QoS Advanced Mode Configuration on 300 Series Managed Switches

Objectives

In QoS advanced mode, the switch uses policies to support per-flow QoS. The policy and its components have the following characteristics:

- A policy may contains one or more class maps.
- A policy contains one or more flows, each with a user defined QoS.
- A single policer applies the QoS to a single class map, and thus to a single flow, based on the policer QoS specification.
- An aggregate policer applies the QoS to one or more class maps, and thus one or more flows.
- Per flow QoS are applied to flows by binding the policies to the desired ports.

Applicable Devices

- SF/SG 300 Series Managed Switches

Software Version

- v1.2.7.76

Work-flow to Configure QoS Advanced Mode

1. Select Advanced Mode for the system.

2. To map the external values to internal values, if internal DSCP values are different from those used on incoming packets, configure the Out of Profile DSCP Mapping on the *Out of Profile DSCP Mapping Page* .

3. Create ACLs. Please refer the document on Creating ACLs for the workflow of ACL's.

4. Create class maps and associate the ACLs with them by using the *Class Mapping Page*.

5. Create a policy using the *Policy Table Page*, and associate the policy with one or more class maps using the *Policy Class Map Page*. The types of Policers used below.

- Single Policer
- A Policy can be created to associate the class map to a single policer.
- Aggregate Policer:

Create a QoS action for each flow that sends all matching frames to aggregate policer by using the *Aggregate Policer Page*

6. Finally, bind the policy to an interface by using the *Policy Binding Page*.

This document illustrates the procedure to configure the above.

QoS Advanced Mode

Enable QoS Advanced Mode

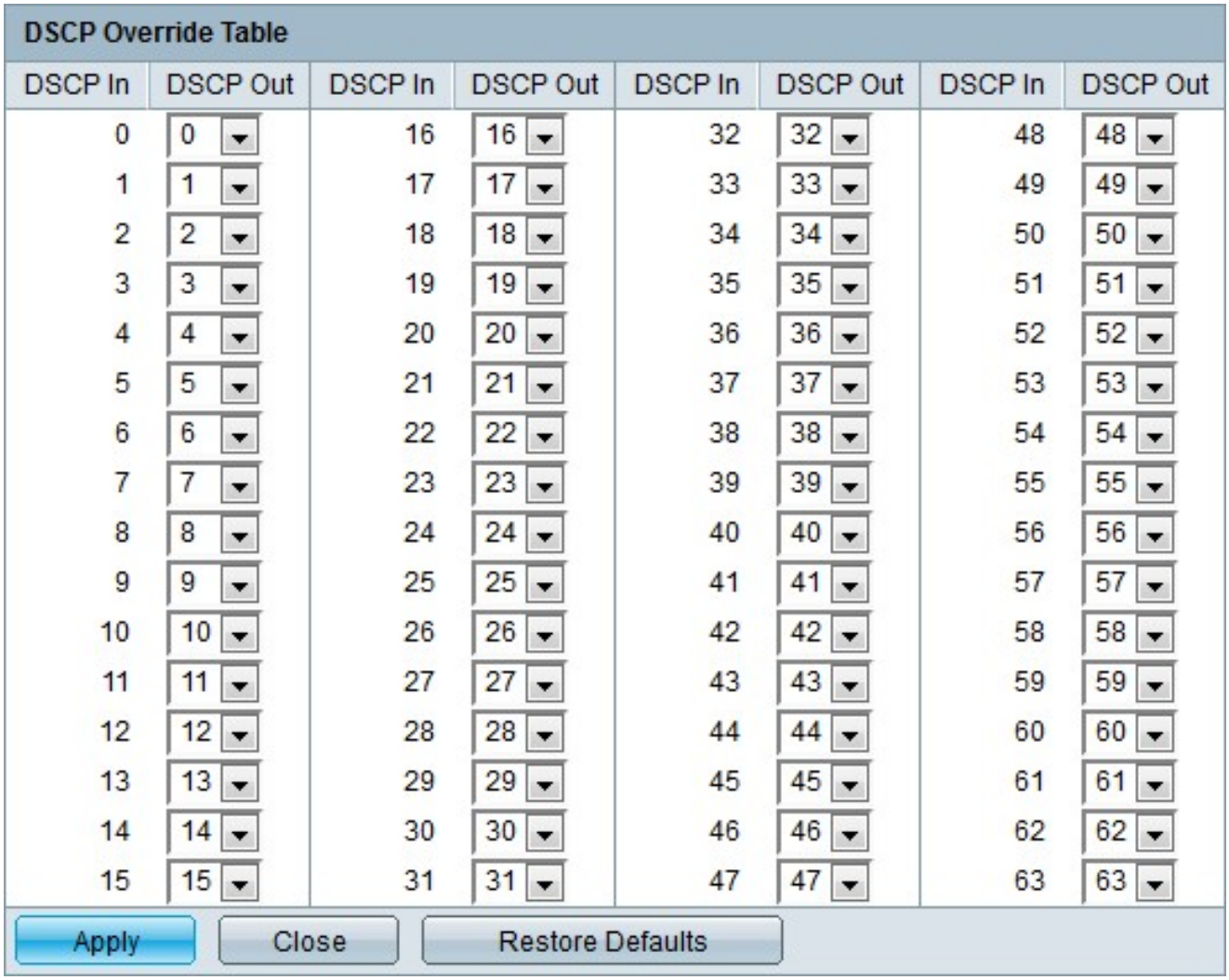
Step 1. Log in to the web configuration utility and choose **Quality of Service > General > QoS Properties**. The *QoS Properties* page opens:

Step 2. Click the **Advanced** radio button in the QoS Mode field.

Step 3. Click **Apply**.

Global Settings

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Global Settings**. The *Out of Profile DSCP Mapping* page opens:



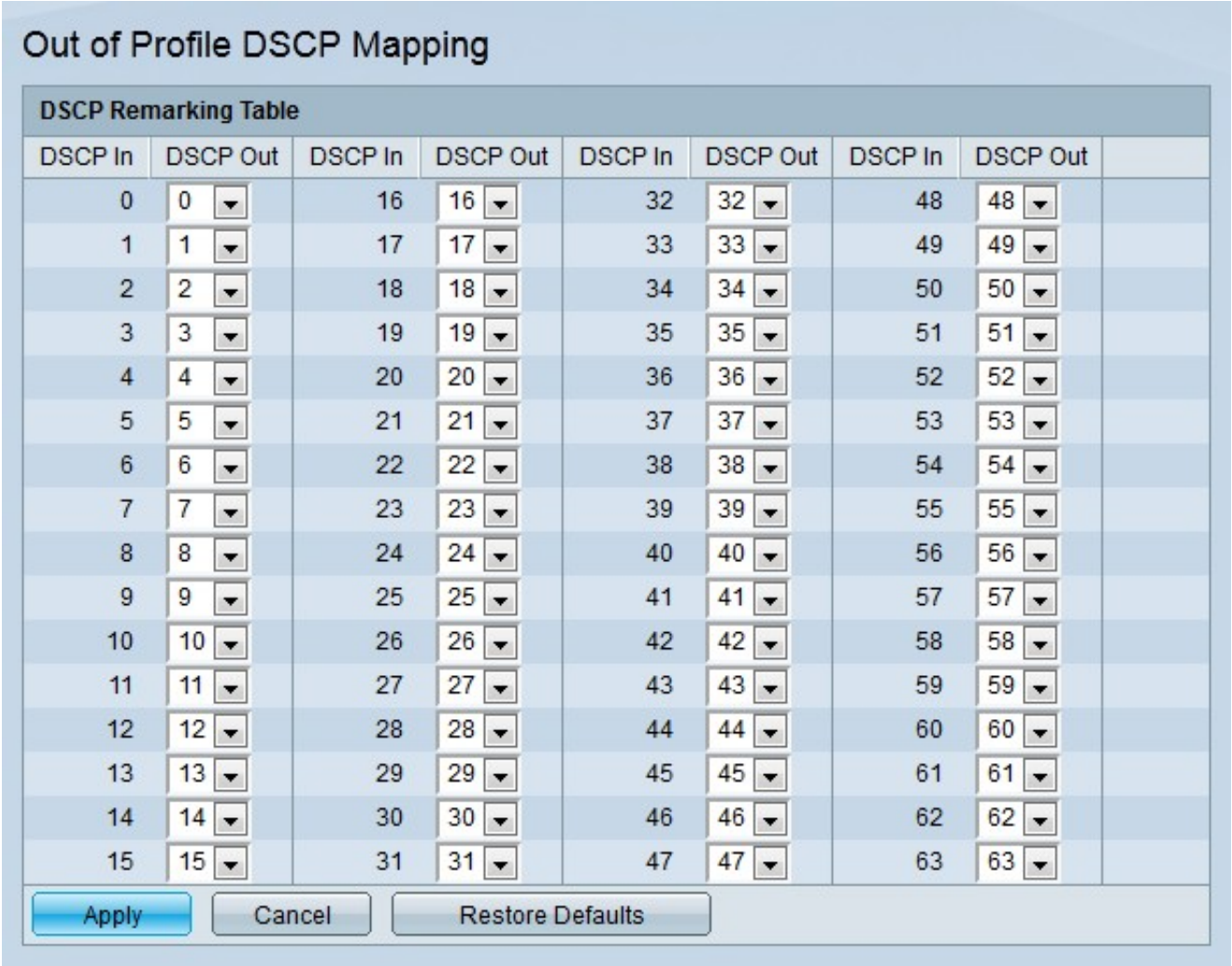
DSCP Override Table

DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	16	16	32	32	48	48
1	1	17	17	33	33	49	49
2	2	18	18	34	34	50	50
3	3	19	19	35	35	51	51
4	4	20	20	36	36	52	52
5	5	21	21	37	37	53	53
6	6	22	22	38	38	54	54
7	7	23	23	39	39	55	55
8	8	24	24	40	40	56	56
9	9	25	25	41	41	57	57
10	10	26	26	42	42	58	58
11	11	27	27	43	43	59	59
12	12	28	28	44	44	60	60
13	13	29	29	45	45	61	61
14	14	30	30	46	46	62	62
15	15	31	31	47	47	63	63

Apply Close Restore Defaults

Out of Profile DSCP Remarking

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Out of Profile DSCP Mapping**. The *Out of Profile DSCP Mapping* page opens:



Step 2. Configure the DSCP Remarking Table.

- DSCP In — Displays the value of the incoming packets that need to be remapped to an alternative value.
- DSCP Out — From the DSCP Out drop-down list choose the desired DSCP Out value that corresponds to the DSCP In value.

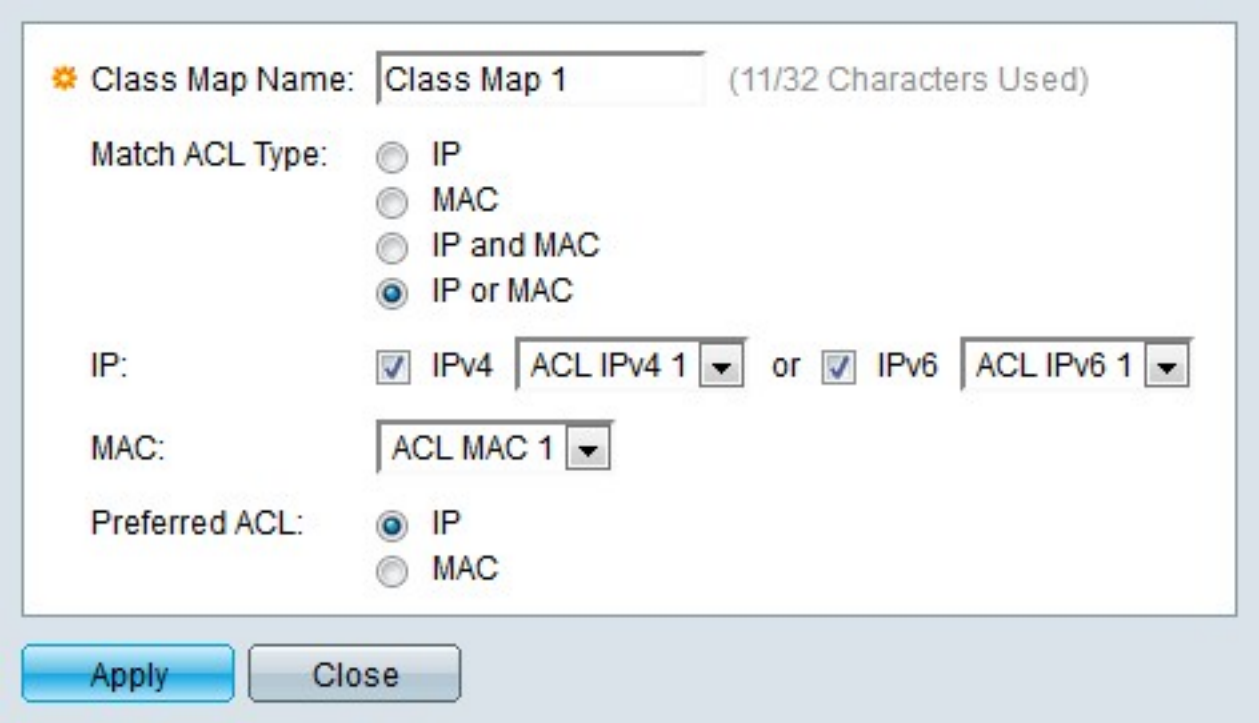
Note: Click Restore Defaults to restore the DSCP remarking table to the default values. The default is when the DSCP Out values match the values of the corresponding DSCP In values.

Step 3. Click **Apply**.

Class Mapping

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Class Mapping**. The *Class Mapping* page opens:

Step 2. Click **Add**. The *Add Class Mapping* window appears.



Step 3. Enter a name for the class map in the Class Map Name field.

Step 4. Click the radio button that corresponds to the desired ACL in the Match ACL Type field.

Step 5. If the defined Match ACL field contains IP, check the box of the desired IP type in the IP field.

- IPv4 — From the IPv4 drop-down list choose the IPv4 ACL to apply to the class map.
- IPv6 — From the IPv6 drop-down list choose the IPv6 ACL to apply to the class map.

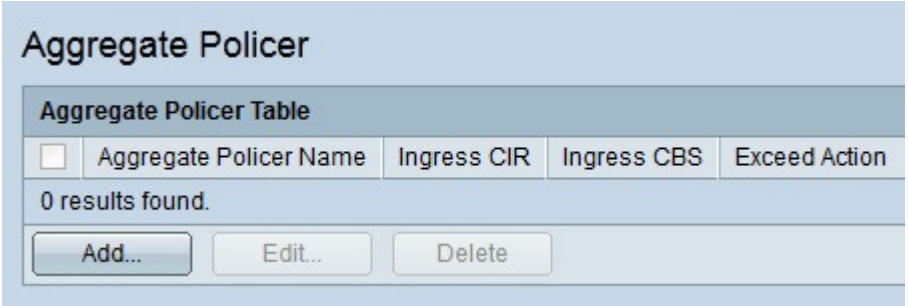
Step 6. If the defined Match ACL field contains MAC, choose the MAC ACL that is to apply to the class map in the MAC field.

Step 7. Click the radio button that corresponds to the preferred ACL type in the Preferred ACL field. This field determines whether the data should first be matched based on IP ACLs or MAC ACLs.

Step 8. Click **Apply**.

Aggregate Policer

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Aggregate Policer**. The *Aggregate Policer* page opens:



Step 2. Click **Add**. The *Add Aggregate Policer Page* window appears.

Step 3. Enter a name for the aggregate policer in the Aggregate Policer Name field.

Step 4. Enter the maximum bandwidth allowed for the ingress queue (in Kilobits per second) in the Ingress Committed Information Rate (CIR) field.

Step 5. Enter maximum burst size for the ingress queue (in bytes) in the Ingress Committed Burst Size (CBS) field. This is the amount of traffic that is allowed to pass as a temporary burst even if it is above the defined CIR.

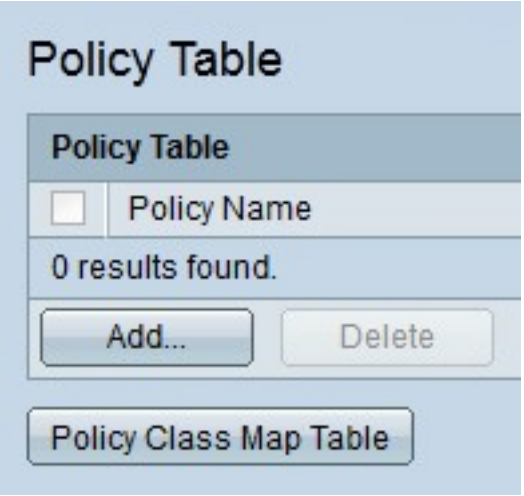
Step 6. Click the radio button that corresponds to the desired action in the Exceed Action field. This action takes place when an incoming packet exceeds the CIR.

- Forward — The packet is forwarded.
- Drop — The packet is dropped.
- Out of Profile DSCP — The DSCP value of the packet is remapped based on the Out of Profile DSCP Mapping Table.

Step 7. Click **Apply**.

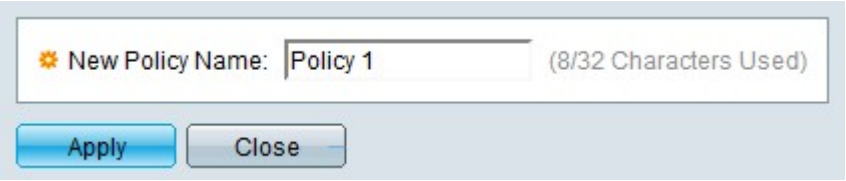
Policy Table

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Policy Table**. The *Policy Table* page opens:



Step 2. Click **Add**. The *Add Policy Page* window appears.

Note: Click **Policy Class Map Table** to open the *Policy Class Maps* page.



Step 3. Enter a name for the policy in the New Policy Name field.

Step 4. Click **Apply**.

Policy Class Maps

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Policy Class Maps**. The *Policy Class Maps* page opens:

Step 2. From the Policy Name Equals to drop-down list choose a policy.

Step 3. Click **Go** to display the class maps mapped to the specified policy.

Step 4. Click **Add** to map a class map to the specified policy. The *Add Policy Class Map* window appears.

//image

The name of the policy is displayed in the Policy Name field.

Step 5. From the Class Map Name drop-down list choose a class map to map to the policy.

Step 6. Click the radio button that corresponds to the desired action in the Action Type field.

- Use Default Trust Mode — The switch ignores the ingress CoS or DSCP value. The packets that match the policy are sent as best effort.
- Always Trust — The switch trusts the CoS or DSCP value of packets that match the policy. If a packet is an IP packet, the packet will be placed in an egress queue based on the DSCP value of the packet. Otherwise, the packet is placed in an egress queue based on the CoS value.
- Set — From the drop-down list choose the method in which packets will be assigned if they match the policy.

  – DSCP — Enter the DSCP value that will be assigned to the packets in the New Value field.

  – Queue — Enter the egress queue that the packets will be sent to in the New Value field.

  – CoS — Enter the CoS value that will be assigned to the packets in the New Value field.

Step 7. Click the radio button that corresponds to the desired policer type in the Police Type field.

- None — No policy is used.
- Single — A single policer is used.
- Aggregate — An aggregate policer is used.

Step 8. If the policer type is aggregate, choose an aggregate policer from the Aggregate Policer drop-down list.

Step 9. If the policer type is single, fill in the following fields.

- Ingress Committed Information Rate (CIR) — Enter the maximum bandwidth allowed for the ingress queue (in Kilobits per second) in the Ingress Committed Information Rate (CIR) field.
- Ingress Committed Burst Size (CBS) — Enter maximum burst size for the ingress queue (in bytes) in the Ingress Committed Burst Size (CBS) field. This is the amount of traffic that is allowed to pass as a temporary burst even if it is above the defined CIR.
- Exceed Action — Click the radio button that corresponds to the desired action in the Exceed Action field. This action takes place when an incoming packet exceeds the CIR.

  – None — No action is taken.

  – Drop — The packet is dropped.

  – Out of Profile DSCP — The DSCP value of the packet is remapped based on the Out of Profile DSCP Mapping Table.

Step 10. Click **Apply**.

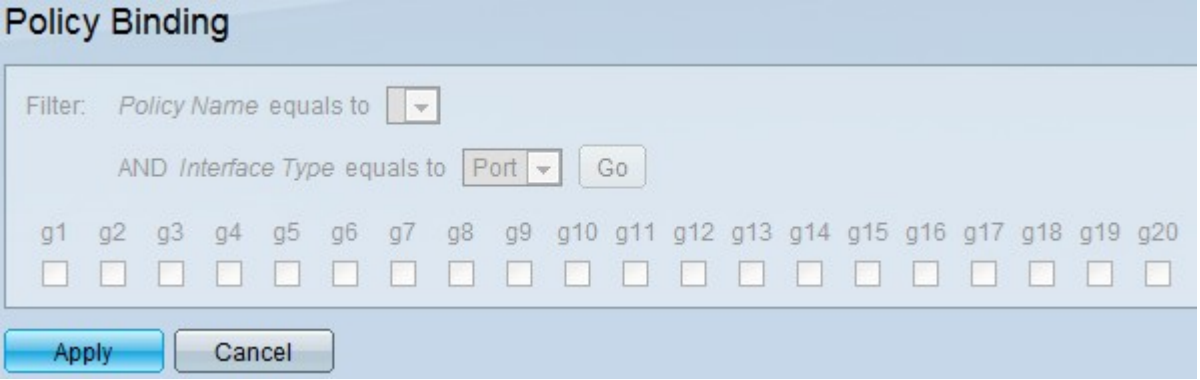
Policy Binding

The *Policy Binding* page is used to bind a policy to ports. A policy is considered active on the port once it is bound to the port. Only one policy can be bound to a port at a time, however a

single policy can be bound to multiple ports. When a policy is bound to a port, it filters and applies QoS to ingress traffic that matches the defined policy.

Note: To edit a policy, it must be unbound from all ports.

Step 1. Log in to the web configuration utility and choose **Quality of Service > QoS Advanced Mode > Policy Binding**. The *Policy Binding* page opens:



Step 2. From the Policy Name equals to drop-down list choose the policy that you want to bind to interfaces.

Step 3. From the Interface Type drop-down list choose the type of interface that you want to bind the policy to.

Step 4. Click **Go**. The interfaces are displayed.

Step 5. Check the desired check boxes in the Binding field to bind the policy to the port. All the packets that do not meet the rules of the policy will be dropped.

Step 6. Check the desired check boxes in the Permit Any field to override the policy and forward all the packets.

Step 7. Click **Apply**.