groups	The Service groups feature allows you to create service groups and apply aggregate features to those service groups.	Cisco IOS XE Release 3.11		Cisco IOS XE Release 3.12	Service Groups, on page 20
Dissimilar PHB support for Egress and Ingress MPLS and VPLS interfaces.	Support for PHB support on Egress and Ingress MPLS and VPLS access interfaces.	Cisco IOS XE Release 3.11		Cisco IOS XE Release 3.12	Dissimilar PHB Support for MPLS and VPLS Interfaces, on page 16
Hierarchical QoS Hierarchical color-aware policer	hierarchical QoS policies with up to three levels, allowing for a high degree of granularity in traffic management.	Cisco IOS XE Release 3.6	Cisco IOS XE Release 3.15	Cisco IOS XE Release 3.12	Ingress and Egress Hierarchical Policing, on page 15
• MQC Limitations • Support for **police** and **set** commands in same class-map.	Lists the MQC scaling limitations on the router. Police and set can be configured on same egress policy class-map.	Cisco IOS XE Release 3.10	Cisco IOS XE Release 3.13	Cisco IOS XE Release 3.12	QoS Features Using MQC Limitations, on page 8 Egress Policing Limitations, on page 50

Feature	Description	ASR 903 RSP1	ASR 903 RSP2	ASR 902	Where Documented
Support for QoS policies on layer 3 Etherchannel interfaces.	Ingress and Egress QoS policies are supported on Etherchannel.	Cisco IOS XE Release 3.9		Cisco IOS XE Release 3.12	Restrictions of Ether Channel QoS, on page 11
QoS on Serial TDM interface	QoS is supported on serial TDM interfaces.	Cisco IOS XE Release 3.9		Cisco IOS XE Release 3.12	Additional Marking Limitations, on page 45
QoS Classification based on EFP	QoS Classification based on EFP is supported.	Cisco IOS XE Release 3.9	Cisco IOS XE Release 3.13	Cisco IOS XE Release 3.12	Restrictions for Egress QoS, on page 9 Restrictions for Ingress QoS, on page 9
QoS EXP Marking for Ingress on TDM and ATM PW	EXP Marking for Ingress on TDM and ATM Psuedowires	Cisco IOS XE Release 3.9		Cisco IOS XE Release 3.12	Additional Marking Limitations, on page 45
QoS Support on POS on OC3 IM	Egress QoS is supported Packet over Sonet (POS).	Cisco IOS XE Release 3.8	Cisco IOS XE Release 3.14	Cisco IOS XE Release 3.12	QoS Support Overview, on page 5
Support for QoS matching on Ethernet service instances	Match EFP is supported on service instances.	Cisco IOS XE Release 3.8		Cisco IOS XE Release 3.12	Traffic Classification Using Match EFP Service Instance Feature, on page 35

Feature	Description	ASR 903 RSP1	ASR 903 RSP2	ASR 902	Where Documented
Support for QoS features on egress MLPPP interfaces Support for QoS features on ingress MLPPP interfaces	Egress Qos is supported on MLPPP interfaces.	Cisco IOS XE Release 3.7.1 Cisco IOS XE Release 3.13		Cisco IOS XE Release 3.12	Traffic Classifying on MLPPP Interfaces, on page 32 Traffic Policing on MLPPP Interfaces, on page 52 Support for Queuing Features on MLPPP Interfaces, on page 57 Egress Congestion Avoidance on MLPPP Interfaces, on page 61 Egress Scheduling on MLPPP Interfaces, on page 62
Support for Egress Policing	Egress policy is supported.	Cisco IOS XE Release 3.6	Cisco IOS XE Release 3.13	Cisco IOS XE Release 3.12	Egress Policing Limitations, on page 50
EFP QoS Support	QoS is supported on EFPs.	Cisco IOS XE Release 3.6	Cisco IOS XE Release 3.13	Cisco IOS XE Release 3.12	QoS Support Overview, on page 5
QoS ACLs	QoS ACLs are supported.	Cisco IOS XE Release 3.5		Cisco IOS XE Release 3.12	Classifying Traffic using an Access Control List, on page 33

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

Quality of Service Configuration

This document provides details on the platform-dependent implementation of QoS on the router. For information about how to understand and configure QoS features, 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 s Global QoS Limitations.

Table 2: QoS Feature Overview

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

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

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

Table 3: QoS Support for TDM Features

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

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

Global QoS Limitations

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

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

- Three-level QoS policies are not supported on the OC-3/OC-12 serial, MLPPP, and PoS interfaces. You can only apply QoS policies on two levels on these interfaces.
- QoS does not account for CRC values on an interface and assumes that the value is 2 bytes. CRC differences can cause accuracy issues for 2 to 3% of the 128-byte traffic.
- The router supports a maximum of 128 internal and reserved labels that represent PHB (cos/dscp/exp/prec) values on a QoS policy. A label exhaustion message is displayed if a policy exceeds the maximum number of labels.
- QoS does not support WRED counters for all the match conditions.
- Configuring **set mpls exp topmost** in edge router does not copy the exp value to MPLS label. At Ingress interface, only VC label is supported as topmost label. At Egress interface, the topmost label is supported which takes MPLS label based on LDP. The outer MPLS label exp value is same as inner MPLS label. When the VC label exp value is zero, the outer MPLS label exp value becomes zero. At Ingress, when the VLAN is pushed, the MPLS exp value also becomes VLAN pushed tag.
- The ICMPv4 packets classification based on ACL attached on the interface is not supported.
- EXP-based classification at the egress of PE routers is not supported by default. To achieve this, the EXP bits are required to be imposed over the cross connect at the ingress of the same PE router using an input policy.
- When a class-map and policy-map are created with match-and-set action(s) and attached to an interface, an internal value called label is allocated for each PHB value used in the class-map. These label values are consumed only when the class-maps and policy-maps are attached to an interface.

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

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

  To avoid this condition, a convention is followed wherein, at the ingress interface for a traffic flow the classes match the PHB values such as CoS, PREC, and so on, and set the internal QoS-Group values. At the egress interface, the classes match the traffic based on the QoS groups that are set at the ingress

QoS Features Using MQC Limitations

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

Table 4: Qos on MQC Limitations

Supported on Cisco ASR 903	Cisco IOS XE 3.5S	Cisco IOS XE 3.6S	Cisco IOS XE 3.7S	Cisco IOS XE 3.8S	Cisco IOS XE 3.9S	Cisco IOS XE 3.10S
No. of unique policy-maps	1024					
No. of unique class-maps	4096					

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

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

Restrictions for Ingress QoS

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

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

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

Restrictions for Egress QoS

- The maximum number of classes supported on the policy map is 8, which includes class class-default; 7 user-defined classes and class class-default is supported.
- The maximum number of port-channel interfaces that can be created and supported for QoS on the router is 16.

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

- EC main interface

- Classification statistics for the policy-map on a port-channel main interface are *not* supported as no queues are allocated for a port-channel main interface.
- Policing and marking actions are only allowed in the policy-map on a port-channel main interface.
- Queuing actions are *not* supported.
- Egress TCAM entries are used even in the absence of member links.

- EC EVC/TEFP
  - Classification statistics for the policy-map on port-channel EVC/TEFP are *not* supported as no queues are allocated for port-channel EVC/TEFP.
  - Policing and marking actions are only allowed in the policy-map on port-channel EVC/TEFP.
  - Queuing actions are *not* supported.
  - Egress TCAM entries are used even if there are no member links present.

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

Restrictions of Ether Channel QoS

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

- Egress QoS policy-map is supported only on a member-link interface and not on a port-channel, port-channel EVC and port-channel TEFP.
- 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 RSP3 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.

Routed Port-Channel

Routed Port-channel Interface

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

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

Example for Routed Port-channel Interface

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

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

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

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

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

Member-links on Routed Port-channel Interface

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

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

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

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

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

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

Port-channel with EFP

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

- Marking
- Policing

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

Example for Port-channel with EFP

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

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

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

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

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

EFP of Port-channel with EFP Configuration

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

Note Match EFP is cannot be configured.

Member Links of Port-channel with EFP Configuration

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

Restrictions for Hierarchical Policies

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

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

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

Sample Hierarchical Policy Designs

The following are examples of supported policy-map configurations:

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

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

Sample Policy

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

Policy-map Vlan_set
```

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

Policy-map child1
Class prec2
Shape average percent 40

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

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

Ingress and Egress Hierarchical Policing

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

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

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

- Port and Class level

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

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

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

Dissimilar PHB Support for MPLS and VPLS Interfaces

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

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

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

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

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

Restrictions for Dissimilar PHB Support for MPLS and VPLS Interfaces

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

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

MPLS VPN QoS Mapping

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

Table 5: Default MPLS QoS Mapping

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

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

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
```

MPLS VPN QoS Mapping

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

Table 6: Default MPLS QoS Mapping

Feature	Imposition	Disposition
L3VPN, MPLS	IP Prec bit copied to MPLS Exp bit.	IP Prec bit is unchanged. If a VLAN tag is pushed at egress, CoS bit is set to 0.

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

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

QoS Policer and Shaper Calculation

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

Table 7: QoS Accounting Calculation

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

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

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

Service Groups

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

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

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

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

Restrictions for Service Groups

- Service groups is *not* supported on port and port-channels.
- Queuing and Marking on service group policy is *not* supported in Cisco IOS XE Release 3.11.
- Classification based on **match input vlan**, **match input interface**, and **match service instance** is *not* supported.
- Service group policies is **not** supported on EFPs configured on port channel.
- The same EFP *cannot* be configured as members of multiple service groups.
- If an EFP is a member of service group with a policy-map present in service group, the same policy-map *cannot* be applied on that EFP. The same policy-map applied on an EFP cannot be used in a service group.
- Limited support for statistics counters is provided.

- The **no policy-map** command cannot be executed for policies attached to service groups or to the policies attached to service instance which are configured as member of service groups.
- Policer percentage policy-maps are *not* supported on service groups.
- If dynamic modification is performed on the service-group policy or policy attached to EFP that is part of service-group, you have to exit of the policy-map sub-mode for the changes to take effect
- Service-group can have EFP members present across ports. If these ports are present across the ASIC in the router, then aggregate policing cannot work. For aggregate policing to work correctly, ports has to be present on same ASIC.
- QoS service groups for port channel sub-interface (BDI) is *not* supported.

Merging Service Groups and EFP Policies

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

Example

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

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

```
GigabitEthernet0/0/1: EFP 1
Service-policy input: ex
Class-map: phb (match-all)
2210042 packets, 3315063000 bytes
5 minute offered rate 82024000 bps, drop rate 77782000 bps
Match: cos 1
police:
cir 50000000 bps, bc 1562500 bytes
conformed 112980 packets, 169470000 bytes; actions:
transmit
exceeded 2097062 packets, 3145593000 bytes; actions:
drop
conformed 4191000 bps, exceeded 77782000 bps
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

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

Example

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

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

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

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

Restrictions for Merging Service Groups and EFP Policies

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

Creating a Service Group

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

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

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

Example:

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

(Optional) Creates a description of the service group.

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

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

Example:

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

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

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

Step 6 **end**

Example:

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

(Optional) Returns to privileged EXEC mode.

Adding Service Instance Members to the Service Group

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

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

    Note The interface module slot number is always 0.

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

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

Example:

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

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

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

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

Example:

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

Creates a service group.

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

Step 6 **exit**

Example:

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

(Optional) Returns to interface configuration mode.

Step 7 **end**

Example:

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

(Optional) Returns to privileged EXEC mode.

Deleting a Service Group

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

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

Example:

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

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

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

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

Step 4 **end**

Example:

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

(Optional) Returns to privileged EXEC mode.

Configuration Examples

- This example shows policing action on the service group:

```
policy-map qos-group-in
class cos1
police cir 64000
policy-map qos-group-out
class cos2
police cir 64000
policy-map qos-member-out1
class cos3
police cir 64000
policy-map qos-member-out2
class cos4
police cir 64000
```

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

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

Verifying the Service Group

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

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

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

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

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

```
Service Group 1
Service-policy input: co1
class-map: co1:
policy name co1, parent class , parent policy
conformed 54645 packets, 3497280 bytes
```

```
exceeded 3705853 packets, 237174592 bytes
violated 0 packets, 0 bytes
conformed 93000 bps, exceeded 6300000 bps
```

MPLS Diffserv Tunneling Modes Implementation

The MPLS specification defines three Diffserv operation modes:

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

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

Implementing Uniform Mode

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

Imposition

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

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

Tag-to-tag Transfer

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

Disposition

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

- Classify based on MPLS Exp bit on the ingress interface.
- Set the qos-group value.
- Classify based on qos-group on the egress interface.
- Mark the IP prec or DSCP bit.

Implementing Pipe Mode

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

Imposition

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

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

  Disposition

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

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

Implementing Short-Pipe Mode

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

Disposition

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

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

Classification

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

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

Table 8: QoS Classification Limitations

Main	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
Fea	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
Mat	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
acc	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
all	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
any	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
cla	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
cos	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
cos	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
dis	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
dsc	X	3.5	X	3.5	X	3.5	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
dsc	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
dsc	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1

Match	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
flow pdp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
flde	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
fldi	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ip dscp	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
ip (IPv4)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
ip (IPv6)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
ip rtp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
mpls	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
not	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
packet length	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
protocol (IPv4)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	3.13	3.7.1
protocol (IPv6)	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
protocol	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
qos-group	X	3.5	X	3.5	X	3.5	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.7.1	X	3.7.1
service instance dot1ad	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X

Match	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
source address	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
vlan	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
vlan inner	3.5	3.5	3.5	3.5	3.5	3.5	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X

Ingress Classification Limitations

The following limitations apply to QoS classification on the router:

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

Egress Classification Limitations

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

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

Traffic Classifying on MLPPP Interfaces

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

- **match discard-class**
- **match dscp**

- **match precedence**
- **match qos-group**

Release 3.13 introduces support for ingress QoS on MLPPP interfaces. The router supports the following **match** commands in a QoS class-map applied to a ingress MLPPP interface.

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

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

Classifying Traffic using an Access Control List

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

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

Limitations and Usage Guidelines

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

- QoS ACLs are supported only for IPv4 and IPv6 traffic
- IPv6 QoS ACLs are supported on the Cisco RSP1 Module starting from Release 3.16
- QoS ACLs are supported only for ingress traffic
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
  - TCP source and destination
  - UDP source and destination
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:
  - 1-99—IP standard access list
  - 100-199—IP extended access list
  - 1300-1999—IP standard access list (expanded range)
  - 2000-2699—IP extended access list (expanded range)

- You must create an ACL before referencing it within a QoS policy.
- Deny statements within an ACL are ignored for the purposes of classification.
- Classifying traffic based on TCP flags using an ACL is not supported.
- Classifying traffic using multiple mutually exclusive ACLs within a **match-all** class-map is not supported.
- Classifying traffic on a logical/physical level using an ACL is not supported.
- Applying QoS ACLs to MAC addresses is not supported.
- Port matching with the **neq** keyword is only supported for a single port.
- A given command can consume multiple matching operations if you specify a source and destination port, as shown in the following examples:
  - **permit tcp any lt 1000 any**—Uses one port matching operation
  - **permit tcp any lt 1000 any gt 2000**—Uses two port matching operations
  - **permit tcp any range 1000 2000 any 400 500**—Uses two port matching operations
- Only the following combination of matches are currently supported for Ingress policies:
  - Combination A: DSCP, Outer COS, UDP/TCP Source and Destination port number, IP SA/DA
  - Combination B: IP SA/DA, Outer COS, Inner COS, DSCP, MPLS EXP
  - Combination C: MAC DA, Outer COS, Inner COS, DSCP, MPLS Exp

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

For more information about configuring QoS, see http://www.cisco.com/en/US/products/ps11610/products_installation_and_configuration_guides_list.html. For more information about configuring access control lists, see the Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S (ASR 900 Series) .

Additional Classification Limitations

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

Configuring Multiple Match Statements

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

Exampe for IOS XE 3.5 Class Map

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

class-map match-any my-restrict-class_01
```

```
   match qos-group 2

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

match cos 3

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

Example for IOS XE 3.6 Class Map

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

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

Traffic Classification Using Match EFP Service Instance Feature

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

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

Restrictions for Configuring Match Service Instances

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

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

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

Example for Configuring Match Service Instances

```
interface GigabitEthernet0/3/4
 no ip address
 negotiation auto
```

```
 service-policy output BTS_Total
 service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
 !
 service instance trunk 20 ethernet
  encapsulation dot1q 20-29
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
 service instance 30 ethernet
  encapsulation dot1q 30
  xconnect 192.44.32.21 101 encapsulation mpls


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

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

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

class-map VOICE
match qos-group 0

class-map SIGNALING
match qos-group 1

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

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


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

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

QoS Marking

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

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

Table 9: Marking QoS Limitations

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
set	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E	I	E
atm-clp	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
cos	3.5	3.6	3.5	3.6	35.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
cos inner	3.5	3.6	3.5	3.6	35.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	X	X	X	X	X	X	X
dscp-dscp-class	X	3.6	X	3.6	X	3.6	X	3.9	X	3.9	X	3.5	X	3.9	X	3.9	X	3.9	X	3.9	3.13	37.1
dscp	3.6	3.6	3.6	3.6	3.6	3.6	3.9	3.9	3.9	3.9	3.6	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	37.1
dscp-transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	X	X
ip dscp	3.5	3.6	3.5	3.6	35.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	37.1
ip precedence	3.5	3.6	3.5	3.6	35.1	3.6	3.9	3.9	3.9	3.9	3.5	3.5	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	37.1
mpls experimental																						

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

Overview of Marking

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

- **set cos**
- **set discard-class**
- **set dscp**

- **set precedence**
- **set ip dscp**
- **set ip precedence**
- **set mpls experimental imposition** (ingress marking)
- **set mpls experimental topmost**
- **set qos-group**

CoS Marking Limitations

The following limitations apply when configuring CoS marking:

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

Ingress Marking Limitations

The following limitations apply to QoS marking on the router:

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

Egress Marking Limitations

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

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

CoS Marking for Pseudowires

The Outer-CoS set in the transport VLAN of the MPLS PW packet, egressing the NNI based on the incoming CoS of the packet coming in on the UNI. With the existing support, a per-EFP or interface QoS policy is applied on the pseudowire originating on the cross-connect on the incoming UNI, to mark the MPLS EXP

imposition using the per-EFP or interface policy. By supporting a default EXP to CoS mapping for all pseudowire (L2VPN), the traffic in the transport L2 ring gets the same priority as the ingress policy in the MPLS network.

- The default marking of COS from EXP imposition impacts all the pseudowires initiating from the router which are configured with EXP marking policy, that is, the policy to mark imposition EXP marks COS as well.
- Egress set cos using egress policy overwrites the S-COS.
- If the topmost EXP is changed through ingress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.
- If the topmost EXP is changed through egress marking, the modified EXP is propagated to the egress outer S-COS. Egress set cos can overwrite S-COS.
- The implicit mapping of this EXP to MPLS transport VLAN COS is *not*supported. This is applicable only for L2VPN traffic for which the EXP value is derived from the user configured policy.

Example

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

Topology

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

PE1 Router

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255

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

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

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

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

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

```
policy-map egress
class cos4

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

Verifying PE 1 Router

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

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

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

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

P router

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

policy-map ingress
class cos4

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

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

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

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

policy-map egress
class exp4

interface GigabitEthernet 0/7
ip address 30.0.0.2 255.255.255.0
```

```
media-type rj45
mpls ip
mpls label protocol ldp
service-policy output egress
```

Verifying P Router

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

Service-policy input: ingress
Target association type: DEFAULT
Class-map: cos4 (match-all)
2000 packets, 188000 bytes
30 second offered rate 6000 bps
Match: cos 4
Class-map: class-default (match-any)
181 packets, 13992 bytes
30 second offered rate 1000 bps, drop rate 0000 bps
Match: any

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

PE 2 Router

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

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

policy-map ingress
class exp4

policy-map egress
class cos3

interface Loopback0
ip address 2.2.2.2 255.255.255.255

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

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

interface GigabitEthernet 0/1
load-interval 30
media-type rj45
service-policy output egress
```

```
service instance 2 ethernet
encapsulation dot1q 2
xconnect 1.1.1.1 10 encapsulation mpls
```

Verifying PE2 Route

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

Service-policy input: ingress
Target association type: DEFAULT
Class-map: exp4 (match-all)
2000 packets, 172000 bytes
5 minute offered rate 0000 bps
Match: mpls experimental topmost 4
Class-map: class-default (match-any)
47 packets, 4222 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

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

CoS Marking for CPU generated Traffic

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

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

Limitation of CoS marking for CPU generated traffic

- Maximum of 8 configuration lines can be supported. Beyond that you need to delete any configuration and apply the new configuration
- The command can be used for classifying multiple IP addresses under a single VLAN ID.
- 8 qos entries will be reserved for use during bootup.
- DEI region for dropping the packet is first 8 entries and after that cos marking entries are programmed in the qos region of TCAM. If CoS marking entries are conflicting with the dei entries, then the packets will be dropped as dei entries have higher priority.
- The packets will go through the high priority queue of the interface
- For double tagged packets, only the outer CoS will be marked in case of ICMP echo reply packets.
- If other control protocols have the same IP and vlanId as is configured for the cos marking scenario, then those packets will also be marked. So you need to be aware of the IP address and VLAN ID while configuring cos marking.

- Initial TFTP/FTP packets can only be cos-marked having RRQ/WRQ with TFTP destination port.
- Use **platform acl drop-dei-1-packets** command to filter DOT1Q and DOT1AD packets marked with CFI/DEI bits. The feature only matches the outermost tag and the matching on the inner tag is not supported.

Supported Protocols

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

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

Configuration Example

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

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

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

interface BDI4083
ip address 172.24.244.37 255.255.255.224

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

Traffic Marking on MLPPP Interfaces

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

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

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

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

IPv6 Traffic Marking

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

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

For more information about IPv6 QoS, see:

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

Additional Marking Limitations

The following additional marking usage guidelines apply in Release 3.9:

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

Traffic Policing

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

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

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

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

Policing QoS Limitations

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

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

Features	Main Layer 3 Interface		EFP Interface		Trunk EFP		L3 Ether-channel		L2 Port Channel		L3 Port Channel Member		L2 Port Channel Member		OC-3		OC-12		T1/E1		MLPPP	
set-dscp-transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-prec-transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-dscp-qos-group-transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
set-mpls-experimental-topmost-transmit	3.5	3.6	3.5	3.6	35.1	3.6	3.9	3.9	3.9	3.9	3.5	3.6	3.9	3.9	X	3.9	X	3.9	X	3.9	3.13	3.9
set-mpls-experimental-imposition-transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	X	X	X	X	X	3.13	X
transmit	3.5	X	3.5	X	35.1	X	3.9	X	3.9	X	3.5	X	3.9	X	X	3.9	X	3.9	X	3.9	3.13	X

Supported Commands

The router supports the following policing commands on ingress interfaces:

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

The router supports the following queuing commands:

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

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

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

Supported Actions

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

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

Percentage Policing Configuration

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

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

Ingress Policing Limitations

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

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

Egress Policing Limitations

IOS XE Release 3.6 introduces support for egress policing. The router supports the **bandwidth** and **bandwidth-remaining** commands on egress interfaces under the following conditions:

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

  The following is a sample supported configuration:

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

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

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

  The following is a sample supported configuration:

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

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

  The following is a sample supported configuration:

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

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

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

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

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

Sample example displaying the error message:

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

- **Egress Policing on Non Priority Queue**

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

Sample configuration:

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

Traffic Policing on MLPPP Interfaces

Release 3.13 introduces support for egress QoS on MLPPP interfaces. 1R2C color-blind policer is supported for egress QoS on MLPPP interfaces.

Release 3.13 introduces support for ingress QoS on MLPPP interfaces. The router supports the following parameters with the **set** command on the ingress MLPPP interfaces:

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

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

Traffic Shaping

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

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

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

Table 10: Shaping Limitations by Interface

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

Additional Shaping Limitations

The following additional shaping usage guidelines apply from Release 3.9:

- Policies using shaping are supported only on individual member links of an etherchannel. Applying a shaping policy directly on an etherchannel interface is not supported.
- Class-based shaping is supported at all levels.
- On the RSP1 module, shaping policy drops UDP traffic at 50% of the configured value, at egress.

Configuring Egress Shaping on EFP Interfaces

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

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

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

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

Congestion Management

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

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

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

Table 11: Congestion Management QoS Limitations

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

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

Ingress Queuing Limitations

The router does not support queuing on ingress interfaces.

Egress Queuing Limitations

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

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

Support for Queuing Features on MLPPP Interfaces

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

- Tail drop queuing uses the **queue-limit** command.
- 3-level policies are *not* supported on MLPPP interfaces.

Support for Low Latency Queuing on Multiple EFPs

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

Additional Queuing Limitations

The following additional queuing usage guidelines apply in Release 3.9:

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

Congestion Avoidance

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

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

Table 12: Congestion Avoidance QoS Limitations

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

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

Congestion Avoidance Configuration

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

Supported Commands

The router supports the following commands for WRED:

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

Supported Interfaces

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

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

Verifying the Configuration

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

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

- 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 Cisco ASR 903 Series Router:

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

- Fair-queue is *not* supported. You can configure WRED with either the **shape** or the **fair-queue** (CBWFQ) commands.
- The default value for **exponential-weighting-constant** is 9.
- The default value for **mark-probability** is 10.
- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.

Egress Congestion Avoidance on MLPPP Interfaces

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

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

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

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

Additional Congestion Avoidance Limitations

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

Verifying the Configuration

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

For more information about configuring congestion avoidance, see 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.
- You can not configure **priority** value and a policer in the same class.

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

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

Egress Scheduling on MLPPP Interfaces

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

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

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

```
  shape average 2000000
!
```

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

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