Contents

1 Configuring QoS

1.1 Introduction

1.1.1 Overview

Quality of service (QoS) can meet users' requirements for different applications and different levels of service quality. It allocates and schedules resources based on users' requirements and provides different levels of service quality for different packets.

On a traditional IP network, a device treats all the packets in the same way, in which the device processes packets based on their arrival time according to the queuing strategy of first in first out (FIFO), and transmits the packets to the destination on a best-effort basis. When the network bandwidth is abundant, all the packets are properly processed; when the network is congested, all the packets may be discarded.

QoS assigns a transmission priority to the packets of a type to highlight the importance of the packets. Then, the devices provide special transmission services for these packets according to forwarding policies for different priorities, congestion avoidance, and other mechanisms. With QoS, a device processes real-time and important packets preferentially, processes non-real-time and common packets with lower priorities and even discards the packets upon network congestion.

QoS enhances the network performance predictability, effectively allocates network bandwidth, and reasonably utilizes network resources.

1.1.2 Principles

1. Basic Concepts

- DiffServ model

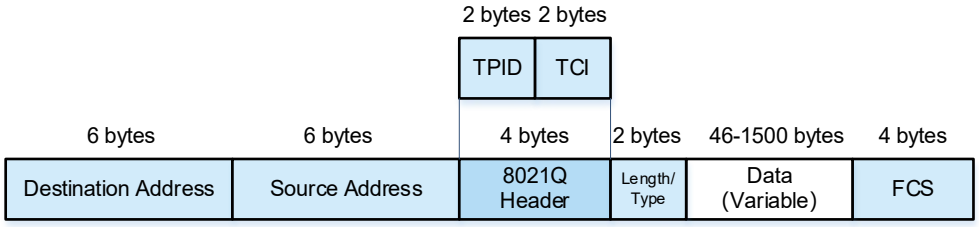
  The differentiated services (DiffServ) model classifies all packets transmitted on a network into different types. The classification information related to QoS priority marking is recorded in some fields of L2 or L3 packets, for example, the PRI field of IEEE 802.1Q frames, type of service (ToS) field of IPv4 packets, and traffic class (TC) field of IPv6 packets.

  In the network of DiffServ model, the classification information of packets can be assigned by hosts or other network devices or based on different application policies or different packet contents. A device applies the same transmission service policy to packets containing the same classification information and applies different transmission service policies to packets containing different classification information. Based on the classification information carried by packets, a device may provide different transmission priorities for different packets, reserve bandwidth for a kind of packets, discard certain packets with lower priorities, or take some other actions.

- PRI field of the IEEE 802.1q frames

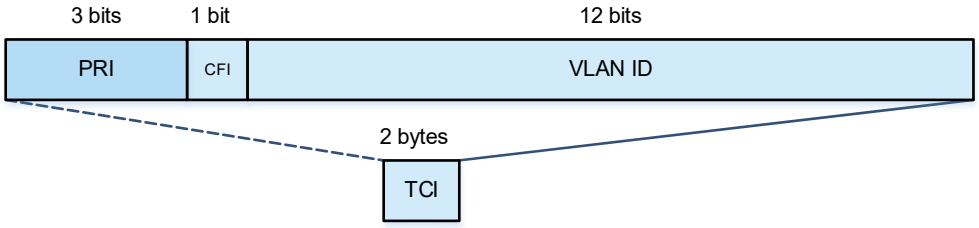
  The PRI field of IEEE 802.1Q frames (namely, the IEEE 802.1p priority) is located in the header of an L2 packet containing an IEEE 802.1Q tag header, as shown in Figure 1-1.

Figure 1-1 Format of an L2 Frame with an IEEE 802.1Q Tag Header



The 4-byte IEEE 802.1Q tag header contains the 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). TCI contains the 3-bit PRI field, as shown in Figure 1-2.

Figure 1-2 PRI Field of the IEEE 802.1q Frames

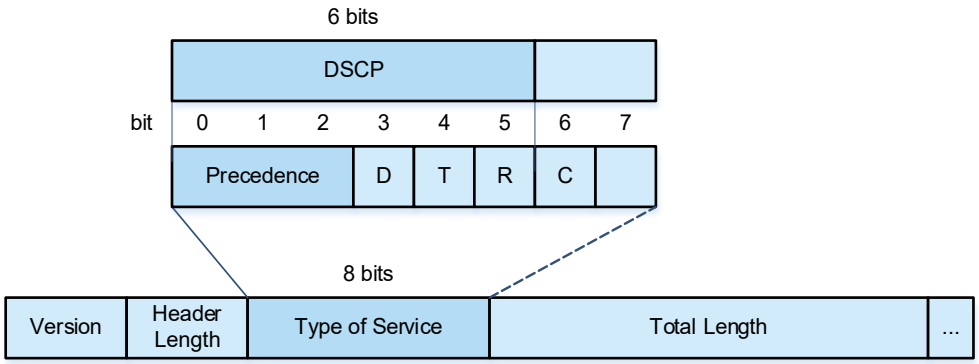


The PRI field represents eight priorities for packet transmission, and the priority values from high to low are 7, 6, ..., 1, and 0. The IEEE 802.1p priority is applicable to scenarios where L3 headers do not need to be analyzed and QoS needs to be implemented only at L2.

- ToS field of the IPv4 packets

  IPv4 packets use the ToS field in the IP header to indicate the priority of the packets, as shown in Figure 1-3.

Figure 1-3 ToS Field in the IP Header



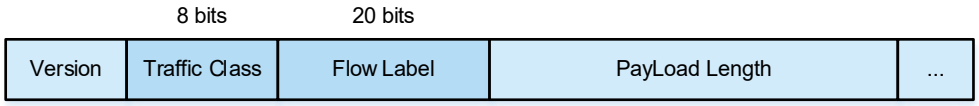
The ToS field contains eight bits, of which the first three bits are the IP PRE (precedence) field and represent eight priorities for packet transmission, with the priority values from high to low being 7, 6, ..., 1, and 0.

RFC2474 redefines the ToS field of the IP header, in which the first 6 bits (bits 0 to 5) represent the differentiated services code point (DSCP). DSCP is used to classify packets into a maximum of 64 different categories.

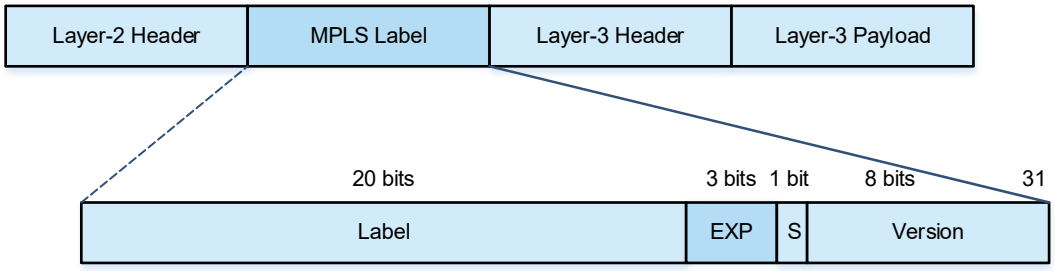
- ToS field of the IPv6 packets

  IPv6 packets use the TC field in the IPv6 header to indicate the packet priority, as shown in Figure 1-4Figure 1-4.

Figure 1-4 TC Field in the IPv6 Header



The TC field contains eight bits and provides the same function as the ToS field of IPv4 packets. The first six bits of the TC field indicate DSCP.



- CoS

  The class of service (CoS) is used to determine the packet queue number when an interface sends packets. The CoS values are 7, 6, ..., 1, and 0 from high to low.

2. Traffic Classification

Traffic classification identifies packets with certain characteristics according to rules. It is the prerequisite and basis for providing differentiated network services. Traffic classification is classified into simple traffic classification and complex traffic classification.

- Simple traffic classification

  Simple traffic classification classifies packets only based on the priorities carried in packets (for example, the PRI value of IEEE 802.1q frames, IP PRE or DSCP value of IP packets, and TC value of IPv6 packets). Simple traffic classification implements the mapping from the priority to the CoS of the device based on whether an interface is configured to trust the priority tag carried in uplink packets.

- Complex traffic classification

  Complex traffic classification classifies packets based on the priorities carried in packets or by identifying packets meeting certain characteristics according to access control list (ACL) rules.

  A QoS policy based on complex traffic classification associates the complex traffic classification with relevant traffic behaviors to form a policy, which is then applied to an interface to take effect. A QoS policy comprises three elements: class, traffic behavior, and policy.

- A class comprises the class name and class rule. A class defines the matching rules of traffic classification to classify packets.
- A traffic behavior defines the action to be taken for the classified packets, including modifying the packet priority (also known as priority re-marking) and monitoring traffic.
- A policy comprises the policy name, and the binding relationship between a class and a traffic behavior. A policy binds a specified class and a traffic behavior and is applied to one or more interfaces to take effect.

- QoS logical interface group

  You can specify a series of interfaces (aggregation ports or Ethernet interfaces) as a QoS logical interface group, and associate a policy with the logical interface group for QoS processing. For example, the rate limiting function of a traffic behavior enables the packets complying with the rate limiting conditions to share the bandwidth limited by the policy on all the interfaces in the same logical interface group.

3. Priority Mapping

Priorities are used to identify the scheduling weights or forwarding priority of packets. Different priority types are defined for different packet types: IEEE 802.1q frames use the IEEE 802.1p priority, IP packets use the IP PRE or DSCP, and so on.

After a packet enters a device interface, the packet priority is mapped to the CoS according to the trust mode configured for the interface. Table 1-1 shows the mappings between trust mode configured for an interface and the priorities.

Table 1-1 Interface Trust Mode and Priority Mapping

Interface Trust Mode	Priority Mapping
Untrusted	● No priority carried in packets is trusted. ● All packets received from an interface use the IEEE 802.1p value configured for the interface. ● The CoS values are obtained from the 802.1p-to-DSCP mapping table and DSCP-to-CoS mapping table. Packets are sent to queues based on their CoS values. ● If an IEEE 802.1Q tagged packet is sent from an egress, the packet priority is changed to the corresponding CoS value.
Trusting 802.1p	● If a packet received by an interface is an IEEE 802.1Q tagged packet, the carried IEEE 802.1p value is directly used. If a packet does not carry any tag, the IEEE 802.1p value configured for the interface is used. ● The CoS values are obtained from the 802.1p-to-DSCP mapping table and DSCP-to-CoS mapping table. Packets are sent to queues based on their CoS values. ● If an IEEE 802.1Q tagged packet is sent from an egress, the packet priority is changed to the corresponding CoS value.
Trusting DSCP	● If a packet received from an interface is a non-IP packet, it is processed in the same way of trusting 802.1p. If the received packet is an IP packet, the

Interface Trust Mode	Priority Mapping
	CoS value is obtained from the DSCP-to-CoS mapping table based on the DSCP value of the packet. Packets are sent to queues based on their CoS values.
Trusting IP PRE	• If a packet received from an interface is a non-IP packet, it is processed in the same way of trusting 802.1p. If the received packet is an IP packet, the CoS value is obtained from the IP PRE-to-DSCP mapping table and DSCP-to-CoS mapping table based on the IP PRE value of the packet. Packets are sent to queues based on their CoS values.

4. Traffic Policing

Traffic policing supervises the rate of the specific traffic, limits the rate within a reasonable range, and discards the traffic out of the limit or re-marks the priority. Traffic policing adopts the committed access rate (CAR) technology to control traffic. CAR uses the single-rate single-token bucket algorithm to judge whether the rate of each packet exceeds the specified traffic limit.

- Single-rate single token bucket

  The single-rate single token bucket contains two parameters: **CIR** and **CBS**.

  - Committed information rate (CIR): Indicates the rate at which a token is added to a token bucket.
  - Committed burst size (CBS): Indicates the capacity of a token bucket.

  The single-rate single token bucket adds tokens to a token bucket at a fixed rate (namely, CIR). When the number (that is, CBS) of tokens in a token bucket reaches the capacity of the token bucket, the excess tokens are discarded. When the device processes packets, it takes tokens out of the token bucket, with the number same as the size of packets (in bytes). When the number of tokens is sufficient, the packets can be forwarded. When the number of tokens is insufficient, the packets are discarded or the priorities of some packets are re-marked before forwarding.

- CAR processing

  CAR uses a token bucket to measure the packets passing through an interface, and implements the preset policing action based on the measurement results. These actions include:

  - Forwarding: Packets within the traffic limit are normally forwarded.
  - Discarding: Packets out of the traffic limit are discarded. The packets out of the total traffic limit of an interface are directly discarded.
  - Changing the priority and forwarding: The priorities of the packets out of the traffic limit are changed and then the packets are forwarded.

5. Congestion Management

When the receiving rate of packets exceeds the sending rate, congestion occurs on the sending interface. If no sufficient buffer is provided to store these packets, packet loss may occur. The congestion management mechanism determines the sending order of packets based on their local priorities. The congestion management function controls congestion and improves the local priorities of packets for some important data. When congestion occurs, the packets of higher priorities are sent first to ensure that key services are provided in time.

Congestion management adopts the queue scheduling mechanism. The processing is as follows:

(1) After each packet undergoes the QoS processing in a device, it obtains a CoS value finally.

(2) The device allocates the packets to the corresponding sending queues according to the CoS values.

(3) The outbound interface selects the packets in a queue for sending according to various queue scheduling policies (such as SP, RR, WRR, DRR, WFQ, SP+WRR, SP+DRR, and SP+WFQ).

- SP scheduling policy

  In strict-priority (SP) scheduling, packets are scheduled strictly based on their queue priorities from high to low.

  The weakness of SP scheduling is that, when congestion occurs, if the packets in a higher priority queue exist for a long time, the packets in a lower priority queue have no opportunity of being scheduled.

- RR scheduling policy

  Round robin (RR) scheduling uses the round robin method to schedule multiple queues. Only one packet in a queue is processed each time.

- WRR scheduling policy

  The weighted round robin (WRR) scheduling solves the problem that weight cannot be set for RR scheduling. WRR scheduling also adopts the round robin method to schedule multiple queues. The number of packets in a queue processed each time is proportional to the weight of the queue. RR scheduling is equivalent to WRR scheduling with the weight 1.

  However, WRR scheduling fails to schedule the services with low delay requirements in time.

- DRR scheduling policy

  The deficit round robin (DRR) scheduling is similar to WRR scheduling, but implements scheduling based on the time slice, instead of the number of packets.

  However, DRR scheduling fails to schedule the services with low delay requirements in time.

- WFQ scheduling policy

  Weighted fair queuing (WFQ) scheduling fixes the problem that the queues using WRR scheduling have no fixed egress bandwidth. WFQ scheduling allocates an egress bandwidth to queues based on the queue weight, and different queues can have the opportunity of fair scheduling.

- SP+WRR scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, can the packets in WRR queues be sent.

- SP+DRR scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the DRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and DRR queues, only after the packets in all SP queues are sent, can the packets in DRR queues be sent.

- SP+WFQ scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WFQ mode. Among SP queues, only after all packets in an SP queue with a higher priority are sent, can

the packets in an SP queue with a next higher priority be sent. Among SP and WFQ queues, only after the packets in all SP queues are sent, can the packets in WFQ queues be sent.

6. Congestion Avoidance

Congestion avoidance monitors the usage of the outbound interface queues, and eliminates the network overload by actively discarding packets and adjusting the network traffic when network congestion occurs. Congestion avoidance avoids congestion by effectively monitoring the network traffic load, forecasting the occurrence of congestion, and discarding packets. Discarding policies include tail-drop, discarding based on random early detection (RED) results, and discarding based on weighted random early detection (WRED) results.

- Tail-drop

  Traditional packet loss policies use the tail-drop method. Tail-drop is effective for all traffic and cannot distinguish service levels. When congestion occurs, data packets at the tail of a queue are discarded until the congestion is removed.

- RED and WRED

  The hosts running Transmission Control Protocol (TCP) decreases the rate of sending packets to respond to massive packet loss. After congestion is removed, the hosts increase the rate of sending packets. Tail-drop may cause TCP global synchronization. Namely, when a queue discards multiple TCP packets simultaneously, multiple TCP connections enter the congestion avoidance and slow startup state simultaneously. In this case, the tail is dropped, and the traffic is reduced and adjusted. When congestion is removed, traffic peaks appear. The process repeats constantly, the network traffic goes up and down suddenly, and the line traffic always fluctuates between the lowest traffic and the full traffic. When TCP global synchronization occurs, the connection bandwidth cannot be fully used, which causes a bandwidth waste.

  To avoid this circumstance, you can use the RED or WRED packet discarding policy. The policy provides a mechanism for discarding packets at random and avoiding TCP global synchronization. When packets of a TCP connection are discarded and the remaining packets of the TCP connection are sent at a lower rate, packets of other TCP connections are still sent at higher rates. There are always some TCP connections whose packets are sent at higher rates, which increases the utilization of line bandwidth.

  When WRED is used, you can set the lower threshold and maximum discarding probability for a queue. When the length of a queue is smaller than the lower threshold, no packets are discarded. When the queue length is between the lower threshold and higher threshold, WRED starts to discard packets randomly and sets a maximum discarding probability. A longer queue leads to a higher discarding probability. When the length of a queue is greater the higher threshold, packets are discarded at the maximum discarding probability.

  Different from RED, WRED uses priorities to distinguish discarding policies. RED is a special case of WRED. When all the CoS values of an interface are mapped to the same lower and higher thresholds, WRED becomes RED.

1.2 Configuration Task Summary

QoS configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Traffic Classification
- Configuring Priority Mapping
- Configuring the Interface Rate Limit
- Configuring Congestion Management
- Configuring Congestion Avoidance
- Configuring the QoS Global Policy
- Disabling the Packet Priority Change

1.3 Configuring Traffic Classification

1.3.1 Overview

Traffic classification uses certain rules to identify the packets with certain characteristics. You can define the binding between multiple traffic classes and traffic behaviors to form policies and apply the policies to interfaces to realize traffic classification and processing.

1.3.2 Configuration Tasks

Traffic classification configuration includes the following tasks:

(1) Configuring a Class

(2) Configuring a Policy

(3) Applying a Policy

(4) (Optional) Configuring a Logical Interface Group

1.3.3 Configuring a Class

1. Overview

This section describes how to create a class, and defines class matching rules in class configuration mode.

2. Restrictions and Guidelines

- A class name comprises a maximum of 31 characters.
- Run the **match** command to define a class matching rule.
- When setting the matching rule of a class to ACL matching, you need to create an ACL and ACL rules first.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a class and enter the class configuration mode.

class-map *class-map-name*

No class is configured by default.

(4) Define a matching rule for the class. Configure at least one of the tasks.

- Set the matching rule of the class to ACL matching.

  match access-group { *acl-number* | *acl-name* }

  Numerically indexed ACLs or named ACLs are supported.

- Set the matching rule of the class to matching the PRE priorities of IP packets.

  match ip precedence *pre-value-list*

  Multiple IP PRE values can be matched at the same time. The value range of IP PRE is from 0 to 7.

- Set the matching rule of the class to matching the DSCP priorities of IP packets.

  match ip dscp *dscp-value-list*

  Multiple DSCP values can be matched at the same time. The value range of DSCP priority is from 0 to 63.

No class matching rules are defined by default.

1.3.4 Configuring a Policy

1. Overview

This section describes how to create a policy, and bind classes and traffic behaviors in the policy configuration mode.

2. Restrictions and Guidelines

- A policy name comprises a maximum of 31 characters.
- When multiple classes are associated with the same policy, you are not advised to match the same flow with multiple classes; otherwise the traffic behavior bound to a class is performed on the flow randomly, and, when the device restarts, the traffic behavior bound to a class is also performed on the flow randomly.
- The **set** command is used to modify the priority tag of a specified packet, such as IEEE 802.1p and DSCP.
- The **police** command is used to limit the bandwidth of the specified traffic and configure the processing action on traffic beyond the limit, for example, discarding the traffic out of the limit, or modifying the CoS or DSCP value.
- The **drop** command is used to drop all the identified streams.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a policy and enter the policy configuration mode.

policy-map *policy-map-name*

No policy is configured by default.

(4) Associate a class and enter the policy class configuration mode.

class *class-map-name*

No class is associated with a policy by default.

(5) Bind the class to a traffic behavior. Configure at least one of the tasks.

- Bind the class to the traffic behavior of modifying the IEEE 802.1p and DSCP values.

  set { **cos** *new-cos* | **ip dscp** *new-dscp* }

- Bind the class to the traffic behavior of limiting the bandwidth and processing packets beyond the limit.

  police *rate-bps burst-byte* [**exceed-action** { **cos** *new-cos* | **drop** | **dscp** *new-dscp* }]

A class is not bound to any traffic behavior by default.

After the traffic behavior of discarding packets is configured, you need to delete the traffic behavior of discarding packets before configuring the above traffic behaviors.

(6) (Optional) Bind the class to the traffic behavior of discarding packets.

drop

A class is not bound to any traffic behavior by default.

This command can be configured only when a class associated with a policy is not bound to any traffic behavior. Namely, after a class associated with a policy is bound to the traffic behavior of discarding packets, you need to first delete the binding and then bind the class to other traffic behaviors.

1.3.5 Applying a Policy

1. Overview

This section describes how to apply a configured policy to a specified interface to make the policy take effect.

2. Restrictions and Guidelines

- A policy can be applied globally or to an interface.
- A policy can be applied to an L2 aggregation port or an L2 Ethernet interface. A policy can be applied to a switch virtual interface (SVI). When an L2 Ethernet interface is added to a VLAN and policies are configured for both the Ethernet interface and an SVI, the priority of the policy applied to the L2 Ethernet interface is higher than that applied to the SVI.
- If a policy is applied globally, the policy is applied to all interfaces which can be configured with policies.
- Configuring the **input** option applies a policy to the input direction of an interface.
- Configuring the **output** option applies a policy to the output direction of an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Apply a policy. Please configure only one task.

- Apply a policy in global configuration mode.

  service-policy { **input** | **output** } *policy-map-name*

  No policy is applied globally by default.

- Apply a policy in interface configuration mode. Run the following commands in turn to apply a policy.

interface *interface-type interface-number*

service-policy { **input** | **output** } *policy-map-name*

No policy is applied to an interface by default.

1.3.6 Configuring a Logical Interface Group

1. Overview

This section describes how to associate a configured policy with a logical interface group.

2. Restrictions and Guidelines

- A maximum of 128 logical interface groups can be created.
- In global configuration mode, run the **virtual-group** command to create a logical interface group and enter the logical interface group configuration mode.
- In interface configuration mode, run the **virtual-group** command to add the interface to a specified logical interface group. If the logical interface group is not created, this command creates the logical interface group and adds the interface to the group.
- Physical interfaces or aggregation ports can be added to a logical interface group. The following types of interfaces cannot be added to a logical interface group:
  - Member interface of an aggregation port
  - VSL member interface

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a logical interface group and add interfaces to it. Please configure only one task.

- Create a logical interface group in global configuration mode and add interfaces to it. Run the following commands in turn to create a logical interface group and add interfaces to it.

  virtual-group *virtual-group-number*

  No logical interface group is defined by default.

  interface *interface-type interface-number*

  virtual-group *virtual-group-number*

  An interface is not added to any logical interface group by default.

- Create a logical interface group in interface configuration mode and add interfaces to it. Run the following commands in turn to create a logical interface group and add interfaces to it.

  interface *interface-type interface-number*

  virtual-group *virtual-group-number*

  An interface is not added to any logical interface group by default.

(4) Return to the global configuration mode.

exit

(5) Enter the logical interface group configuration mode.

virtual-group *virtual-group-number*

(6) Apply a policy to the logical interface group.

service-policy { **input** | **output** } *policy-map-name*

1.4 Configuring Priority Mapping

1.4.1 Overview

Priority mapping can be implemented based on the trust mode configured for an interface.

1.4.2 Restrictions and Guidelines

Priority mapping can be configured only on L2 and L3 Ethernet interfaces.

1.4.3 Configuration Tasks

Priority marking and mapping configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Trust Mode
- Configuring Mappings

1.4.4 Configuring the Trust Mode

1. Overview

- You can set various priorities for packets according to the trust mode configured for an interface.
- Run the **mls qos trust** command to configure the trust mode for an interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the trust mode for the interface. Please configure only one task.

- Configure trusting IEEE 802.1p.

  mls qos trust cos

- Configure trusting DSCP.

  mls qos trust dscp

- Configure trusting IP PRE.

  mls qos trust ip-precedence

An interface is in untrusted mode by default.

(5) (Optional) Configure the IEEE 802.1p value for the interface.

mls qos cos *cos-value*

The default IEEE 802.1p value of an interface is **0**.

1.4.5 Configuring Mappings

1. Overview

This section describes how to configure mappings, including:

- IEEE 802.1p-to-DSCP mappings.
- DSCP-to-CoS mappings.
- IP PRE-to-DSCP mappings.

2. Restrictions and Guidelines

- Run the **mls qos map cos-dscp** command to configure the mappings from IEEE 802.1p values to DSCP values.
- Run the **mls qos map dscp-cos** command to configure the mappings from DSCP values to CoS values.
- Run the **mls qos map ip-precedence-dscp** command to configure the mappings from IP PRE values to DSCP values.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure mappings. Configure at least one of the tasks.

- Configure the IEEE 802.1p-to-DSCP mappings.

  mls qos map cos-dscp *dscp-value-list*

  The IEEE 802.1p values 0 to 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

- Configure the DSCP-to-CoS mappings.

  mls qos map dscp-cos *dscp-value*&<1-8> **to** *cos-value*

  DSCP values 0 to 7 are mapped to CoS 0, DSCP values 8 to 15 are mapped to CoS 1, DSCP values 16 to 23 are mapped to CoS 2, DSCP values 24 to 31 are mapped to CoS 3, DSCP values 32 to 39 are mapped to CoS 4, DSCP values 40 to 47 are mapped to CoS 5, DSCP values 48 to 55 are mapped to CoS 6, and DSCP values 56 to 63 are mapped to CoS 7 by default.

- Configure the IP PRE-to-DSCP mappings.

  mls qos map ip-precedence-dscp *dscp-value-list*

  The IP PRE values 0 to 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48, and 56 respectively by default.

1.5 Configuring the Interface Rate Limit

1.5.1 Overview

This section describes how to configure traffic limit for an interface.

1.5.2 Restrictions and Guidelines

The interface type that can be configured depends on the product.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure traffic limit for the interface. Configure at least one of the tasks.

- Configure the rate limit for the traffic in the input direction of an interface.

  rate-limit input *bps burst-size*

- Configure the rate limit for the traffic in the output direction of an interface.

  rate-limit output *bps burst-size*

No traffic limit is configured for an interface by default.

1.6 Configuring Congestion Management

1.6.1 Overview

This section describes how to control congestion. The priorities of important data packets can be raised so that they are sent first when congestion occurs, thereby ensuring that key services are provided in time.

1.6.2 Restrictions and Guidelines

Congestion management can be configured only on an L2 Ethernet aggregation port or an L3 Ethernet interface.

1.6.3 Configuration Tasks

The congestion management configuration includes the following tasks:

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the CoS-to-Queue Mappings
- Configuring the Scheduling Policy and Round Robin Weights for Output Queues
- Configuring Bandwidth for a Queue

1.6.4 Configuring the CoS-to-Queue Mappings

1. Overview

This section describes how to configure the CoS-to-queue mappings so that packets can enter various output queues based on their CoS values.

2. Restrictions and Guidelines

- Run the **priority-queue cos-map** command to configure the CoS-to-queue mappings.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the CoS-to-queue mappings.

priority-queue cos-map *qid cos*&<1-8>

The CoS values 0 to 7 are mapped to the queues 1 to 8 respectively by default.

1.6.5 Configuring the Scheduling Policy and Round Robin Weights for Output Queues

1. Overview

This section describes how to configure the scheduling policy and round robin weights for output queues. The scheduling policy and round robin weight ratio for output queues are configured globally. Some products support both global configuration and interface-based configuration. Interface-based configuration has a higher priority than global configuration. The global scheduling policy works with the corresponding global round robin weight ratio, while the interface scheduling policy works with the corresponding interface round robin weight ratio. If only the global scheduling policy or interface scheduling policy is configured but no corresponding round robin weight ratio is configured, the default round robin weight ratio is used for the scheduling policy.

2. Restrictions and Guidelines

- Run the **priority-queue** command to set the scheduling policy to SP scheduling.
- Run the **mls qos scheduler sp** command to set the scheduling policy to SP scheduling for output queues.
- Run the **mls qos scheduler rr** command to set the scheduling policy to RR scheduling for output queues.
- Run the **mls qos scheduler wrr** command to set the scheduling policy to WRR scheduling based on the packet quantity for output queues.
- Run the **mls qos scheduler drr** command to set the scheduling policy to WRR scheduling based on the packet size for output queues.
- Run the **mls qos scheduler wfq** command to set the scheduling policy to WFQ scheduling for output queues.
- Run the **drr-queue bandwidth** command to configure the round robin weight for the DRR scheduling policy of output queues. A higher weight means that more packet bytes can be sent.
- Run the **wrr-queue bandwidth** command to configure the round robin weight for the WRR scheduling policy of output queues. A higher weight means longer output time. The configurable weight range depends on the

product.

- Run the **wfq-queue bandwidth** command to configure the round robin weight for the WFQ scheduling policy of output queues. A higher weight means that more packet bytes can be sent. The configurable weight range depends on the product.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the scheduling policy for output queues. Please configure only one task.

- Set the scheduling policy to SP scheduling.

  priority-queue

- Configure the scheduling policy for global output queues.

  mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

  The default scheduling policy of global output queues is **WRR**.

- Configure the scheduling policy for interface output queues. Run the following commands in turn to configure the scheduling policy for interface output queues.

  interface *interface-type interface-number*

  mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

  No scheduling policy is configured on an interface by default.

(4) Configure the round robin weight for the scheduling policy of output queues. Please configure only one task.

- Configure the round robin weight for the scheduling policy of global output queues.

  { **drr-queue** | **wfq-queue** | **wrr-queue** } **bandwidth** *weight&<1-8>*

  The default round robin weight ratio of global queues is **1:1:1:1:1:1:1:1**.

- Configure the round robin weight for the scheduling policy of interface output queues. Run the following commands in turn to configure the round robin weight for the scheduling policy of interface output queues.

  interface *interface-type interface-number*

  { **drr-queue** | **wfq-queue** | **wrr-queue** } **bandwidth** *weight&<1-8>*

  The default round robin weight ratio of interface queues is **1:1:1:1:1:1:1:1**.

1.6.6 Configuring Bandwidth for a Queue

1. Overview

This section describes how to configure the minimum guaranteed bandwidth and maximum limited bandwidth for a queue.

2. Restrictions and Guidelines

- This command can be configured globally or on an interface, depending on the product.

- The configuration support is different in global configuration mode and interface configuration mode.
- Whether the **max** option can be carried in the configuration command depends on the product.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the minimum guaranteed bandwidth and maximum limited bandwidth for a queue.

qos queue *queue-id* **bandwidth** { **maximum** { *bandwidth* } | **minimum** *bandwidth* }

No minimum guaranteed bandwidth or maximum limited bandwidth is configured for a queue by default.

The value ranges of the minimum guaranteed bandwidth and maximum limited bandwidth depend on the product.

1.7 Configuring Congestion Avoidance

1.7.1 Overview

Congestion avoidance monitors the usage of queues in an outbound interface and eliminates the network overload by actively discarding packets and adjusting the network traffic in the case of network congestion.

1.7.2 Configuration Tasks

Congestion avoidance configuration includes the following tasks:

(1) Enabling the WRED Function

(2) (Optional) Configuring Higher and Lower Threshold Values

(3) (Optional) Configuring the Maximum Discarding Probability

(4) (Optional) Configuring the Sampling Weight

(5) (Optional) Configuring the CoS-to-Threshold Mappings

1.7.3 Enabling the WRED Function

1. Overview

This section describes how to configure WRED as the packet discarding policy.

2. Restrictions and Guidelines

The default packet discarding policy is tail-drop.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the WRED function.

queueing wred

The WRED function is disabled by default.

1.7.4 Configuring Higher and Lower Threshold Values

1. Overview

This section describes how to configure the higher and lower threshold values for WRED.

2. Restrictions and Guidelines

- When the packet length of a queue is smaller than the lower threshold, no packets are discarded. When the queue length is between the lower threshold and the higher threshold, WRED starts to discard packets randomly.
- Because the maximum value of the configuration range is equal to the current higher threshold, you need to pay attention to the configured higher threshold when configuring the lower threshold.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure a lower threshold value. Please configure only one task.

- Configure a lower threshold value in percentage.

  wrr-queue random-detect min-threshold *queue-id threshold*&<1-2>

  The queue value range is from 1 to 8. The value range of the lower threshold value is from 1 to the set value of the higher threshold. The default threshold value depends on the product.

The threshold value is configured in percentage by default.

1.7.5 Configuring the Maximum Discarding Probability

1. Overview

When the packet length in a queue is between the lower threshold and the higher threshold, you can configure the maximum probability for discarding packets at random.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the maximum discarding probability.

wrr-queue random-detect probability *queue-id probability*&<1-2>

The maximum discarding probability is not configured by default.

1.7.6 Configuring the Sampling Weight

1. Overview

You can configure the sampling weight for the WRED discarding function to affect the calculation result of the average queue length.

2. Restrictions and Guidelines

- When packets are forwarded, WRED determines the discarding probability based on the average queue length of the egress queue. When the queue length is between the lower threshold and the higher threshold, WRED starts to discard packets randomly. A longer queue leads to a higher discarding probability but the probability cannot be higher than the maximum discarding probability. When the queue length is greater than the higher threshold, packets are discarded at the maximum discarding probability.
- The sampling weight indicates the weight factor of sampled data updates. A larger sampling weight indicates a longer update interval of the average queue length and a larger average queue length.
- To make the sampling weight effective, you need to first configure the WRED discarding function on an interface. Namely, the sampling weight must be configured after the higher threshold and lower threshold are configured for the WRED discarding function on an interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the sampling weight.

wrr-queue random-detect sample-weight *queue-id weight*

No sampling weight is configured by default.

1.7.7 Configuring the CoS-to-Threshold Mappings

1. Overview

This section describes how to configure the CoS-to-threshold mappings.

2. Restrictions and Guidelines

- Multiple threshold groups can be configured for the lower threshold and maximum discarding probability.
- By configuring the mappings from CoS values and threshold groups, you can select the effective threshold group mapped to a CoS, for example, you can map CoS 0 to threshold group 1, and CoS 1 to threshold

group 2.

- If the packets of CoS values 0 and 1 are all added to queue 1 for scheduling, the packets of CoS 0 are processed based on the lower threshold and maximum discarding probability in group 1, and the packets of CoS 1 are processed based on the lower threshold and maximum discarding probability in group 2.
- When all the CoS values are mapped to the same threshold group, the enabled WRED becomes RED.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L2 or L3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) Configure the CoS-to-threshold mappings.

wrr-queue cos-map *threshold-id cos*&<1-8>

All the CoS values are mapped to the threshold in group 1 by default.

1.8 Configuring the QoS Global Policy

1.8.1 Overview

Enabling the QoS global policy enables some QoS policies by default, for example, changing the DSCP value of L2 flows.

1.8.2 Restrictions and Guidelines

Different QoS policies may be enabled on different devices by default.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global QoS policy.

mls qos enable

1.9 Disabling the Packet Priority Change

1.9.1 Overview

When a packet is sent out of a device, the priority of the packet is changed to the priority configured on the device. You can disable packet priority change, that is, the priority of a packet sent out of a device is the same as that when the packet is sent to the device.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable packet priority change.

mls qos remark disable

1.10 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠ Caution

Running the **clear** commands may interrupt services due to loss of important information.

Run the **debug** command to output debugging information.

⚠ Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 QoS Monitoring

Command	Purpose
show class-map [*class-map-name*]	Displays the traffic classification information.
show policy-map [*policy-map-name* [**class** *class-map-name*]]	Displays the QoS policy information.
show policy-map interface *interface-type interface-number*	Displays information about a policy applied to an interface.
show virtual-group [*virtual-group-number* | **summary**]	Displays information about a logical interface group.
show mls qos virtual-group [*virtual-group-number* | **policers**]	Displays information about a policy applied to a logical interface group.
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]	Displays various mappings.
show mls qos rate-limit [**interface** *interface-type interface-number*]	Displays the rate limit information of an interface.
show mls qos queueing [**interface** *interface-*	Displays information about the QoS queues, scheduling

Command	Purpose
type interface-number]	policies, and round robin weights.
show mls qos scheduler [**interface** *interface-type interface-number*]	Displays the scheduling policy information of an output queue.
show queueing wred [**interface** *interface-type interface-number*]	Displays the WRED configuration.
show mls qos interface *interface-type interface-number* [**policers**]	Displays the QoS information of an interface.
show qos bandwidth [**interface** *interface-type interface-number*]	Displays information about the queue bandwidth.
debug qos lib [**event** | **message**]	Debugs the QoS library.
debug qos server [**event** | **message**]	Debugs the QoS communication server.
debug qos mls	Debugs QoS user command processing.
debug qos vmsup	Debugs VMSUP configurations.

1.11 Configuration Examples

1.11.1 Configuring the Interface Rate Limit and Priority Re-marking

1. Requirements

To meet the service requirements of normal teaching, a school puts forwards the following requirements:

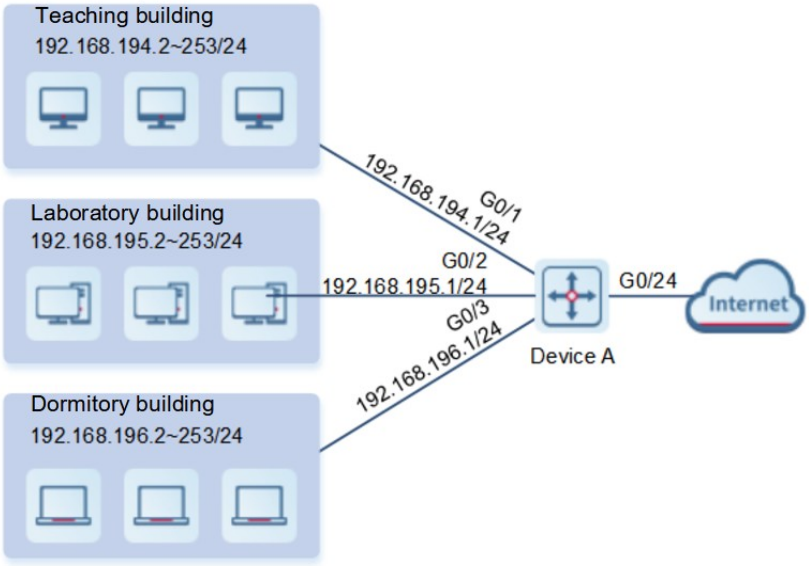
- Controlling the Internet access traffic of the school within 100 Mbps and discarding the packets out of the limit.
- Controlling the egress traffic of the dormitory building within 50 Mbps and discarding the packets out of limit.
- Controlling the rate of packets with DSCP priority 7 sent from laboratory building within 20 Mbps, and changing the DSCP priorities of the packets whose rates exceed 20 Mbps to 16.
- Controlling the egress traffic of the teaching building within 30 Mbps and discarding the packets out of limit.

Note

The school connects to the Internet through G0/24 of device A, and G0/1, G0/2, and G0/3 of device A connect to the teaching building (192.168.194.2~253/24), laboratory building (192.168.195.2~253/24), and dormitory building (192.168.196.2~253/24) respectively.

2. Topology

Figure 1-1 Application Scenario of Interface Rate Limit and Priority Re-marking



3. Notes

(1) For Internet access traffic on the outbound interface, configure the egress traffic limit on interface G0/24 of device A, and set the bandwidth limit to 102,400 kbps and burst traffic limit to 256 Kbytes per second.

(2) For the dormitory building, configure the ingress traffic limit on interface G0/3 of device A, and set the bandwidth limit to 51,200 kbps and burst traffic limit to 256 Kbytes per second.

(3) For the teaching building, configure the ingress traffic limit on interface G0/1 of device A, and set the bandwidth limit to 30,720 kbps and burst traffic limit to 256 Kbytes per second.

(4) For the laboratory building, create the class cmap_dscp7 to match DSCP priority 7, create the policy pmap_shiyan, associate cmap_dscp7 with the policy, bind the traffic behavior of changing the DSCP value of packets whose rates exceed 20 Mbps to 16, to the class, apply pmap_shiyan to interface G0/2, and configure the interface to trust DSCP.

4. Procedure

(1) Configure IP addresses for interfaces (omitted).

(2) Configure rate limits for the interfaces.

For Internet access traffic on the outbound interface, configure the egress traffic limit on interface G0/24.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/24
DeviceA(config-if-GigabitEthernet 0/24# rate-limit output 102400 256
DeviceA(config-if-GigabitEthernet 0/24)# exit
```

For the dormitory building, configure the ingress traffic limit on interface G0/3.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3# rate-limit input 51200 256
```

```
DeviceA(config-if-GigabitEthernet 0/3)# exit
```

For the teaching building, configure the ingress traffic limit on interface G0/1.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1# rate-limit input 30720 256
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(3) Configure traffic classification.

For the laboratory building, configure a class, traffic behavior, and policy.

```
DeviceA(config)# class-map cmap_dscp7
DeviceA(config-cmap)# match ip dscp 7
DeviceA(config-cmap)# exit
DeviceA(config)# policy-map pmap_shiyan
DeviceA(config-pmap)# class cmap_dscp7
DeviceA(config-pmap-c)# police 20480 128 exceed-action dscp 16
DeviceA(config-pmap-c)# exit
DeviceA(config-pmap)# exit
```

Apply the policy to an interface and configure the interface to trust DSCP.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2# service-policy input pmap_shiyan
DeviceA(config-if-GigabitEthernet 0/2)# mls qos trust dscp
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

Check whether the interface rate limits are successfully configured.

```
DeviceA# show mls qos rate-limit
Interface: GigabitEthernet 0/1
  rate limit input Kbps = 30720 burst = 256
Interface: GigabitEthernet 0/3
  rate limit input Kbps = 51200 burst = 256
Interface: GigabitEthernet 0/24
  rate limit output Kbps = 102400 burst = 256
```

Check whether the class is successfully created.

```
DeviceA# show class-map cmap_dscp7

 Class Map cmap_dscp7
   Match ip dscp 7
```

Check whether the policy is successfully created.

```
DeviceA# show policy-map pmap_shiyan

 Policy Map pmap_shiyan
    Class cmap_dscp7
      police 20480 128 exceed-action dscp 16
```

Check whether the policy is applied to the interface successfully.

```
DeviceA# show mls qos interface gigabitethernet 0/2
```

```
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: pmap_shiyan
Attached output policy-map:
Default trust: dscp
Default cos: 0
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
class-map cmap_dscp7
 match ip dscp 7
!
policy-map pmap_shiyan
 class cmap_dscp7
  police 20480 128 exceed-action dscp 16
!
interface GigabitEthernet 0/1
 ip add 192.168.194.1 255.255.255.0
 rate-limit input 30720 256
!
interface GigabitEthernet 0/2
 ip add 192.168.195.1 255.255.255.0
 service-policy input pmap_shiyan
 mls qos trust dscp
!
interface GigabitEthernet 0/3
 ip add 192.168.196.1 255.255.255.0
 rate-limit input 51200 256
!
interface GigabitEthernet 0/24
 rate-limit output 102400 256
!
```

1.11.2 Configuring Queue Scheduling and Congestion Avoidance

1. Requirements

Priority re-marking and queue scheduling need to be configured to meet the following requirements:

- When the R&D department and market department access the servers, the priorities of the server packets are as follows: packets destined for the mail server > packets destined for the file server > packets destined for the salary query server.
- No matter when the HR management department accesses the Internet or servers, device A processes the corresponding packets with the highest priority.
- Network congestion often occurs during operation of device A. WRR queue scheduling must be used to

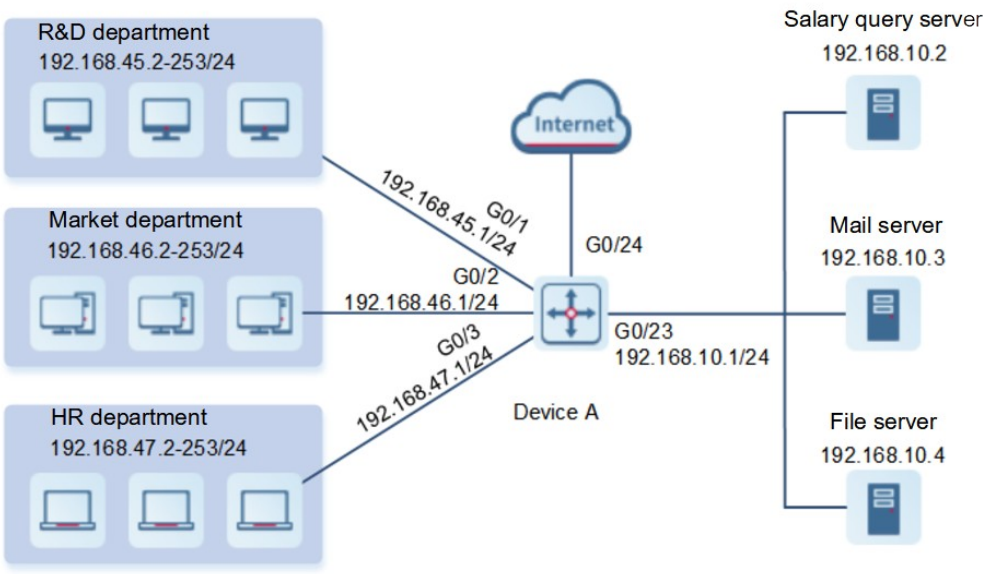
schedule IP packets from the R&D and market departments to access the mail database, file database, and salary query database based on the ratio of 6:2:1.

Note

The R&D department (192.168.45.2~253/24), market department (192.168.46.2~253/24), and HR department (192.168.47.2~253/24) are connected to interfaces G0/1, G0/2, and G0/3 of device A respectively; the salary query server (192.168.10.2/24), mail server (192.168.10.3/24), and file server (192.168.10.4/24) are connected to interface G0/23 of device A.

2. Topology

Figure 1-1 Application Scenario of Queue Scheduling and Congestion Avoidance



3. Notes

(1) On device A, create ACLs to filter packets used for accessing servers, create classes, and associate the classes with these ACLs.

(2) Create policies to associate with the classes and specify the IEEE 802.1p values for the packets accessing various servers in the policies: Set the IEEE 802.1p value to 4 for the packets accessing the mail server, to 3 for the packets accessing the file server, and to 2 for the packets accessing the salary query server. Apply the policies to the inbound interfaces connected to the R&D and market departments and configure the interfaces to trust IEEE 802.1p.

(3) Assign the highest priority 7 to the IEEE 802.1p value of the interface connected to the HR department, to ensure that packets from the HR department are sent with the highest priority.

(4) Set the scheduling policy to WRR for output queues and set the round robin weight to 1:1:1:2:6:1:1:0 for the queues. This means that SP scheduling is used for packets of the HR department, and the packets for accessing the mail database, file database, and salary query database from the R&D and market departments are scheduled based on the ratio of 6:2:1.

(5) Enable the WRED function.

(6) Set the lower thresholds to 10 and 20 for queue 2 of interface G0/2.

(7) Set the higher thresholds to 60 and 90 for queue 2 of interface G0/2.

(8) Set the maximum discarding probabilities to 60 and 80 for queue 2 of interface G0/2.

4. Procedure

(1) On device A, configure ACLs to filter packets used for accessing the servers and add ACL rules.

Configure the ACL for matching packets used for accessing the salary query server as well as ACL rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list extended salary
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.2
DeviceA(config-ext-nacl)# exit
```

Configure the ACL for matching packets used for accessing the mail server as well as ACL rules.

```
DeviceA(config)# ip access-list extended mail
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.3
DeviceA(config-ext-nacl)# exit
```

Configure the ACL for matching packets used for accessing the file server as well as ACL rules.

```
DeviceA(config)# ip access-list extended file
DeviceA(config-ext-nacl)# permit ip any host 192.168.10.4
DeviceA(config-ext-nacl)# exit
```

(2) Configure classes on device A.

Configure a class named salary and associate it with the ACL for matching packets used for accessing the salary query server.

```
DeviceA(config)# class-map salary
DeviceA(config-cmap)# match access-group salary
DeviceA(config-cmap)# exit
```

Configure a class named mail and associate it with the ACL for matching packets used for accessing the mail server.

```
DeviceA(config)# class-map mail
DeviceA(config-cmap)# match access-group mail
DeviceA(config-cmap)# exit
```

Configure a class named file and associate it with the ACL for matching packets used for accessing the file server.

```
DeviceA(config)# class-map file
DeviceA(config-cmap)# match access-group file
DeviceA(config-cmap)# exit
```

(3) Configure policies on device A.

Configure a policy and associate the class named class with a traffic behavior in the policy.

```
DeviceA(config)# policy-map toserver
DeviceA(config-pmap)# class salary
DeviceA(config-pmap-c)# set cos 2
```

```
DeviceA(config-pmap-c)# exit
```

Configure a policy and associate the class named salary with a traffic behavior in the policy.

```
DeviceA(config-pmap)# class mail
DeviceA(config-pmap-c)# set cos 4
DeviceA(config-pmap-c)# exit
```

Configure a policy and associate the class named mail with a traffic behavior in the policy.

```
DeviceA(config-pmap)# class file
DeviceA(config-pmap-c)# set cos 3
DeviceA(config-pmap-c)# exit
DeviceA(config-cmap)# exit
```

(4) Apply policies on device A.

Apply a policy to the interface of device A that is connected to the R&D department.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# service-policy input toserver
DeviceA(config-if-GigabitEthernet 0/1)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Apply a policy to the interface of device A that is connected to the market department.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# service-policy input toserver
DeviceA(config-if-GigabitEthernet 0/2)# mls qos trust cos
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(5) On device A, configure the 802.1p field for an interface.

Configure the highest priority for the 802.1p field for the interface connected to the HR department.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# mls qos cos 7
DeviceA(config-if-GigabitEthernet 0/3)# exit
```

(6) On device A, configure a scheduling policy for output queues.

Set the scheduling policy to WRR for output queues.

```
DeviceA(config)# wrr-queue bandwidth 1 1 1 2 6 1 1 0
DeviceA(config)# mls qos scheduler wrr
```

(7) Configure congestion avoidance on device A.

Enable the WRED function.

```
DeviceA(config)# queueing wred
```

Configure the higher and lower threshold values.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue random-detect min-threshold
2 10 20
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue random-detect probability 2
60 80
```

Configure the CoS-to-threshold mappings.

```
DeviceA(config-if-GigabitEthernet 0/2)# wrr-queue cos-map 2 0 1 2 3
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

5. Verification

Check whether ACLs are successfully created.

```
DeviceA# show access-lists

ip access-list extended file
 10 permit ip any host 192.168.10.4

ip access-list extended mail
 10 permit ip any host 192.168.10.3

ip access-list extended salary
 10 permit ip any host 192.168.10.2
```

Check whether the classes are successfully associated with the ACLs.

```
DeviceA# show class-map

 Class Map salary
   Match access-group salary
 Class Map mail
   Match access-group mail
 Class Map file
   Match access-group file
```

Check whether policies are successfully created, and whether the classes and traffic behaviors are successfully bound.

```
DeviceA# show policy-map

 Policy Map toserver
    Class mail
      set cos 4
    Class file
      set cos 3
    Class salary
      set cos 2
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/1.

```
DeviceA# show mls qos interface gigabitethernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/2.

```
DeviceA# show mls qos interface gigabitethernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input  policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

Check whether a policy is successfully applied to interface GigabitEthernet 0/3.

```
DeviceA# show mls qos interface gigabitethernet 0/3
Interface: GigabitEthernet 0/3
Ratelimit input:
Ratelimit output:
Attached input  policy-map:
Attached output policy-map:
Default trust: none
Default cos: 7
```

Check whether the 802.1p value is successfully configured for the interface and whether the scheduling policy and the round robin weight are successfully configured.

```
DeviceA# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8

wrr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   2
5   6
6   1
7   1
8   0
```

```
drr bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
6   1
7   1
8   1

wfq bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
6   1
7   1
8   1
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
wrr-queue bandwidth 1 1 1 2 6 1 1 0
queueing wred
wrr-queue cos-map 2 0 1 2 3
!
class-map salary
 match access-group salary
class-map mail
 match access-group mail
class-map file
 match access-group file
!
policy-map toserver
 class salary
  set cos 2
 class mail
  set cos 4
 class file
  set cos 3
```

```
!
interface GigabitEthernet 0/1
 ip add 192.168.45.1 255.255.255.0
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/2
 ip add 192.168.46.1 255.255.255.0
 wrr-queue random-detect min-threshold 2 10 20
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/3
 ip add 192.168.47.1 255.255.255.0
 mls qos cos 7
!
```