Quality of Service (QoS) Policy Class Maps Configuration on Sx500 Series Stackable Switches

Objective

Quality of Service (QoS) Policy consists of predefined rules that can measure the rate of traffic on the interface. They are used to enforce limits such as limiting the rate of file transfer traffic on the port. This helps to ensure that the bandwidth is not exceeded. A class map defines the type of packets that are considered to belong to the same traffic flow.

This article explains how to configure QoS policy class maps on the Sx500 Series Stackable Switches.

Applicable Devices

• Sx500 Series Stackable Switches

Software Version

• 1.3.0.62

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 drop-down list choose a policy.

Note: To create a new policy, click **Policy Table**. Please refer the section Policy Table Configuration in this article to configure the policy name.

Step 3. Click **Go** to bring up a list of class maps defined to the policy.

Step 4. Click **Add** to add a new class map to the policy.

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

Note: Class Maps can be created on the *Class Mapping* page. Please refer to the article, *Define QoS Class Mapping on Sx500 Series Stackable Switches,* for this configuration.

Step 6. Click the radio button that corresponds to the desired action in the Action type field. This action regards the ingress CoS/802.1p and/or Differential Services Code Point (DSCP) value of all the matching packets.

• Use Default Trust Mode — Ignore the ingress CoS/802.1p and/or DSCP value. The matching packets are sent as best effort.

• Always Trust — The switch will trust CoS/802.1p and DSCP of the matching packet. If a packet is an IP packet, the switch will put the packet in the egress queue based on the DSCP value of the packet and the DSCP to Queue Table. If a packet is a non-IP packet, the switch will put the packet in the egress queue based on the CoS/802.1p value of the packet and the CoS/802.1p to Queue Table.

• Set — From the drop-down list choose a mode regarding the matching packets.

– DSCP — Enter a value to determine the egress queue (0-63) in the New Value field. This value is based on the DSCP and the DSCP to Queue Table.

– Queue — Enter a value to determine the egress queue (1-4) in the New Value field.

– CoS/802.1p — Enter a value to determine the egress queue (0-7) in the New Value field. This value is based on the CoS/802.1p priority value and the CoS/802.1p to Queue Table.

Step 7. Click the radio button that corresponds to the desired policer type.

• None — No policy is used.

• Single — A single policer is used. A single policer applies the QoS to a single class map and a single flow based on the policer's QoS specification. Follow the steps from 9 to 11 if Single is chosen.

• Aggregate — An aggregate policy is used. An aggregate policer applies the QoS to one or more class maps and one or more flows.

Step 8. If the Aggregate radio button is clicked in Step 7, choose an aggregate policer from the Aggregate Policer drop-down list.

Note: Aggregate policers can be created on the *Aggregate Policer* page. Please refer to the article, *Add Aggregate Policer in QoS Advanced Mode on Sx500 Series Stackable Switches* for this configuration.

Step 9. If the Single radio button is clicked in the Police Type field, enter a value for the Committed Information Rate (CIR) measured in bits per second in the Ingress Committed Information Rate (CIR) field. This is the average maximum number of data that can be

received from the ingress interface. If this rate is exceeded, the data is discarded.

Step 10. Enter the maximum burst size (even if it goes beyond the CIR) in bytes in the Ingress Committed Burst Size (CBS) field. The maximum burst size is the amount of data which can be sent on the link even if it exceeds beyond the allowable limit and increases the bandwidth of the link.

Step 11. Click the radio button that corresponds to the desired exceed action. This action is taken when the incoming packets exceed the CIR.

• None — No action is taken.

• Drop — Packets that exceed the defined CIR value are dropped.

• Out of Profile DSCP — IP packets that exceed the defined CIR are forwarded with a new DSCP derived from the Out Of Profile DSCP Mapping Table.
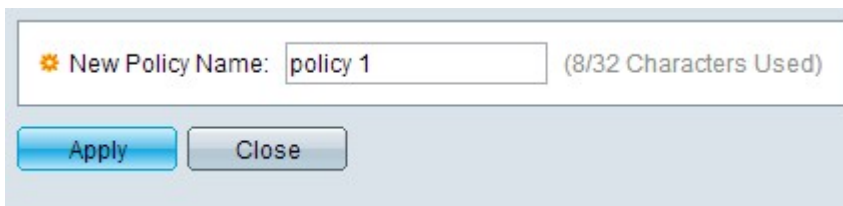

Step 12. Click **Apply**.

Policy Table Configuration

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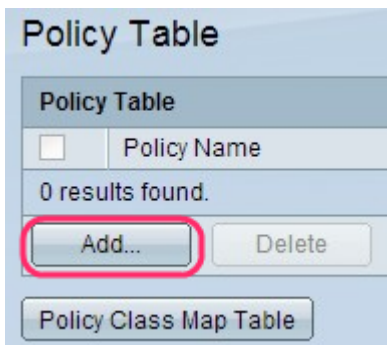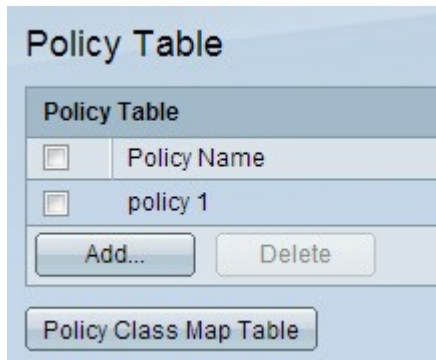

Step 2. Click **Add** to add a Policy Name. The *Add Policy Table* window appears.

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

Step 4. Click **Apply** to apply the settings.

Step 5. (Optional) Click **Delete** to delete the Policy Name.

Note: To go to the *Policy Class Map Table* page, Click Policy Class Map Table in the *Policy Table* page.