FiberstoreOS

Traffic Managemant Configuration Guide

Contents

Tables

1 Configuring QoS

1.1 Overview

Quality of Service (QoS) can be used to give certain traffic priority over other traffic.

Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped.

With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

QoS Functionality

Classification information can be carried in the Layer-3 IP packet header or the Layer-2 frame. IP packet headers carry the information using 6 bits or 3 bits from the deprecated IP type of service (TOS) field. Layer-2 802.1Q frames carry the information using a 2-byte Tag Control Information field.

All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

- End hosts or switches along a path, based on a configured policy
- Detailed packet examination, expected to occur nearer to the network edge, to prevent overloading core switches and routers
- A combination of the above two techniques

Class information can be used by switches and routers along a path to limit the amount of allotted resources per traffic class.

Per-hop behavior is an individual device’s behavior when handling traffic in the DiffServ architecture. An end-to-end QoS solution can be created if all devices along a path have consistent per-hop behavior.

1.2 Terminology

Following is a brief description of terms and concepts used to describe QoS.

ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP ACLs, and non-IP traffic is classified using MAC ACLs.

The ACL can have multiple access control entries (ACEs), which are commands that match fields against the fiberstore of the packet.

CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network.

QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic.

Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS values in the 3 most significant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN.

Other frame types cannot carry Layer-2 CoS values.

CoS values range from 0 to 7.

DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network.

DSCP values range from 0 to 63.

IP-Precedence Value

IP-Precedence is a 3-bit value used to classify the priority of Layer-3 packets upon entry into a network.

IP-Precedence values range from 0 to 7.

EXP Value

EXP value is a 3-bit value used to classify the priority of MPLS packets upon entry into a network.

MPLS EXP values range from 0 to 7.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. The process generates an internal priority for a packet, which identifies all future QoS actions to be taken on the packet.

Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the priority is determined based on ACLs or the configuration. The Layer-2 CoS value is then mapped to a priority value.

The classification is carried in the IP packet header using 6 bits or 3 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer-2 frame.

Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs.

Classification occurs on an ingress physical port, but not at the switch virtual interface level.

Classification can be based on CoS/inner-CoS/DSCP/IP-Precedence, default port cos, or class maps and policy maps.

Shaping

Shaping is to change the rate of incoming traffic flow to regulate the rate in such a way that the outgoing traffic flow behaves more smoothly. If the incoming traffic is highly bursty, it needs to be buffered so that the output of the buffer is less bursty and smoother.

Shaping has the following attributes:

- Shaping can be deployed base on physical port.
- Shaping can be deployed on queues of egress interface.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal priority to the configured policer.

The policer limits the bandwidth consumed by a traffic flow. The result is given to the marker.

There are two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, the aggregate policer is shared by multiple classes of traffic within one or multiple policy map.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration information to determine the action required for the packet, and then handles the packet using one of the following methods:

- Let the packet through and mark color down
- Drop the packet

Marking can occur on ingress and egress interfaces.

Queuing

Queuing maps packets to a queue. Each egress port can accommodate up to 8 unicast queues, 4 multicast queues and 1 SPAN queue.

The packet internal priority can be mapped to one of the egress queues. The unit of queue depth is buffer cell. Buffer cell is the granularity, which is 288 bytes, for packet storing.

After the packets are mapped to a queue, they are scheduled.

Tail Drop

Tail drop is the default congestion-avoidance technique on the interface. With tail drop, packets are queued until the thresholds are exceeded. The packets with different priority and color are assigned to different drop precedence. The mapping between priority and color to queue and drop precedence is configurable. You can modify the three tail-drop threshold to every egress queue by using the queue threshold interface configuration command. Each threshold value is packet buffer cell, which ranges from 0 to 16383.

WRED

Weighted Random Early Detection (WRED) differs from other congestion-avoidance techniques because it attempts to anticipate and avoid congestion, rather than controlling congestion when it occurs.

WRED reduces the chances of tail drop by selectively dropping packets when the output interface begins to show signs of congestion. By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once. Thus, WRED allows the transmission line to be fully used at all times. WRED also drops more packets from large users than small. Therefore, sources that generate the most traffic are more likely to be slowed down versus sources that generate little traffic.

You can enable WRED and configure the two thresholds for a drop-precedence assigned to every egress queues. The WRED's color drop precedence map is the same as tail-drop's. Each min-threshold represents where WRED starts to randomly drop packets. After min-threshold is exceeded, WRED randomly begins to drop packets assigned to this threshold. As the queue max-threshold is approached, WRED continues to drop packets randomly with the rate of drop-probability. When the max-threshold is reached, WRED drops all packets assigned to the threshold. By default, WRED is disabled.

Scheduling

Scheduling forwards conditions packets using combination of WDRR and SP. Every queue belongs to a class. The class range from 0 to 7, and 7 is the highest priority. Several queues can be in a same class, or non queue in some class. Packets are scheduled by SP between classes and WDRR between queues in a class.

- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted.
- Weighted Deficit Round Robin (WDRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.

Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can match several access groups defined by the ACL.

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

- Set a specific priority and color in the traffic class.
- Set a specific trust policy to map priority and color.
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.
- Redirect the matched traffic class to a specific physical interface.
- Mirror the matched traffic class to a specific monitor session, which's destination is defined in mirror module(please refer to the "monitor session destination " command).
- Enable statistics of matching each ace or each class-map(if the class-map operator is match-any).
- Policy maps have the following attributes:
- A policy map can contain multiple class statements, each with different match criteria and action.
- A separate policy-map class can exist for each type of traffic received through an interface.
- There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.
- Before a policy map can be effective, it must be attached to an interface.
- A policy map can be applied on physical interface(not link agg member), link agg interface, or vlan interface.

Mapping Tables

During QoS processing, the switch represents the priority of all traffic (including non-IP traffic) with an internal priority value:

- During classification, QoS uses configurable mapping tables to derive the internal priority (a 6-bit value) from received CoS, EXP(3-bit), DSCP or IP precedence (3-bit) values. These maps include the CoS-to-priority-color/COS-to-PHB map, EXP-to-priority-color/EXP-to-PHB map,

DSCP-to-priority-color/DSCP-to-PHB map and the IP-precedence-to- priority-color/IP-PREC-to-PHB map.

- During policing, QoS can assign another priority and color to an IP or non-IP packet (if the packet matches the class-map). This configurable map is called the policed-priority-color map.
- Before the traffic reaches the scheduling stage, and replace CoS or DSCP is set, QoS uses the configurable priority-color-to-CoS or priority-color-to-DSCP map to derive a CoS or DSCP value from the internal priority color.
- Each QoS domain has an independent set of map tables mentioned above.

Time-range

By using time-range, the aces in the class-map can be applied based on the time of day or week. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when adding an ace. You can use the time-range to define when the aces in the class-map are in effect, for example, during a specified time period or on specified days of the week.

These are some of the many possible benefits of using time-range:

- You can control over permitting or denying a user access to resources, such as an application, which is identified by an IP address and a port number.
- You can obtain the traffic statistics during appointed time.
- You can define when the action of a traffic class is in effect.

SRTCM

Single Rate Three Color Marker

TRTCM

Two Rate Three Color Marker

CIR

Committed Information Rate

CBS

Committed Burst Size

EBS

Excess Burst Size

PIR

Peak Information Rate

1.3 Modular QoS CLI

Input traffic is classified to a specified traffic class. All qos policies are attached to this traffic class.

class-map type qos

Type qos of class-map is used to identify traffic. The identification rules can be CoS/DSCP/IP Precendence/EXP/ACL.

policy-map type qos

Type qos of policy-map is used to assign traffic class. Type qos of class-map is refered by same type of policy-map.

class-map type traffic-class

Type traffic-class of class-map is used to identify traffic class. The identification rules is traffic class value.

policy-map type traffic-class

Type traffic-class of policy-map is used to specify qos policies. Type traffic-class of class-map is refered by same type of policy-map.

1.4 Configuration Guidelines

The following provides information to consider before configuring QoS:

- QoS policing cannot be configured on Linkagg interface.

- Traffic can be only classified per ingress port.
- There can be multiple ACLs per class map. An ACL can have multiple access control entries that match fields against the packet fiberstore.
- Policing cannot be done at the switch virtual interface level.

1.5 Topology

Figure 1-1 Bridge 1

1.6 Configurations

1.6.1 Configure egress queue

Tail Drop

Tail drop is the default congestion-avoidance technique on every egress queue. With tail drop, packets are queued until the thresholds are exceeded.

The following shows configuring tail drop threshold for different drop-precedence. Follow these steps from Privileged Exec mode.

- configure terminal
- create class-map with type traffic-class, matching traffic-class value
- create policy-map with type traffic-class, refer previous defined class-map
- specified queue threshold to this traffic class under policy-map class mode
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface

The following example shows configuring tail drop threshold for traffic class 3. In this example, packet drop threshold is 2000.

Table 1-1 Configure egress queue for tail drop

Switch# configure terminal	Enter the Configure mode

Switch(config)# class-map type traffic-class tc3	Create class-map
Switch(config-cmap-tc)# match traffic-class 3	Match traffic class 3
Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# policy-map type traffic-class tc	Create policy-map
Switch(config-pmap-tc)# class type traffic-class tc3	Refer class-map
Switch(config-pmap-tc-c)# queue-limit 2000	Configure packet drop threshold is 2000
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# exit	Exit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type traffic-class tc	Apply qos policies to interface
Switch(config-if)# end	Exit to EXEC mode
Switch# show qos interface eth-0-1 egress	Display QoS configuration

Validation

Switch# show qos interface eth-0-1 egress

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Max-Queue-Limit(Cell)	ECN
0	0	-	-	dynamic	level 0	-
1	0	-	-	dynamic	level 0	-
2	0	-	-	dynamic	level 0	-
3	0	-	-	tail-drop	2000	2000
4	0	-	-	dynamic	level 0	-
5	0	-	-	dynamic	level 0	-
6	0	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

WRED

WRED reduces the chances of tail drop by selectively dropping packets when the output interface detects congestion.

By dropping some packets early rather than waiting until the queue is full, WRED avoids TCP synchronization dropping and thereafter improves the overall network throughput.

The following shows configuring WRED threshold for different color. Follow these steps from Privileged Exec mode.

- configure terminal
- create class-map with type traffic-class, matching traffic-class value
- create policy-map with type traffic-class, refer previous defined class-map
- specified WRED threshold to this traffic class under policy-map class mode
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface

The following example shows configuring WRED threshold for traffic class 1. In this example, the max-threshold is 596, min-threshold is 596/8=71. If buffered packets exceed min-threshold, the subsequent packet will be dropped randomly.

Table 1-2 Configure egress queue for WRED

Switch# configure terminal	Enter the Configure mode
Switch(config)# class-map type traffic-class tc1	Create class-map
Switch(config-cmap-tc)# match traffic-class 1	Match traffic class 1
Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# policy-map type traffic-class tc	Create policy-map
Switch(config-pmap-tc)# class type traffic-class tc1	Refer class-map
Switch(config-pmap-tc-c)# random-detect maximum-threshold 596	Configure packet drop max-threshold is 596
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# exit	Exit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type traffic-class tc	Apply qos policies to interface
Switch(config-if)# end	Exit to EXEC mode
Switch# show qos interface eth-0-1 egress	Display QoS configuration

Validation

Switch# show qos interface eth-0-1 egress

```
TC Priority Bandwidth Shaping(kbps) Drop-Mode   Max-Queue-Limit(Cell)   ECN
```

```
0  0        -        -        dynamic     level 0                -
1  0        -        -        random-drop 596                    Disable
2  0        -        -        dynamic     level 0                -
3  0        -        -        tail-drop   2000                   2000
4  0        -        -        dynamic     level 0                -
5  0        -        -        dynamic     level 0                -
6  0        -        -        dynamic     level 0                -
7  7        -        -        tail-drop   64                     -
```

Schedule

Packets are scheduled by SP between different classes and WDRR between queues in the same class.

The following shows mapping queue to different classes and configuring WDRR weight. Follow these steps from Privileged Exec mode.

- configure terminal
- create class-map with type traffic-class, matching traffic-class value
- create policy-map with type traffic-class, refer previous defined class-map
- specified schedule class to this traffic class under policy-map class mode
- specified bandwidth to this traffic class under policy-map class mode
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface

The following example shows configuring schedule parameters for egress queues. In this example, traffic 5 and 6 belongs to class 6, which is highest priority. traffic 2 belongs class 0, the bandwidth is 20%.

Table 1-3 Configure egress queue for schedule

Switch# configure terminal	Enter the Configure mode
Switch(config)# class-map type traffic-class tc5	Create class-map
Switch(config-cmap-tc)# match traffic-class 5	Match traffic class 5
Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# class-map type traffic-class tc6	Create class-map
Switch(config-cmap-tc)# match traffic-class 6	Match traffic class 6
Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# class-map type traffic-class tc2	Create class-map
Switch(config-cmap-tc)# match traffic-class 2	Match traffic class 2

Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# policy-map type traffic-class tc	Create policy-map
Switch(config-pmap-tc)# class type traffic-class tc5	Refer class-map
Switch(config-pmap-tc-c)# priority level 6	Specifiy class 6
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# class type traffic-class tc6	Refer class-map
Switch(config-pmap-tc-c)# priority level 6	Specifiy class 6
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# class type traffic-class tc2	Refer class-map
Switch(config-pmap-tc-c)# bandwidth percentage 20	Specifiy bandwidth to 20% of link bandwidth
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode
Switch(config-pmap-tc)# exit	Exit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type traffic-class tc	Apply qos policies to interface
Switch(config-if)# end	Exit to EXEC mode
Switch# show qos interface eth-0-1 egress	Display QoS configuration

Validation

Switch# show qos interface eth-0-1 egress

```
TC  Priority  Bandwidth  Shaping(kbps)  Drop-Mode    Max-Queue-Limit(Cell)    ECN
0   0         -          -              dynamic      level 0                  -
1   0         -          -              random-drop  596                      Disable
2   0         20         -              dynamic      level 0                  -
3   0         -          -              tail-drop    2000                     2000
4   0         -          -              dynamic      level 0                  -
5   6         -          -              dynamic      level 0                  -
6   6         -          -              dynamic      level 0                  -
7   7         -          -              tail-drop    64                       -
```

Configure port policing

All traffic received or transmitted in the physical interface can be limited rate, and all the exceeding traffic will be dropped.

The following shows creating a port-policer to limit bandwidth. Follow these steps from Privileged Exec mode.

- configure terminal.
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface
- qos port-policer input|output color-blind|color-aware cir <8-100000000> cbs <1000-640000> ebs <1000- 640000>| eir <8-100000000> ebs <1000-640000> drop-color exceed|violate drop statistics to specify a port policer.

The no port-policier input|output command deletes a port policer.

The following example shows creating an ingress port policer. In this example, if the received traffic exceeds a 48000-kbps average traffic rate, it is dropped.

Table 1-4 Configure port policing

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop	Configure 48000-kbps average traffic rate to be limited
Switch(config-if)# end	Exit to EXEC mode
Switch# show qos interface eth-0-1 statistics policer port input	Display QoS status

Validation

Switch# show qos interface eth-0-1 statistics policer port input

```
Interface: eth-0-1
  input port policer:
   color blind
    CIR 48000 kbps, CBS 10000 bytes, EBS 20000 bytes
    drop violate packets
```

1.6.2 Configure shaping

Port shaping

All traffic transmitted in the physical interface can be shaped, and all the exceeding traffic will be buffered. If no buffer, it is dropped.

The following shows creating a port shaping to shape traffic. Follow these steps from Privileged Exec mode.

- configure terminal.
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface
- qos shape rate <0-100000000> to specify a port shaping.

The no shape command deletes a port shaping.

The following example shows creating a port shaping. In this example, if the received traffic exceeds a 1000Mbps, it is buffered.

Table 1-5 Configure port shaping

Switch#configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# qos shape rate 1000000	Configure the received traffic exceeds 1000Mbps, it will be buffered
Switch(config-if)# end	Exit to EXEC mode
Switch# show running-config interface eth-0-1	Display QoS status

Validation

Switch# show running-config interface eth-0-1

```
Building configuration...
!
interface eth-0-1
 service-policy type traffic-class tc
```

```
 qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop
 qos shape rate 1000000
!
```

Queue shaping

All the traffic in the egress queue can be shaped, and all the exceeding traffic will be buffered. If no buffer, it is dropped.

The following shows creating a queue shaping to shape traffic. Follow these steps from Privileged Exec mode.

- configure terminal
- create class-map with type traffic-class, matching traffic-class value
- create policy-map with type traffic-class, refer previous defined class-map
- specified shaping rate to this traffic class under policy-map class mode
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface

NOTE

The no shape rate command deletes a queue shaping.

The following example shows creating a queue shaping for queue 3. In this example, if the traffic in queue 3 exceeds 1000Mbps, it is buffered.

Table 1-6 Configure queue shaping

Switch# configure terminal	Enter the Configure mode
Switch(config)# class-map type traffic-class tc3	Create class-map
Switch(config-cmap-tc)# match traffic-class 3	Match traffic class 3
Switch(config-cmap-tc)# exit	Exit to Configure mode
Switch(config)# policy-map type traffic-class tc	Create policy-map
Switch(config-pmap-tc)# class type traffic-class tc3	Refer class-map
Switch(config-pmap-tc-c)# shape rate 1000000	Configure queue shape rate to 1000Mbps
Switch(config-pmap-tc-c)# exit	Exit to policy-map mode

Switch(config-pmap-tc)# exit	Exit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type traffic-class tc	Apply qos policies to interface
Switch(config-if)# end	Exit to EXEC mode
Switch# show qos interface eth-0-1 egress	Display QoS configuration

Validation

Switch# show qos interface eth-0-1 egress

```
TC  Priority  Bandwidth  Shaping(kbps)  Drop-Mode    Max-Queue-Limit(Cell)    ECN
0   0         -          -              dynamic      level 0                  -
1   0         -          -              random-drop  596                      Disable
2   0         20         -              dynamic      level 0                  -
3   0         -          1000000        tail-drop    2000                     2000
4   0         -          -              dynamic      level 0                  -
5   6         -          -              dynamic      level 0                  -
6   6         -          -              dynamic      level 0                  -
7   7         -          -              tail-drop    64                       -
```

1.6.3 Configure Policy

To configure a QoS policy, the following is usually required:

- Categorize traffic into classes.
- Configure policies to apply to the traffic classes.
- Attach policies to interfaces.

Classify Traffic Using ACLs

IP traffic can be classified using IP ACLs.

The following shows creating an IP ACL for IP traffic. Follow these steps from Privileged Exec mode.

- configure terminal.
- ip access-list ACCESS-LIST-NAME. ACCESS-LIST-NAME = name of IP ACL
- create ACEs, Repeat this step as needed. For detail, please refer to ACL configuration Guide

NOTE

The no ip access-list command deletes an access list.

The following example shows allowing access only for hosts on three specified networks. Wildcard bits correspond to the network address host portions. If a host has a source address that does not match the access list statements, it is rejected.

Table 1-7 Configure IP ACL

Switch#configure terminal	Enter the Configure mode
Switch(config)# ip access-list ip-acl	Enter the IP access list mode
Switch(config-ip-acl)# permit any 128.88.12.0 0.0.0.255 any	Configure permit source ip address 128.88.12.x into ACL list
Switch(config-ip-acl)# permit any 28.88.0.0 0.0.255.255 any	Configure permit source ip address 28.88.x.x into ACL list
Switch(config-ip-acl)# permit any 11.0.0.0 0.255.255.255 any	Configure permit source ip address 11.x.x.x into ACL list
Switch(config-ip-acl)# end	Exit to EXEC mode
Switch# show access-list ip ip-acl	Display ACL status

Validation

Switch# show access-list ip ip-acl

```
ip access-list ip-acl
  10 permit any 128.88.12.0 0.0.0.255 any
  20 permit any 28.88.0.0 0.0.255.255 any
  30 permit any 11.0.0.0 0.255.255.255 any
```

Create class-map

The following shows classifying IP traffic on a physical-port basis using class maps. This involves creating a class map, and defining the match criterion.

- configure terminal.
- ip access-list ACCESS-LIST-NAME. ACCESS-LIST-NAME = name of IP ACL
- create ACEs, Repeat this step as needed. For detail, please refer to ACL configuration Guide

- class-map (match-any|match-all) NAME to create a class map. match-any = Use the match-any keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched. match-all = Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. NAME = name of the class map.

If neither the match-any or match-all keyword is specified, the default is match-any.

- match access-group NAME to define the match criterion. NAME = name of the ACL created using the ip access-list command.

The no class-map command deletes an existing class-map.

The following example shows configuring a class map named cmap1 with 1 match criterion: IP access list ip-acl, which allows traffic from any source to any destination.

Table 1-8 Configure class map

Switch# configure terminal	Enter the Configure mode
Switch(config)# ip access-list ip-acl	Enter the IP access list mode
Switch(config-ip-acl)# permit any any any	Configure permit any into ACL list
Switch(config-ip-acl)# quit	Quit to Configure mode
Switch(config)# class-map cmap1	Create and enter into class-map cmap1 mode
Switch (config-cmap)# match access-group ip-acl	Configure ip-acl into cmap1
Switch (config-cmap)# end	Exit to EXEC mode
Switch# show class-map cmap1	Display Class Map status

Validation

Switch# show class-map cmap1

```
    CLASS-MAP-NAME: cmap1 (match-any)
```

```
      match access-group: ip-acl
```

Create Policy Map

The following shows creating a policy map to classify, policer, and mark traffic.

- configure terminal.
- ip access-list to create an IP ACL.
- class-map type qos NAME to create a class map.
- policy-map type qos NAME to create a policy map. NAME = name of the policy map.
- class NAME to define a traffic classification. NAME = name of the class map.
- exit.
- interface IFNAME to specify the interface to match to the policy map. IFNAME = name of interface
- service-policy type qos input NAME to apply a policy map to the input of the specified interface. NAME = policy-map name to apply the specified policy-map to the interface.

There can be only one policy map per interface per direction.

The no policy-map command deletes an existing policy-map. The no set priority color command removes a specified priority color value. The no policer command removes an existing policer. The no trust command removes trust policy. The no service-policy input|output command removes a policy map from interface.

The following example shows creating a policy map, and attaching it to an ingress interface. In this example, the IP ACL allows traffic from network 10.1.0.0. If the matched traffic exceeds a 48000-kbps average traffic rate, it is dropped.

Table 1-9 Configure policy map

Switch#configure terminal	Enter the Configure mode
Switch(config)# ip access-list ip-acl	Enter the IP access list mode
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	Configure permit 10.1.x.x into ACL list

Switch(config-ip-acl)# quit	Quit to Configure mode
Switch(config)# class-map type qos cmap1	Create and enter into class-map cmap1 mode
Switch(config-cmap)# match access-group ip-acl	Configure ip-acl into cmap1
Switch(config-cmap)# quit	Quit to Configure mode
Switch(config)# policy-map type qos pmap1	Create and enter into policy-map pmap1 mode
Switch(config-pmap)# class type qos cmap1	Attach class-map cmap1 into policy-map pmap1
Switch(config-pmap-c)# policer color-blind cir 48000 cbs 10000 ebs 128000	Configure 48000-kbps average traffic rate to be limited
Switch(config-pmap-c)# quit	Quit to policy-map mode
Switch(config-pmap)# quit	Quit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type qos input pmap1	Attach policy-map pmap1 to interface
Switch(config-if)# end	Exit to EXEC mode
Switch# show policy-map pmap1	Show police-map

Validation

Switch# show policy-map pmap1

```
  POLICY-MAP-NAME: pmap1( type qos)
    State: attached

    CLASS-MAP-NAME: cmap1
      match access-group: ip-acl
        mode rfc2697, CIR 48000 kbps, CBS 10000 bytes, EBS 16000 bytes, color blind mode, drop color
is red
```

Create Aggregate Policer

The following shows creating an aggregate policer to classify, police, and mark traffic.

- configure terminal.

- qos aggregate-policer NAME color-blind|color-aware cir <8-100000000> cbs <1000-640000> ebs <1000- 640000>| eir <8-100000000> ebs <1000-640000> drop-color exceed|violate drop statistics to specify policer parameters to apply to multiple traffic classes in the same or different policy-map.
- class-map type qos NAME to create a class map.
- policy-map type qos NAME to create a policy map.
- class type qos NAME to define a traffic classification.
- aggregate-policer NAME to apply the previously named aggregate policer to multiple classes in the same or different policy-map.
- exit.
- exit.
- interface IFNAME to specify the interface to match to the policy map.
- service-policy input/output NAME to apply a policy map to the input or output of the specified interface.

There can be only one policy map per interface per direction.

The no policer-aggregate command deletes an aggregate policer from a policy map. The no qos aggregate-policer command deletes an aggregate policer.

The following example shows creating an aggregate policer, and attaching it to multiple classes within a policy map. In this example, the IP ACLs allow traffic from network 10.1.0.0 and host 11.3.1.1. The traffic rate from network 10.1.0.0 and host 11.3.1.1 is policed. If the traffic exceeds a 48000-kbps average traffic rate and an 8000-byte normal burst size, it is considered out of profile, and is dropped. The policy map is attached to an ingress interface.

Table 1-10 Configure aggregate policing

Switch#configure terminal	Enter the Configure mode
Switch(config)# ip access-list ip-acl1	Enter the IP access list mode

Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	Configure permit source ip address 10.1.x.x into ACL list
Switch(config-ip-acl)# exit	Quit to Configure mode
Switch(config)# ip access-list ip-acl2	Enter the IP access list mode
Switch(config-ip-acl)# permit any host 11.3.1.1 any	Configure permit source ip address 11.3.1.1 into ACL list
Switch(config-ip-acl)# exit	Quit to Configure mode
Switch(config)# qos aggregate-policer transmit1 color-blind cir 48000 cbs 8000 ebs 10000 violate drop	Configure 48000-kbps average traffic rate to be limited
Switch(config)# class-map type qos cmap1	Create and enter into class-map cmap1 mode
Switch(config-cmap)# match access-group ip-acl1	Configure ip-acl1 into cmap1
Switch(config-cmap)# exit	Quit to Configure mode
Switch(config)# class-map type qos cmap2	Create and enter into class-map cmap2 mode
Switch(config-cmap)# match access-group ip-acl2	Configure ip-acl2 into cmap2
Switch(config-cmap)# exit	Quit to Configure mode
Switch(config)# policy-map type qos aggflow1	Create and enter into policy-map aggflow1mode
Switch(config-pmap)# class type qos cmap1	Attach class-map cmap1 into policy-map aggflow1
Switch(config-pmap-c)# aggregate-policer transmit1	Set cmap1 as policer-aggregate transmit1
Switch(config-pmap-c)# exit	Quit to policy-map mode
Switch(config-pmap)# class type qos cmap2	Attach class-map cmap2 into policy-map pmap1
Switch(config-pmap-c)# aggregate-policer transmit1	Set cmap2 as policer-aggregate transmit1
Switch(config-pmap-c)# exit	Quit to policy-map mode
Switch(config-pmap)# exit	Quit to Configure mode
Switch(config)# interface eth-0-1	Enter the Interface mode
Switch(config-if)# service-policy type qos input aggflow1	Attach aggregator-policer aggflow1 to interface
Switch(config-if)# exit	Quit to Configure mode

Switch(config)# exit	Exit to EXEC mode
Switch# show qos aggregate-policer	Show aggregator-policer configuration

Validation

Switch# show qos aggregate-policer

```
Aggreate policer: transmit1
  color blind
  CIR 48000 kbps, CBS 8000 bytes, EBS 10000 bytes
  drop violate packets
```