

Cisco Catalyst 3750 QoS Configuration Examples

Document ID: 91862

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

QoS Overview

- Cisco Catalyst 3750 Switch without QoS
- Cisco Catalyst 3750 Switch QoS Features

Ingress QoS Features

- Default Ingress QoS Configuration
- Classification and Marking
- Policing
- Congestion Management and Avoidance

Egress QoS Features

- Egress QoS Commands
- Default Configuration
- Queuing, Dropping and Scheduling

Related Information

Introduction

Cisco Catalyst 3750 Switches support various QoS features such as classification, marking, policing, queueing and scheduling. This document explains these QoS features with configuration examples.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Configuring QoS.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 3750 Switch – WS-C3750-24TS
- Cisco IOS® Software Release 12.2(35)SE2

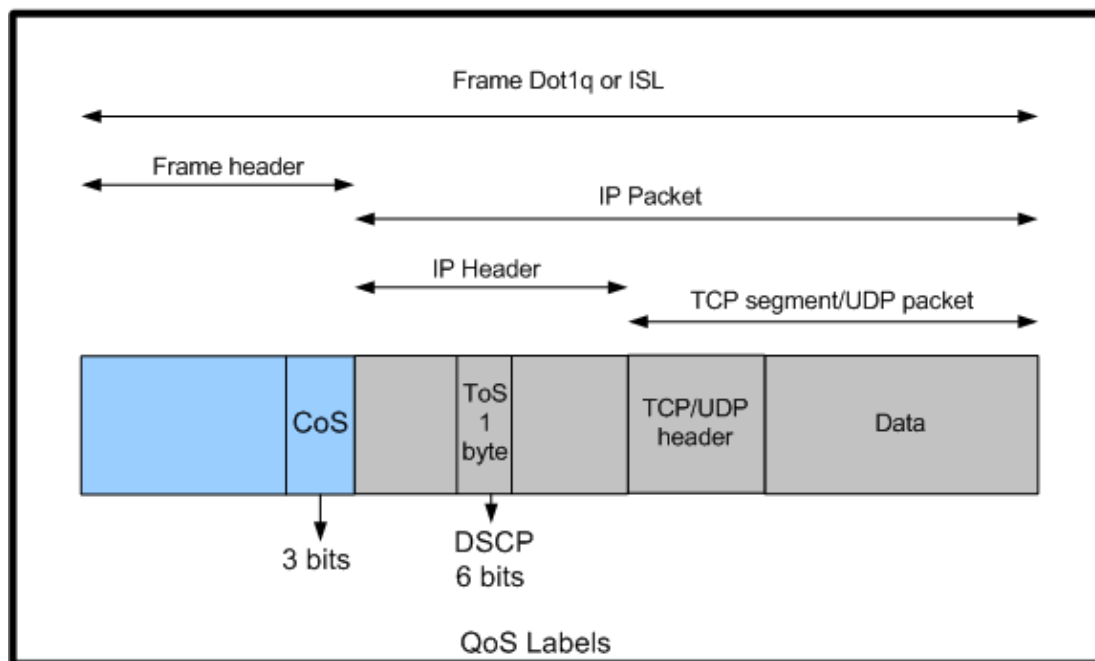
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

QoS Overview

With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. You can differentiate the traffic using QoS labels. The two most commonly used QoS labels in the Layer 3 IP header are the IP precedence field and the DSCP field. The QoS label in the Layer 2 frame header is called Class of Service (CoS). Catalyst switch QoS tools can provide the preferential treatment based on either Layer 3 QoS labels or Layer 2 QoS labels. This document provides various examples that can give you an idea of the Layer 2 and Layer 3 QoS labels usage in Cisco Catalyst switches.



Cisco Catalyst 3750 Switch without QoS

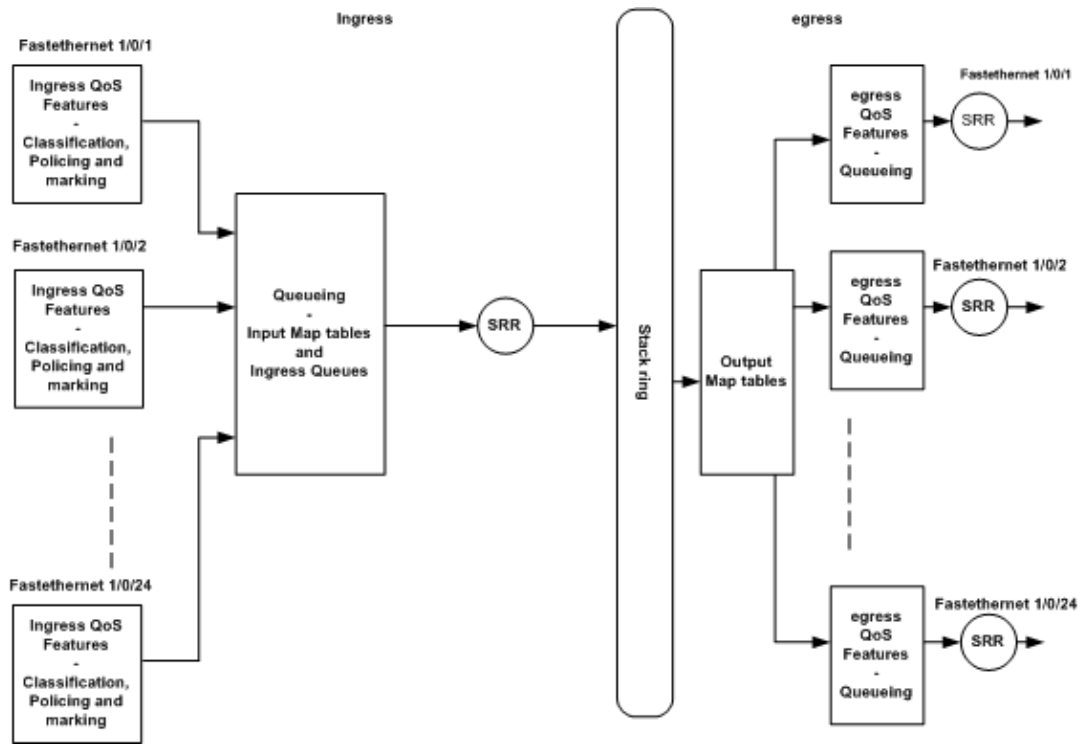
QoS is disabled by default on the Catalyst 3750 Switches. While QoS is disabled, all frames/packets are passed-through the switch unaltered. For example, if a frame with CoS 5 and the packet inside the frame with DSCP EF enters the switch, the CoS and DSCP labels are not changed. The traffic leaves with the same CoS and DSCP values as it enters. All the traffic, which includes voice, are delivered on the best effort basis.

```
Switch#show mls qos
QoS is disabled
QoS ip packet dscp rewrite is enabled
```

*!--- Even then it says QoS ip packet dscp rewrite is enabled,
!--- the switch does not alter the DSCP label on the packets when the QoS is disabled.*

Cisco Catalyst 3750 Switch QoS Features

After the QoS is enabled on the 3750 Switch, there are few ingress and egress QoS features enabled by default. This diagram shows the high level view of the QoS architecture of the switch:



This is a summary of points based on the diagram:

- Ingress QoS features such as classification, marking and policing can be configured per port basis.
- Input map tables and ingress queueing can be configured globally. These cannot be configured per port basis.
- SRR for ingress queue can be configured globally.
- Stack ring bandwidth depends on the stack cabling. If the stack is connected at full bandwidth, you receive 32Gbps bandwidth. This bandwidth is shared by all the switches in the stack.
- Output map tables and egress queues are configured globally. You can have two sets of queue configurations and you can apply any one of the queue set configurations to a port.
- SRR for egress queue can be configured on per port basis.

Ingress QoS Features

This section explains the concepts of various possible ingress QoS configurations. This section covers these topics:

- Default Ingress QoS Configuration
- Classification and Marking
- Policing
- Congestion Management and Avoidance

Default Ingress QoS Configuration

This is how the switch treats frames by default after the QoS is enabled:

- A frame enters the switch port and it does not have the frame tagged (it means the port is access port and the frame enters the switch does not have ISL or dot1q encapsulation).
- The switch encapsulates the frame with the dot1q (ignore ISL because dot1q is the default on all the new switches).
- Inside the dot1q frame tag, there are three bits called 802.1p priority bits available which are also

called CoS. These bits are set to 0.

- Then, the switch calculates DSCP value based on the CoS–DSCP map table. As per the table, the switch sets the DSCP value to 0. DSCP value is located at the IP header of the packet.

In summary, the CoS and DSCP values of the frame enter the switch set to 0 by default if the QoS is enabled on the switch.

Classification and Marking

Unlike the routers, the QoS classification and marking act differently in Cisco Catalyst switches. In Cisco routers, you can classify the packets using MQC either based on the incoming packet DSCP value or based on the access control list (ACL). This depends on whether you trust the QoS label of the incoming packet or not. In the Cisco Catalyst 3750 Switch, you can classify the frames either based on the incoming CoS/DSCP values or based on the ACL.

The configuration based on the incoming CoS/DSCP value is achieved in three different ways:

- Port based configuration using the **mls qos** interface based commands
- MQC based configuration using class–map and policy–map
- VLAN based configuration

You can use either one of these three methods. You cannot use more than one method in a port. For example, you have configured the **mls qos trust cos** command on a port. When you configure the port with the **service–policy input** *<policy–map–name>* command, it removes the **mls qos trust cos** command automatically.

The Classification and Marking – Port Based section explains the port based configuration.

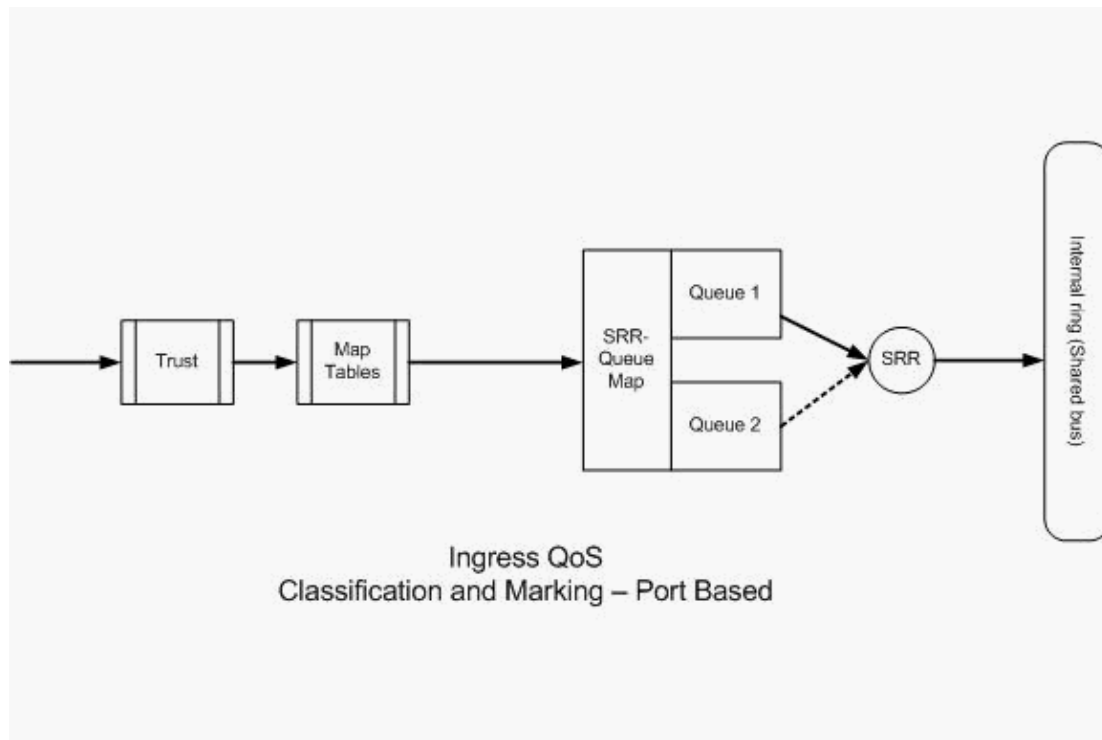
The Classification and Marking – MQC Based section explains the MQC based classification.

Classification and Marking – Port Based

This section explains the classification based on the interface specific configuration. A question can arise with the section title classification and marking. This is because in the Cisco Catalyst 3750 Switch, CoS or DSCP values of the frames (packet inside the frame) are remarked using the map tables. Map tables are not available in Cisco routers. These are available only in the Cisco Catalyst switches. You will see the functionality of these tables throughout this section.

This section discusses these two configurations:

- Classification – Port Trust Configuration
- Marking – QoS Map Tables Configuration



Classification – Port Trust Configuration

An incoming packet or frame can already have a QoS label assigned. These questions can arise:

- Do you trust the QoS label of the incoming packet/frame on a port?
- If an IP phone and PC are connected to a port, do you trust QoS labels of the phone, PC or both?

If you do not trust the QoS labels of the incoming packet/frame, you need to classify the packet based on an access-list and mark QoS label. If you trust the QoS labels of the incoming packet/frame, another question is do you need to trust the CoS value or DSCP value of the incoming packet/frame on a port? This depends on the scenario. You can see the different scenarios with examples in this section.

The port trust configuration options are:

```
Switch(config-if)#mls qos trust ?
cos                cos keyword
device            trusted device class
dscp              dscp keyword
ip-precedence     ip-precedence keyword
<cr>
```

- **Example 1:** If the port is an access port or Layer 3 port, you need to configure the **mls qos trust dscp** command. You cannot use the **mls qos trust cos** command because the frame from the access port or Layer 3 port does not contain dot1q or ISL tag. CoS bits are present in the dot1q or ISL frame only.

```
interface GigabitEthernet1/0/1
description **** Layer 3 Port ****
no switchport
ip address 192.168.10.1 255.255.255.0
mls qos trust dscp
end

interface GigabitEthernet1/0/2
description **** Access Port ****
switchport access vlan 10
```

```

switchport mode access
mls qos trust dscp
end

```

- **Example 2:** If the port is trunk port, you can configure either the **mls qos trust cos** or **mls qos trust dscp** command. The dscp–cos map table is used to calculate the CoS value if the port is configured to trust DSCP. Similarly, the cos–dscp map table is used to calculate the DSCP value if the port is configured to trust CoS.

```

interface GigabitEthernet1/0/3
description **** Trunk Port ****
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 5
switchport trunk allowed vlan 5,10,20,30,40,50
mls qos trust cos
end

```

```

interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
spanning-tree portfast
end

```

!--- The Cisco IP Phone uses IEEE 802.1Q frames for Voice VLAN traffic.

- **Example 3:** If the port is a dot1q trunk port and the port is configured with the **mls qos trust cos** command, native VLAN frames will have CoS and DSCP values as 0. Because native VLAN frames are untagged and the frame is tagged after it enters the switch, the switch will set the default CoS value to 0 and the CoS–to–DSCP table sets the DSCP value to 0.

Note: The DSCP value of the packet coming from native VLAN will be reset to 0.

You can also configure the switch port to change the default CoS value of the untagged frames from 0 to any other values between 0–7 using the **mls qos cos<0–7>** command. This command does not change the CoS values of the tagged frames.

For example, the port GigabitEthernet1/0/12 is configured with access VLAN 10 and voice VLAN 20.

```

interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
spanning-tree portfast

```

*!--- The Cisco IP Phone uses IEEE 802.1Q frames for Voice VLAN traffic.
!--- Voice VLAN is only supported on access ports and not on trunk ports,
!--- even though the configuration is allowed.*

```

end

```

By default, the PC sends data untagged. Untagged traffic from the device attached to the Cisco IP Phone passes through the phone unchanged, regardless of the trust state of the access port on the phone. The phone sends dot1q tagged frames with voice VLAN ID 20. Therefore, if you configure the port with the **mls qos trust cos** command, it trusts the CoS values of the frames from the phone

(tagged frames) and sets the CoS value of the frames (untagged) from the PC to 0. After that, the CoS–DSCP map table sets the DSCP value of the packet inside the frame to 0 because the CoS–DSCP map table has DSCP value 0 for the CoS value 0. If the packets from the PC have any specific DSCP value, that value will be reset to 0. If you configure the **mls qos cos 3** command on the port, it sets the CoS value of all the frames from the PC to 3 and does not alter the CoS value of the frames from the phone.

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
mls qos cos 3
spanning-tree portfast
end
```

If you configure the port with the **mls qos cos 3 override** command, it sets the CoS values of all the frames (both the tagged and untagged) to 3. It overrides the previously configured trust values.

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
mls qos cos 3 override

!--- Overrides the mls qos trust cos.

!--- Applies CoS value 3 on all the incoming packets on both the vlan 10 and 20.

spanning-tree portfast
end
```

- **Example 4:** For example, take a look at the port gi 1/0/12 configuration:

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
spanning-tree portfast
end
```

If the PC tags its frame with the VLAN 20, it also sets the CoS value to 5. The switch processes tagged data traffic (traffic in IEEE 802.1Q or IEEE 802.1p frame types) from the device attached to the access port on the Cisco IP Phone. Because the interface is configured to trust the CoS value, all traffic received through the access port on the Cisco IP Phone passes through the phone unchanged. The switch also trusts and allows the traffic from the PC, and gives the same priority as the IP phone traffic. This is not a desirable result you want to see. This can be avoided using the **switchport priority extend cos <cos-value>** command.

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
switchport priority extend cos 0
```

```
!--- Overrides the CoS value of PC traffic to 0.
```

```
spanning-tree portfast  
end
```

The **switchport priority extend cos <cos-value>** command configures the phone such that the IP phone changes the CoS value of the PC traffic to 0.

- **Example 5:** For example, in the same interface, someone connects the PC directly to the switch and tags the PC data with dot1q frame with a higher CoS value. This can be avoided using the **mls qos trust device cisco-phone** command.

```
interface GigabitEthernet1/0/12  
description **** Cisco IP Phone ****  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust cos  
switchport priority extend cos 0  
mls qos trust device cisco-phone
```

```
!--- Specify that the Cisco IP Phone is a trusted device.
```

```
spanning-tree portfast  
end
```

- **Example 6:** For example, in the interface GigabitEthernet1/0/12, you have to trust the QoS labels from the PC. Also, the PC is connected to the native VLAN 10. In this case, the **mls qos trust cos** command does not help because the PC packet does not tag the CoS value. It is going to tag only the DSCP value. Therefore, the switch adds the dot1q frame and configures the default CoS value to 0. Then, the CoS–DSCP table calculates and resets the DSCP value to 0.

In order to fix this problem, you have two choices. One is to configure classification and marking using MQC. You can create an ACL to match your PC traffic based on source, destination IP addresses, and source/destination port numbers. Then, you can match this ACL in class-map. You can create a policy-map to trust this traffic. This solution is discussed in the next section. This section discusses the second method. The second method is to trust the DSCP label instead of the CoS label. Then the DSCP–CoS label calculates and sets the CoS value that corresponds to the DSCP value.

```
interface GigabitEthernet1/0/12  
description **** Cisco IP Phone ****  
switchport access vlan 10  
switchport mode access  
switchport voice vlan 20  
mls qos trust dscp  
spanning-tree portfast  
end
```

The first method is the preferred one because it is not recommended to trust all the PC traffic's QoS labels.

Marking – QoS Map Tables Configuration

After the QoS is enabled, the map tables are created with the default values and are enabled.

```
Distribution1#show mls qos maps cos-dscp  
Cos-dscp map:  
cos:    0  1  2  3  4  5  6  7  
-----  
dscp:   0  8 16 24 32 40 48 56
```

```
Distribution1#show mls qos maps dscp-cos
Dscp-cos map:
dl :  d2 0  1  2  3  4  5  6  7  8  9
-----
0 :    00 00 00 00 00 00 00 00 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07
```

- **Example 1:** If the port is configured to trust CoS, all the incoming CoS values are trusted and the DSCP values are remarked based on the CoS–DSCP table. As per the default CoS–DSCP configuration, the values are mapped as shown here:

CoS	DSCP (decimal)	DSCP
0	0	Default
1	8	CS1
2	16	CS2
3	24	CS3
4	32	CS4
5	40	CS5
6	48	CS6
7	56	CS7

One important value you need to note here is the DSCP value corresponds to CoS value 5. It is CS5. Example 2 talks about this value.

- **Example 2:** For example, the interface GigabitEthernet1/0/12 is configured to trust CoS.

```
interface GigabitEthernet1/0/12
description **** Cisco IP Phone ****
switchport access vlan 10
switchport mode access
switchport voice vlan 20
mls qos trust cos
spanning-tree portfast
end
```

The Cisco IP Phone marks the voice payload with CoS 5 and DSCP EF when it sends the traffic to the switch. When the traffic enters the port Gi 1/0/12, the switch trusts the CoS value. Then, the switch derives the DSCP value CS5 (40) for the CoS value 5 from the CoS–DSCP table. All the voice payloads with CoS 5 are marked with the DSCP value CS5. This is not the desirable value. The required DSCP value for the voice payload is DSCP EF. By default, the other CoS values to DSCP values are mapped correctly as per the RFCs.

This configuration helps you to configure the CoS–DSCP map table to change the DSCP value EF that corresponds to CoS 5.

```
Distribution1(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
!--- DSCP 46 is EF
```

After this configuration, the values are mapped as shown here:

CoS	DSCP (decimal)	DSCP
0	0	Default
1	8	CS1
2	16	CS2
3	24	CS3
4	32	CS4
5	46	EF
6	48	CS6
7	56	CS7

- **Example 3:** If the port is configured to trust DSCP, all the incoming DSCP values are trusted and the CoS values are remarked based on the DSCP–CoS table. As per the default DSCP–CoS configuration, the values are mapped as shown here:

DSCP	DSCP (decimal)	CoS
Default	0–7	0
CS1		
AF11		
AF12		
AF13	8–15	1
CS2		
AF21		
AF22		
AF23	16–23	2
CS3		
AF31		
AF32		
AF33	24–31	3
CS4		
AF41		
AF42		
AF43	32–39	4
CS5	40–47	5

EF		
CS6	48-55	6
CS7	56-63	7

You do not need to change these default values.

This table summarizes the DSCP values and CoS values just for reference:

DSCP (Decimal)	DSCP	CoS
0	Default	0
8	CS1	1
10	AF11	1
12	AF12	1
14	AF13	1
16	CS2	2
18	AF21	2
20	AF22	2
22	AF23	2
24	CS3	3
26	AF31	3
28	AF32	3
30	AF33	3
32	CS4	4
34	AF41	4
36	AF42	4
38	AF43	4
40	CS5	5
42		5
44		5
46	EF	5
48	CS6	6

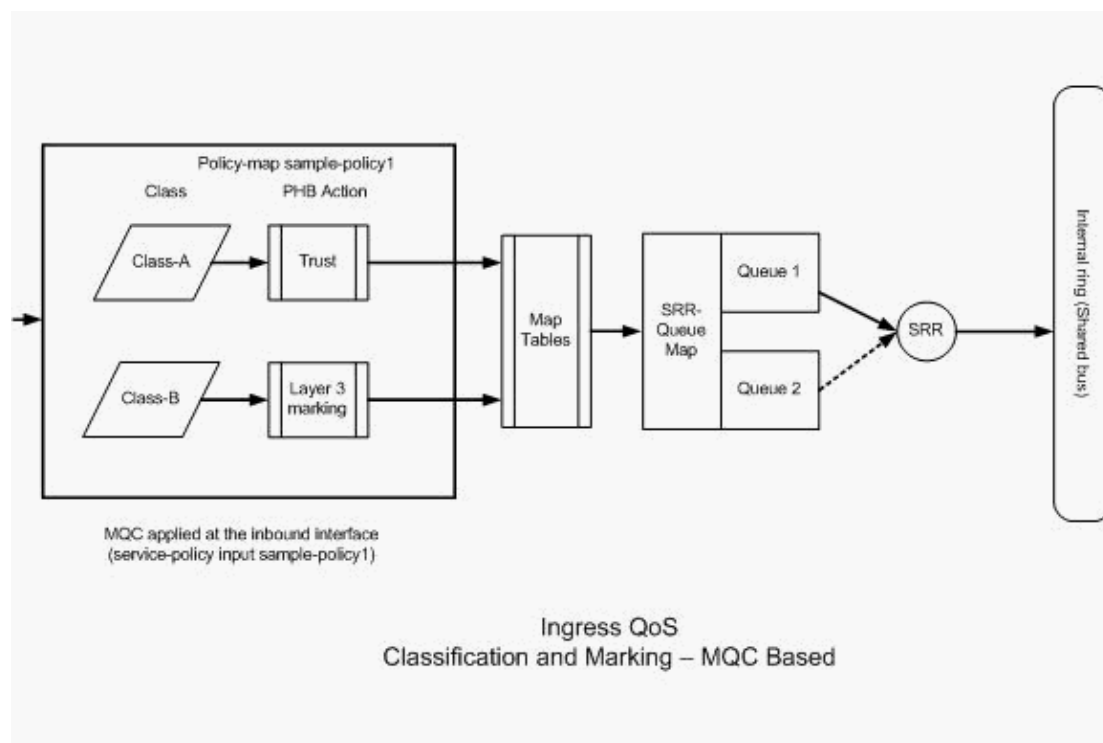
Note: In a network, all the Cisco Catalyst switches should have identical map tables. Different map table values in different switches cause undesirable QoS behavior.

Classification and Marking – MQC Based

As explained in the Classification and Marking section, you can use MQC to classify and mark the packet. You can use MQC instead of the port specific configuration. You can also mark the incoming packets with the policy-map.

The requirements of this example are:

- Trust the CoS values of the IP phone traffic.
- Mark DSCP value of the softphone application packets from the PC which is connected the IP phone.
- Untrust all other traffic from the PC.



This diagram shows that a policy-map is attached to the input of an interface. You cannot apply a policy-map to the output of any interfaces in the Catalyst 3750 Switch. The next configuration represents the diagram. This section does not focus on the queuing portion of the QoS feature. The section just focuses on the MQC applied on the interface.

It is assumed the the data VLAN is 10 and its subnet address is 172.16.10.0/24. The voice VLAN is 100 and its subnet address is 192.168.100.0/24.

!--- Section A

```
Distribution1(config)#ip access-list extended voice-traffic
Distribution1(config-std-nacl)#permit ip 192.168.100.0 0.0.0.255 any

Distribution1(config-std-nacl)#ip access-list extended database-application
Distribution1(config-ext-nacl)#permit tcp any any eq 1521
```

```

Distribution1(config-ext-nacl)#permit tcp any any eq 1810
Distribution1(config-ext-nacl)#permit tcp any any eq 2481
Distribution1(config-ext-nacl)#permit tcp any any eq 7778
Distribution1(config-ext-nacl)#exit

Distribution1(config)#class-map Class-A
Distribution1(config-cmap)#match access-group name voice-traffic
Distribution1(config-cmap)#exit
Distribution1(config)#class-map Class-B
Distribution1(config-cmap)#match access-group name database-application
Distribution1(config-cmap)#exit

!--- Section B

Distribution1(config)#policy-map sample-policy1
Distribution1(config-pmap)#class Class-A
Distribution1(config-pmap-c)#trust cos
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#class Class-B
Distribution1(config-pmap-c)#set dscp af21
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#exit

!--- Section C

Distribution1(config)#interface gigabitEthernet 1/0/13
Distribution1(config-if)#switchport access vlan 10
Distribution1(config-if)#switchport mode access
Distribution1(config-if)#switchport voice vlan 100
Distribution1(config-if)#spanning-tree portfast
Distribution1(config-if)#service-policy input sample-policy1
Distribution1(config-if)#exit

```

Section A:

- Classifies the IP phone traffic to Class-A. The IP phone belongs to voice VLAN and has an IP address in the 192.168.100.0 subnet.
- Classifies the database application traffic to Class-B. The PC traffic (actually any traffic as per the configuration) destined to any destination with the port numbers 1521, 1810, 2481, 7778 are classified into the Class-B class map.

Section B:

- The traffic matches Class-A are configured to trust the CoS label. This means the CoS values of all the traffic from the IP phone are trusted. As it is shown in the diagram, the DSCP value is derived from the CoS-DSCP map table for the Class-A traffic.
- The traffic matches Class-B are configured to set the DSCP value to AF21. As it is shown in the diagram, the DCoS value is derived from the DSCP-CoS map table for the Class-B traffic.
- The configurations under each class of policy-map are called PHB actions. Marking, queuing, policing, shaping, and congestion avoidance are the supported PHB actions in Cisco routers. Marking and policing are the only supported PHB actions in the Cisco Catalyst 3750 Switch.

```

Distribution1(config)#policy-map test
Distribution1(config-pmap)#class test
Distribution1(config-pmap-c)#?
QoS policy-map class configuration commands:
  exit          Exit from QoS class action configuration mode
  no            Negate or set default values of a command
  police       Police
  service-policy  Configure QoS Service Policy

```

```

set          Set QoS values
trust       Set trust value for the class
<cr>

```

The **set** and **trust** commands are **Marking** PHB actions. You can configure either **set** or **trust** PHB action. You cannot configure both the actions in one class of policy-map. However, you can configure **set** in one class and **trust** in another class in the same policy-map.

The **police** command is the **Policing** PHB action. This is discussed in detail in the next section.

Shaping is not supported in the Cisco Catalyst 3750 Switch. Queuing and congestion avoidance are supported in the Cisco Catalyst 3750 Switch, but are not configurable using MQC. Queuing and congestion avoidance configurations are discussed in detail later in this document.

Section C:

- The policy-map can be applied only to the input on the interface. When you apply to the output interface, you receive this error message:

```

Distribution1(config)#int gi 1/0/3
Distribution1(config-if)#service-policy output test
Warning: Assigning a policy map to the output side of an interface not supported

Service Policy attachment failed
Warning: Assigning a policy map to the output side of an interface not supported

```

- If any other QoS Classification methods, such as port based or VLAN based, are configured on the port gi 1/0/3, those configurations are removed when you apply the policy-map. For example, the port Gi 1/0/13 is configured to trust CoS as shown here:

```

interface GigabitEthernet1/0/13
description **** Access Port ****
switchport access vlan 10
switchport mode access
switchport voice vlan 100
mls qos cos 3
mls qos trust cos
spanning-tree portfast

```

- When you apply the policy-map to the interface, it removes the **trust** command.

```

Distribution1(config)#int gi 1/0/13
Distribution1(config-if)#service-policy input sample-policy1
Distribution1(config-if)#do show run int gi 1/0/13
Building configuration...

```

```

Current configuration : 228 bytes
!
interface GigabitEthernet1/0/13
description **** Access Port ****
switchport access vlan 10
switchport mode access
switchport voice vlan 100
service-policy input sample-policy1

```

```

!--- It replaces the mls qos trust or mls qos
!--- vlan-based command.

```

```

mls qos cos 3

```

```

!--- This command is not removed.

```

```

spanning-tree portfast

```

end

You can see the `service-policy input` replaces only the `mls qos trust` or `mls qos vlan-based` command. It does not change the other commands, such as the `mls qos cos` or `mls qos dscp-mutation` commands. In summary, it replaces the QoS classification command and does not replace the QoS marking commands.

- In the policy-map, you see only two class-maps. Class-A matches the IP phone traffic and Class-B matches the database application traffic from the PC. All other PC traffic (except database application defined in the access-list) is classified under the class-default class of the policy-map. This is a catch-all traffic which catches the traffic that does not match the defined class-maps attached to the policy-map. Therefore, this traffic that belongs to the class-default is not trusted by the port, and those packets are set with the default CoS and DSCP labels as 0. You can configure to set any default CoS or DSCP value to this class-default traffic.

You can set the default DSCP value using MQC. The CoS value is derived from the DSCP-CoS map table.

```
Distribution1(config)#policy-map sample-policy1
Distribution1(config-pmap)#class class-default
Distribution1(config-pmap-c)#set dscp af13
Distribution1(config-pmap-c)#exit
```

You can set the default CoS value as shown here. The DSCP value is derived from the CoS-DSCP map table.

```
Distribution1(config)#int gi 1/0/13
Distribution1(config-if)#mls qos cos 3
Distribution1(config-if)#do show run int gi 1/0/13
Building configuration...
```

```
Current configuration : 228 bytes
!
interface GigabitEthernet1/0/13
 description **** Access Port ****
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
 service-policy input sample-policy1
 mls qos cos 3
 spanning-tree portfast
```

Policing

On the Cisco Catalyst 3750 Switch, policing can only be configured on the ingress port. Policing can only be configured through MQC. This means there is no interface specific command to police the traffic. You can configure policing in the policy-map and you can apply the policy-map using only the `service-policy input` `<policy-name>` command. You cannot apply any policy-map to the output side of an interface.

```
Distribution1(config-if)#service-policy output test
police command is not supported for this interface
Configuration failed!
Warning: Assigning a policy map to the output side of an interface not supported
```

This section discusses these topics:

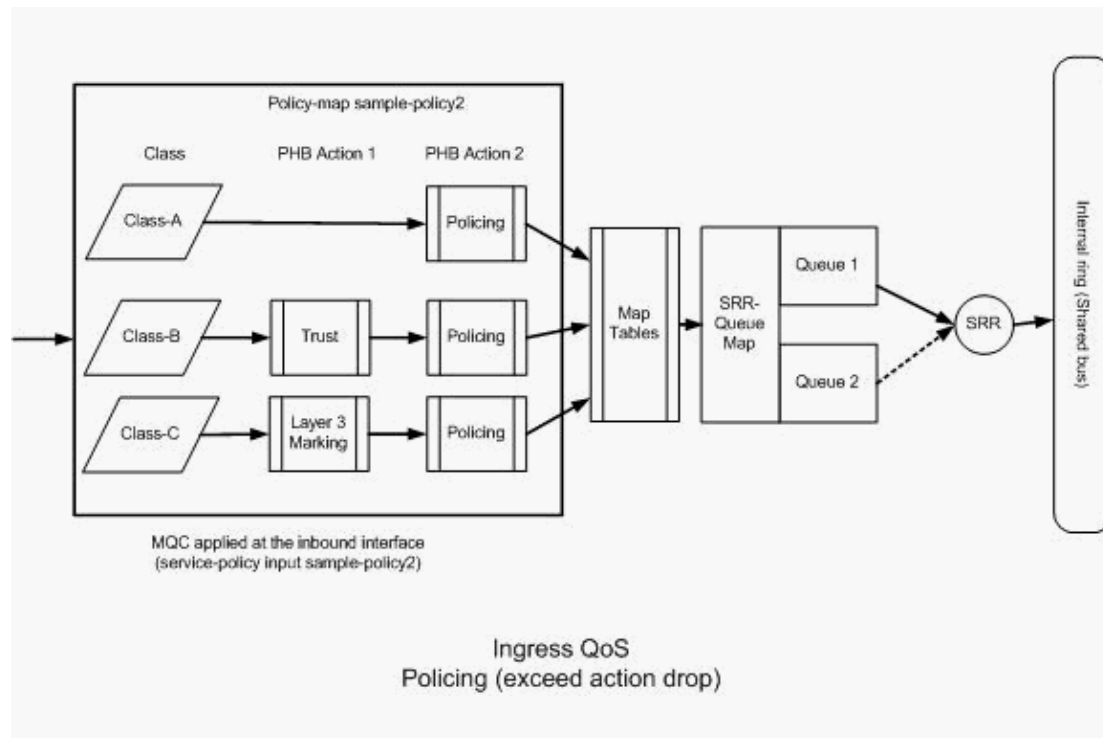
- Classification, Marking and Policing (exceed action – drop)
- Classification, Marking and Policing (exceed action – policed-dscp-transmit)

Classification, Marking and Policing (exceed action – drop)

This section explains the policing configuration that drops the excessive traffic. Policing meters the incoming traffic and maintains the incoming rate to the configured bits per second. The Cisco Catalyst 3750 Switch supports only single rate, single bucket policing. This means the switch meters at only one rate and it can profile the traffic in two colors conform and exceed action. The diagram shows a policy-map sample-policy2 with three class-maps.

The requirements of this example are:

- Police ftp, pop3, imap traffic to 10Mbps.
- Trust the DSCP value of the IP communicator application packets from the PC which is connected to the IP phone. Also, the requirement is to police this traffic to 1Mbps.
- Mark and police the finlet application.



This configuration represents the policy-map mentioned in the diagram:

```
!--- Create Access-list and Class map Class-A

Distribution1(config)#ip access-list extended BULK-DATA
Distribution1(config-ext-nacl)#permit tcp any any eq ftp
Distribution1(config-ext-nacl)#permit tcp any any eq ftp-data
Distribution1(config-ext-nacl)#permit tcp any any eq pop3
Distribution1(config-ext-nacl)#permit tcp any any eq 143
Distribution1(config-ext-nacl)#exit

Distribution1(config)#class-map Class-A
Distribution1(config-cmap)#match access-group name BULK-DATA
Distribution1(config-cmap)#exit

!--- Create Access-list and Class map Class-B

Distribution1(config)#ip access-list extended IP-Communicator
Distribution1(config-ext-nacl)#remark *** Voice Payload ***
```

```

Distribution1(config-ext-nacl)#permit udp any any range 16384 32767
Distribution1(config-ext-nacl)#remark *** Voice Signalling ***
Distribution1(config-ext-nacl)#permit tcp any any range 2000 2002
Distribution1(config-ext-nacl)#exit

Distribution1(config)#class-map Class-B
Distribution1(config-cmap)#match access-group name IP-Communicator
Distribution1(config-cmap)#exit

!--- Create Access-list and Class map Class-C

Distribution1(config)#ip access-list extended application
Distribution1(config-ext-nacl)#remark *** Application for example ***
Distribution1(config-ext-nacl)#permit tcp any any eq 32768
Distribution1(config-ext-nacl)#permit udp any any eq 32768
Distribution1(config-ext-nacl)#permit tcp any any eq 32769
Distribution1(config-ext-nacl)#permit udp any any eq 32769
Distribution1(config-ext-nacl)#exit

Distribution1(config)#class-map Class-C
Distribution1(config-cmap)#match access-group name application
Distribution1(config-cmap)#exit

!--- Create Policy map

Distribution1(config-cmap)#policy-map sample-policy2
Distribution1(config-pmap)#class Class-A
Distribution1(config-pmap-c)#police 10000000 8000 exceed-action drop
Distribution1(config-pmap-c)#class Class-B
Distribution1(config-pmap-c)#trust dscp
Distribution1(config-pmap-c)#police 256000 8000 exceed-action drop
Distribution1(config-pmap-c)#class Class-C
Distribution1(config-pmap-c)#set dscp CS2
Distribution1(config-pmap-c)#police 25000000 8000 exceed-action drop
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#exit

!--- Apply Policy map to the interface

Distribution1(config)#interface GigabitEthernet1/0/20
Distribution1(config-if)#service-policy input sample-policy2

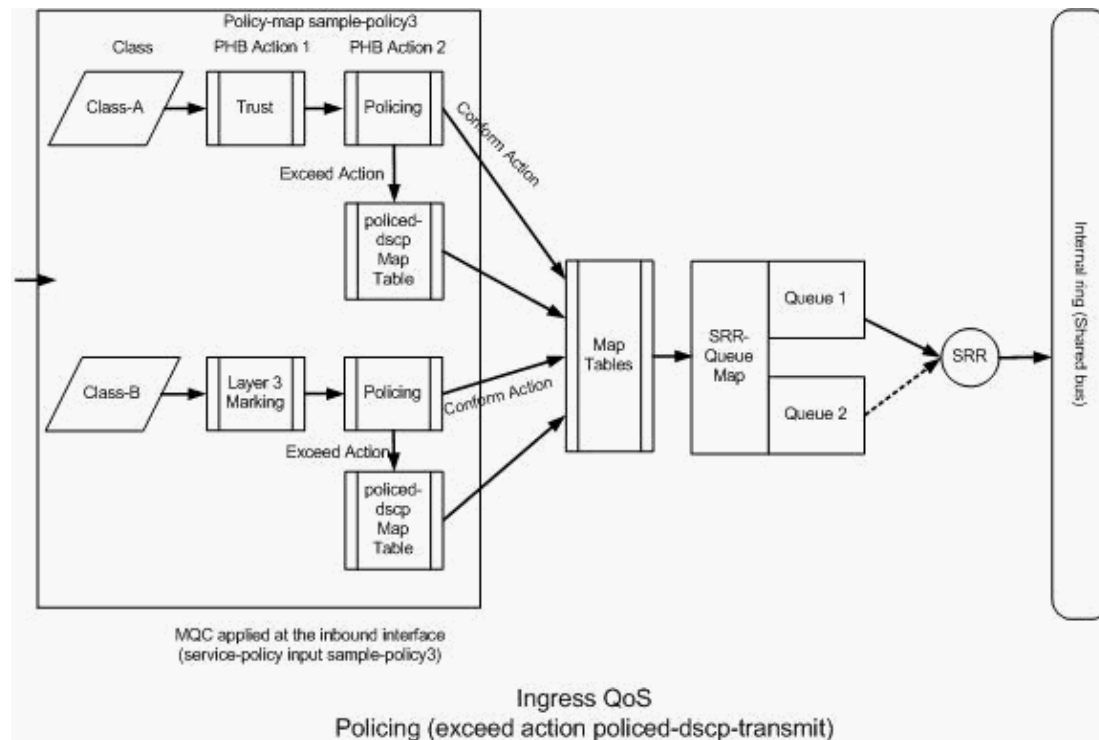
```

The configuration in the policy-map is explained here:

- **Class-A:** The traffic matching Class A is policed at the rate of 10 Mbps. The QoS labels on Class A traffic are not trusted. The CoS and DSCP values are marked as 0. The excessive packets are dropped by the policer.
- **Class-B:** There are two PHB actions performed on the traffic matching Class B. One is trust and the second one is policing. The DSCP value for Class-B traffic is trusted. The CoS value will be derived the DSCP-CoS table. Then, the Class B traffic is policed at the rate of 256 Kbps. The excessive packets are dropped by the policer.
- **Class-C:** There are two PHB actions performed on the traffic matching Class B. One is marking and the second one is policing. The incoming packets that match Class C are marked with the DSCP value CS2, and the CoS value is derived from the DSCP-CoS table which is 2. Then, the Class C traffic is policed at the rate of 25 Mbps. The excessive packets are dropped by the policer.

Classification, Marking and Policing (exceed action – policed-dscp-transmit)

This section explain the policing configuration that marks and transmits the excessive traffic. This diagram shows a policy-map sample-policy3 with two class-maps:



The switch marks the traffic that exceeds the configured policing rate based on the policed-DSCP map table values. The policed-DSCP map is used only when it is configured in the policing configuration. The default policed-DSCP map table is listed here:

```
Distribution1(config)#do show mls qos map policed-dscp
Policed-dscp map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```

From this table, you can see the same DSCP values are matched. For example, DSCP 34 is mapped to DSCP 34. The traffic that conforms to the policer rate is transmitted without altering the DSCP value. The traffic that exceeds the policer rate can be transmitted with a different DSCP value. For example, it can be marked with the DSCP value that has more probability to get dropped.

If you use the default policed-DSCP values, it does not make sense to use policing. For example, you have configured to police the traffic at the rate of 10 Mbps. The incoming packet has the DSCP value of CS4. If you keep the default DSCP value, the traffic that conforms 10Mbps is transmitted with the DSCP value of CS2. Also, the traffic that exceeds the 10 Mbps is transmitted with the DSCP value of CS2. This is because the policed-DSCP map default values map the same values. Therefore, it is recommended to configure the policed-DSCP map table appropriately in order to differentiate the DSCP values.

The requirements of this example are:

- Configure the policed-DSCP map table to map:
 - ◆ EF to AF31
 - ◆ CS3 to AF13
 - ◆ CS2 to AF11
- Trust the DSCP values of the IP communicator packets and police it to 256Kbps. If the traffic exceeds 256Kbps, remark the DSCP values using the policed-DSCP map table.
- Mark and police the filnet application. If the traffic exceeds 25Mbps, remark the DSCP values using the policed-DSCP map table.

This configuration represents the policy-map mentioned in the diagram:

```
!--- Policed DSCP table Configuration
```

```
Distribution1(config)#mls qos map policed-dscp 46 to 26
Distribution1(config)#mls qos map policed-dscp 24 to 14
Distribution1(config)#mls qos map policed-dscp 16 to 10
```

```
!--- Create Access-list and Class map Class-A
```

```
Distribution1(config)#ip access-list extended IP-Communicator
Distribution1(config-ext-nacl)#remark *** Voice Payload ***
Distribution1(config-ext-nacl)#permit udp any any range 16384 32767
Distribution1(config-ext-nacl)#remark *** Voice Signalling ***
Distribution1(config-ext-nacl)#permit tcp any any range 2000 2002
Distribution1(config-ext-nacl)#exit
```

```
Distribution1(config)#class-map Class-A
Distribution1(config-cmap)#match access-group name IP-Communicator
Distribution1(config-cmap)#exit
```

```
!--- Create Access-list and Class map Class-C
```

```
Distribution1(config)#ip access-list extended application
Distribution1(config-ext-nacl)#remark *** Application for example ***
Distribution1(config-ext-nacl)#permit tcp any any eq 32768
Distribution1(config-ext-nacl)#permit udp any any eq 32768
Distribution1(config-ext-nacl)#permit tcp any any eq 32769
Distribution1(config-ext-nacl)#permit udp any any eq 32769
Distribution1(config-ext-nacl)#exit
```

```
Distribution1(config)#class-map Class-B
Distribution1(config-cmap)#match access-group name application
Distribution1(config-cmap)#exit
```

```
!--- Create Policy map
```

```
Distribution1(config-cmap)#policy-map sample-policy3
Distribution1(config-pmap-c)#class Class-A
Distribution1(config-pmap-c)#trust dscp
Distribution1(config-pmap-c)#police 256000 8000 exceed-action policed-dscp-transmit
Distribution1(config-pmap-c)#class Class-B
Distribution1(config-pmap-c)#set dscp CS2
Distribution1(config-pmap-c)#police 25000000 8000 exceed-action policed-dscp-transmit
Distribution1(config-pmap-c)#exit
Distribution1(config-pmap)#exit
```

```
!--- Apply Policy map to the interface
```

```
Distribution1(config)#interface GigabitEthernet1/0/21
Distribution1(config-if)#service-policy input sample-policy3
```

The configuration in the policy-map is explained here:

- **Policed-DSCP:** There are three values modified in the policed-DSCP map table.

- ◆ EF to AF31
- ◆ CS3 to AF13
- ◆ CS2 to AF11

The first two values are modified based on the types of traffic classified in the Class-A and Class-B class maps.

- **Class-A:** The voice payload and the voice control from the softphone are classified in the Class-A class map. Voice payload traffic has the DSCP value of EF and the voice control has the DSCP value of CS3. As per the policy-map configuration, these DSCP values are trusted. The traffic is policed at the rate of 256 Kbps. The traffic that conforms this rate will be sent with the incoming DSCP value. The traffic that exceeds this rate will be remarked by the policed DSCP table and transmitted. The policed DSCP table will remark the EF to AF31 and the CS3 to AF13 as per the configured values. Then, the CoS values that correspond will be derived from the DSCP-CoS table.
- **Class-B:** Incoming packets that match Class-B are marked with the DSCP value of CS2. The Class-B traffic is policed at the rate of 25 Mbps. The traffic that conforms this rate will be sent with the DSCP value of 2 and the CoS value is derived from the DSCP-CoS table which is 2. The traffic that exceeds this rate will be remarked by the policed DSCP table and transmitted. The policed DSCP table will remark the EF to AF31 and the CS3 to AF13 as per the configured values. Then, the CoS values that correspond will be derived from the DSCP-CoS table.

Congestion Management and Avoidance

Congestion management and avoidance is a three step process. The steps are queueing, dropping and scheduling. Queueing places the packets into the different software queues based on the QoS labels. The Cisco Catalyst 3750 Switch has two ingress queues. After the traffic is classified and marked with QoS labels, you can assign the traffic into two different queues based on the QoS labels.

Weighted tail drop (WTD) is used to manage the queue lengths and to provide drop precedences for different traffic classifications.

Both the ingress and egress queues are serviced by SRR, which controls the rate at which packets are sent. On the ingress queues, SRR sends packets to the stack ring. SRR can operate in two modes called shaped and shared. For ingress queues, sharing is the default mode, and it is the only mode supported. In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it.

This section explains three types of configurations.

- Default Queueing, Dropping and Scheduling Configuration
- Queueing and Scheduling
- Queueing, Dropping and Scheduling

The commands available to configure these are:

```
Distribution1(config)#mls qos srr-queue input ?
!--- Queueing
buffers          Configure buffer allocation
```

```

cos-map          Configure cos-map for a queue id
dscp-map         Configure dscp-map for a queue id

```

!--- Scheduling

```

bandwidth        Configure SRR bandwidth
priority-queue   Configure priority scheduling

```

!--- Dropping

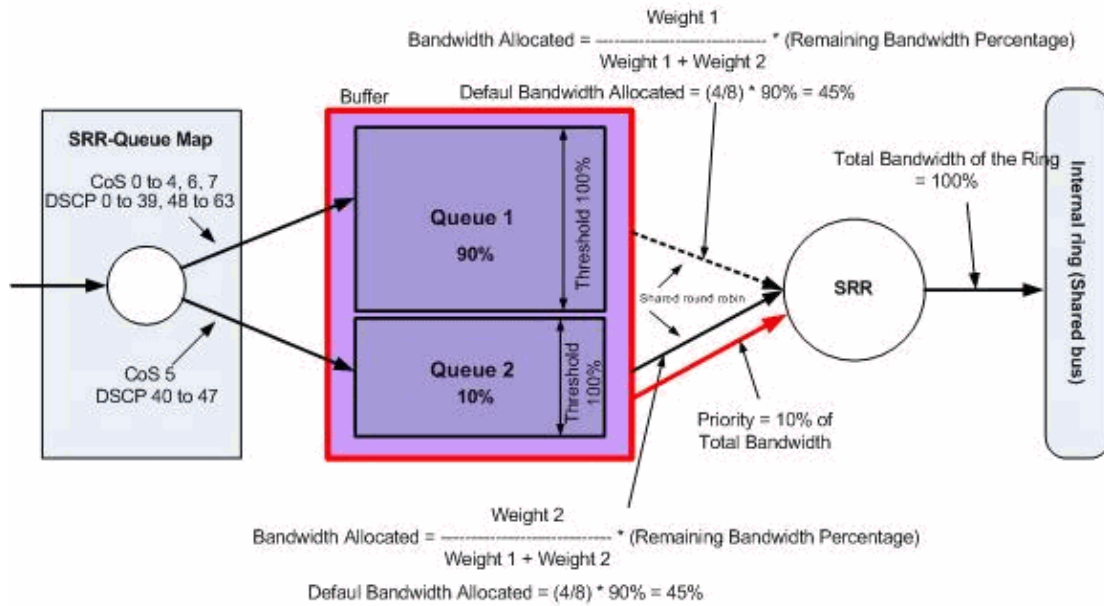
```

threshold        Configure queue tail-drop thresholds

```

Default Queueing, Dropping and Scheduling Configuration

This output shows the default QoS label to queue mapping. Each queue can support three threshold levels. By default, each queue support has only one threshold value that is 100%.



Default Queueing, Dropping & Scheduling

- **Default Queue Map Configuration:**

Packets with CoS 5 (DSCP 40 to 47) are placed into queue 2. The packets that remain are placed in queue 1.

```

Distribution1#show mls qos maps cos-input-q
Cos-inputq-threshold map:
cos:  0  1  2  3  4  5  6  7
-----
queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

```

```

Distribution1#show mls qos maps dscp-input-q
Dscp-inputq-threshold map:
d1 :d2  0  1  2  3  4  5  6  7  8  9
-----
0 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
3 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 : 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01

```

```

5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 :    01-01 01-01 01-01 01-01

```

This table represents the default CoS/DSCP to input queue mapping:

CoS	DSCP	Ingress Queue
0	0 to 7	1
1	8 to 15	1
2	16 to 23	1
3	24 to 31	1
4	32 to 39	1
5	40 to 47	2
6	48 to 55	1
7	56 to 63	1

• **Default Queue Configuration:**

The Ingress Queue buffer is shared 90% by queue 1 and 10% by queue 2. Threshold levels 1, 2 and 3 are 100%.

```

Distribution1#show mls qos input-queue
Queue      :      1      2
-----
buffers   :      90     10
bandwidth :       4      4
priority  :       0     10
threshold1:     100    100
threshold2:     100    100

```

• **Default Scheduler Configuration:**

Queue 2 is the priority queue. SRR services the priority queue for its configured weight which is 10%. Then, SRR shares the remaining bandwidth (90%) with both ingress queues and services them as specified by the configured weights. In this case, queue 1 and queue 2 are serviced at the rate of 45% each.

```

Distribution1#show mls qos input-queue
Queue      :      1      2
-----
buffers   :      90     10
bandwidth :       4      4
priority  :       0     10
threshold1:     100    100
threshold2:     100    100

```

Queueing and Scheduling

There are three steps to configure the queueing and scheduling. The steps are:

1. **Queue Map Configuration:**

Queue map configuration maps the packets to the two ingress queues based on the DSCP or CoS values.

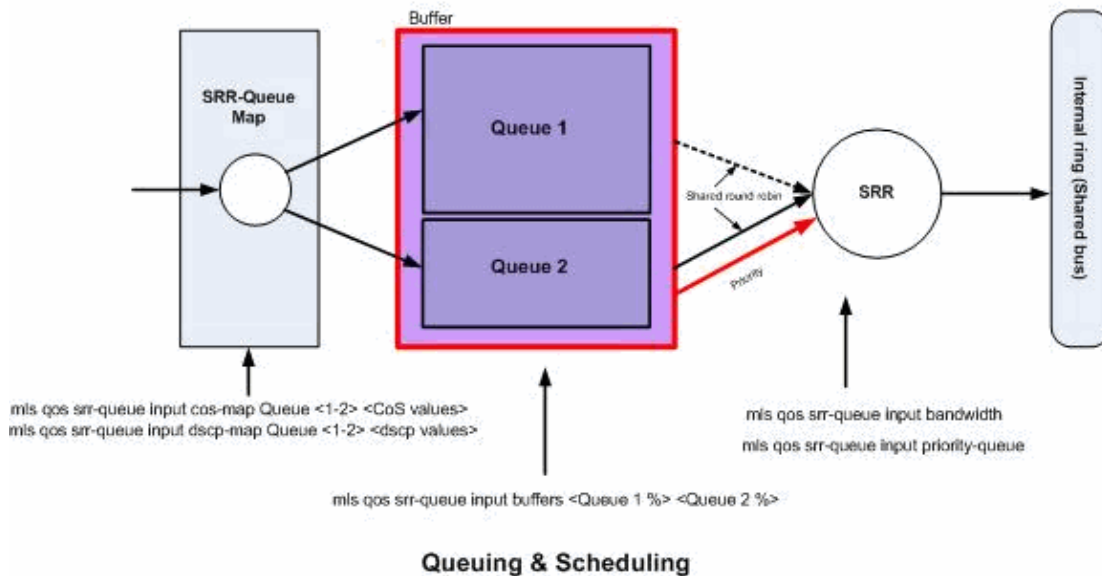
2. **Queue Configuration:**

Queue configuration defines the ratio (allocate the amount of space) with which to divide the ingress buffers between the two queues.

3. Scheduler Configuration:

SRR configures the ratio of the weights that controls the frequency of dequeuing packets from the queues to the stack ring.

Queue and scheduler configurations control how much data can be buffered before packets are dropped.



In this section, the WTD drop levels are not configured. This means the packets will be dropped if the queue is 100%.

• Queue Map Configuration:

First, CoS values are mapped to the queues. In this section, the threshold values are not configured.

!--- Assign the frames into the queue based on the CoS value.

```
Distribution1(config)#mls qos srr-queue input cos-map queue 1 0 1
Distribution1(config)#mls qos srr-queue input cos-map queue 2 2 3 4 5 6 7
```

!--- Show output.

```
Distribution1#show mls qos maps cos-input-q
Cos-inputq-threshold map:
      cos:  0   1   2   3   4   5   6   7
      -----
queue-threshold: 1-1 1-1 2-1 2-1 2-1 2-1 2-1 2-1
```

```
Distribution1#show mls qos maps dscp-input-q
Dscp-inputq-threshold map:
d1 :d2   0   1   2   3   4   5   6   7   8   9
-----
0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
```

```

1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
3 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 :    01-01 01-01 01-01 01-01

```

You can see the conflict in the Cos-inputq-threshold and Dscp-inputq-threshold maps. For example, CoS 3 is mapped to queue 2 in the Cos-inputq-threshold table. However, the DSCP value 24 (which corresponds to CoS 3) is mapped to queue 1 in the Dscp-inputq-threshold map. Actually, the Dscp-inputq-threshold map overrides the Cos-inputq-threshold map. These mappings should be as consistent as possible in order to ensure predictable behavior and to simplify troubleshooting. Therefore, the Dscp-inputq-threshold map is configured to sync with the Cos-inputq-threshold map.

```
!--- Assign the frames into the queue based on the DSCP value.
```

```

Distribution1(config)#mls qos srr-queue input dscp-map queue 2 16 17 18 19 20 21 22
Distribution1(config)#mls qos srr-queue input dscp-map queue 2 24 25 26 27 28 29 30
Distribution1(config)#mls qos srr-queue input dscp-map queue 2 32 33 34 35 36 37 38
Distribution1(config)#mls qos srr-queue input dscp-map queue 2 48 49 50 51 52 53 54
Distribution1(config)#mls qos srr-queue input dscp-map queue 2 56 57 58 59 60 61 62

```

```
Distribution1#show mls qos maps dscp-input-q
```

```
Dscp-inputq-threshold map:
```

```

d1 :d2    0      1      2      3      4      5      6      7      8      9
-----
0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 02-01 02-01 02-01 02-01
2 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
3 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
4 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
5 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
6 :    02-01 02-01 02-01 02-01

```

• Queue Configuration:

The IOS allocates default space in the buffer to queue ingress packets after QoS is enabled. Both the ingress queues, queue1 and queue 2, share this buffer space. In the Catalyst 3750 Switch, you can configure the percentage of this buffer space that each queue can use. 67% of the total available memory for ingress queue is allocated to queue 1 and 33% is allocated to queue 2.

```
Distribution1(config)#mls qos srr-queue input buffers 67 33
```

```
Distribution1(config)#do show mls qos input
```

```

Queue      :      1      2
-----
buffers    :      67     33
bandwidth  :       4     4
priority   :       0    10
threshold1:     100   100
threshold2:     100   100

```

• Scheduler Configuration:

This configuration is performed with the **mls qos srr-queue input bandwidth** command. Here, this bandwidth states that the amount of bits serviced by SRR on the queues.

```
Distribution1(config)#mls qos srr-queue input bandwidth 90 10
```

```
Distribution1(config)#mls qos srr-queue input priority-queue 2 bandwidth 20
```

```
Distribution1(config)#do show mls qos input
```

```

Queue      :      1      2
-----

```

```

buffers      :      67      33
bandwidth    :      90      10
priority     :       0      20
threshold1   :     100     100
threshold2   :     100     100

```

By default, queue 2 is the priority queue and 10% of total internal ring bandwidth is allocated to the priority queue. You can also configure queue 1 as the priority queue. However, you cannot configure both the queues as the priority queue.

If you have the bandwidth of the ring to 10Gbps, SRR services 20% of 10Gbps to queue 2 first which is 2 Gbps. The remaining 8 Gbps ring bandwidth is shared by queue 1 and queue 2. As per the configuration, queue 1 is serviced 90% of 8 Gbps and queue 2 is again serviced 10% of 8 Gbps. This 8 Gbps bandwidth is serviced by SRR in shared mode. This means the percentages of bandwidth configured are guaranteed but not limited to it.

Note: You can disable the priority queue with the **mls qos srr-queue input priority-queue 2 bandwidth 0** command.

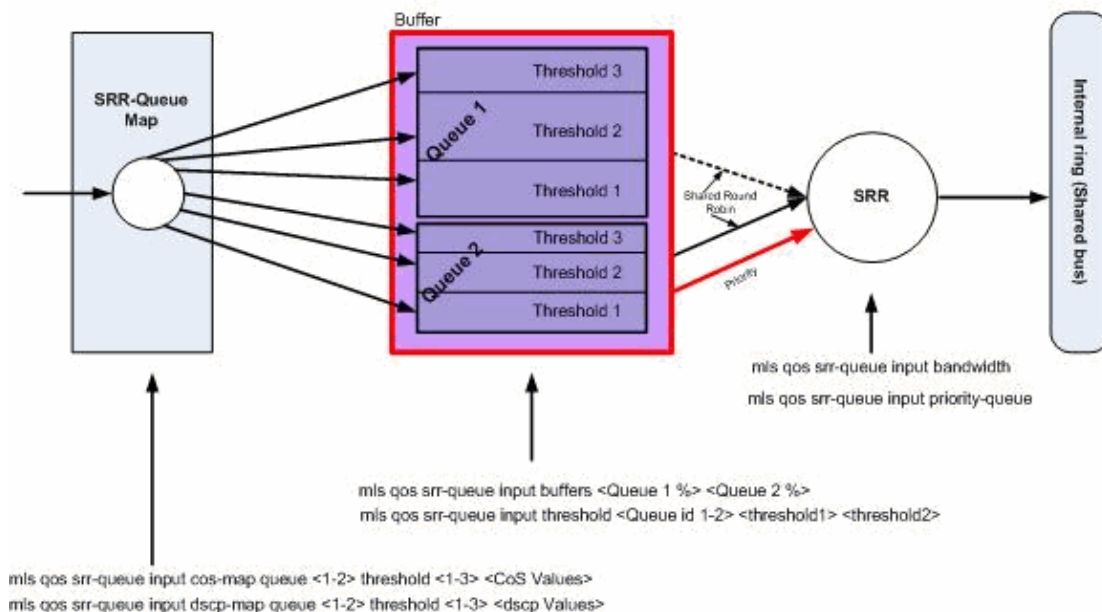
```

Distribution1(config)#do show mls qos input
Queue      :      1      2
-----
buffers    :      90      10
bandwidth  :      90      10
priority   :       0       0
threshold1 :     100     100
threshold2 :     100     100
Distribution1(config)#

```

Queueing, Dropping and Scheduling

In this section, WTD threshold levels are configured in addition to the queue buffer size. You can assign each packet that flows through the switch to a queue and to a threshold.



Queueing, Dropping & Scheduling

These are the configuration examples and explanations:

• Queue Configuration:

By default, threshold 3 is 100% and cannot be changed.

```
Distribution1(config)#mls qos srr-queue input buffers 67 33
Distribution1(config)#mls qos srr-queue input threshold 1 8 16
Distribution1(config)#mls qos srr-queue input threshold 2 34 66
```

```
Distribution1(config)#do show mls qos input
```

```
Queue      :          1          2
-----
buffers    :          67          33
bandwidth  :           4           4
priority   :           0          10
threshold1:           8          34
threshold2:          16          66
```

• Scheduler Configuration:

The IOS allocates default space in the buffer for each ingress ports after QoS is enabled. Both the queues shares this buffer space. In the Catalyst 3560/3750 Switch, you can configure the percentage of this buffer space each queue can use.

```
Distribution1(config)#mls qos srr-queue input bandwidth 90 10
Distribution1(config)#mls qos srr-queue input priority-queue 2 bandwidth 20
```

```
Distribution1(config)#do show mls qos input
```

```
Queue      :          1          2
-----
buffers    :          67          33
bandwidth  :          90          10
priority   :           0          20
threshold1:           8          34
threshold2:          16          66
```

By default, queue 2 is the priority queue and 10% of total internal ring bandwidth is allocated to the priority queue. You can also configure queue 1 as the priority queue. However, you cannot configure both queues as the priority queue.

If you have bandwidth of the ring to 10Gbps, SRR services 20% of 10Gbps to queue 2 first which is 2 Gbps. The remaining 8 Gbps ring bandwidth is shared by queue 1 and queue 2. As per the configuration, queue 1 is serviced 90% of 8 Gbps and queue 2 is again serviced 10% of 8 Gbps. This 8 Gbps bandwidth is serviced by SRR in shared mode. This means the percentages of bandwidth configured are guaranteed but not limited to it.

Note: You can disable the priority queue with the **mls qos srr-queue input priority-queue 2 bandwidth 0** command.

```
Distribution1(config)#do show mls qos input
```

```
Queue      :          1          2
-----
buffers    :          90          10
bandwidth  :          90          10
priority   :           0           0
threshold1:         100         100
threshold2:         100         100
Distribution1(config)#
```

Egress QoS Features

Congestion management and avoidance are the egress QoS features supported by Cisco Catalyst 3750 Switches. Congestion management and avoidance is a three step process. The steps are queueing, dropping and scheduling.

Queueing places the packets into the different software queues based on the QoS labels. The Cisco Catalyst 3750 Switch has 4 egress queues, 3 threshold per queue. After the traffic is classified and marked with QoS labels, you can assign the traffic into four different queues based on the QoS labels.

Each queue can be configured with buffer size, reserved threshold, threshold levels, and maximum threshold. Weighted tail drop (WTD) is used to manage the queue lengths and to provide drop precedences for different traffic classifications. Ingress queue parameters are configured globally. Ingress queue parameters are not per port basis. However, egress queue parameters are configured per port basis. Even then the configuration is per port. You cannot configure each port differently. You can configure each port in two different ways. This is called a queue set. You can configure a maximum of two different queue sets in global configuration. Then, you can apply either one of these two sets on the interface.

Both the ingress and egress queues are serviced by SRR, which controls the rate at which packets are sent. On the ingress queues, SRR sends packets to the stack ring. SRR can operate in two modes called shaped and shared. For ingress queues, sharing is the default mode, and it is the only mode supported. In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. In shaped mode, the egress queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Shaping provides a more even flow of traffic over time and reduces the peaks and valleys of bursty traffic. Queue 1 can be configured as the priority queue.

Egress QoS Commands

This section categorizes all the available egress QoS commands.

- **Queue Map Configuration:**

In order to map the CoS values to the egress queues:

```
Rack1SW1(config)#mls qos srr-queue output cos-map queue ?  
<1-4> enter cos-map output queue id
```

```
Rack1SW1(config)#mls qos srr-queue output cos-map queue 1 threshold ?  
<1-3> enter cos-map threshold id
```

```
Rack1SW1(config)#mls qos srr-queue output cos-map queue 1 threshold 1 ?  
<0-7> 8 cos values separated by spaces
```

In order to map the DSCP values to the egress queues:

```
Rack1SW1(config)#mls qos srr-queue output dscp-map queue ?  
<1-4> enter dscp-map output queue id
```

```
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 1 threshold ?  
<1-3> enter dscp-map threshold id
```

```
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 1 threshold 1 ?  
<0-63> dscp values separated by spaces (up to 8 values total)
```

- **Queue Configuration:**

Egress queue configuration allows you to configure two queue sets. Each queue set has the option to configure the buffer size and threshold value for the four egress queues. Then, you can apply any one of the queue sets to any of the ports. By default, queue set 1 is assigned to all the ports when you enable QoS on the switch.

```
Rack1SW1(config)#mls qos queue-set output ?
<1-2> queue-set id

Rack1SW1(config)#mls qos queue-set output 1 ?
buffers    assign buffers to each egress queue
threshold  Assign threshold values to a queue
```

In order to configure buffer size for all the four egress queues:

```
Rack1SW1(config)#mls qos queue-set output 1 buffers ?
<0-99> enter buffer percentage for queue 1 0-99

Rack1SW1(config)#mls qos queue-set output 1 buffers 10 ?
<1-100> enter buffer percentage for queue 2 1-100 (includes CPU buffer)

Rack1SW1(config)#mls qos queue-set output 1 buffers 10 20 ?
<0-99> enter buffer percentage for queue 3 0-99

Rack1SW1(config)#mls qos queue-set output 1 buffers 10 20 30 ?
<0-99> enter buffer percentage for queue 4 0-99
```

In order to configure two threshold values, reserved and maximum threshold values for each queue (threshold 3 is 100% by default and it cannot be changed):

```
Rack1SW1(config)#mls qos queue-set output 1 threshold ?
<1-4> enter queue id in this queue set

Rack1SW1(config)#mls qos queue-set output 1 threshold 1 ?
<1-400> enter drop threshold1 1-400

Rack1SW1(config)#mls qos queue-set output 1 threshold 1 50 ?
<1-400> enter drop threshold2 1-400

Rack1SW1(config)#mls qos queue-set output 1 threshold 1 50 60 ?
<1-100> enter reserved threshold 1-100

Rack1SW1(config)#mls qos queue-set output 1 threshold 1 50 60 100 ?
<1-400> enter maximum threshold 1-400
```

In order to apply the queue-set to the interface (by default, queue set 1 is assigned to all the ports when you enable qos on the switch):

```
Rack1SW1(config-if)#queue-set ?
<1-2> the qset to which this port is mapped
```

• Scheduler Configuration:

Three different configurations are available for the switch interface. The configurations are bandwidth shape, share, and limit. You can also configure egress queue 1 as the priority queue. If the priority queue is enabled, SRR services it until it is empty before servicing the other three queues. However, in ingress priority queue, SRR services the priority queue with the configured value.

```
Rack1SW1(config-if)#srr-queue bandwidth ?
limit  Configure bandwidth-limit for this interface
shape  Configure shaping on transmit queues
share  Configure shared bandwidth
```

```
Rack1SW1(config-if)#priority-queue ?  
out egress priority queue
```

Bandwidth limit configuration:

```
Rack1SW1(config-if)#srr-queue bandwidth limit ?  
<10-90> enter bandwidth limit for interface as percentage
```

Bandwidth shape configuration:

```
Rack1SW1(config-if)#srr-queue bandwidth shape ?  
<0-65535> enter bandwidth weight for queue id 1  
  
Rack1SW1(config-if)#srr-queue bandwidth shape 10 ?  
<0-65535> enter bandwidth weight for queue id 2  
  
Rack1SW1(config-if)#srr-queue bandwidth shape 10 20 ?  
<0-65535> enter bandwidth weight for queue id 3  
  
Rack1SW1(config-if)#srr-queue bandwidth shape 10 20 30 ?  
<0-65535> enter bandwidth weight for queue id 4
```

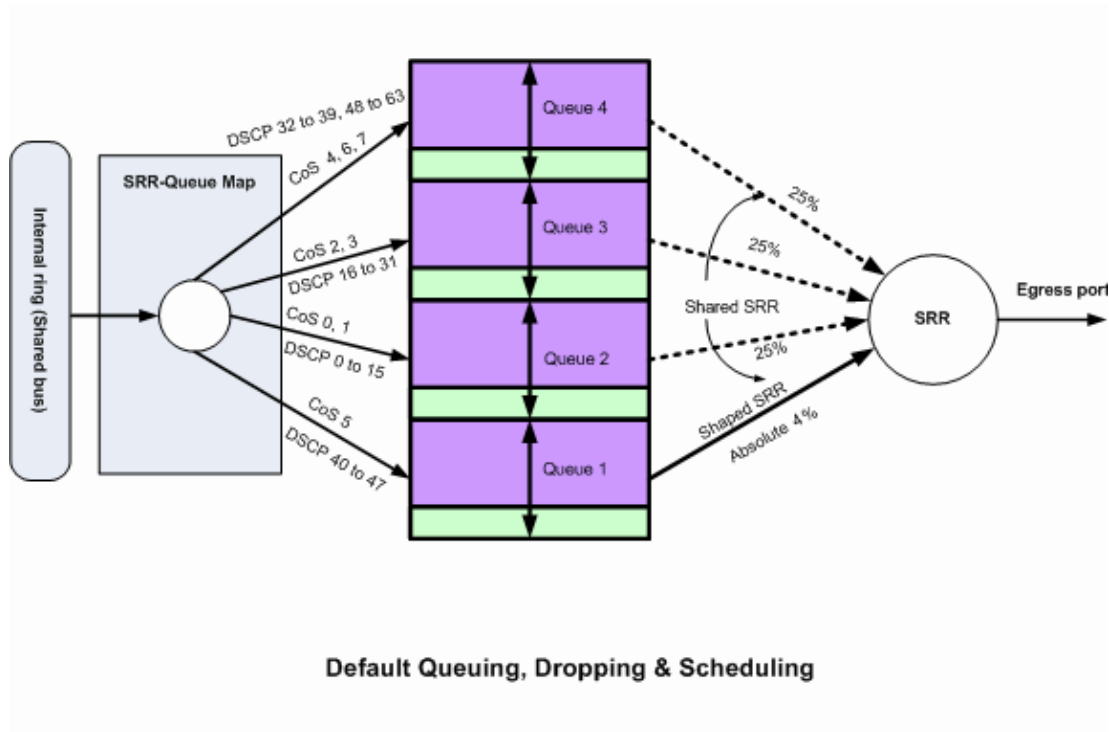
Bandwidth share configuration:

```
Rack1SW1(config-if)#srr-queue bandwidth share ?  
<1-255> enter bandwidth weight for queue id 1  
  
Rack1SW1(config-if)#srr-queue bandwidth share 10 ?  
<1-255> enter bandwidth weight for queue id 2  
  
Rack1SW1(config-if)#srr-queue bandwidth share 10 20 ?  
<1-255> enter bandwidth weight for queue id 3  
  
Rack1SW1(config-if)#srr-queue bandwidth share 10 20 30 ?  
<1-255> enter bandwidth weight for queue id 4
```

All four queues participate in the SRR unless the priority queue is enabled, in which case the first bandwidth weight is ignored and is not used in the ratio calculation. Priority queue is serviced until empty before the other queues are serviced. You enable the priority queue by using the **priority-queue out** interface configuration command.

Default Configuration

Default Queue Map Configuration:



These default mappings can be changed as per your requirement:

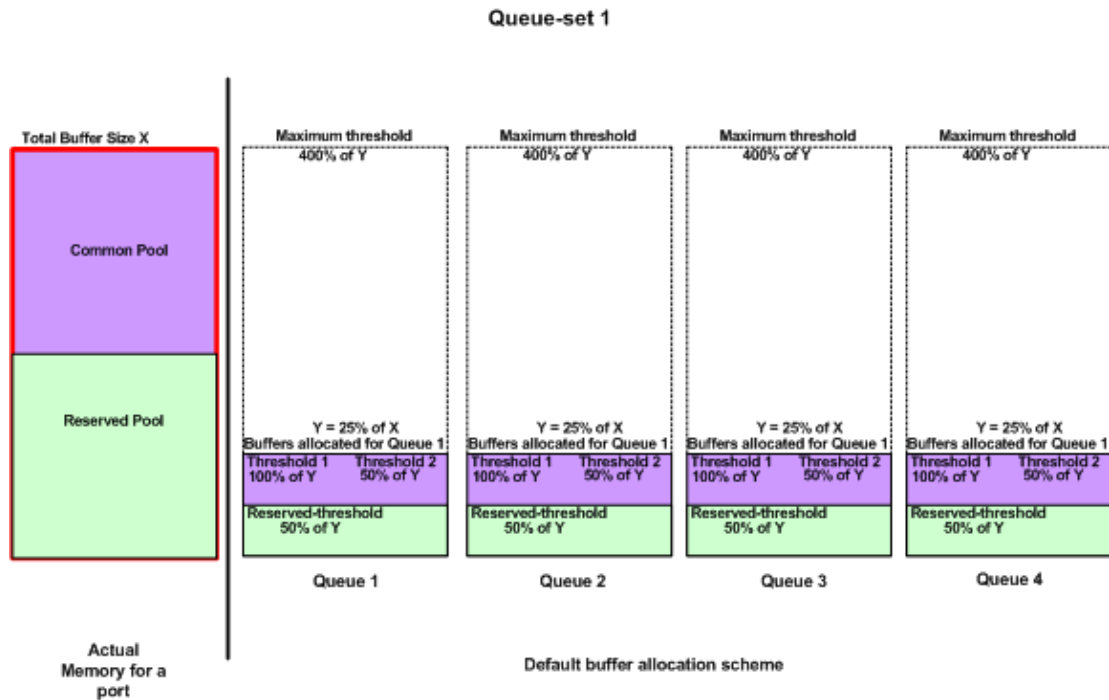
!--- Map CoS to Egress Queue

```
Distribution1#show mls qos maps cos-output-q
Cos-outputq-threshold map:
  cos:  0   1   2   3   4   5   6   7
-----
queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1
```

!--- Map DSCP to Egress Queue

```
Distribution1#show mls qos maps dscp-output-q
Dscp-outputq-threshold map:
d1 :d2  0   1   2   3   4   5   6   7   8   9
-----
0 :    02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
1 :    02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01
2 :    03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
3 :    03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
5 :    04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
6 :    04-01 04-01 04-01 04-01
```

Default Queue Configuration:



The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Two queue sets are configured and queue set 1 is assigned to all the ports by default. Each queue is allocated 25 percent of the total buffer space. Each queue is reserved 50 percent of allocated buffer space which is 12.5 percent of the total buffer space. The sum of all the reserved buffers represents the reserved pool, and the remaining buffers are part of the common pool. The default configuration sets 400 percent as the maximum memory that this queue can have before packets are dropped.

```
Distribution1#show mls qos queue-set 1
Queueset: 1
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum  :      400     400     400     400
```

```
Distribution1#show mls qos queue-set 2
Queueset: 2
Queue   :      1      2      3      4
-----
buffers  :      25      25      25      25
threshold1:    100     200     100     100
threshold2:    100     200     100     100
reserved  :      50      50      50      50
maximum  :      400     400     400     400
```

```
Distribution1#show mls qos int gigabitEthernet 1/0/20 buffers
GigabitEthernet1/0/20
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

Default Scheduler Configuration:

The priority queue is disabled. Both the shaped and shared mode are configured for the SRR. Shaped mode weights override the shared mode value. Therefore, the net result is queue 1 is serviced in shaped mode and queues 2, 3, and 4 are serviced in shared mode. This means queue 1 is serviced with an absolute value that is (1/25) percent, or four percent, of the bandwidth. Queues 2, 3 and 4 are serviced at 25 percent of the bandwidth. If the bandwidth is available, then queues 2, 3 and 4 can be serviced at more than 25 percent of the bandwidth.

```
Distribution1#show mls qos int gigabitEthernet 1/0/20 queueing
GigabitEthernet1/0/20
Egress Priority Queue : disabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

Queuing, Dropping and Scheduling

These are the sample configurations:

- **Queue Map Configuration:**

```
Rack1SW1(config)#mls qos srr-queue output cos-map queue 1 threshold 3 5
Rack1SW1(config)#mls qos srr-queue output cos-map queue 1 threshold 1 2 4
Rack1SW1(config)#mls qos srr-queue output cos-map queue 2 threshold 2 3
Rack1SW1(config)#mls qos srr-queue output cos-map queue 2 threshold 3 6 7
Rack1SW1(config)#mls qos srr-queue output cos-map queue 3 threshold 3 0
Rack1SW1(config)#mls qos srr-queue output cos-map queue 4 threshold 3 1

Rack1SW1(config)#mls qos srr-queue output dscp-map queue 1 threshold 3 46
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 16
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 18 20 22
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 25
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 32
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 34 36 38
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24 26
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
Rack1SW1(config)#mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14
```

- **Queue Configuration:**

This configuration shows the configuration of both the queue sets 1 and 2. By default, queue set 1 is applied on all the interfaces.

```
Rack1SW3(config)#mls qos queue-set output 1 buffers 10 10 26 54
Rack1SW3(config)#mls qos queue-set output 2 buffers 16 6 17 61

Rack1SW3(config)#mls qos queue-set output 1 threshold 2 70 80 100 100
Rack1SW3(config)#mls qos queue-set output 1 threshold 4 40 100 100 100

Rack1SW3(config)#mls qos queue-set output 2 threshold 1 149 149 100 149
Rack1SW3(config)#mls qos queue-set output 2 threshold 2 118 118 100 235
Rack1SW3(config)#mls qos queue-set output 2 threshold 3 41 68 100 272
Rack1SW3(config)#mls qos queue-set output 2 threshold 4 42 72 100 242

Rack1SW3(config)#int fa 1/0/11
Rack1SW3(config-if)#queue-set 2
```

Interface 1/0/11 is applied with queue set 2.

```
Rack1SW3(config-if)#do show mls qos int fa 1/0/10 buffers
FastEthernet1/0/10
The port is mapped to qset : 1
The allocations between the queues are : 10 10 26 54
```

```
Rack1SW3(config-if)#do show mls qos int fa 1/0/11 buffers
FastEthernet1/0/11
The port is mapped to qset : 2
The allocations between the queues are : 16 6 17 61
```

• **Scheduler Configuration:**

```
Rack1SW3(config-if)#srr-queue bandwidth share 1 75 25 5
Rack1SW3(config-if)#srr-queue bandwidth shape 3 0 0 0
```

Cisco Catalyst 3750 egress queue does not support Low Latency Queueing (LLQ). It supports priority queueing. When you configure priority-queue out, queue 1 is always serviced when it has a packet.

```
Rack1SW3(config-if)#srr-queue bandwidth share 1 75 25 5
Rack1SW3(config-if)#srr-queue bandwidth shape 3 0 0 0
Rack1SW3(config-if)#priority-queue out
```

When you configure this command, the SRR weight and queue size ratios are affected because there is one fewer queue participating in SRR. This means that weight1 in the **srr-queue bandwidth shape** or the **srr-queue bandwidth share** command is ignored (not used in the ratio calculation).

This is the command to see drops on specific queues:

Step 1:

```
1/ #show platform pm if-numbers
```

use sh platform pm if-numbers and check the port info corresponding to your interface (This is the OUTGOING INTERFACE on your 3750!!!!!!) for example fas 0/3 will be port 0/4 --> keep 4 as port value, if the first value is not a zero then give the asic number after the port number.

```
interface gid  gpn  lpn  port slot unit slun port-type lpn-idb gpn-idb
-----
-----
Gi0/1          1    1    25  0/1  1    1    1    local    Yes    Yes
Gi0/2          2    2    26  0/0  1    2    2    local    Yes    Yes
Fa0/1          3    3    1   0/2  1    1    3    local    Yes    Yes
Fa0/2          4    4    2   0/3  1    2    4    local    Yes    Yes
Fa0/3         5    5    3   0/4 1    3    5    local    Yes    Yes
Fa0/4          6    6    4   0/5  1    4    6    local    Yes    Yes
Fa0/5          7    7    5   0/6  1    5    7    local    Yes    Yes
Fa0/6          8    8    6   0/7  1    6    8    local    Yes    Yes
```

Port Value corresponding to the interface fa 0/3 is 0/4. Now you can see the queue drops with the command sh platform port-asic stats drop port 4

Step 2:

```
2/ #show platform port-asic stats drop port 4
```

```
Port-asic Port Drop Statistics - Summary
```

```
=====
RxQueue 0 Drop Stats: 0
RxQueue 1 Drop Stats: 0
RxQueue 2 Drop Stats: 0
RxQueue 3 Drop Stats: 0
```

...

```
Port 4 TxQueue Drop Statistics
Queue 0
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
Queue 1
  Weight 0 Frames 0
  Weight 1 Frames 2755160 <--- Here is an example of drops
  Weight 2 Frames 0
Queue 2
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
Queue 3
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 8
```

• **Bandwidth Limit Configuration:**

In order to limit maximum output on a port, configure the `srr-queue bandwidth limit` interface configuration command. If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six. This command is not available on a 10-Gigabit Ethernet interface.

```
srr-queue bandwidth limit weight1
```

where *weight1* is the percentage of the port speed to which the port should be limited. The range is 10 to 90.

Note: The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

Related Information

- [Configuring QoS](#)
- [Cisco Catalyst 3750 Series Switches – Support Documentation](#)
- [LAN Product Support](#)
- [LAN Switching Technology Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 17, 2007

Document ID: 91862
