PURPOSE
The existing policy definition infrastructure is enhanced to provide the capability to specify a meter with the commit and peak rate. The admin can use the CLI to specify a traffic flow that is defined by a number of matched criteria. This traffic flow is associated with a policy command that is enhanced to allow the user to specify a meter with the rates and actions. Traffic Policing is typically deployed in access layer switches to protect against excessive burst traffic from an endpoints or distribution layer switches. Similarly, if Traffic Policing is enabled in distribution layer switches then, the distribution layer switches is protected against excessive burst traffic from an access and core layer switches. You can implement Traffic Policing in all three layers (core, distribution, and access) to protect against excessive traffic.

Traffic Policing is an implementation of RFC-2698 which states that the Two Rate Three Color Marker (trTCM) meters an IP packet stream and marks its packets either green, yellow, or red. A packet is marked red if it exceeds the Peak Information Rate (PIR). Otherwise, it is marked either yellow or green depending on whether it exceeds or does not exceed the Committed Information Rate (CIR). The trTCM is useful, for example, for ingress policing of a service, where a Peak Rate needs to be enforced separately from a committed rate.

ArubaOS-Switch already have a Single Rate Marker which rate limits any incoming/outgoing traffic; however, the violation action of this meter is dropped. With Traffic Policing feature being introduced in ArubaOS-Switch version 16.06, the trTCM are Commit and Peak where any incoming excessive traffic rate is being committed with an action to reprioritized the packets using Differentiated Services Code Point (DSCP) remarking. The DSCP determines the priority of the packet. As for Peak Rate, any incoming excessive traffic have two options or actions to take where either the packets are reprioritized using DSCP remarking or the packets are dropped similar to Single Rate Meter.

Traffic rates
The RFC-2698: A two rate three color marker, provides you an option to categorize the incoming traffic based on the following two rates (in kilobits per seconds).

Commit Information Rate (CIR)
Specifies the bandwidth limit for guaranteed traffic. Once it exceeds the limit, you can only perform DSCP remarking (changing priority).

Peak Information Rate (PIR)
Specifies the bandwidth limit for peak traffic. Once it exceeds the limit, you can either remark the DSCP again or drop the incoming traffic.

You can configure the meter with preceding traffic rates using the CLI. The ‘show’ command output provides the administrator a statistical overview of the metered packets. Traffic Policing is supported only on IPv4 and IPv6 traffic classes and not on MAC class. Traffic Policing also does not support burst size.

CONFIGURATION
Use the class command to configure a traffic policy by specifying a meter with commit and peak-rates. Traffic Policing helps the administrator to monitor the traffic flow from the configured value. Execute the class command from the user policy context. Set the user policy from the config context with the policy user <policyname> command before executing the class command.
Class

Syntax

[<SEQ-NUM>] class { ipv4 | ipv6 } <CLASS-NAME>

  { action meter
    commit-rate kbps <1-10000000> dscp-remark
    peak-rate kbps <1-10000000> {drop | dscp-remark} }

no [<SEQ-NUM>] class { ipv4 | ipv6 } <CLASS-NAME>

  { action meter
    commit-rate kbps <1-10000000> dscp-remark
    peak-rate kbps <1-10000000> {drop | dscp-remark} }

Description

Allows you to configure the traffic as per two rate three color policy specified in RFC 2698. The no form of this command removes the metered traffic rate entries from the running configuration output.

Command context

config, config-class, and policy-qos.

Parameters

commit-rate
 Configures the commit-rate as per RFC 2698.

commit-rate kbps<1-10000000>
 Configures the commit-rate in Kb/s. Range: 1-10000000.

dscp-remark
 Remarks the DSCP for traffic that exceeds the commit or peak-rate.

peak-rate
 Configures the peak-rate as per RFC 2698.

peak-rate kbps<1-10000000>
 Configures the peak-rate in Kb/s. Range: 1-10000000.

drop
 Drops the traffic which exceeds the peak-rate.

Usage

If the traffic on the interface on which the policy is applied exceeds:

- For the commit-rate, its DSCP is remarked to the configured value.
- For the peak-rate, traffic is either dropped or DSCP remarked again.

Scenarios

Scenario 1
The commit-rate is greater or equal to peak rate, an error is displayed when the commit-rate exceeds the peak rate value.

switch(policy-qos)# 10 class ipv4 class1 action meter commit-rate kbps 1000 dscp-remark cs7
peak-rate kbps 1000 drop
The commit rate must be less than the peak rate.
Scenario 2
If you apply a policy action meter on a MAC class, an error "Only IPv4 and IPv6 classes are supported" appears.

Scenario 3
If the commit-rate and peak-rate are not in the range <1 to 1000000>, an error that the rates are not within the configured values appears.

Scenario 4
If you apply a policy with action meter on an interface with 'out' direction, an error "QoS policy with action meter cannot be applied for a port with outbound direction" appears.

```
switch(config)# interface 1 service-policy qos-policy-1
in    Apply the policy to inbound packets on the port.
Out   Apply the policy to outbound packets on the port.

switch(config)# interface 1 service-policy qos-policy-1
out   The QoS policy with the action 'meter' cannot be applied to a port in the outbound direction.
```

Scenario 5
Meter classifier action is supported only on Ethernet ports. An error "QoS policy with classifier action meter is applicable only on Ethernet ports" appears.

```
switch(vlan-1)# service-policy test in
QoS policy with classifier action meter is applicable only on Ethernet ports.
```

Scenario 6
When you configure a class with action meter for a policy applied on trunk or VLAN, an error "Class with meter action cannot be configured for the policy applied on trunk or VLAN" appears.

Scenario 7
Remarking of 802.1q priority (CoS) field with the corresponding DSCP value is not supported. If attempted, the CoS field of the packet will be set to zero and only the DSCP field of the packet is remarked. The following behavior is noted due to this restriction:

**Meter has a higher precedence over ACLs**
Occurs if you apply CoS through QoS ACL on the same port as two rate meter. The CoS value of the packet is set to zero as CIR/PIR DSCP are applied through a meter.

**Packets that are remarked by meter are always egressed out of the default-priority queue**
Occurs if the egress queue is selected based on the CoS value and ASIC limitation.
**Metered outcome is undetermined if multiple meters are applied on the same port**

Occurs when you meter the traffic on a port using a QoS policy, and apply a new meter on the same port for that class of traffic using a user-policy. Due to ASIC limitation, the outcome of the metered rate is not determined.

The following example shows difference in rate limit when a QoS policy and user policy is applied on the same port:

```
'policy-qos' is a QoS policy
'policy-user' is an user policy
'c1' is a class which matches all IP traffic

switch(config)# show policy policy-qos
Statements for policy "policy-qos"
policy qos "policy-qos"
10 class ipv4 "c1" action rate-limit kbps 2000
exit

switch(config)# show policy policy-user
Statements for policy "policy-user"
policy user "policy-user"
10 class ipv4 "c1" action rate-limit kbps 1000
exit

switch(config)# show class ipv4 c1
Statements for class IPv4 "c1"
300 Aruba 3810 / 5400R Advanced Traffic Management Guide for ArubaOS-Switch 16.05
class ipv4 "c1"
10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

The QoS Policy, policy-qos is applied to the interface
```

switch(config)# show run int 1
Running configuration:
```
interface 1
service-policy "policy-qos" in
untagged vlan 10
aaa port-access mac-based
exit

In the preceding example, we observe that the rate at which traffic is limited is as per the configuration (2000 kbps). We also observe that port 1 is enabled with mac-based authentication. As part of mac-based authentication, user-policy is applied to the client.

The following show command displays the client details.

A mac-auth client is applied on the same port with user policy, policy-user
switch(config)# show port-access client detail

Port Access Client Status Detail

Client Base Details :
Port : 1                   Authentication Type : mac-based
Client Status : authenticated       Session Time : 145 seconds
Client Name : 00000087b9fe         Session Timeout : 0 seconds
MAC Address : 000000-87b9fe       IP : n/a

User Role Information
Name : authRole
Type : local
Reauthentication Period (seconds) : 0
Untagged VLAN : 10
Tagged VLANs :
Captive Portal Profile :
Policy : policy-user

Statements for policy "policy-user"
 policy user "policy-user"
   10 class ipv4 "c1" action rate-limit kbps 1000
exit

Statements for class IPv4 "c1"
class ipv4 "c1"
   10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit

Tunnelednode Server Redirect : Disabled
Secondary Role Name :

After the port is applied with the meter specified in user policy, policy-user (1000 kbps), the rate of traffic varies between 0 kbps and 1000 kbps.

You can overcome the preceding restrictions using the following work-around:

- Stop the incoming traffic or the lower the rate to less than 100 kbps for a couple of seconds after you apply the second meter on the port.
- Before the traffic flow, apply the meters on the interface.

Restrictions
Traffic policing comes with the following restrictions:

- Does not support MAC classes.
- Cannot configure burst size even though RFC 2698 allows you to specify committed burst size and peak burst size.
Incorrect burst sizes can either lead to excessive traffic loss, or poor rate-limiting thus reducing the performance.

- Cannot configure rates in packets-per-second.
- Exceeded commit-rate packets are only DSCP remarked.
- Operates only in color blind mode.
- Applicable only for QoS policies and not PBR or mirror policies.
- Cannot configure using Next Gen WEBUI or switch menu.
- QoS policy containing a two-rate meter can only be applied on individual physical interfaces, and not on logical interfaces (VLANs or LAG).
- The Egress ACLs do not support DSCP remarking. As DSCP remarking is the only supported action for commit-rate violation, traffic policing cannot be enabled on an outward interface.
- If you apply CoS through QoS ACL on the same port as two rate meter, the meter has a higher precedence over ACLs. The CoS value of the packet is set to zero as CIR/PIR DSCP is applied through a meter.

The following is another sample configuration for Traffic Policing feature, and it is combined with all three part of the feature such as class, QoS, and Interface commands.

```plaintext
class ipv4 "class1"
10 match ip 10.28.0.1 255.255.0.0 any vlan 2
policy qos "policy1"
10 class ipv4 "class1" action meter commit-rate kbps 100 dscp-remark 32 peak-rate kbps 500 drop
interface 1
service-policy "policy1" in
```

In the sample configuration above, traffic from any host in the 10.28.0.0/16 subnet to any host on VLAN 2 received on port 1 is metered. As a result, the traffic that exceeds 100 Kbps will be remarked with DSCP value 32 and the traffic that exceeds 500 Kbps will be dropped.

The action supported when the commit rate is exceeded is to remark the DSCP value of the flow. The user has the option to specify the remarked DSCP value.

There will be one of two actions supported when the peak rate is exceeded. The user can choose to either remark the DSCP again, or drop the traffic. Based on the updated DSCP value, the egress queue used by the flow will be changed.

**SUPPORTED PLATFORMS**

This feature, Traffic Policing, is supported on the following ArubaOS-Switch software version 16.06.

- Aruba 2930M/F Series Switch
- Aruba 3810M Series Switch
- Aruba 5400R Series Switch