

15_{QoS}

Quality of service (QoS) is a mechanism to ensure that user requirements for bandwidth, latency, jitter, and packet loss rate are met.

[15.1 Introduction to QoS](#)

[15.2 QoS Models](#)

[15.3 QoS Scheme](#)

[15.4 QoS Processing](#)

[15.5 Traffic Classification](#)

Traffic classification differentiates services by packet classification according to the characteristics of user Ethernet packets and certain rules, to implement different processing operations and provide different services.

[15.6 Priority Marking](#)

According to different priority marking policies, the inner and outer VLAN priorities can be set for service-ports, or the user-side priority can be copied for service-ports.

[15.7 Traffic Policing](#)

Before service providers provide subscribers with specific services, a service level agreement (SLA) is generally assigned, in which all service parameters are defined. To ensure that the user traffic can meet the SLA, the user traffic must be policed.

[15.8 Traffic Shaping](#)

[15.9 Congestion avoidance](#)

[15.10 Congestion Management](#)

[15.11 ACL](#)

Using the preset access control list (ACL) policy, the system permits or refuses data packets to pass.

[15.12 ACLv6](#)

[15.13 HQoS](#)

Traditional quality of service (QoS) schedules traffic based on port. Hierarchical quality of service (HQoS) not only controls port traffic at a finer service granularity but also schedules traffic based on service priorities.

15.14 End-to-End QoS

15.1 Introduction to QoS

Definition

Quality of service (QoS) is a mechanism that guarantees an expected service level with respect to bandwidth, latency, jitter, and packet loss in a communication network. The following indicators are used to measure QoS:

- Bandwidth: theoretical transmission capacities of a connection.
- Latency: the time required for information to travel from one network node to another network node. A high latency impacts the quality of real-time services (for example, IP telephone service).
- Jitter: variations in latency. Jitter can severely affect the quality of multimedia services (for example, VoD).
- Packet loss rate: the percentage of lost packets to the total packets during network transmission.

Purpose

QoS achieves the following purposes:

- Provides users with assured bandwidth.
- Regulates and controls IP network traffic.
- Reduces packet loss rate.
- Specifies packet priorities.
- Avoids and manages network congestion.
- Provides differentiated services for users.

15.2 QoS Models

QoS Models

The following table describes three types of QoS models that may be used in a network. The QoS model implemented on the MA5800 is the differentiated service (DiffServ) model. The following topics use the DiffServ model to describe QoS unless otherwise specified.

Type	Feature	Application
Best-effort service model	In this model, the network forwards data at best-effort rates and no guarantees are provided. The network drops data after all bandwidth is exhausted. This is a simple and unitary service model. It is the default service model for IP networks.	This service model applies to most data services, for example, Email services.
Integrated service model	This model is based on resource reservation. In this model, applications instruct a network to reserve bandwidth using the Resource Reservation Protocol (RSVP), and each unit in the network has to reserve bandwidth for specific data streams.	This service model is not widely used because of the following limitations: • End-to-end support is required for RSVP. • RSVP is not highly extendible. • RSVP protocol packets require large overhead.
DiffServ model	This model is based on priorities. In this model, the network identifies each data stream and provides corresponding QoS guarantees for the data streams. Traffic classification and priority marking are the prerequisites for using this model.	This model involves simple packet processing and is highly extendible. It is used for the following services: • VoD • Streaming media • VoIP • Video conferencing • Private-line services

QoS Components in the DiffServ Model

The DiffServ model uses four QoS components, which are described in the following table. You can design holistic QoS policies through flexible combinations of these components.

Component	Description
Traffic classification and priority marking	DiffServ operates on the principle of traffic classification and priority marking. Traffic classification: Data packets are placed into different traffic classes. Traffic classification does not modify the data packets. Priority marking: Data packets of each traffic class are marked with a specific priority. Priority marking modifies the data packets because the marking changes the values of some packet fields.
Traffic policing and shaping	Before providing services for a subscriber, service providers usually sign a service level agreement (SLA) with the subscriber to define the level of service. Traffic policing: Packets exceeding the SLA will be dropped. Traffic shaping: Packets exceeding the SLA are buffered and the transmission of these packets is resumed when bandwidth is sufficient.
Congestion management	Congestion management controls the sequence of data transmission when congestion occurs in a network.
Congestion avoidance	Congestion avoidance is a traffic control mechanism that actively drops packets when congestion occurs in a network. This mechanism addresses network overload by regulating the network traffic.

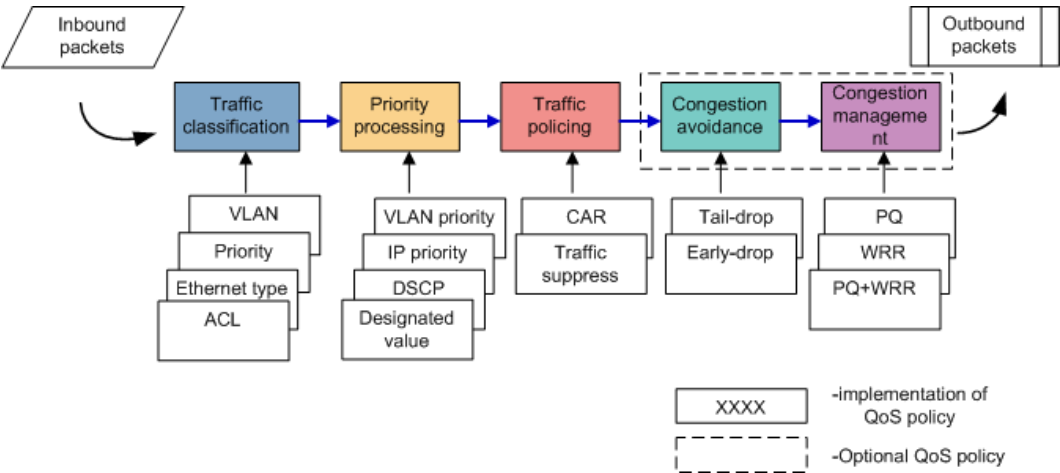
15.3 QoS Scheme

QoS Scheme

The MA5800 use the differentiated service (DiffServ) model. [Figure 15-1](#) shows the QoS scheme of this model. The QoS scheme works as follows:

- Before forwarding the packets through an outbound interface, QoS policies, such as traffic classification, priority processing, traffic policing, congestion avoidance, and congestion management, are implemented on the packets.
- Congestion avoidance and congestion management are optional. They are not required if no congestion occurs (when the backplane bandwidth is higher than or equal to the maximum bandwidth actually required by a board).
- Each QoS policy can be implemented using multiple techniques. For details, see description about the QoS policies.

Figure 15-1 QoS scheme

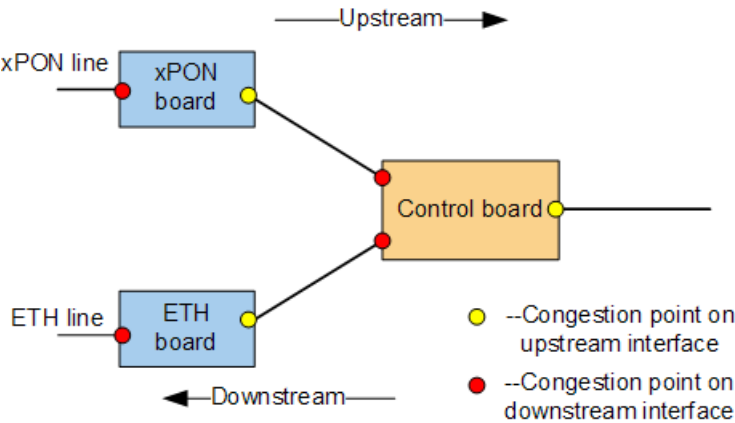


QoS Congestion Point

A network point where traffic congestion is likely to occur is defined as a QoS congestion point. Congestion avoidance and congestion management must be applied to such a point. As shown in Figure 15-2, there are QoS congestion points on both the control boards and service boards.

- There is a QoS congestion point on each service board in the downstream direction.
- In the upstream direction of a service board, congestion control is applied depending on the actual demand on bandwidth.

Figure 15-2 Upstream and downstream QoS congestion points



QoS Policies for Service Boards and Control Boards

The following table provides the QoS policies for service boards and control boards.

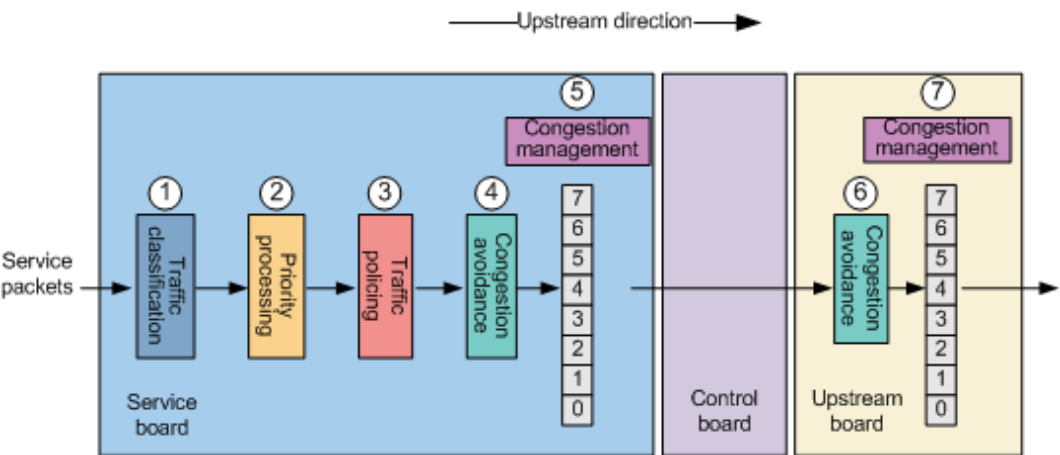
Board Type	QoS Policy	Remarks
Service board	Traffic classification Priority processing Traffic policing Congestion avoidance Congestion management	- Traffic classification on a service board is performed only in the upstream direction. - Congestion avoidance and congestion management are performed on an outbound interface of a service board.
Control board	Traffic classification (based on ACL) Priority processing (based on ACL) Traffic policing (based on ACL) Congestion avoidance Congestion management	Congestion avoidance and congestion management are performed on an outbound interface of a control board. For traffic classification, priority processing, and traffic policing based on ACL on the control board, see " 15.11 ACL ".

15.4 QoS Processing

General QoS Processing - Upstream Direction

[Figure 15-3](#) shows the general QoS processing in the upstream direction.

Figure 15-3 QoS processing in the upstream direction



After the user packets enter a service board from a user port, the service board implements QoS processing on the packets. The following table describes the QoS processing.

Step	QoS Policy	Example
1	Traffic classification: The service board places the Ethernet user packets into different classes based on packet characteristics and predefined QoS rules, and services the traffic differently.	Plan different VLANs or priorities for Internet, voice, and IPTV services to distinguish them, because these services have different QoS requirements.
2	Priority processing: When congestion occurs on the local device or the upper-layer network, the service board marks or remarks priorities for the user packets so that the packets are scheduled based on their priorities.	Assign priorities 0, 5, and 4 for Internet, voice, and IPTV services respectively.
3	Traffic policing: The service board implements traffic policing to limit the traffic and burst size of the user packets destined for a connection on the network. When the packets meet certain conditions, for example, when the traffic destined for the connection is too heavy, the service board takes actions accordingly, such as dropping or coloring (resetting the priorities) the packets. Traffic policing enables a port to work at a stable rate, preventing impact on lower-layer devices.	For Internet services, traffic policing provides a committed information rate (CIR) of 8 Mbit/s and limits the peak information rate (PIR) to 10 Mbit/s. When the rate of the Internet service packets is between the CIR and PIR, the service board marks the packets yellow. When the rate exceeds the PIR, the service board drops the packets.
4	Congestion avoidance: When congestion occurs during enqueueing on an outbound interface, the service board drops non-conformant packets to avoid further congestion.	To promptly drop packets based on priority, set the early drop threshold to 30% for 0-priority Internet services. After this setting takes effect, if 30% of the packets that arrive at a queue are Internet service packets, subsequent Internet service packets will be dropped.
5	Congestion management: When congestion occurs during dequeuing on an outbound interface, the service board uses queuing mechanisms to provide QoS guarantees to high-priority packets preferentially.	Use the strict priority (SP) scheduling algorithm to ensure that voice services with priority 5 are scheduled preferentially and Internet services with priority 0 are scheduled last when congestion occurs.

Packets on the control board are not processed for QoS but are processed for only switching.

After the packets enter the upstream board, the upstream board implements the following QoS processing.

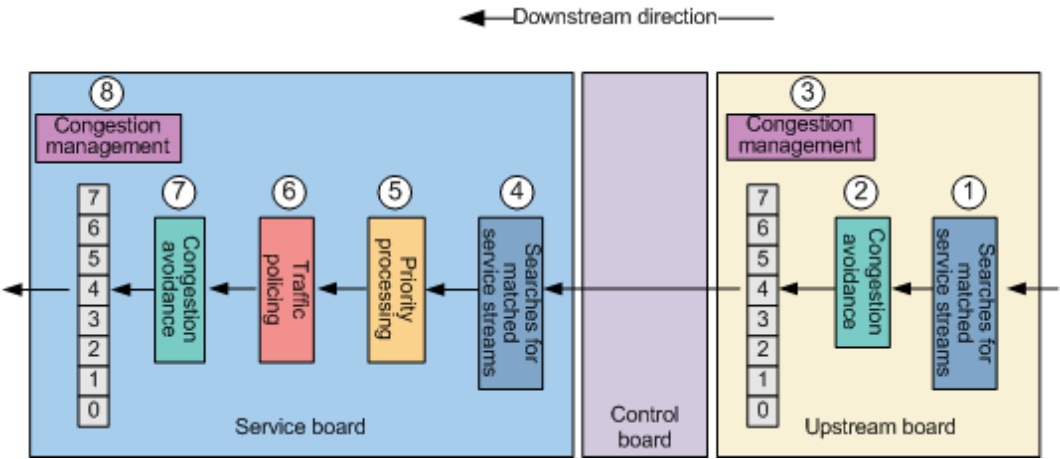
Step	QoS Policy	Example
6	Congestion avoidance: When congestion occurs during enqueueing on an inbound interface, the control board drops non-conformant packets to avoid further congestion.	To promptly drop packets based on priority, set the early drop threshold to 30% for 0-priority Internet services. After this setting takes effect, if 30% of the packets that arrive at a queue are Internet service packets, subsequent Internet service packets will be dropped.
7	Congestion management: When congestion occurs during dequeuing on an outbound interface, the control board uses queuing mechanisms to provide QoS guarantees to high-priority packets preferentially.	Use the SP scheduling algorithm to ensure that voice services with priority 5 are scheduled preferentially and Internet services with priority 0 are scheduled last when congestion occurs.

General QoS Processing - Downstream Direction

Figure 15-4 shows QoS processing in the downstream direction. Different from QoS processing in the upstream direction, QoS processing in the downstream direction is performed in the following way:

- Packets are first processed by the upstream board. After being switched on the control board, packets are processed by the service board.
- In the downstream direction, service flows are searched based on VLAN+MAC or SVLAN+CVLAN at the ingress of the upstream board.
- The service board does not perform traffic classification in the downstream direction. Instead, the service board searches for matched service flows based on a forwarding mode (VLAN+MAC or SVLAN+CVLAN).

Figure 15-4 QoS processing in the downstream direction



15.5 Traffic Classification

Traffic classification differentiates services by packet classification according to the characteristics of user Ethernet packets and certain rules, to implement different processing operations and provide different services.

15.5.1 Introduction to Traffic Classification

Traffic

Service flow or data streams are a type of traffic. A service flow is a set of packets that have common properties. For example, the Internet service packets of a user are one service flow and voice service packets of the user are another service flow.

In the MA5800, a service flow is also called a service port.

For more details about the traffic, please refer to "[10.3 Service Flow](#)".

Traffic Classification

Traffic classification is a technique that categorizes user packets into different classes based on the properties of Ethernet packets and predefined QoS rules. Traffic classes are processed differently and this allows for the provision of differentiated services.

For example, to provide Internet, voice, and IPTV services simultaneously to the same user, the service packets must be separated into three classes.

Purpose

Traffic classification is used to support concurrent uses of multiple services. It differentiates service flows allowing predefined QoS guarantees to be provided for each of the service flows. The system performs service mappings based on service flows and performs QoS actions based on the service mappings. The QoS actions include switching between a user VLAN and the network VLAN, upstream and downstream CAR policing, priority marking, and queue scheduling.

15.5.2 Implementation Principle of Traffic Classification

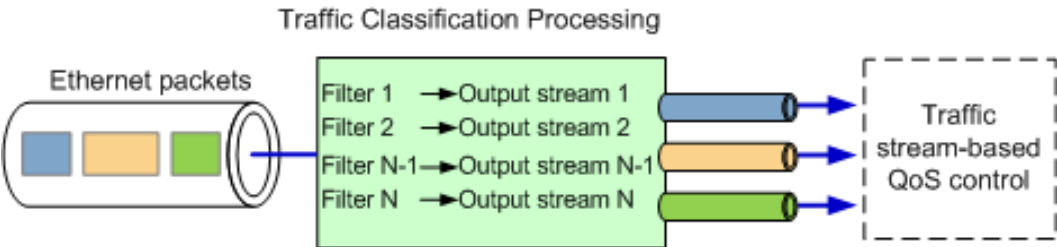
Traffic Classification Process

[Figure 15-5](#) shows the traffic classification process. Traffic classification is performed using classifiers. Each classifier includes a filter (one or more classification rules as described in [Table 15-1](#)) and an output flow. The classifiers separate Ethernet packets received by a device into different traffic classes. QoS guarantees are then provided for each of the traffic classes.

Traffic classification is based on Ethernet packets. For PON access mode, the system segments and reassembles incoming service packets to recover Ethernet frames. The system then performs traffic classification for the Ethernet frames.

Therefore, each GEM port can be regraded as a logical port of an Ethernet port. Traffic classification is performed based on this logical port and this logical port receives and sends Ethernet frames.

Figure 15-5 Traffic classification process



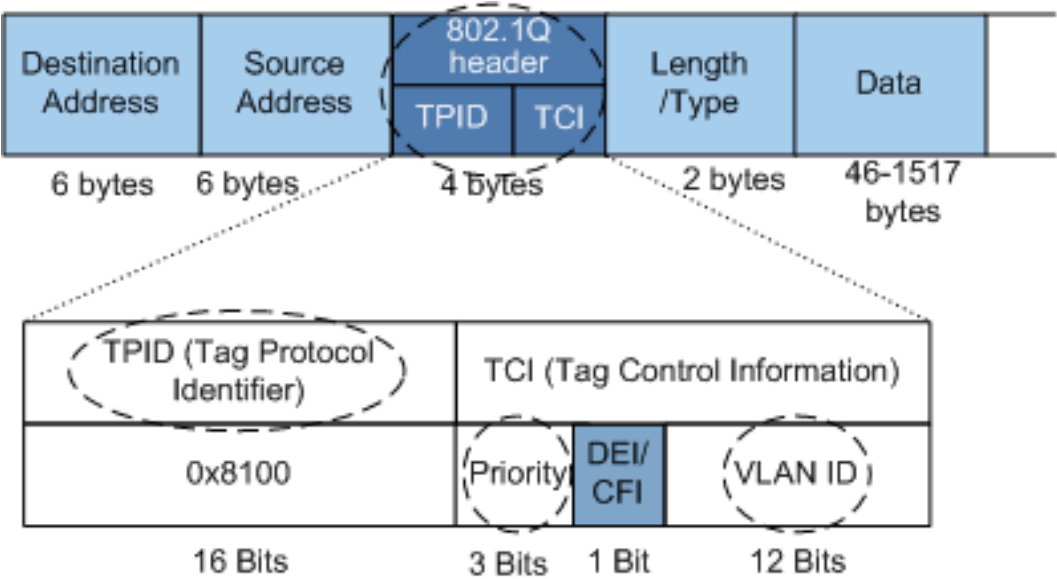
The system performs traffic classification only for upstream packets. Meanwhile, the system learns the MAC addresses of the packets when the packets are forwarded based on VLAN+MAC forwarding mode, and records the indexes of service flows. In the downstream direction, the system searches for the service flow based on the VLAN and MAC address.

Traffic Classification Method and Application

Traffic classification is performed to distinguish user services based on the properties of Ethernet packets. Traffic classification is usually performed based on the following fields in Ethernet frame headers (shown in the Figure 15-6):

- VLAN
- Priority
- Ethernet type

Figure 15-6 Ethernet frame format defined by 802.1q



For detailed traffic classification rules, see [Table 15-1](#).

Table 15-1 Traffic classification rules

Traffic Classification Rule	Application Scenario
Based on CVLAN	If services have different C-VLANs, traffic classification can be performed based on the C-VLANs. For example, traffic classification can be based on the C-VLAN of 100 for Internet services and 200 for voice services.
Based on priority	If the user-side priorities are different, traffic classification can be performed based on priority. For example, the priority of the Internet access service is 1 and the priority of the voice service is 5.
Based on Ethernet type	If the user-side Ethernet types are different, traffic classification can be performed based on Ethernet type. For example, traffic classification can be performed based on IPoE packets or PPPoE packets.
Based on C-VLAN +Ethernet type	If a single field cannot be used to distinguish the service type of packets, traffic classification can be based on combinations of the three fields in Ethernet packets. For example, if services have the same VLANs and priorities, the C-VLAN+Ethernet type combination can be used to distinguish the services.
Based on C-VLAN+priority	
Based on S-VLAN+C-VLAN	This rule is used when users of a service type must be identified uniquely. For example, if a C-VLAN is allocated to a specific user, the S-VLAN+C-VLAN combination can be used to identify this user.
Based on other-all	When a common service and a transparent LAN service exist in a system, other-all can be used to distinguish the two services. For example, a system has an Internet service (VLAN 100) and other transparent LAN services. If the Internet service must be distinguished from the other transparent LAN services, the transparent LAN services can be mapped into the other-all traffic class.

 NOTE

- S-VLAN refers to service VLAN and is usually used to identify a service. In a service flow, S-VLAN is also called network-side VLAN or outer VLAN.
- C-VLAN refers to customer VLAN and is usually used to identify a user. In a service flow, C-VLAN is also called inner VLAN.

Generally, one logical port supports only one traffic classification rule, excluding the following two situations:

- The single-tagged VLAN-based (**user-vlan { untagged | user-vlanid }**) traffic classification and the double-tagged VLAN-based (**double-vlan outer-vlan vlanid inner-vlan vlanid**) traffic classification can coexist.
- The single-service-based traffic classification and multi-service-based traffic classification can coexist on the port whose PVC encapsulation type is auto-sensing (**encapsulation type auto**). The system automatically matches the single-service flows or multi-service flows according to the learned PVC ATM adaptation layer type 5 (AAL5). Then, the single-service flows are used for IPoA/PPPoA services and multi-service flows are used for the Ethernet service.

Packet Matching Priority

- Packets are matched first to the rules that define specific classifiers (for example, C-VLAN or priority) and, if they cannot be matched to a specific traffic class, they are matched to the other-all class.
- If no other-all traffic class has been configured, all incoming packets are matched with specific traffic classes.
- If incoming packets cannot be matched with any traffic class, they are dropped.

15.5.3 Configuring the Traffic Classification

Context

A service flow is the result of traffic classification based on physical ports or logical ports.

Procedure

Step 1 Run the **service-port** command to perform traffic classification.

```
huawei(config)#service-port
{ desc<K>|index<U><0,131071><U>|remote-desc<K>|source<K>|statistics<K>|uplink-po
rt<K>|vlan<K> }: vlan
{ INTEGER<1-4093><U>|name<K> }: 100
{ eth<K>|gpon<K>|port<K>|vdsl<K> }: eth
{ STRING<5-18><S> }: 0/2/0
{ <cr>|bundle<K>|inbound<K>|multi-service<K>|rx-cttr<K>|tag-transform<K> }: mult
i-service
{ double-vlan<K>|user-8021p<K>|user-encap<K>|user-vlan<K> }: user-vlan
{ INTEGER<1-4095><U>|other-all<K>|priority-tagged<K>|untagged<K> }:
```

The key parameters related to traffic classification for this command are as follows:

- **multi-service**: indicates multiple services. Traffic classification is required when a service port carries multiple services.
- **double-vlan**: Traffic classification is performed based on S-VLAN+C-VLAN.
- **user-8021p**: Traffic classification is performed based on the user-side 802.1p priority.
- **user-encap**: Traffic classification is performed based on the user-side encapsulation type, IPoE or PPPoE.

- **user-vlan:** Traffic classification is performed based on the user-side VLAN. Valid values for the user-side VLAN are 1-4095, untagged, priority-tagged (the user packet is tagged as VLAN 0), and other-all.

 NOTE

For details on this command, see "Service Virtual Port Configuration" in Command Reference.

- Step 2** Run the **display service-port** command to verify that the traffic classification has been applied to the service port.

----End

Example

- Traffic classification based on C-VLAN
To perform traffic classification for Ethernet port 0/2/0 based on C-VLAN 100, do as follows:
`huawei(config)#service-port vlan 8 eth 0/2/0 multi-service user-vlan 100`
- Traffic classification based on Ethernet type
To perform traffic classification for Ethernet port 0/2/0 based on Ethernet type PPPoE, do as follows:
`huawei(config)#service-port vlan 8 eth 0/2/0 multi-service user-encap pppoe`
- Traffic classification based on C-VLAN+Ethernet type
To perform traffic classification for Ethernet port 0/2/0 based on C-VLAN 100 and Ethernet type PPPoE, do as follows:
`huawei(config)#service-port vlan 8 eth 0/2/0 multi-service user-vlan 100 user-encap pppoe`
- Traffic classification based on C-VLAN+priority
To perform traffic classification for Ethernet port 0/2/0 based on C-VLAN 100 and priority 3, do as follows:
`huawei(config)#service-port vlan 8 eth 0/2/0 multi-service user-vlan 100 user-8021p 3`
- Traffic classification based on C-VLAN+S-VLAN
To perform traffic classification for Ethernet port 0/2/0 based on S-VLAN 100 and C-VLAN 10, do as follows:
`huawei(config)#service-port vlan 8 eth 0/2/0 multi-service double-vlan outer-vlan 100 inner-vlan 10`

15.6 Priority Marking

According to different priority marking policies, the inner and outer VLAN priorities can be set for service-ports, or the user-side priority can be copied for service-ports.

15.6.1 Introduction to Priority Marking

Definition

Priority processing is a process of marking or re-marking the priority for a packet so that equipment or network can process the packet based on the defined priority. This process is performed in the following way:

- Priorities of packets are usually marked at an inbound interface of equipment or a network and is re-marked inside the equipment or network.
- Packet priorities include both forwarding and drop priorities. These two priorities form the basis for QoS processing. With respect to drop priority processing, the equipment or network uses the drop eligibility indicator (DEI) in an Ethernet packet to mark the color of the packet.

Purpose

Priority processing is the basis for equipment or a network to schedule packets. When congestion occurs, equipment or a network schedules packets based on priorities.

15.6.2 Basic Concepts of Priority Marking

Priorities that equipment processes mainly include the VLAN priority (802.1p priority) and IP precedence.

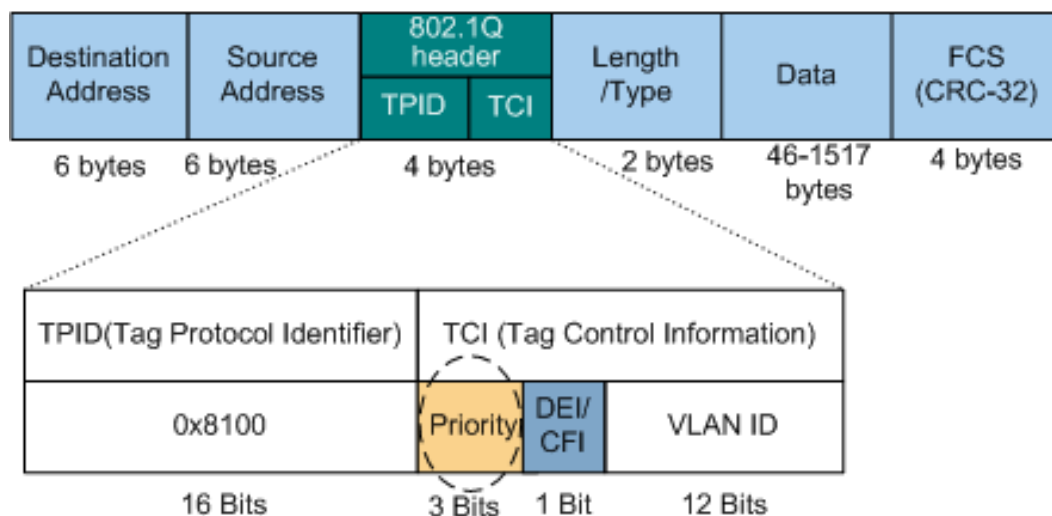
VLAN Priority

VLAN priority, also called 802.1p priority, refers to the packet priority defined at the link layer. This priority represents the class of service (CoS). As defined in IEEE 802.1q, the VLAN priority uses three bits in the VLAN tag (Figure 15-7 shows the position of the VLAN priority in an Ethernet frame).

As shown in the figure, the Priority field indicates the 802.1p priority. This field consists of three bits. The value of the three bits ranges from 0 to 7. The value 0 is the lowest priority and 7 the highest. The priority values set in these fields determine the order in which packets are transmitted when congestion occurs on a port.

The DEI field consists of one bit and represents the drop eligible indicator defined in the 802.1ad protocol. It is used to color the packet. For example, the value 0 means green and 1 means yellow. When the function of is enabled, yellow packets are dropped with preference in case of congestion.

Figure 15-7 Ethernet frame format defined by 802.1q



IP Precedence

The IP protocol defines differentiated services code point (DSCP) and type of service (ToS). They occupy the same field (one byte) in an IP header. IP bearer network devices schedule and forward packets based on the DSCP or ToS filled to provide QoS guarantees for different services.

ToS in the IP header specifies a traffic class for a packet rather than a priority (which is determined by the device). The ToS field consists of eight bits, including a 3-bit IP precedence sub-field, 4-bit ToS sub-field, and one reserved bit (set to 0). The four bits in the ToS sub-field represent the minimum latency, maximum throughput, maximum reliability, and minimum cost. Only one of the four bits can be set to 1. If all the four bits are set to 0, the service is a common service.

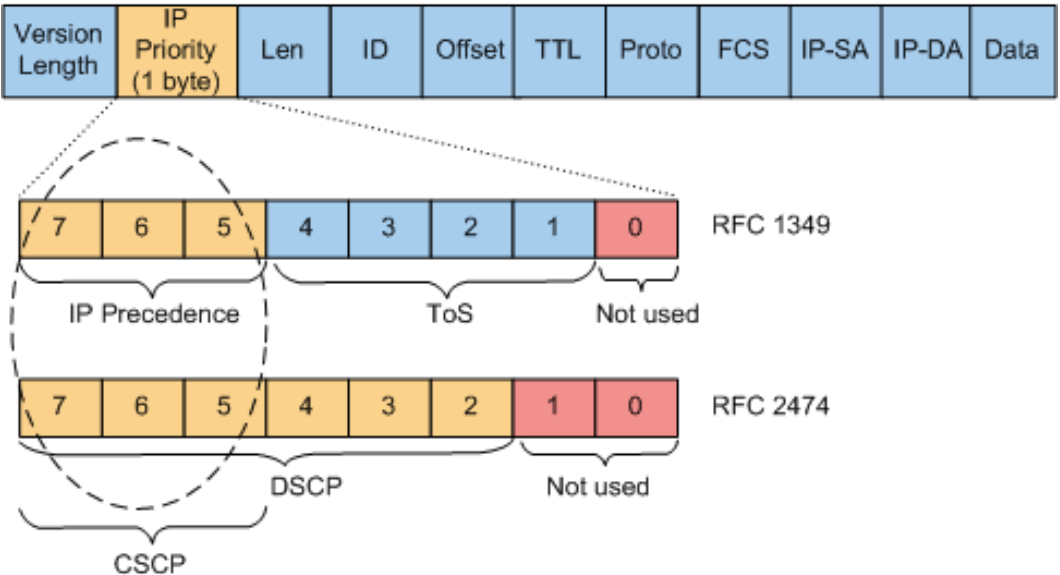
DSCP is defined in the RFC 2474, it is a re-defined object based on an IPv4 type of service (ToS) and an IPv6 traffic class.

 NOTE

The traffic class (TC) field in the IPv6 packet header has the same functions as the IP priority field in the IPv4 packet header. This topic uses the IP priority field in the IPv4 packet header as an example to describe the IP priority.

As shown in [Figure 15-8](#), the six most significant bits in the DS field (bits 7-2) are used as the DS CodePoint (DSCP) and the two least significant bits (bits 1 and 0) are reserved. The three most significant bits in the DS field (bits 7-6-5) are the class selector code point (CSCP), which indicates a DSCP type.

Figure 15-8 IPv4 packet format



DSCP is used to select per-hop behavior (PHB) on each node of a network. PHBs describe the visible external behavior when the DS node is used for data stream aggregation. IETF has defined the following types of PHBs:

- Class selector (CS)
- Expedited forwarding (EF)
- Assured forwarding (AF)
- Best-effort (BE)

Table 15-2 shows the structure of PHBs.

Table 15-2 Structure of PHBs

PHB	Bit 7-6-5	Bit 4-3-2
CS	aaa (Remark)	000
BE	000	000
EF	101	110
AF	bbb (Remark)	cc0 (Remark)

Remark: a, b and c indicates a single bit, whose value is 0 or 1. Where,

- The "aaa" has eight values, from 000 to 111, it corresponds to the decimal number 0-7. The 3 bits can map with IP precedence individually.
- The "bbb" has four values: 001, 010, 011 and 100, it corresponds to the decimal number 1-4.
- The "cc" has three values, from 01 to 11, it corresponds to the decimal number 1-3.

Table 15-3 shows the common DSCP service types and corresponding priorities.

Table 15-3 Common DSCP service types and corresponding priorities

DSCP type	IPv4 precedence/ 802.1P priority	DSCP value (binary)	Application
BE	0	0	Internet
AF1	1	001 010	Leased Line
AF1	1	001 100	Leased Line
AF1	1	001 110	Leased Line
AF2	2	010 010	IPTV VoD
AF2	2	010 100	IPTV VoD
AF2	2	010 110	IPTV VoD
AF3	3	011 010	IPTV Broadcast
AF3	3	011 100	IPTV Broadcast
AF3	3	011 110	IPTV Broadcast

DSCP type	IPv4 precedence/ 802.1P priority	DSCP value (binary)	Application
AF4	4	100 010	NGN/3G Signaling
AF4	4	100 100	NGN/3G Signaling
AF4	4	100 110	NGN/3G Signaling
EF	5	101 110	NGN/3G voice
CS6	6	110 000	Protocol
CS7	7	111 000	Protocol

15.6.3 Priority Sources

Priority processing includes copying, designating, and mapping inner and outer VLAN priorities.

Priority Processing for an Outer VLAN (or Single-Tagged VLAN) of Ethernet Service Flows

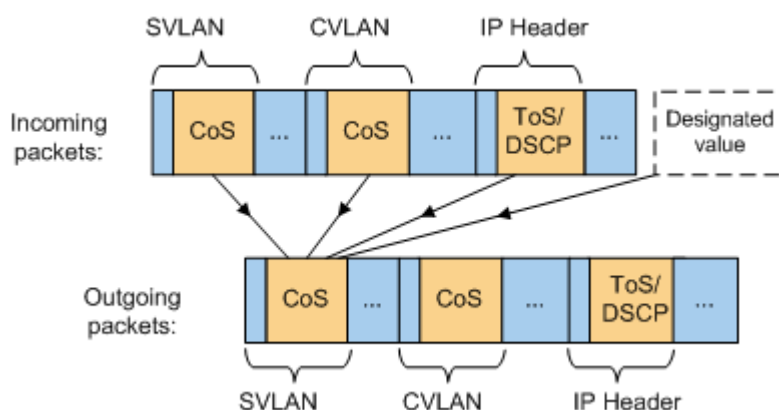
Figure 15-9 shows how the priority of an outer VLAN or the single-tagged VLAN is processed. The priority of an outer VLAN can be derived from multiple sources:

- Copied from the outer VLAN priority (user-cos) of an incoming packet
- Copied from the inner VLAN priority (user-inner-cos) of an incoming packet
- Copied or mapped from the IP ToS priority (user-tos) of an incoming packet
- Mapped from the IP DSCP priority (user-dscp) of an incoming packet
- Copied from the priority of a designated packet (prival)

NOTE

Currently, the downstream equipment of a service flow cannot copy the user-dscp priority.

Figure 15-9 Priority processing for an outer VLAN (or single-tagged VLAN) of Ethernet Service Flows



Some boards support several priority mapping choices:

- 802.1p priority -> 802.1p priority (To implement this mapping, run the **pbits-to-pbits mapping table** command. It's only valid for inner VLAN priority)
- IP priority -> 802.1p priority (To implement this mapping, run the **ipprec-to-pbits mapping table** command.)
- DSCP priority -> 802.1p priority (To implement this mapping, run the **dscp-to-pbits mapping table** command.)

Figure 15-10 shows the mappings between incoming and outgoing priorities of packets.

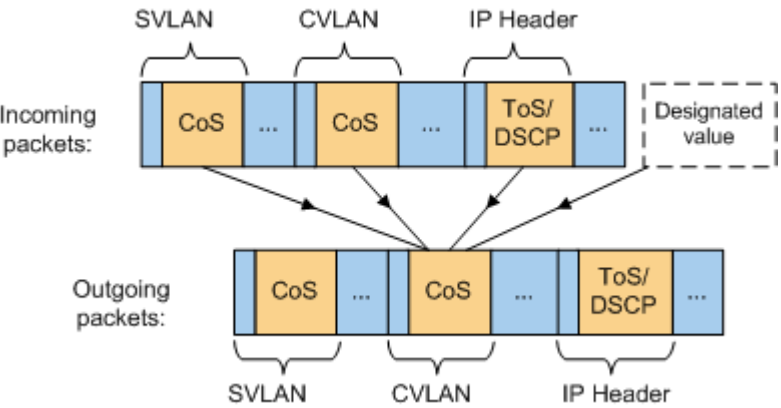
Figure 15-10 Mapping between the incoming and outgoing priorities of packets

802.1p/IP priority (Incoming packets)	DSCP priority (Incoming packets)	802.1p priority of outgoing packets (Copy priority by default, and priority can't be modified)	802.1p priority of outgoing packets (Mapping, priority can be modified)
0	0-7	0	0
1	8-15	1	1
2	16-23	2	2
3	24-31	3	3
4	32-39	4	3
5	40-47	5	3
6	48-55	6	4
7	56-63	7	5

Priority Processing for an Inner VLAN of Ethernet Service Flows

Figure 15-11 shows how the priority of an inner VLAN is processed. The sources of an inner VLAN priority are the same as those of an outer VLAN priority.

Figure 15-11 Priority processing for an inner VLAN

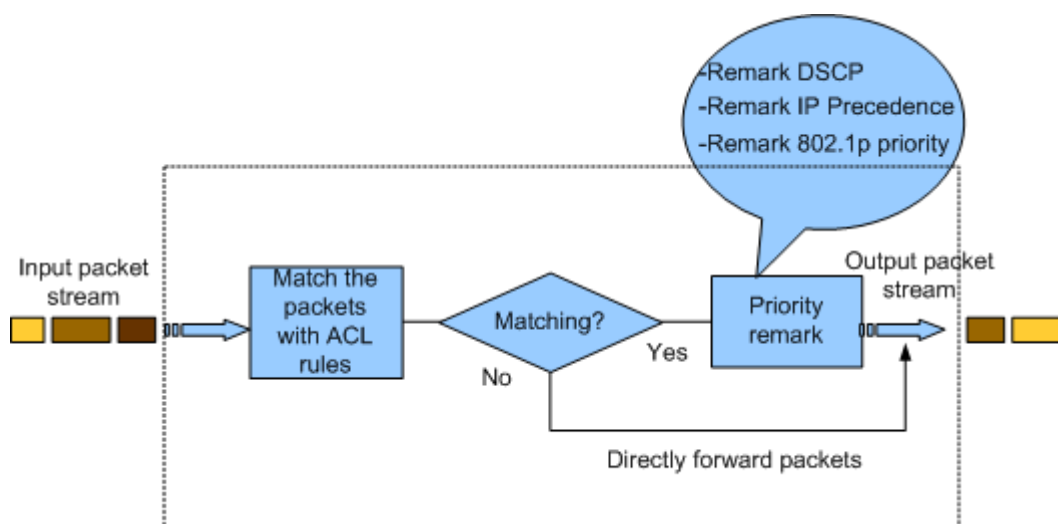


Priority Processing for ACL-based Packets

Figure 15-12 shows the policy of priority processing for ACL-based packets. The system processes the input packets according to ACL rules. After packets match ACL rules, the system remarks these packets by running the **traffic-priority** command.

- Specifies the DSCP priority of the packets.
- Specifies or copies the 802.1p priority of packets as the IP precedence priority of packets.
- Specifies or copies the IP precedence priority of packets as the 802.1p priority of packets.

Figure 15-12 Priority processing for ACL-based packets



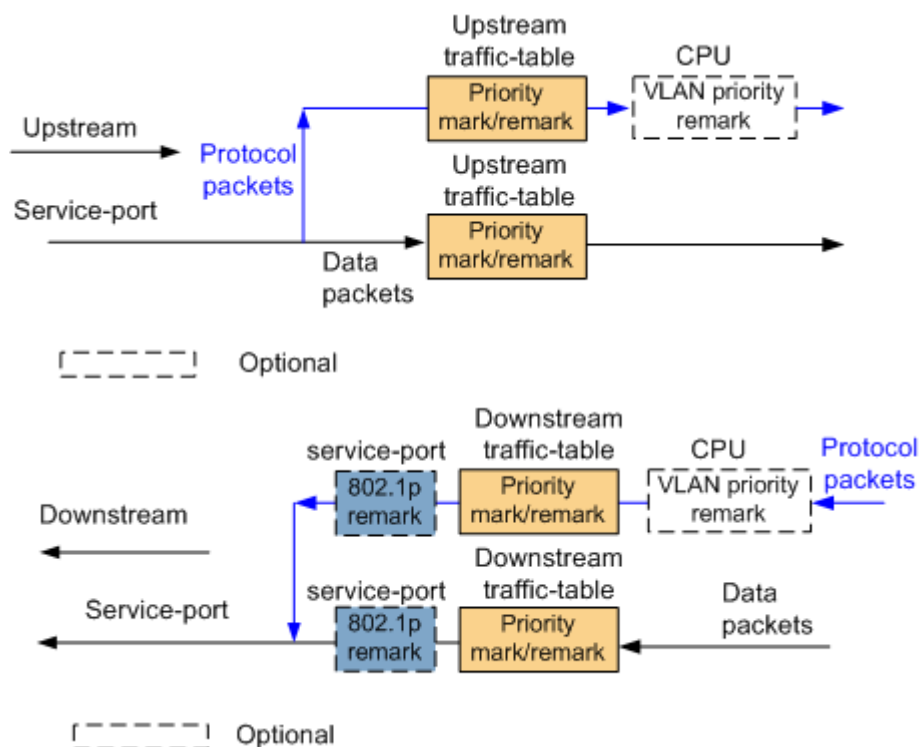
15.6.4 Implementation Principle of Priority Marking

Priority processing applies to common data packets and specific protocol packets. The priority processing mechanisms for data packets and protocol packets are different, because protocol packets are captured and processed by the CPU.

In addition, priority processing is affected by the following factors:

- Attribute parameters of service flows (whether user-802.1p is configured)
- **Priority source**
- VLAN priority
- Packet forwarding mode (Layer 2 or Layer 3 forwarding)

Figure 15-13 describes packet priority processing in the non-service-bundle scenario.

Figure 15-13 Packet priority processing in the non-service-bundle scenario

Note that the packet priority processing described in the preceding scenarios is a general processing model. Not all types of packets strictly comply with this model. For details on priority processing for packets of a particular type, refer to the priority processing mechanism for the packet type.

15.6.4.1 Priority Processing for Data Packets

Priority Processing for Data Packets in the Non-Service-Bundle Scenario

Priority processing for data packets in the non-service-bundle scenario has the following characteristics:

- The service flow priority is irrelevant to the VLAN priority (Run the **vlan priority** *vlanid* *priority* command to set VLAN priority).
- Priority processing in the upstream /downstream direction is based on the priority processing policy (specify or copy/map priorities, as shown in [Figure 15-14](#) and [Figure 15-15](#)) configured in the upstream /downstream traffic profile.
- If the user-cos, user-tos, or user-inner-cos parameter is selected but no such priority exists in the packet (in other words, priority copying fails), the system uses the default 802.1p priority for the packet.

Figure 15-14 Priority processing for upstream data packets in the non-service-bundle scenario

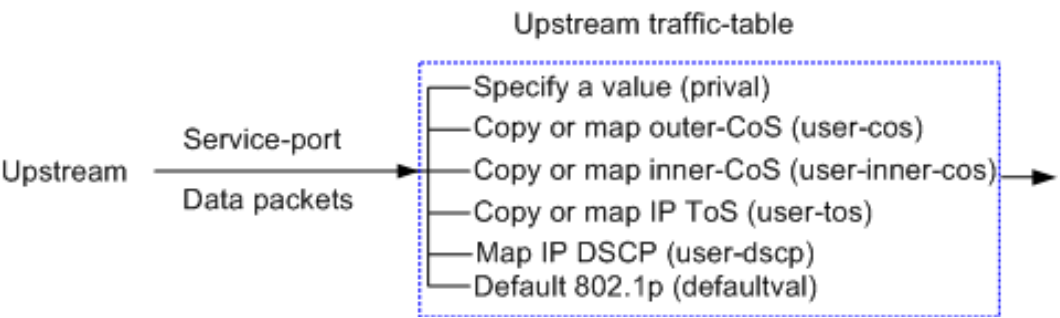


Figure 15-15 Priority processing for downstream data packets in the non-service-bundle scenario

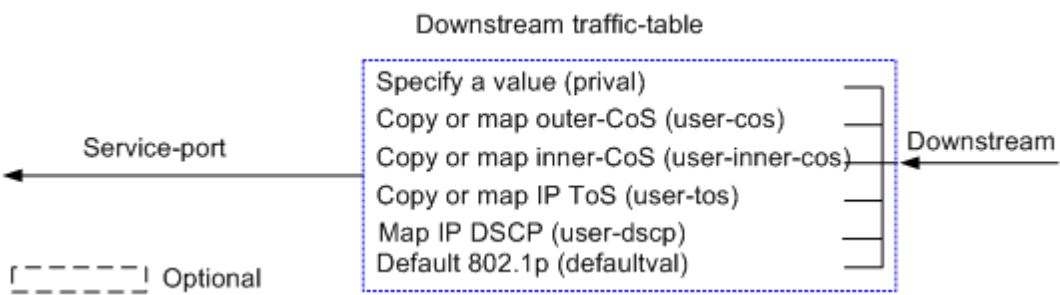


Figure 15-16 shows the detailed processing results.

Figure 15-16 Priority processing results of upstream and downstream data packets in the non-service-bundle scenario

service-port		traffic table				vlan priority	Forwarding mode	ONT gemport mapping	xPON & P2P System Behavior	
user-8021p	user-vlan	priority	user-cos	user-tos	default				Upstream direction	Downstream direction
-	✓	✓	-	-	-	NA	L2	Priority Mapping	traffic table priority	traffic table priority
-	✓	✓	-	-	-	NA	L3	Priority Mapping	traffic table priority	traffic table priority
✓	✓	✓	-	-	-	NA	L2	Priority Mapping	traffic table priority	traffic table priority
✓	✓	✓	-	-	-	NA	L3	Priority Mapping	traffic table priority	traffic table priority
-	✓	-	✓	-	✓	NA	L2	Priority Mapping	user-cos	user-cos
-	✓	-	✓	-	✓	NA	L3	Priority Mapping	user-cos	user-cos
✓	✓	-	✓	-	✓	NA	L2	Priority Mapping	user-cos	user-cos
✓	✓	-	✓	-	✓	NA	L3	Priority Mapping	user-cos	user-cos
-	✓	-	-	✓	✓	NA	L2	Priority Mapping	user-tos	user-tos
-	✓	-	-	✓	✓	NA	L3	Priority Mapping	user-tos	user-tos
✓	✓	-	-	✓	✓	NA	L2	Priority Mapping	user-tos	user-tos
✓	✓	-	-	✓	✓	NA	L3	Priority Mapping	user-tos	user-tos
✓: Configured		-: Unconfigured								

15.6.4.2 Priority Processing for DHCP & PPPoE Packets

Priority Processing for DHCP & PPPoE Packets in the Non-Service-Bundle Scenario

DHCP protocol packets can work in Layer 2 or Layer 3 relay mode. The DHCP protocol packets in this document refer to DHCP Option82 packets in Layer 2 relay mode and DHCP Layer 3 relay packets.

PPPoE protocol packets work only in Layer 2 mode. The PPPoE packets in this document refer to PPPoE PTP packets.

When DHCP and PPPoE packets work in Layer 2 mode, the priority processing mechanism is the same as that for common data packets, which has the following characteristics:

- The service flow priority is irrelevant to the VLAN priority.
- Priority processing in the upstream /downstream direction is based on the priority processing policy (specify or copy/map priorities) configured in the upstream /downstream traffic profile.
- If the **user-cos**, **user-tos**, or **user-inner-cos** parameter is selected but no such priority exists in the packet (in other words, priority copying fails), the system uses the default 802.1p priority for the packet.

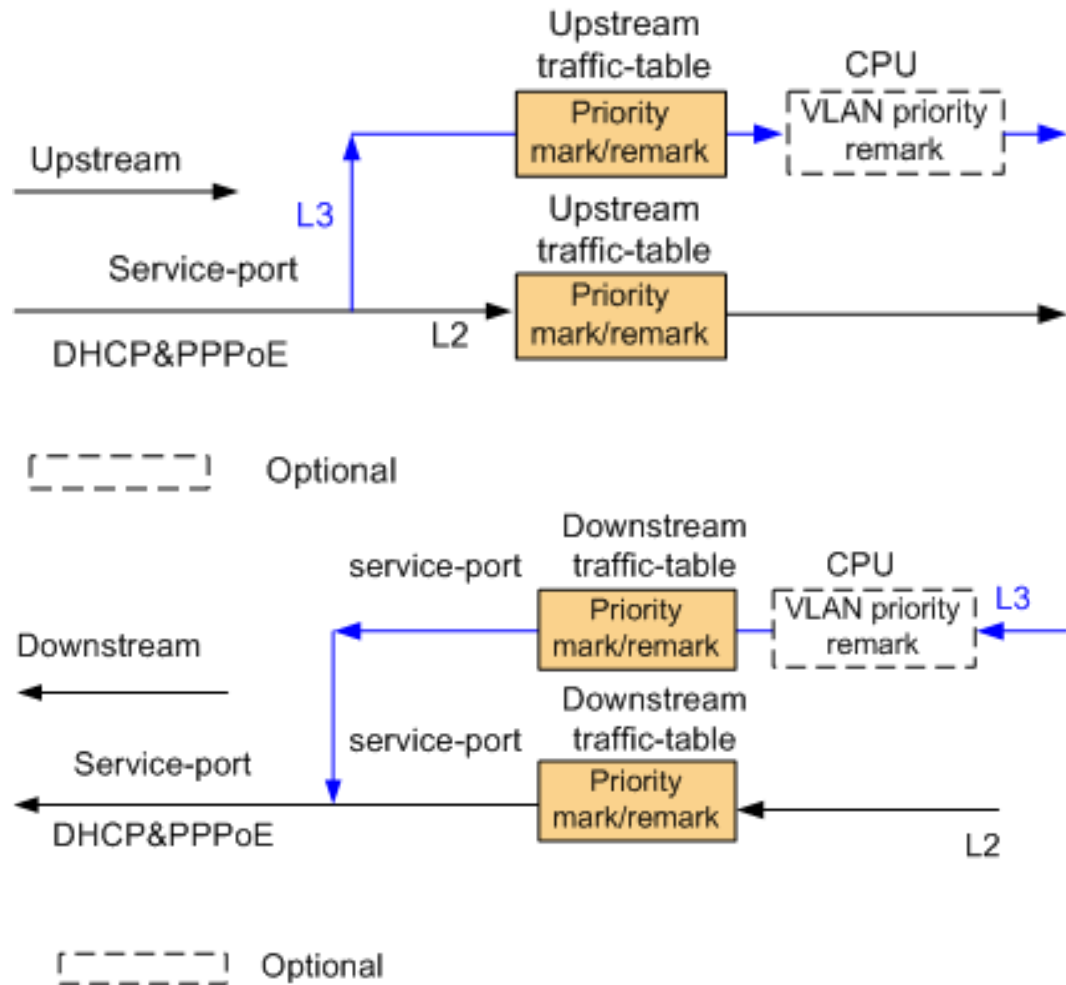
NOTE

When the user-tos priority policy is specified in the traffic profile, ToS copying fails for PPPoE PTP packets. When this occurs, the default 802.1p priority in the traffic profile will be used.

When DHCP packets work in Layer 3 mode, the priority processing mechanism has the following characteristics:

- Priority processing in the upstream direction is based on the priority processing policy (specify or copy/map priorities) configured in the upstream traffic profile.
- When the **prival** parameter or the **user-cos/user-inner-cos/user-tos** parameter in the upstream traffic profile is set to 0, the network-side VLAN priority takes effect.
- In the downstream direction, if the network-side priority of the packet is **0**, the packet priority is remarked as the user-side VLAN priority, and then is remarked based on the downstream traffic profile.
- In the downstream direction, if the priority processing policy specified in the traffic profile is **user-tos**, the user-side priority of the packet is fixedly remarked as **0**.

Figure 15-17 Priority processing for upstream and downstream DHCP & PPPoE packets



Priority Processing for DHCP & PPPoE Packets in the Service-Bundle Scenario

Priority processing for DHCP & PPPoE packets in the service-bundle scenario has the following characteristics:

- The priority of upstream packets is the priority specified for the service-bundle group. The settings in the traffic profile do not apply.
- The priority processing for downstream packets is the same as that in the non-service-bundle scenario.

15.6.4.3 Priority Processing for DHCPv6 Packets

Priority Processing for DHCPv6 Packets in the Non-Service-Bundle Scenario

DHCPv6 protocol packets can work in Layer 2 or Layer 3 relay mode. The DHCPv6 protocol packets in this document refer to DHCP Option18/Option37 packets in Layer 2 relay mode and DHCP Layer 3 relay packets.

When DHCPv6 packets work in Layer 2 mode, the priority processing mechanism is the same as that for DHCPv4 packets in Layer 2 mode, which has the following characteristics:

- The service flow priority is irrelevant to the VLAN priority.
- Priority processing in the upstream /downstream direction is based on the priority processing policy (specify or copy/map priorities) configured in the upstream /downstream traffic profile.
- If the **user-cos**, **user-tos**, or **user-inner-cos** parameter is selected but no such priority exists in the packet (in other words, priority copying fails), the system uses the default 802.1p priority for the packet.

When DHCPv6 packets work in Layer 3 mode, the priority processing mechanism is the same as that for DHCPv4 packets in Layer 3 mode, which has the following characteristics:

- Priority processing in the upstream direction is based on the priority processing policy (specify or copy/map priorities) configured in the upstream traffic profile.
- When the **prival** parameter or the **user-cos/user-inner-cos/user-tos** parameter in the upstream traffic profile is set to 0, the network-side VLAN priority takes effect.
- In the downstream direction, if the network-side priority of the packet is **0**, the packet priority is remarked as the user-side VLAN priority, and then is remarked based on the downstream traffic profile.
- In the downstream direction, if the priority processing policy specified in the traffic profile is **user-tos**, the user-side priority of the packet is fixedly remarked as **0**.

Priority Processing for DHCPv6 Packets in the Service-Bundle Scenario

Priority processing for DHCPv6 packets in the service-bundle scenario has the following characteristics:

- The priority of upstream packets is the priority specified for the service-bundle group. The settings in the traffic profile do not apply.
- The priority processing for downstream packets is the same as that in the non-service-bundle scenario.

15.6.4.4 Priority Processing for IGMP Packets

The IGMP packets in this document refer to IGMP packets for IPv6 and IPv4. The priority processing applies to IGMP packets for both IPv4 and IPv6 unless otherwise specified.

Priority Processing for IGMP Packets in the Non-Service-Bundle Scenario

The IGMP mode for multicast VLANs can be IGMP snooping or IGMP proxy. The priority processing mechanism for IGMP packets varies with the IGMP mode.

Figure 15-18 describes the priority processing mechanism for IGMP packets in IGMP snooping mode.

- Priority processing in the upstream direction is based on the priority processing policy (specify or copy/map priorities) configured in the upstream traffic profile.
- In the downstream direction, if the multicast VLAN tag mode is set to "dual" by running the **igmp multicast-tag dual** command, then the inner VLAN priority of IGMP packet is the same as the outer VLAN priority.
- In the downstream direction, priority processing is implemented based on the settings in the downstream traffic profile.

 NOTE

The current version does not support the copying policy for IGMP protocol packets in the downstream direction. Therefore, when the priority processing policy specified is user-cos or user-tos, the default priority (defaultval) in the downstream traffic profile is used.

Figure 15-18 Priority processing for IGMP packets in IGMP snooping mode

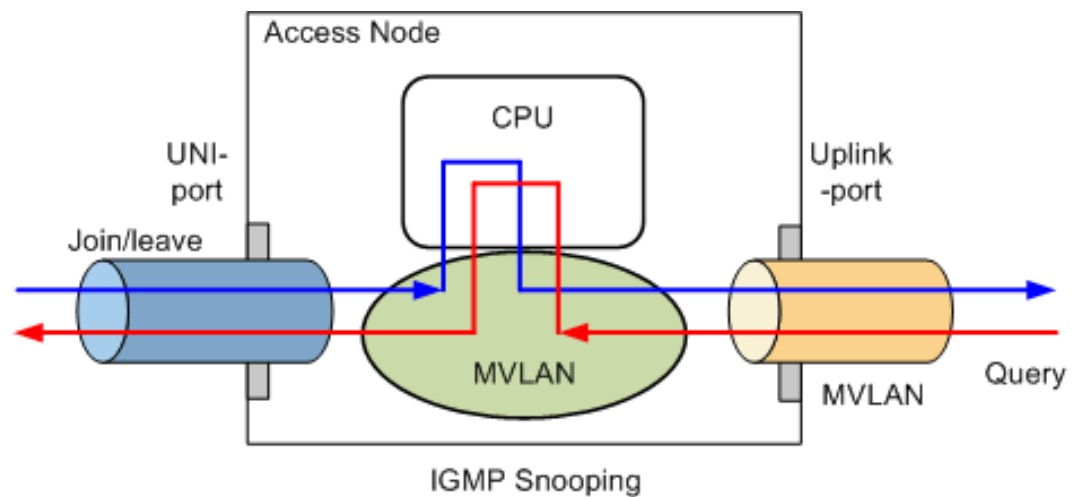
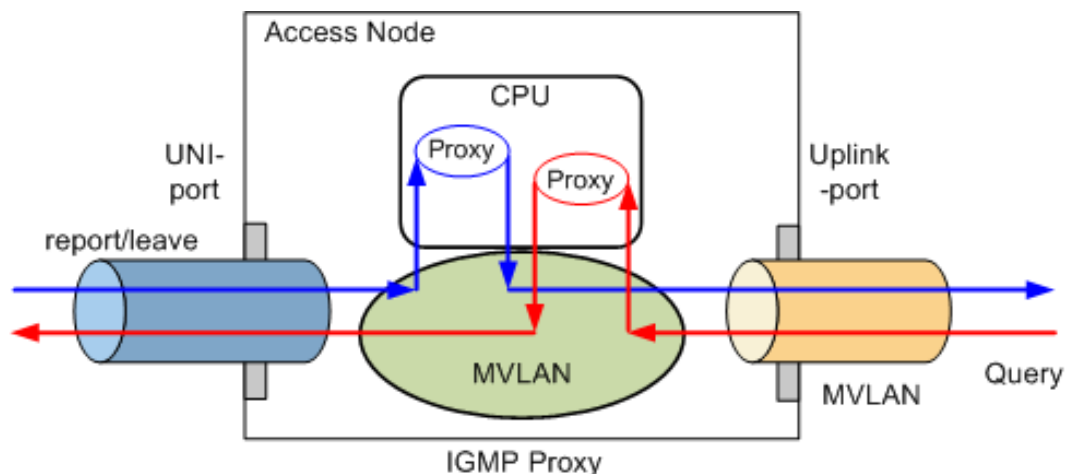


Figure 15-19 describes the priority processing mechanism for IGMP packets in IGMP proxy mode.

- The priority processing in the upstream direction depends on the specified IGMP packet priority. Command for setting the IGMP packet priority: **igmp priority** (IPv4)/**igmp ipv6 priority** (IPv6)
- In the downstream direction, priority processing is implemented based on the settings in the downstream traffic profile.

 NOTE

The current version does not support the copying policy for IGMP protocol packets in the downstream direction. Therefore, when the priority processing policy specified is user-cos or user-tos, the default priority (defaultval) in the downstream traffic profile is used.

Figure 15-19 Priority processing for IGMP packets in IGMP proxy mode

Priority Processing for IGMP Packets in the Service-Bundle Scenario

Priority processing for IGMP packets in the service-bundle scenario has the following characteristics:

- In IGMP proxy mode, the priority processing for upstream and downstream packets is the same as that in the non-service-bundle scenario.
- In IGMP snooping mode, the priority processing mechanism has the following characteristics:
 - The priority of upstream packets is the priority specified for the service-bundle group. The settings in the traffic profile do not apply.
 - The priority processing for downstream packets is the same as that in the non-service-bundle scenario.

15.6.4.5 Priority Processing for ARP Packets

ARP packets in this document refer to ARP packets sent by access nodes in the upstream and downstream directions. For ARP packets sent by non-access nodes, the priority processing mechanism is the same as that for common data packets.

For ARP packets, the upstream/downstream direction has a meaning that differs from the meaning for other protocol packets:

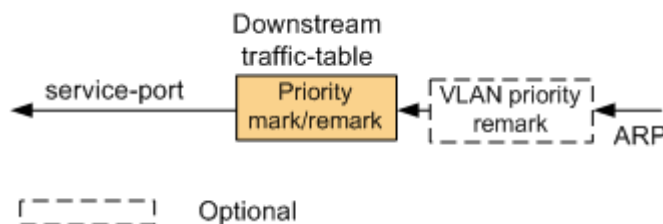
- Upstream direction: In this direction, an access node gives ARP responses or initiates ARP requests to the network side.
- Downstream direction: In this direction, an access node gives ARP responses or initiates ARP requests to the user side.

Priority Processing for ARP Packets in the Non-Service-Bundle Scenario

The priority processing mechanism for ARP packets has the following characteristics:

- In the upstream direction, priority processing depends only on the VLAN priority and is irrelevant to the priority configuration of the service flow.
 - If no VLAN priority is configured, the packet priority will be remarked as 0 (the default priority for ARP packets).
 - If the VLAN priority is configured, the packet priority will be remarked as the VLAN priority.
- **Figure 15-20** describes the priority processing in the downstream direction.
 - The priority processing in the downstream direction involves VLAN priority remarking, priority remarking based on the traffic profile, and service flow 802.1p remarking.
 - If the service flow is created on the GPON/ETH board and the priority processing policy specified in the traffic profile is **user-cos**, the 802.1p remarking is skipped. In this case, if the VLAN priority is configured, the packet priority will be remarked based on the VLAN priority; if no VLAN priority is configured, the packet priority will be remarked as 0.
 - If the priority processing policy specified in the traffic profile is user-tos or user-inner-cos, priority copying fails because ARP packets do not have such fields. In this case, the packet priority is remarked as the default value (defaultval) specified in the traffic profile.

Figure 15-20 Priority processing for downstream ARP packets in the non-service-bundle scenario



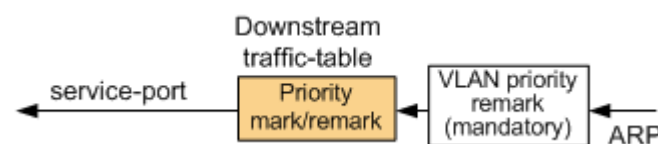
Priority Processing for ARP Packets in the Service-Bundle Scenario

In the upstream direction, priority processing for ARP packets is irrelevant to the priority configuration of the service flow and is the same as that in the non-service-bundle scenario.

In the service-bundle scenario, the priority of ARP packets sent by an access node to the user side must be the bundle-cos of the service flow; otherwise, the ARP packets fail to be received. Therefore, the VLAN priority must be configured.

Figure 15-21 describes the priority processing mechanism for downstream ARP packets in the service-bundle scenario. According to **Figure 15-21**, the priority processing is almost the same as that in the non-service-bundle scenario. The difference is that the VLAN priority is mandatory in this scenario while it is optional in the non-service-bundle scenario.

Figure 15-21 Priority processing for downstream ARP packets in the service-bundle scenario



15.6.4.6 Priority Processing for ND Packets

This topic describes the priority processing for neighbor discovery (ND) packets. For detailed processing rules and results, refer to [Priority Processing Rules](#).

ND packets apply to the IPv6 scenario. Similar to the ARP function for IPv4 packets, the ND function is used to determine the link-layer address and reachability of a neighboring node for IPv6 packet forwarding.

Because the function of ND packets is similar to that of ARP packets, the priority processing mechanism for ND packets is also similar to that for ARP packets. For details, refer to [Priority Processing for ARP Packets](#). The difference is that

- The default priority for ARP packets is 0 while that for ND packets is 6.
- The ARP packet does not carry any IP header, and therefore the user-tos copying in the downstream direction is not supported. In this case, the priority of the ARP packet is remarked as the default priority specified in the traffic profile. The ND packet carries an IP header, and therefore the user-tos copying in the downstream direction is supported. In this case, the priority of the ND packet is remarked as 6.

15.6.5 Configuring the Priority Processing

Context

Priority processing is the basis for equipment or a network to schedule packets. When congestion occurs, equipment or a network schedules packets based on priority.

A priority processing policy is configured in a traffic profile for equipment.

Procedure

- Step 1** Run the **traffic table ip** command to configure priority processing.

```
huawei(config)#traffic table ip index 11
cir<K>|name<K> |:cir
{ cir<U><64,10240000>|off<K> |:off
{ color-policy<K>|priority<K> |:priority
{ prival<U><0,7>|user-cos<K>|user-inner-cos<K>|user-tos<K> |:user-cos
{ defaultval<U><0,7>|mapping-profile<K> |:3
{ inner-priority<K>|priority-policy<K> |:inner-priority
{ inner-prival<U><0,7>|user-cos<K>|user-inner-cos<K>|user-tos<K> |:user-inner-cos
{ defaultval<U><0,7>|mapping-profile<K> |:3
{ priority-policy<K> |:priority-policy
{ priority-policy<E><Local-Setting,Tag-In-Package,Tag-In-Ingress-Package> |:tag-In-package
Command:
      traffic table ip index 11 cir off priority user-cos 3 inner-priority u
ser-inner-cos 3 priority-policy tag-In-package

Create traffic descriptor record successfully
-----
Traffic Table Index      : 11
Traffic Table Name      : ip-traffic-table_11
Specified Outer-Priority : -
Outer-Priority Mapping Source: user-cos
Outer-Priority Mapping Index : 0
Default Outer-Priority  : 3
Specified Inner-Priority : -
```

```
Inner-Priority Mapping Source: user-inner-cos
Inner-Priority Mapping Index : 0
Default Inner-Priority      : 3
Specified DSCP              : -
DSCP Mapping Source         : -
DSCP Mapping Index         : -
CIR                          : off
CBS                          : off
PIR                          : off
PBS                          : off
Fix                          : off
CAR Threshold Profile       : -
Color Mode                  : color-blind
Coupling Flag               : enable
Rate Profile Index          : -
Rate Profile Name           : -
Color Policy                : dei
Color DEI                   : unmark-dei
Color Source                : outer-dei
Drop Precedence             : remarked-outer-priority
Priority Policy              : tag-pri
Que-Policy Profile ID       : -
Pri-Group Profile ID        : -
Pri-Group Profile Name      : -
Referenced Status           : not used
E2E Mapping Priority        : -
E2E Mapping Index          : -
E2E Default Priority        : -
Yellow WRR Weight           : auto
Green WRR Weight            : auto
-----
```

The parameters for this command are as follows:

- **priority**: specifies the S-VLAN priority policy, including the priority source and queue scheduling policy. The upstream priority determines which queue that upstream packets enter. Valid values for this parameter are as follows:
 - **prival**: specifies a priority for upstream and downstream packets. When **priority-policy** is set to **Local-Setting**, the priority is determined by the value of **Local-Setting**.
 - **user-cos**: copies the priority from the outer 802.1q tag of an incoming packet as the S-VLAN priority.
 - **user-inner-cos**: copies the priority from the inner 802.1q tag of an incoming packet as the S-VLAN priority.
 - **user-tos**: copies the priority from the IP ToS field of an incoming packet as the S-VLAN priority.
- **inner-priority**: specifies the C-VLAN priority policy. The parameter values are the same as those for the parameter that specifies the S-VLAN priority policy. C-VLAN and S-VLAN can be set independently.
- **priority-policy**: specifies the priority policy for queue scheduling. The queue scheduling priority of a packet is generally the same as the priority of the packet. If queue scheduling and packet priorities are different, the queue scheduling priority must be manually specified. Valid values for this parameter are as follows:
 - **Local-Setting**: uses a manually specified priority as the queue scheduling priority.
 - **Tag-In-Package**: uses the priorities of outgoing packets (after VLAN translation) as the queue scheduling priority.

- **Tag-In-Ingress-Package:** uses the priorities of incoming packets (before VLAN translation) as the queue scheduling priority for the downstream direction.

 NOTE

For details on this command, see "QoS Configuration" in "QoS Command" of Command Reference.

Step 2 Run the **display traffic table ip** command to verify the configuration result.

----End

Follow-up Procedure

After configuring a traffic profile, run the **service-port** command to bind service flows to the profile to ensure that different priority processing policies are applied to different types of traffic.

15.7 Traffic Policing

Before service providers provide subscribers with specific services, a service level agreement (SLA) is generally assigned, in which all service parameters are defined. To ensure that the user traffic can meet the SLA, the user traffic must be policed.

15.7.1 Introduction to Traffic Policing

Definition

Traffic policing (also called traffic policy) sets limits on the rate of incoming and outgoing service flow packets. Policing measures packet rates to monitor service flow bursts. Incoming and outgoing packets must meet user-defined conditions and, if they do not meet these conditions, the device that the packets pass through is configured to take countermeasures. For example, if the incoming packet rate exceeds a threshold, the device can take actions such as dropping or coloring the packets (re-setting the packet priorities).

Traffic policing is usually implemented using the committed access rate (CAR). In a PON system, upstream bandwidth conflict between ONUs is resolved by the dynamic bandwidth assignment (DBA) technology.

Purpose

Traffic policing enables carriers to achieve the following goals:

- Ensure that user traffic stays within the service level agreement (SLA).
- Ensure service quality by regulating outgoing traffic and suppressing burst traffic.
- Control the rate of broadcast packets using packet suppression.

15.7.2 Basic Concepts of Traffic Policing

Figure 15-22 shows the basic concepts of traffic policing and Table 15-4 describes these concepts.

Figure 15-22 Key concepts of traffic policing

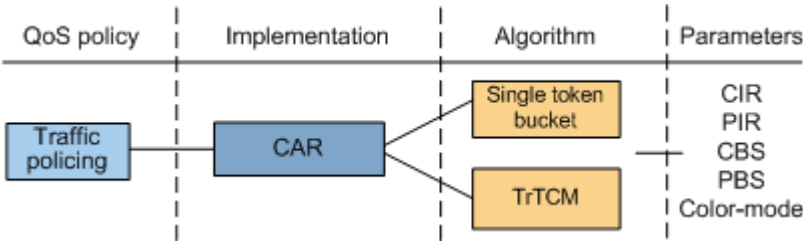


Table 15-4 Description of the basic concepts

Concept	Description
CAR	Stands for committed access rate. It is a technique commonly used to provide the specified rate for specific traffic. And it is widely used to limit the rate of ethernet ports, xDSL ports and xPON ports. CAR is usually implemented using token bucket algorithms.
Token bucket	A token bucket is a container that stores tokens, and it is used for controlling data traffic. A token bucket allows burst data transmission while controlling the traffic. There are two token bucket algorithms: single token bucket algorithm and dual token bucket algorithm. According to the principle of token bucket algorithms, a packet is transmitted when there is equivalent size of tokens in the token bucket. After a packet is transmitted, the number of tokens in the buckets decreases accordingly.
trTCM	Stands for two rate three color marker. It is defined in RFC2698 developed by the Internet Engineering Task Force (IETF). The trTCM algorithm sets the DEI bit for an ethernet packet based on two rates (PIR and CIR) and the burst size to mark the packet green, yellow, or red.
DEI	Stands for drop eligible indicator and is defined by 802.1ad. The DEI field in an ethernet packet consists of 1 bit and is the same as the CFI field defined by 802.1q. This field is used to mark an Ethernet packet with a corresponding color.
CIR	Stands for committed information rate. The unit is bit/s.
PIR	Stands for peak information rate. It provides users the maximum bandwidth when the system is idle. The unit is bit/s.

Concept	Description
CBS	Stands for committed burst size. It is used to define the capacity of token bucket C, that is, the maximum burst IP packet size when information is transferred at the committed information rate. The unit is byte.
PBS	Stands for peak burst size. It is used to define the capacity of token bucket P, that is, the maximum burst IP packet size when the information is transferred at the peak information rate. The unit is byte.
Color mode	The trTCM algorithm uses two modes: color-blind and color-aware. In the color-blind mode, the trTCM algorithm assumes that the packet is uncolored. In the color-aware mode, the trTCM algorithm assumes that the packet is pre-colored.

15.7.3 Implementation Principle: CAR

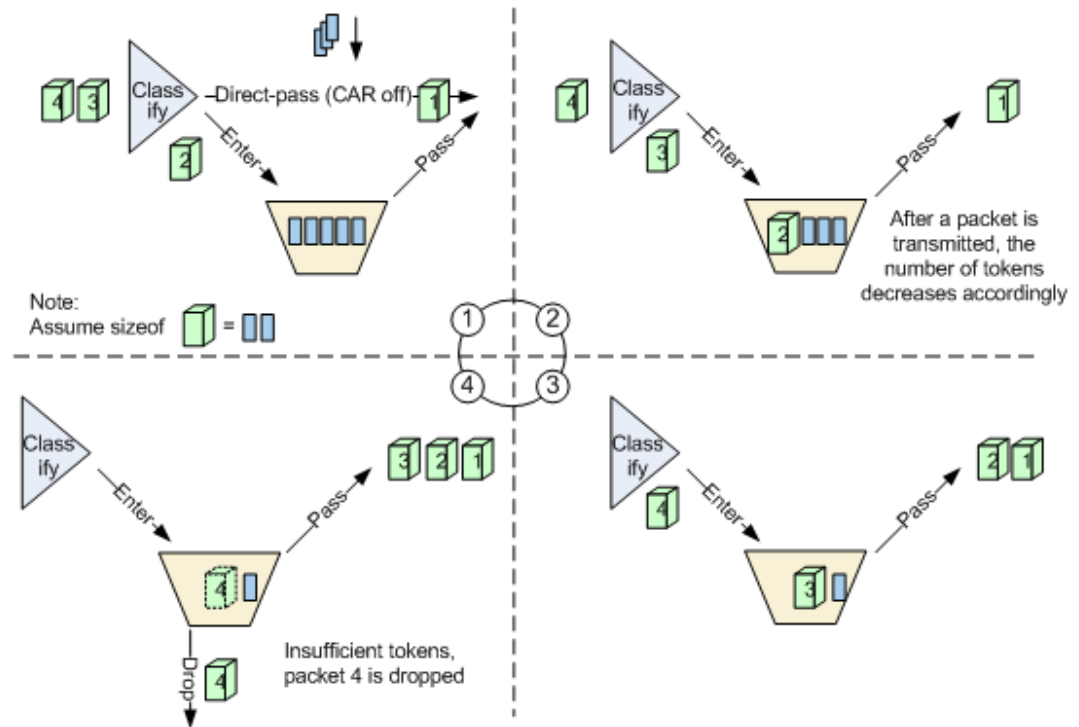
Principle of Single Token Bucket

A packet is transmitted when the number of tokens in the token bucket is sufficient to allow transmission. After a packet is transmitted, the number of tokens decreases accordingly. The details are as follows:

1. Incoming packets are categorized into different traffic classes. If the packets belong to a traffic class for which the rate is limited, for example, packets 2, 3, and 4 in [Figure 15-23](#), the packets are sent to the token bucket for processing. If the packets do not belong to any traffic class, for example, packet 1 in [Figure 15-23](#), the rate of the packets is not limited and the packets are transmitted directly.
2. If the token bucket stores sufficient tokens, packets are transmitted, for example, packets 2 and 3 in [Figure 15-23](#).
3. If the token bucket stores insufficient tokens, packets are dropped, for example, packet 4 in [Figure 15-23](#).
4. The system places tokens in the token bucket at a user-defined rate. When new tokens are generated in the bucket, successive packets can be transmitted.

When the token bucket is full, the system transmits all packets that are the same size as the tokens in the bucket. This process allows for burst transmission. When the token bucket is empty, the system cannot transmit any packet. The system resumes transmissions only after new tokens have been generated. This means that the traffic transmission rate is consistently lower than or equal to the token generation rate, so as to achieve the rate limiting goal.

Figure 15-23 CAR implementation using a single token bucket (process in clockwise direction)



In the figure above, the digits 1, 2, 3, and 4 are the numbers of packets. After a packet passes through the bucket, the number of tokens decreases by the size of the packet. For easy understanding, we suppose that all packets have the same size.

Principle of Dual Token Buckets (trTCM)

The two rate three color marker (trTCM) algorithm defined by RFC2698 is used for traffic policing and marking to achieve effective bandwidth management. If static bandwidth is planned for a network, the trTCM algorithm can at least ensure the basic bandwidth (CIR) for users, and allows users to obtain extra bandwidth (PIR) when the network has sufficient bandwidth. In this way, network resources are used more efficiently.

trTCM principles are as follows:

- trTCM uses two token buckets (P and C buckets). The maximum capacity of the P bucket is represented by the peak burst size (PBS) and that of the C bucket is represented by the committed burst size (CBS). The two token buckets are initially full.

NOTE

PBS must be larger than CBS.

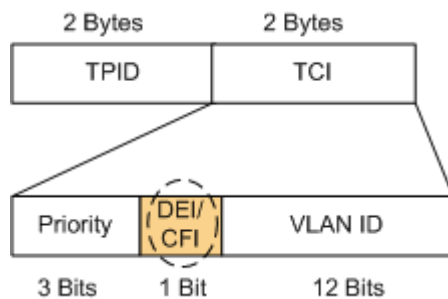
- After a packet passes through the tokens, the number of tokens in the buckets decreases accordingly.

- The system generates tokens in the P bucket at the PIR and in the C bucket at the CIR ($PIR \geq CIR$) per second. The total tokens in the buckets are always less than maximum capacity.
- Based on the size of tokens in the buckets, the system marks the DEI bit (as shown in [Figure 15-24](#)) in an incoming packet with a corresponding color (green, yellow, or red). Color coded packets help the system to prevent or manage congestion during data processing.

 NOTE

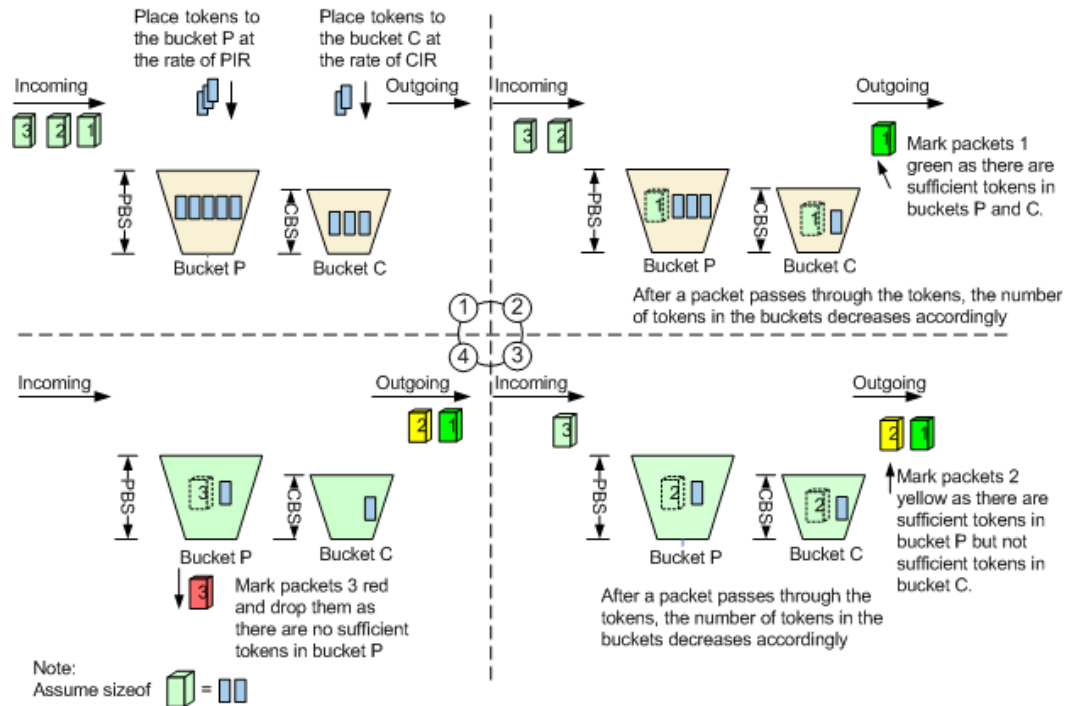
The MA5800 uses the CFI bit defined by 802.1q as the DEI.

Figure 15-24 DEI bit defined by 802.1ad (same as the CFI bit defined by 802.1q)



As shown in [Figure 15-25](#):

1. If a packet does not exceed CIR, it is marked green (the DEI bit in the packet is set to 0) and is allowed to pass. Packet 1 in the figure is an example.
2. If a packet exceeds CIR but does not exceed PIR, it is marked yellow (the DEI bit in the packet is set to 1) and is allowed to pass. Packet 2 in the figure is an example.
3. If a packet exceeds PIR, the packet is marked red and is directly dropped. Packet 3 in the figure is an example.

Figure 15-25 CAR implementation using the trTCM algorithm (process in clockwise direction)

In the figure above, the digits 1, 2, and 3 are the numbers of packets. After a packet passes through the bucket, the number of tokens decreases by the size of the packet. For easy understanding, we suppose that all packets have the same size.

Enhanced trTCM: Coloring Packets Based on CAR Threshold

The trTCM algorithm ensures that different types of packets are all forwarded when they do not exceed CIR and are forwarded fairly when they reach PIR. The trTCM algorithm policies packets based on the bandwidth and it does not mark colors for packets based on priorities. Therefore, the trTCM algorithm cannot guarantee bandwidth for high-priority services. The enhanced trTCM algorithm can resolve the issue of the trTCM algorithm because it marks colors for packets based on CAR thresholds.

The implementation principle is as follows:

- When the enhanced trTCM algorithm is implemented for equipment, users can set different CAR thresholds for different packets by running the **car-threshold** command, ensuring that a high CAR threshold is set for high-priority packets.

NOTE

The CAR threshold is the percentage by which tokens in the C and P buckets have decreased. The percentage of the remaining tokens in the buckets is obtained by subtracting the CAR threshold from 1.

- When packets of different priorities sequentially pass the P bucket and C bucket:

- If a packet of a certain priority in the P bucket exceeds the CAR threshold, the packet is directly dropped. Otherwise, the packet enters the C bucket.
- If a packet of a certain priority in the C bucket exceeds the CAR threshold, the packet is marked yellow; otherwise, it is marked green.
- After a packet passes through the tokens, the number of tokens in the buckets decreases accordingly.

As shown above, enhanced trTCM ensures that packets with higher priorities are marked green and their bandwidths are guaranteed.

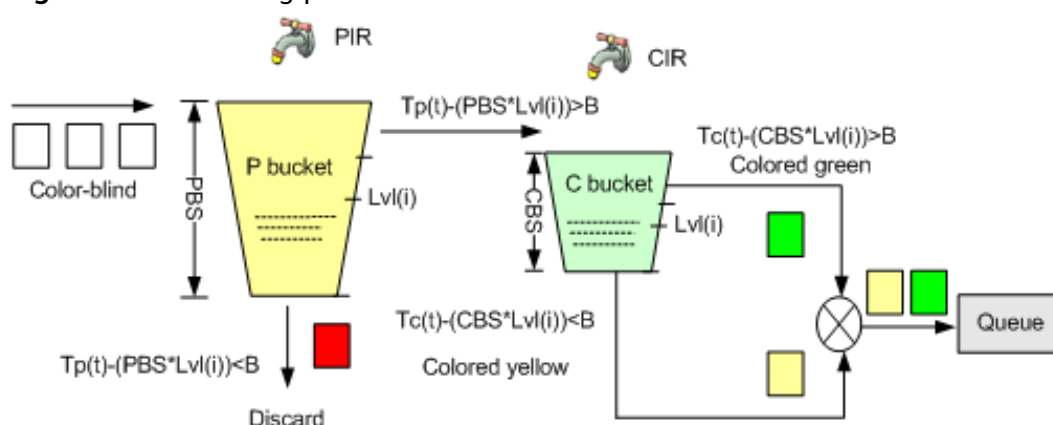
As shown in [Figure 15-26](#), there are two token buckets C and P with depths CBS and PBS respectively. The two buckets have token counts T_c and T_p , respectively. $T_p(t)$ and $T_c(t)$ represent the number of tokens in the P and C buckets respectively at time t . Initially ($t = 0$), the P and C buckets are full, that is, $T_p(0) = PBS$ and $T_c(0) = CBS$. Then, T_p increases by one for PIR times per second until reaching PBS and T_c increases by one for CIR times per second until reaching CBS. $Lvl(i)$ represents the percentage of the remaining tokens corresponding to a specific priority.

When an i -priority packet with length of B bytes arrives at time t :

1. If $T_p(t) - (PBS * Lvl(i)) < B$, the device drops the packet; otherwise, the device sends the packet to the C bucket, and $T_p(t)$ decreases by B bytes.
2. If $T_c(t) - (CBS * Lvl(i)) < B$, the device marks the packet yellow and $T_c(t)$ decreases by B bytes; otherwise, the device marks the packet green and $T_c(t)$ decreases by B bytes.

For example, when the CAR threshold is 12% for 0-priority packets and is 100% for 6-priority packets, the enhanced trTCM algorithm enables the device to behave as follows:

- When the incoming packets enter the P bucket at a certain time, if the percentage of the remaining tokens in the bucket is less than 88%, the device drops 0-priority packets and sends 6-priority packets to the C bucket. When the incoming packets enter the C bucket at a certain time, if the percentage of the remaining tokens in the bucket is less than 88%, the device marks 0-priority packets yellow and 6-priority packets green.
- When the incoming packets enter the P bucket at a certain time, if there is no token in the bucket, the device also drops 6-priority packets. When the incoming packets enter the C bucket at a certain time, if there is no token in the bucket, the device drops 0-priority packets and marks 6-priority packets yellow.

Figure 15-26 Coloring packets based on CAR threshold

15.7.4 Traffic Policing Mode

As shown in [Table 15-5](#), the MA5800 supports multiple traffic policies:

- Rate limiting based on service flows
- Rate limiting based on port+priority
- Rate limiting based on GEM port+CoS group
- Rate limiting based on service flow+priority
- Rate limiting based on groups of service flows
- Rate limiting based on port+VLAN
- Rate limiting based on priority group
- Rate limiting based on priority groups of service flow groups
- Rate limiting based on ONT
- Rate limiting based on Ethernet port on ONT

Table 15-5 Traffic policing mode and token bucket algorithm

Traffic Policy	Description	Token Bucket Algorithm
Rate limiting based on service flows	When configuring service flows, you can limit the rate of the service flows by binding upstream and downstream service flows to an upstream and downstream profile, respectively. If there is no limit on the rate, you can configure the upstream and downstream profiles as car-off. Rate limiting based on service flows and rate limiting based on port+CoS cannot be applied to the same board or port at the same time. The configuration commands are: • car-mode service-port • service-port • and traffic table ip.	trTCM
Rate limiting based on port +priority	Rate limiting based on GEM port+CoS is used for GPON applications. Rate limiting based on service flows and rate limiting based on port+CoS cannot be applied to the same board or port at the same time. The configuration commands are: • car-mode port-cos • car-port <i>portid</i> cos • car-port <i>portid</i> ont <i>ontid</i> gemindex <i>gemindex</i> and cos.	trTCM

Traffic Policy	Description	Token Bucket Algorithm
Rate limiting based on GEM port+CoS group	One GEM port can carry services with different priorities. After the priority of the specific service is added to the CoS group, rate limiting is performed based on this CoS group. This meets the carrier requirement that rates of various services carried on the same GEM port are limited. The configuration commands are: • car-mode port-cos • cos-group-table • car-port <i>portid</i> ont <i>ontid</i> gemindex <i>gemindex</i> cos-group-table <i>table-index</i> • car-port <i>portid</i> ont <i>ontid</i> gemindex <i>gemindex</i> cos-group and <i>group-id</i>.	trTCM
Rate limiting based on service flow +priority	When configuring service flows, you can limit the rate of the service flows by binding upstream and downstream service flows to an upstream and downstream profile, respectively. If there is no limit on the rate, you can configure the upstream and downstream profiles as car-off (system default). The configuration command is: car-threshold profile.	Enhanced trTCM
Rate limiting based on groups of service flows	You can bind multiple upstream or downstream service flows into one group and apply the same CAR to the group. The configuration command is: car-group.	trTCM
Rate limiting based on port +VLAN	You can limit the rates for packets with specified VLANs on specified ports. Only the Ethernet board supports this traffic policy. The configuration commands are: car-port <i>portid</i> and vlan.	trTCM

Traffic Policy	Description	Token Bucket Algorithm
Rate limiting based on priority group	In this rate limiting, priority groups are of the same service flow. Priorities are grouped based on inner and outer 802.1p tags. The configuration commands are: • priority-group profile • and car-group.	trTCM

Traffic Policy	Description	Token Bucket Algorithm
Rate limiting based on priority groups of service flow groups	Create service flow groups first. Then, run the car-group priority group profile command to enable priority group CAR of service flow groups. Run the car-group command to configure the traffic-table parameter and apply the priority-group profile to achieve rate limiting based on priority groups of service flow groups. The configuration commands are: • car-group add-member service-port • car-group priority group profile • and car-group.	TrTCM Description: • Priority group CAR of service flow groups, and CAR of service flows or priority group CAR of service flows are mutually exclusive. That is, after priority group CAR of service flow groups is configured, CAR of service flows or priority group CAR of service flows cannot be configured. On the contrary, after CAR of service flows or priority group CAR of service flows is configured, priority group CAR of service flow groups cannot be configured. CAR of service flows and priority group CAR of service flows are not mutually exclusive. • Connection-oriented service flows can be added to groups based on source and destination. • CAR of service flows and priority group CAR of service flow groups support specification sharing. The shared CAR specification is twice the CAR

Traffic Policy	Description	Token Bucket Algorithm
		specification of service flows on boards. For example, if the CAR specification of service flows on boards is 16K, the shared CAR specification is 32K.
Rate limiting based on ONT	You can limit the rates for downstream packets of a specified ONU. The configuration command is: traffic-limit ont .	Single token bucket Note: This rate limiting policy applies when the single token bucket algorithm and the rate limiting policy is bound to the trTCM traffic profile. In the trTCM traffic profile, CIR must be equal to PIR; otherwise, the preconfigured PIR will supersede the specified rate limiting policy.
Rate limiting based on Ethernet port on ONT	You can limit the rates for upstream and downstream packets of specified Ethernet ports on an ONT. The configuration command is: ont port car .	Single token bucket Note: This rate limiting policy applies when the single token bucket algorithm and the rate limiting policy is bound to the trTCM traffic profile. In the trTCM traffic profile, CIR must be equal to PIR; otherwise, the preconfigured CIR will supersede the specified rate limiting policy.

Traffic Policy	Description	Token Bucket Algorithm
Traffic suppression	Using this policy, the system suppresses broadcast, unknown multicast, and unknown unicast packets for inbound ports. The traffic suppression prevents these packets from consuming excessive network resources and therefore protects the network from congestion. The configuration command is: traffic-suppress .	-

15.7.5 Configuring the Traffic Policing

15.7.5.1 Configuring Rate Limitation Based on Service Port

This topic describes how to limit rate on a specific service flow (on behalf of a different type of service or users) through the traffic parameters defined in the IP traffic profile.

Context

- The system has seven default IP traffic profiles with the IDs of 0-6. You can run the **display traffic table** command to query the traffic parameters of the default traffic profiles.
- It is recommended that you use the default traffic profiles. A new IP traffic profile is created only when the default traffic profiles cannot meet the requirements.

Procedure

- Step 1** Configure the rate limitation mode to be service-port.
- In the service board mode, run the **car-mode [portlist] service-port** command to set the rate limitation mode of board or port to be service-port.
- Step 2** Configure the parameters of IP traffic profile.
- When the default traffic profiles cannot meet the requirements, run the **traffic table ip** command to configure the IP traffic profile.

Table 15-6 shows the traffic parameters related to rate limitation in IP traffic profile.

Table 15-6 Traffic parameters and parameter Description

Item	Parameter Description
cir <i>cir</i>	Stands for committed information rate. The unit is bit/s. CIR is mandatory, and must be an integer multiple of 64. If it is not, the value is rounded down to a nearest integer multiple of 64 but cannot be smaller than 64.
cbs <i>cbs</i>	Stands for committed burst size. It indicates the maximum capacity that a token bucket buffers tokens. The unit is byte. CBS is optional. If the parameter is not specified, it can be obtained by the formula $\min(2000 + 32 \times \text{cir}, 10240000)$.
pir <i>pir</i>	Stands for peak information rate. It provides users the maximum bandwidth when the system is idle. The unit is bit/s. PIR is optional. If the parameter is not specified, it can be obtained by the formula $\min(2 \times \text{cir}, 10240000)$. The pir cannot be smaller than cir.
pbs <i>pbs</i>	Stands for peak burst size. It indicates the maximum capacity that a token bucket buffers tokens. The unit is byte. PBS is optional. If the parameter is not specified, it can be obtained by the formula $\min(2000 + 32 \times \text{pir}, 10240000)$.

 NOTE

The system marks the service packets with colors according to the CIR and PIR parameters. To be specific, for the packets whose rate is equal to or lower than CIR, the system marks them as green (allowed to pass). For the packets whose rate is higher than CIR and lower than PIR, the system marks them as yellow (allowed to pass). For the packets whose rate is higher than PIR, the system marks them as red, and drops such packets.

Step 3 Run the **service port** command to bind the specified IP traffic profile.

----End

Example

Assume that the CIR is 2048 Kbit/s, 802.1p priority of the outbound packet is 6, and the scheduling policy of the inbound packet is Tag-In-Package. To add traffic profile 9 with these settings, do as follows:

```
huawei(config)#traffic table ip index 9 cir 2048 priority 6 priority-policy tag-In-Package
Create traffic descriptor record successfully
-----
Traffic Table Index      : 9
Traffic Table Name      : ip-traffic-table_9
Specified Outer-Priority : 6
Outer-Priority Mapping Source: -
Outer-Priority Mapping Index: -
Default Outer-Priority  : -
Specified Inner-Priority : -
Inner-Priority Mapping Source: -
Inner-Priority Mapping Index: -
Default Inner-Priority  : -
Specified DSCP          : -
```

```
DSCP Mapping Source      : -
DSCP Mapping Index      : -
CIR                      : 2048 kbps
CBS                      : 67536 bytes
PIR                      : 4096 kbps
PBS                      : 133072 bytes
Fix                      : 0 kbps
CAR Threshold Profile    : -
Color Mode               : color-blind
Coupling Flag            : enable
Rate Profile Index       : -
Rate Profile Name        : -
Color Policy             : dei
Color DEI                : unmark-dei
Color Source             : outer-dei
Drop Precedence          : remarked-outer-priority
Priority Policy           : tag-pri
Que-Policy Profile ID    : -
Pri-Group Profile ID     : -
Pri-Group Profile Name   : -
Referenced Status        : not used
E2E Mapping Priority     : -
E2E Mapping Index       : -
E2E Default Priority     : -
Yellow WRR Weight        : auto
Green WRR Weight         : auto
```

huawei(config)#**display traffic table ip index 9**

```
Traffic Table Index      : 9
Traffic Table Name       : ip-traffic-table_9
Specified Outer-Priority : 6
Outer-Priority Mapping Source: -
Outer-Priority Mapping Index : -
Default Outer-Priority   : -
Specified Inner-Priority  : -
Inner-Priority Mapping Source: -
Inner-Priority Mapping Index : -
Default Inner-Priority    : -
Specified DSCP           : -
DSCP Mapping Source      : -
DSCP Mapping Index      : -
CIR                      : 2048 kbps
CBS                      : 67536 bytes
PIR                      : 4096 kbps
PBS                      : 133072 bytes
Fix                      : 0 kbps
CAR Threshold Profile    : -
Color Mode               : color-blind
Coupling Flag            : enable
Rate Profile Index       : -
Rate Profile Name        : -
Color Policy             : dei
Color DEI                : unmark-dei
Color Source             : outer-dei
Drop Precedence          : remarked-outer-priority
Priority Policy           : tag-pri
Que-Policy Profile ID    : -
Pri-Group Profile ID     : -
Pri-Group Profile Name   : -
Referenced Status        : not used
E2E Mapping Priority     : -
E2E Mapping Index       : -
E2E Default Priority     : -
Yellow WRR Weight        : auto
Green WRR Weight         : auto
```

15.7.5.2 Configuring Rate Limitation Based on Port+CoS

This topic describes how to configure Rate limiting based on port+CoS so that different IP traffic profiles can be specified for the traffic streams that have different 802.1p priorities on a port.

Prerequisites

The IP traffic profile is configured. For details, see [15.7.5.1 Configuring Rate Limitation Based on Service Port](#).

Context

- Rate limiting based on service ports conflicts with Rate limiting based on port+CoS. By default, the system supports Rate limiting based on service ports.
- If service ports are configured on the board, the rate limiting mode of the board cannot be changed.

Procedure

Step 1 Configure the rate limitation mode to be port-cos.

In the service board mode, run the **car-mode** [*portlist*] **port-cos** command to configure the rate limiting mode of the service board to rate limiting based on port+CoS.

Step 2 Configure rate limitation for service flows with specified 802.1p priority.

Run the **car-port** command to specify the 802.1p priority for the port, and bind an IP traffic profile to the traffic streams that meet the specified 802.1p priority.

When rate limiting based on port+CoS is selected for a board, pay attention to the following points:

- For a non-xPON board, you can bind the corresponding traffic profile in the inbound/outbound direction according to a CoS value of a port on the board.
- For a GPON board, you can bind the corresponding traffic profile in the inbound/outbound direction according to a CoS value of a GEM port on the board.

----End

Example

To configure GEM port 1 on ONT 0 of the board in port 0/2/0, and bind traffic profile 2 to the packets with priority 5, do as follows:

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#car-mode port-cos
huawei(config-if-gpon-0/2)#car-port 0 ont 0 gemindex 1 cos 5 inbound 2 outbound 2
huawei(config-if-gpon-0/2)#display car-mode
The CAR mode of the board: port-cos
-----
```

15.7.5.3 Configuring User-based Rate Limitation

In the user-based rate limitation, the VoIP, IPTV service, and Internet access service of each user share a total user bandwidth. When there is no voice or IPTV service,

the Internet access service can hold a burst of the total user bandwidth so that the total user bandwidth can be managed in a unified manner.

Context

When the user uses the Triple play service, the VoIP, IPTV service, and Internet access service of each user share a total user bandwidth. All services of the user hold the total user bandwidth, and the service with the highest CoS priority is ensured first. When other services carry no traffic, each service can hold a burst of the total user bandwidth. The multicast bandwidth is determined by the bandwidth of demanded programs. The total bandwidth of demanded programs cannot exceed the total user bandwidth. The bandwidth of voice services is fixed.

NOTE

PON multicast services do not support rate limitation in CAR-group mode.

Procedure

- For PON access users.
 - In the user-based rate limitation, multiple service ports of a user are added to a rate-limited group. Through the QoS strategy applied on the rate-limited group, the total user bandwidth is ensured on the basis that the committed information rate (CIR) and peak information rate (PIR) of each service are ensured, and each service is allowed to hold a burst of the total user bandwidth.
 - Only the GPON service boards support user-based rate limitation.
- a. Run the **traffic table ip** command to create an IP traffic profile to configure the CoS priority of each service and ensure the CIR and PIR.
 - The CoS priorities of services are VoIP, IPTV service, and Internet access service in a descending order.
 - In the IP traffic profile used by the rate-limited group, the PIR must be equal to or larger than the sum of CIRs of all services in other IP traffic profiles.
- b. Run the **service-port** command to create service ports of the VoIP, IPTV service, and Internet access service, using the IP traffic profile created in step 1.
- c. Run the **car-group** command to create the rate-limited group of service ports to manage the total user bandwidth of multiple services.
 - To ensure the user bandwidth, the PIR of the rate-limited group must be equal to or larger than the sum of CIRs of all services in the rate-limited group.
 - The PIR is equal to the total user bandwidth. In the case that any two services carry no traffic, the third service can hold a burst of the total user bandwidth.
- d. Run the **car-group add-member service-port** command to add service ports to the rate-limited group.

Pay attention to the following points when adding service ports to the rate-limited group:

- Only service ports of the same PON port can be added to the same rate-limited group.
- For Type C and Type D, only service ports of the same ONT can be added to the same rate-limited group.
- One service port cannot be added to multiple rate-limited groups.
- A maximum of eight service ports can be added to a rate-limited group.

----End

Example

Assume that under GPON port 0/2/1, the user with the ONT 1 is provided with the VoIP, IPTV, and Internet access services. Set the total user bandwidth to 10 Mbit/s, add rate-limited group 0, add service ports 100, 101, and 102 of the user to rate-limited group 0, and use traffic profile 30 to control traffic of rate-limited group 0. In the case that any two services carry no traffic, the third service can hold a burst of the total user bandwidth. To perform such a configuration with the following parameters, do as follows:

- Service port 100 of the Internet access service uses traffic profile 10, with the CIR 2 Mbit/s and the 802.1p priority 4.
- Service port 101 of the VoIP service uses traffic profile 11, with the CIR 1 Mbit/s and the 802.1p priority 6.
- Service port 102 of the IPTV service uses traffic profile 12, with the packet rate not limited and the 802.1p priority 5.

```
huawei(config)#traffic table ip index 10 cir 2048 pir 10240 priority 4 priority-policy local-Setting
huawei(config)#service-port 100 vlan 2 gpon 0/2/1 ont 1 gempport 4 multi-service user-vlan 20 rx-cttr
10 tx-cttr 10
huawei(config)#traffic table ip index 11 cir 1024 pir 10240 priority 6 priority-policy local-Setting
huawei(config)#service-port 101 vlan 2 gpon 0/2/1 ont 1 gempport 5 multi-service user-vlan 30 rx-cttr
11 tx-cttr 11
huawei(config)#traffic table ip index 12 cir off priority 5 priority-policy local-Setting
huawei(config)#service-port 102 vlan 2 gpon 0/2/1 ont 1 gempport 6 multi-service user-vlan 40 rx-cttr
12 tx-cttr 12
huawei(config)#traffic table ip index 30 cir 10240 pir 10240 priority 3 priority-policy local-Setting
huawei(config)#car-group 0 inbound traffic-table index 30 outbound traffic-table index 10
huawei(config)#car-group 0 add-member service-port 100-102
huawei(config)#display car-group 0
```

Command:

```
display car-group 0
```

GroupID	Member List	RX	TX
0	10	30	

Note: S--Source of connection-oriented flow,
D--Destination of connection-oriented flow

15.7.5.4 Configuring Rate Limitation Based on Port+VLAN

After configuring rate limitation based on port+VLAN, you can specify different IP traffic profiles for different VLAN packets carried on the same port.

Prerequisites

- A proper IP traffic profile must be created and the index of the IP traffic profile to be used must be confirmed. For details about the configuration method, see [15.7.5.1 Configuring Rate Limitation Based on Service Port](#).
- Currently, only the ETH board supports rate limitation based on port+VLAN.

Procedure

- Step 1** In the global config mode, run the **interface eth** command to enter the ETH mode.
- Step 2** Run the **car-port portid vlan** command to configure rate limitation based on port+VLAN.

This command can be used to configure IP traffic profiles for the packets in the specified VLAN range on the specified port, implementing inbound and outbound rate limitation.

----End

Example

To configure port 0 on the ETH board in slot 0/9/0, and use traffic profile 6 for controlling the packets with VLAN 10, do as follows:

```
huawei(config)#display traffic table ip index 6
-----
Traffic Table Index      : 6
Traffic Table Name       : ip-traffic-table_6
Specified Outer-Priority : 0
Outer-Priority Mapping Source: -
Outer-Priority Mapping Index: -
Default Outer-Priority   : -
Specified Inner-Priority : 0
Inner-Priority Mapping Source: -
Inner-Priority Mapping Index: -
Default Inner-Priority   : -
Specified DSCP           : -
DSCP Mapping Source      : -
DSCP Mapping Index       : -
CIR                      : off
CBS                      : off
PIR                      : off
PBS                      : off
Fix                      : off
CAR Threshold Profile    : -
Color Mode               : color-blind
Coupling Flag            : enable
Rate Profile Index       : -
Rate Profile Name        : -
Color Policy             : dei
Color DEI                : unmark-dei
Color Source             : outer-dei
Drop Precedence          : remarked-outer-priority
Priority Policy           : tag-pri
Que-Policy Profile ID    : -
Pri-Group Profile ID     : -
Pri-Group Profile Name   : -
Referenced Status        : not used
E2E Mapping Priority     : -
E2E Mapping Index       : -
E2E Default Priority     : -
Yellow WRR Weight        : auto
```

```
Green WRR Weight      : auto
-----
huawei(config)#interface eth 0/9
huawei(config-if-eth-0/9)#car-port 0 vlan 10 inbound 6 outbound 6
```

15.7.5.5 Configuring GPON Rate Limitation

This topic describes how to configure rate limitation for GPON services, thereby providing differentiated quality of service (QoS) for various GPON services.

Context

- There are multiple methods of rate-limiting GPON services, for example, rate-limiting downstream traffic by using an IP traffic profile and ACL rules, rate-limiting the ONT upstream bandwidth by using a DBA profile, and rate-limiting the GEM port and GEM port traffic on an ONT.
- Rate limitation on GPON services can be performed on the OLT and the ONT concurrently. If more than one rate limitation modes are configured in the system, the minimum rate prevails.
- Which method of rate-limiting the ONT upstream bandwidth is used depends on the ONT capability. Specifically, if an ONT supports various rate limitation methods and the ONT upstream traffic is small (for example, FTTH service), a DBA profile is a best choice to rate-limit the ONT upstream traffic. If a T-CONT carries upstream traffic for multiple users (for example, FTTB/FTTC service), rate limitation on GEM port is generally used to prevent a user from occupying bandwidth for a long time. If the priority of user packets is trustworthy (for example, an enterprise user), priority queue (PQ) scheduling is generally used.

Procedure

- Perform rate limitation on the OLT.
 - Rate limitation using an IP traffic profile includes two modes. For details, see [Configuring Traffic Management Based on Service Port](#), and [Configuring Traffic Management Based on Port+CoS](#).
 - Performing rate limitation by configuring an ACL rule can control the traffic matching the ACL rule. For details, see [Controlling the Traffic Matching an ACL Rule](#).
- Perform rate limitation on the ONT.
 - a. Run the **dba-profile add** command to add a DBA profile. The DBA profile is used to schedule the ONT upstream bandwidth properly, achieving the best bandwidth utilization.

A DBA profile supports five types (Type1 to Type5). Generally, services with higher priorities adopt Type1 or Type2 DBA profiles and services with lower priorities adopt Type3 or Type4 profiles. [Table 15-7](#) shows the features of the DBA profile of each type.

Table 15-7 The features of the DBA profile

Profile Type	Features
Type1	Indicates the fixed bandwidth. After the DBA profile of Type1 is bound, the system assigns a specified bandwidth, regardless of whether there is upstream traffic.
Type2	Indicates the assured bandwidth. After the DBA profile of Type2 is bound, the system meets the bandwidth requirements if the upstream traffic does not exceed a specified value. When there is no upstream traffic, the system does not assign any bandwidth.
Type3	Indicates the hybrid of assured bandwidth and non-assured bandwidth. The DBA profile of Type3 specifies an assured value and non-assured value. After assigning the fixed bandwidth and assured bandwidth, the system assigns the remaining bandwidth (if any) to the user bound with the DBA profile of Type3 (the assigned bandwidth does not exceed the non-assured bandwidth).
Type4	Indicates the best-effort bandwidth. The DBA profile of Type4 just specifies a maximum value. After the DBA profile of Type4 is bound, its priority for obtaining the bandwidth is the lowest. That is, after assigning the fixed bandwidth, assured bandwidth, and non-assured bandwidth, the system assigns the remaining bandwidth (if any) to the user bound with the DBA profile of Type4 (the assigned bandwidth does not exceed the maximum value).
Type5	Indicates the hybrid bandwidth. The preceding four types of values need to be specified.

- b. Run the **ont-lineprofile gpon** command to add a GPON ONT line profile, and then enter the GPON ONT line profile mode.
- c. Run the **tcont** command to bind a T-CONT to the DBA profile.

It is recommended that one service type use one T-CONT and different T-CONTs be planned with different bandwidth assurance types.

- d. Run the **qos-mode** command to configure a QoS mode of the GPON ONT line profile to ensure that the QoS mode is the same as that of the GEM port.

By default, the QoS mode of the GPON ONT line profile (that is, the ONT scheduling mode) is priority queue (PQ). The QoS mode includes:

- **gem-car**: Indicates the rate limitation mode based on the GEM port of the T-CONT. Rate limitation is performed on a specified GEM port in the ONT upstream direction. To select the gem-car mode, set **gem add** to **gem-car**. The maximum traffic is determined by the DBA profile bound to the GEM port. If a T-CONT contains multiple GEM

ports, the scheduling mechanism of packets between multiple GEM ports depends on the default scheduling mechanism of the ONT.

- **flow-car**: Indicates the rate limitation mode based on traffic streams of a GEM port. Rate limitation is performed on a specified traffic stream in the ONT upstream direction. To select the flow-car mode, set **gem mapping** to **flow-car**. The maximum traffic is determined by the DBA profile bound to the traffic stream. Flow-car is more specific than gem-car. After rate limitation based on traffic streams is performed, traffic is scheduled in the T-CONT queue. The scheduling mechanism depends on the default scheduling mechanism of the ONT. Before configuring flow-car, make sure that the required traffic profile is created by running the **traffic table ip** command.

NOTE

The traffic stream in this topic refers to the service channel between an ONT and OLT. It is different the service port created by running the **service-port** command.

- **priority-queue**: Indicates the PQ mode based on the GEM port of the T-CONT. Traffic is scheduled based on PQ between multiple GEM ports in the ONT upstream direction. To select priority-queue mode, set **gem add** to **priority-queue**. By default, the system supports eight (0–7) queues. Queue 7 has the highest priority and services of queue 7 are preferentially scheduled. The maximum traffic is determined by the DBA profile to which the T-CONT is bound.
- e. Run the **commit** command to make the profile configuration take effect. The configuration of the line profile takes effect only after you run this command.

----End

Example

Assume that:

- A user under ONT 1 connected to GPON port 0/2/1 requires 2 Mbit/s high-speed Internet access service.
- The priority of user packets is trustworthy. The PQ scheduling mechanism is used, with priority 1.
- The default IP traffic profile, namely IP traffic profile 5 is used for rate limitation on a GPON port, with CIR of 2048 Kbit/s.
- DBA profile 10 of Type4 is used and the maximum bandwidth in the ONT upstream direction is 100 Mbit/s.

To perform the preceding configurations, do as follows:

```
huawei(config)#dba-profile add profile-id 10 type4 max 102400
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 10
huawei(config-gpon-lineprofile-5)#qos-mode Priority-queue
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 1 priority-queue 1
huawei(config-gpon-lineprofile-5)#mapping-mode vlan
huawei(config-gpon-lineprofile-5)#gem mapping 1 2 vlan 10
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
huawei(config)#interface gpon 0/2
```

```
huawei(config-if-gpon-0/2)#ont confirm 1 ontid 1 sn-auth 32303131B39FD641 snmp ont-lineprofile-id 5
huawei(config-if-gpon-0/2)#quit
huawei(config)#service-port 101 vlan 100 gpon 0/2/1 ont 1 gempport 1 rx-cttr 5 tx-cttr 5
```

15.7.5.6 Configuring Rate Limiting Based on Priority Group

By configuring rate limiting based on priority group, you can specify different IP traffic profiles for 802.1p groups over a service flow.

Procedure

- Step 1** In global config mode, run the **rate profile** command to create a rate profile.
- Step 2** In rate profile mode, run the **cir** command to configure rate limiting parameters and then exit rate profile mode.
- Step 3** In global config mode, run the **priority-group profile** command to enter priority group profile mode and create a priority group profile.
- Step 4** In priority group profile mode, run the **priority-source(priority-group profile)** and **car-group(priority-group profile)** commands to configure the source of the priority group and specify the priority group rate profile.
- Step 5** Run the **traffic table ip** command to bind the priority group profile.

----End

Example

To create 2 priority groups by using the outer priority of packets and rate profile 1 for rate limiting, do as follows:

```
huawei(config)#rate profile
huawei(config-rate-profile-1)#cir 64
huawei(config-rate-profile-1)#quit
huawei(config)#priority-group profile
huawei(config-priority-group-profile-1)#priority-source outer-8021p cos-group-table 2 0
huawei(config-priority-group-profile-1)#car-group 0 rate profile profile-id 1
huawei(config-priority-group-profile-1)#car-group 1 rate profile profile-id 1
huawei(config-priority-group-profile-1)#quit
huawei(config)#traffic table ip index 1000 rate profile profile-id 1 priority user-cos mapping-profile 0 0 priority-policy local-Setting priority-group profile profile-id 1
```

Create traffic descriptor record successfully

```
-----
Traffic Table Index      : 1000
Traffic Table Name      : ip-traffic-table_1000
Specified Outer-Priority : -
Outer-Priority Mapping Source: user-cos
Outer-Priority Mapping Index : 0
Default Outer-Priority   : 0
Specified Inner-Priority  : -
Inner-Priority Mapping Source: -
Inner-Priority Mapping Index : -
Default Inner-Priority    : -
Specified DSCP           : -
DSCP Mapping Source      : -
DSCP Mapping Index       : -
CIR                      : -
CBS                      : -
PIR                      : -
PBS                      : -
```

```
Fix : -
CAR Threshold Profile : -
Color Mode : -
Coupling Flag : -
Rate Profile Index : 1
Rate Profile Name : rate-profile_1
Color Policy : dei
Color DEI : unmark-dei
Color Source : outer-dei
Drop Precedence : remarked-outer-priority
Priority Policy : local-pri
Que-Policy Profile ID : -
Pri-Group Profile ID : 1
Pri-Group Profile Name : priority-group-profile_1
Referenced Status : not used
E2E Mapping Priority : -
E2E Mapping Index : -
E2E Default Priority : -
Yellow WRR Weight : auto
Green WRR Weight : auto
-----
```

15.8 Traffic Shaping

15.8.1 Introduction to Traffic Shaping

Definition

Traffic shaping is to shape irregular traffic or traffic that does not comply with preset traffic features to realize bandwidth matching between upstream and downstream networks.

Purpose

Control network traffic and prevent traffic bursts so that packets are transmitted at an even rate.

15.8.2 Basic Concepts of Traffic Shaping

Traffic shaping is generally implemented by using a buffer and a token bucket. When the network traffic is heavy, packets are first stored in the buffer, and then the buffered packets are sent at a specified rate through the token bucket.

Table 15-8 Basic concepts

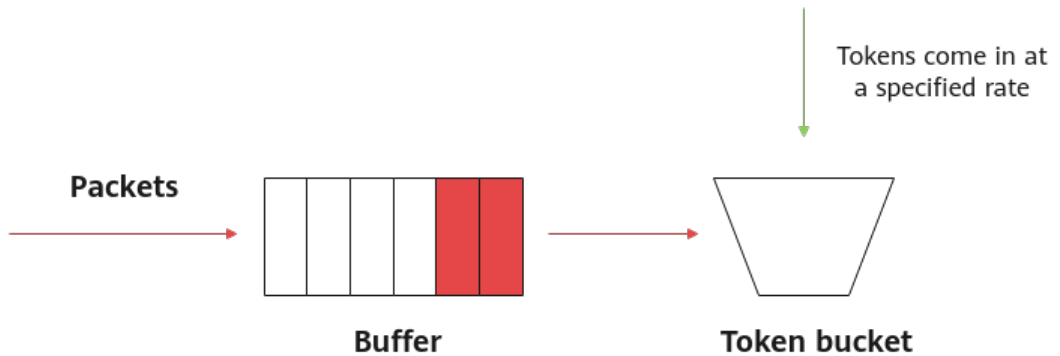
Concept	Description
Buffer	A buffer is a space used to store packets. When tokens in the egress token bucket are used up, packets are stored in the buffer. Packets are discarded only when the buffer is full.

Concept	Description
Token bucket	A token bucket is a container that stores tokens and is used to control data traffic. A token bucket allows burst data transmission while controlling the traffic. There are two types of token buckets: single bucket and dual buckets. Principle: A packet is transmitted only when there is a token of the equivalent size in the token bucket. After a packet is transmitted, the number of tokens of the equivalent size in the bucket decreases accordingly.

15.8.3 Traffic Shaping Implementation

This section describes the buffer function in traffic shaping. For token bucket principles, see [15.7.3 Implementation Principle: CAR](#).

Figure 15-27 Traffic shaping implementation



Tokens are put into a token bucket at a specified rate. Packets can be transmitted only after obtaining tokens. When there is no token in the token bucket, the packets are not discarded. Instead, the packets are stored in the buffer and wait until there are tokens in the token bucket. Then, the buffered packets are sent. When the buffer is full, packets cannot be sent or stored in the buffer. In this case, packets are discarded.

Differences Between Traffic Shaping and Traffic Policing

[Table 15-9](#) lists the differences between traffic shaping and traffic policing.

Table 15-9 Differences between traffic shaping and traffic policing

Traffic Policing	Traffic Shaping
Marks packets with priorities or discards packets in the case of burst traffic.	Stores packets in a buffer and discards packets only when the buffer is full in the case of burst traffic.

Traffic Policing	Traffic Shaping
No extra buffer space is required.	Extra buffer space is required.
The packet loss rate is high.	The packet loss rate is reduced, but the latency is increased.
Jitter occurs during TCP rate limiting.	There is no jitter in TCP rate limiting.

15.8.4 Configuring Traffic Shaping

In traffic limiting scenarios, you can configure traffic shaping to reduce the packet loss rate and ensure that the traffic is even and stable.

15.8.4.1 Configuring a Rate Limit for an ONT

Traffic shaping can be used to limit the downstream traffic of an ONT.

Procedure

- Step 1** Run the **traffic-limit ont** command to use an IP traffic profile to limit the traffic of downstream packets on an ONT. After this command is executed successfully, the traffic of downstream packets on the ONT is limited by traffic shaping. The packets that exceed the traffic limit are buffered to reduce packet loss.

NOTE

- You can select an IP traffic profile by name or SN.
- You can run the **display traffic table ip** command to query the IP traffic profiles in the system.
- You can run the **traffic table ip** command to create a new IP traffic profile.

- Step 2** Run the **display traffic-limit ont** command to query the traffic limit information of the ONT. If the configured traffic limit is displayed, the configuration is successful.

----End

Example

To use IP traffic profile 6 to limit the traffic of downstream packets on ONT 1 connected to port 0/3/0, do as follows:

```
huawei(config)#traffic-limit ont
{ frameid/slotid/portid<S><Length 5-18> }:0/3/0
{ ontid<U><0,127> }:1
{ down-stream<K> }:down-stream
{ traffic-table<K> }:traffic-table
{ index<K>|name<K> }:index
{ index<U><0,1023> }:6
```

Command:

```
traffic-limit ont 0/3/0 1 down-stream traffic-table name ontraffictable
```

```
huawei(config)#display traffic-limit ont 0/3/0 1
```

F/ S/ P	ONT ID	DownTrafficProfile
0/ 3/ 0	1	6

15.8.4.2 Configure Queue-based Traffic Shaping for an ONT

Traffic shaping can be configured for ONT queue groups or queues to ensure even and stable egress traffic.

Procedure

Step 1 Run the **queue-shaping** command to configure traffic shaping and specify an IP traffic profile.

NOTE

- An IP traffic profile can be specified only by SN.
- You can run the **display traffic table ip** command to query the IP traffic profiles in the system.
- You can run the **traffic table ip** command to create a new IP traffic profile.

Step 2 Run the **display queue-shaping** command to check the traffic shaping configuration. If the configured information is displayed, the configuration is successful.

----End

Example

To configure traffic shaping for queue 1 on port 0/3/0 and specify IP traffic profile 15, do as follows:

NOTE

- The command formats for Ethernet access, xDSL access, and GPON access are slightly different. The following uses Ethernet access as an example.
- You can run this command to configure traffic shaping for a queue group and a queue. If **queue** is specified, traffic shaping is configured for a queue group. If **queue-list** is specified, traffic shaping is configured for a specified queue.

```
huawei(config)#queue-shaping
{ frameid/slotid/portid<S><Length 5-18>|frameid/slotid<S><Length 3-15> }:0/3/0
{ ont<K>|queue<K>|queue-list<K> }:queue-list
{ queue-list<S><Length 1-16> }:1
{ outbound<K> }outbound { ip-traffic-table-index<U><0,1023> }:15
```

Command:
queue-shaping 0/3/0 queue-list 1 outbound 15

```
huawei#display queue-shaping 0/3/0
```

F / S / P	QUEUE-ID1	QUEUE-ID2	OUTBOUND-INDEX	CIR	CBS
0 / 3 / 0	3	4	15	6400	12800

15.8.4.3 Configuring Rate Limit for an Ethernet Port

The traffic of a specified Ethernet port can be limited by traffic shaping. In traffic shaping mode, the packets exceeding the preset traffic limit are first stored in a buffer instead of directly discarded.

Procedure

- Step 1** Run the **line-rate** command to configure the maximum rate in the inbound or outbound direction of a port.

 NOTE

When **inbound** is specified for a port, the traffic shaping mode is used by default to limit the rate and buffer packets. If **inbound CAR** is specified, the port directly discards the packets that exceed the traffic limit.

- Step 2** Run the **display qos-info** command to check the port configurations. If the configured information is displayed, the configuration is successful.

----End

Example

To limit the maximum rate of the inbound traffic transmitted from the user side to the network side on port 0/3/0 to 64 kbit/s, do as follows:

```
huawei(config)#line-rate
{ inbound<K>|integer<U><64,100000000>|outbound<K> }:inbound
{ car<K>|integer<U><64,100000000> }:64
{ port<K> }:port { frameid/slotid/portid<S><Length 5-18> }:0/3/0
```

Command:
line-rate inbound 64 port 0/3/0

```
huawei#display qos-info line-rate port 0/3/0
line-rate:
port 0/3/0:
Inbound:
line rate: 64Kbps
Outbound:
line rate: 128Kbps
```

15.9 Congestion avoidance

15.9.1 Introduction to Congestion avoidance

Definition

Congestion avoidance refers to a traffic control mechanism that monitors the utilization of network resources (such as queues or buffers), and drops packets to adjust the network traffic when congestion occurs, avoiding traffic overload on the network.

Congestion avoidance solves the issue of how to place packets in queue and how to drop packets.

Purpose

It uses some algorithms to avoid worse congestion and utilizes network bandwidth.

15.9.2 Basic Concepts of Congestion avoidance

Congestion avoidance is implemented using packet drop algorithms. The MA5800 supports the following drop algorithms:

- Tail drop
- Priority-based early drop
- Color-based early drop
- Weighted random early discard (WRED)

Table 15-10 Basic concepts

Concept	Description	Effective Time
Tail drop	When a port queue is fully filled (to its maximum depth), the newly arriving packets are dropped until the queue has enough space to accept incoming traffic. Tail drop cannot ensure effective transmission of important data streams.	When the port queue is fully filled
Priority-based early drop	Packets with different priorities can be configured with different drop thresholds. Specifically, packets with higher priorities are configured with higher drop thresholds, while packets with lower priorities are configured with lower drop thresholds. When traffic congestion occurs on a port but the port queue is not fully filled, packets with higher priorities can enter queues that have a greater depth and are more burst-tolerant. In this way, these packets are less likely to be dropped. While packets with lower priorities are dropped preferentially because of the smaller queue depth.	When the port queue is partially filled
Color-based early drop	The system assigns different drop thresholds to different packets by marking the packets with different colors (yellow, green, or red; red packets are dropped directly) using the two rate three-color marker (trTCM) algorithm. In this way, when traffic congestion occurs on a port but the port queue is not fully filled, packets that do not exceed CIR (such packets are marked green) and packets that exceed CIR but do not exceed PIR (such packets are marked yellow) are forwarded; packets that exceed PIR (such packets are marked red) are dropped.	When the port queue is partially filled

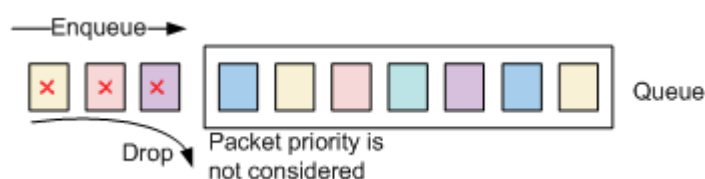
Concept	Description	Effective Time
WRED	Based on RED, WRED uses classification marks such as IP precedence, DSCP value, and MPLS EXP to differentiate drop policies. WRED effectively improves the quality of services with higher priorities.	When the port queue is partially filled

15.9.3 Implementation Principle

Tail Drop

When a port queue is fully filled (to its maximum depth), the newly arriving packets are dropped until the queue has enough space to accept incoming traffic, as shown in [Figure 15-28](#).

Figure 15-28 Tail drop



Tail drop applies to all queues and cannot be manually configured.

Priority-based Early Drop

Packets with different priorities can be configured with different drop thresholds. Specifically, packets with higher priorities are configured with higher drop thresholds, while packets with lower priorities are configured with lower drop thresholds. When traffic congestion occurs on a port but the port queue is not fully filled, packets with higher priorities can enter queues that have a greater depth and are more burst-tolerant. In this way, these packets are less likely to be dropped. While packets with lower priorities are dropped preferentially because of the smaller queue depth.

Priority-based early drop applies to scenarios in which packets with different priorities enter the same queue.

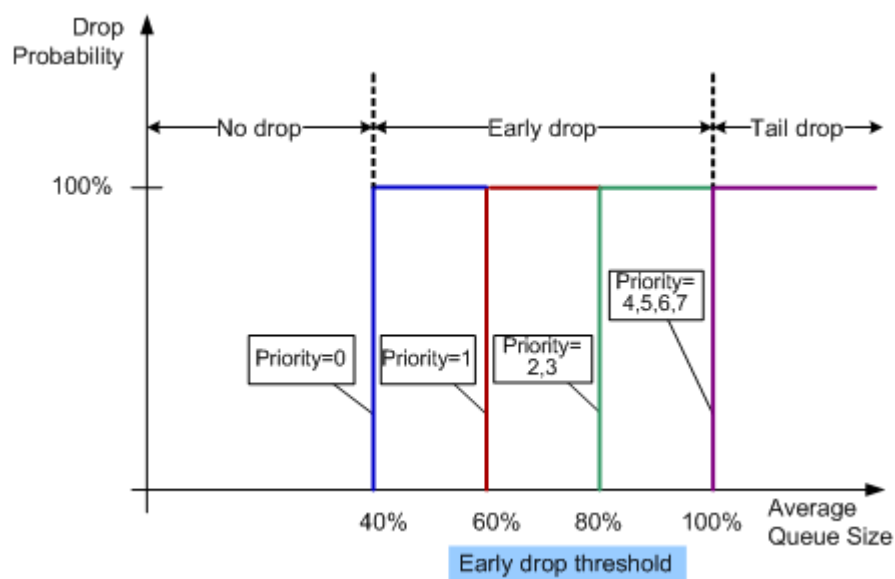
The **early-drop** command can be used to configure the early drop thresholds for packets of different priorities.

As shown in [Figure 15-29](#), assume that packets with different priorities enter the same queue, the early drop thresholds are set to 40% and 60% for 0-priority and 1-priority packets, respectively, to 80% for 2-priority and 3-priority packets, and to 100% for 4-, 5-, 6-, and 7-priority packets.

- When the packets in the queue are less than 40% of the queue depth, all subsequent packets with different priorities can be enqueued.

- When packets in the queue increase to or exceed 40% of the queue depth, subsequent 0-priority packets are dropped while packets with higher priorities are enqueued.
- When packets in the queue increase to or exceed 60% of the queue depth, subsequent 1-priority packets are also dropped while packets with higher priorities (except 0 and 1) are enqueued.
- When packets in the queue increase to or exceed 80% of the queue depth, subsequent 2-priority and 3-priority packets are also dropped, while packets with higher priorities (4, 5, 6, and 7) are enqueued.
- When packets in the queue increase to 100% of the queue depth, tail drop occurs. In this case, all subsequent packets are dropped.

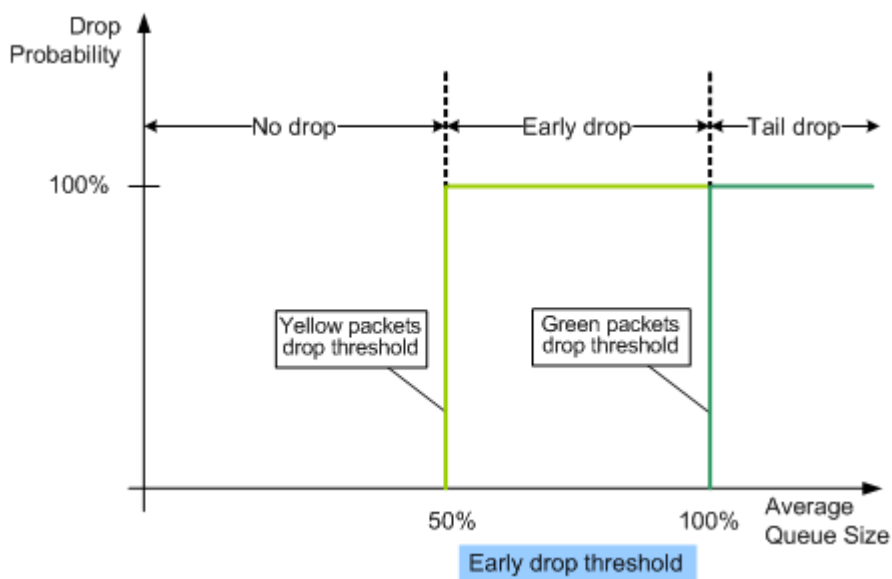
Figure 15-29 Priority-based early drop



Color-based Early Drop

The system assigns different drop thresholds to different packets by marking the packets with different colors (yellow, green, or red; red packets are dropped directly) using the two rate three-color marker (trTCM) algorithm. In this way, when traffic congestion occurs on a port but the port queue is not fully filled, packets that do not exceed CIR (such packets are marked green) and packets that exceed CIR but do not exceed PIR (such packets are marked yellow) are forwarded; packets that exceed PIR (such packets are marked red) are dropped.

As shown in [Figure 15-30](#), the drop threshold is 50% for yellow packets and 100% for green packets. The drop thresholds cannot be modified manually. If more than 50% of a queue is occupied, subsequent yellow packets cannot enter the queue but green packets can. When the queue is 100% occupied, green packets are also dropped.

Figure 15-30 Color-based early drop

In addition, users can run the **early-drop color yellow** command to set the drop threshold for yellow packets with different priorities. Early drop for yellow packets is implemented in a similar way to priority-based early drop shown in [Figure 15-29](#). The difference is that the former applies only to yellow packets with different priorities.

Color-based Early Drop - Weighted Random Early Discard (WRED)

The system assigns different drop thresholds to different packets by marking the packets with different colors (yellow, green, or red; red packets are dropped directly) using the trTCM algorithm. In this way, when traffic congestion occurs on a port but the port queue is not fully filled, packets that do not exceed CIR (such packets are marked green) and packets that exceed CIR but do not exceed PIR (such packets are marked yellow) are forwarded; packets that exceed PIR (such packets are marked red) are dropped.

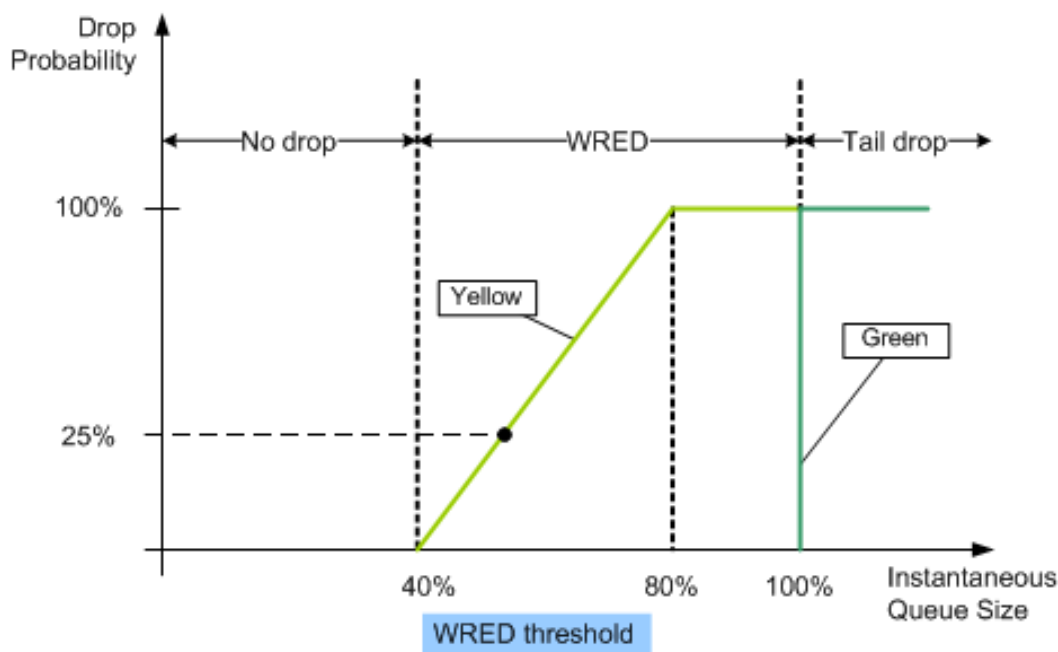
The **wred-profile** command can be used to set the low drop limit (**low-limit**) and high drop limit (**high-limit**) for yellow and green packets, and the drop probability (**discard-probability**) for red packets.

The drop probability at a specific time point derives from the following formula:
Packet drop probability = (Usage of the packet buffer area - Low drop limit) ÷ (High drop limit - Low drop limit) × Drop probability of the packets reaching the high drop limit.

As shown in [Figure 15-31](#), run the **wred-profile** command to specify the low drop limit to 40%, high drop limit to 80%, and drop probability to 100% for yellow packets, and no drop for green packets.

- When yellow packets in the queue are less than 40% of the queue depth, all subsequent yellow and green packets are enqueued.
- When yellow packets in the queue increase to or exceed 40% of the queue depth, all subsequent green packets are enqueued while subsequent yellow packets are dropped based on the drop probability specified for this time point (for example, 25%).

- When yellow packets in the queue increase to or exceed 80% of the queue depth, all subsequent yellow packets are directly dropped, while all subsequent green packets are enqueued.
- When packets in the queue increase to 100% of the queue depth (the queue is fully filled), tail drop occurs. In this case, all subsequent packets are dropped.

Figure 15-31 Color-based early drop - WRED**NOTE**

In the figure above, the yellow line represents the drop probability curve.

15.9.4 Configuring the Congestion Avoidance

Context

- Congestion avoidance is implemented using packet drop algorithms, which include tail drop, priority-based early drop, and color-based weighted random early detection (WRED) early drop.
- The MA5800 can differentiate the services with different priorities in the same queue. The packet priority serves as a criterion for dropping packets.
- The MA5800 can also implement early drop based on the color of packets. When congestion occurs, the yellow packets are dropped.

Procedure

- Configure priority-based early drop.
 - a. Configure the early drop mode.

Run the **early-drop mode pri-base** command to configure the priority-based early drop. After the configuration is completed, the system performs early drop according to the outer 802.1p priorities of the

packets. When congestion occurs in a queue, the packets are dropped according to the early drop thresholds of the priorities.

- b. Configure the early drop threshold.

Run the **early-drop** command to configure the mapping between service priorities and drop thresholds. After configuration is successful, if the packets of the specified service priority reach the threshold of the queue (the percentage of the queue depth), subsequent packets of the same service priority will be dropped instead of entering the queue.

- c. Query the configured early drop threshold.

Run the **display early-drop** command to query the configured early drop threshold.

- Configure color-based early drop.

- a. Configure the early drop mode.

Run the **early-drop mode color-base** command to configure the color-based early drop.

According to the *CIR* and *PIR* parameters in the IP traffic profile, the system marks packets with colors. The packets within the CIR bandwidth are marked as green, and the packets between the CIR and PIR bandwidth are marked as yellow.

After the configuration is completed, green packets are allowed to pass, yellow packets that do not exceed the bandwidth can also pass, and yellow packets that exceed the bandwidth are dropped.

- b. (Optional) Configure the early drop threshold of yellow packets.

Run the **early-drop color yellow** command to configure the mapping between service priorities of yellow packets and drop thresholds. After the configuration is successful, if the yellow packets of the specified service priority reach the threshold of the queue (the percentage of the queue depth), subsequent yellow packets will be discarded instead of entering the queue.

- c. Query the configured early drop threshold.

Run the **display early-drop** command to query the configured early drop threshold.

- Configure color-based WRED early drop.

- a. Configure the early drop mode.

Run the **early-drop mode color-wred** command to configure the color-based WRED early drop.

In this mode, a WRED profile can bind to a packet queue. Then the packet color-based early-discard can be implemented according to the parameter settings in the WRED profile

- b. Set a WRED profile.

Run the **wred-profile** command to set the early discard threshold and discard ratio of the green or yellow packet.

- c. Bind the packet queue to the WRED profile.

Run the **queue-wred** command to bind the packet queue to the WRED profile. After the WRED profile is bound, the color-based early discard is performed for packets according to the parameters in the WRED profile.

----End

Example

To configure the priority-based early drop, where,

- The early drop thresholds are set to 40% and 60% for 0-priority and 1-priority packets.
- The early drop thresholds are set to 80% for 2-priority and 3-priority packets.
- The early drop thresholds are set to 100% for 4-, 5-, 6-, and 7-priority packets.

Do as follows.

```
huawei(config)#early-drop mode pri-base
huawei(config)#early-drop cos0 40 cos1 60 cos2 80 cos3 80
{ <cr>|cos4<K>|cos5<K>|cos6<K>|cos7<K> }:
```

Command:

```
early-drop cos0 40 cos1 60 cos2 80 cos3 80
huawei(config)#display early-drop
{ <cr>|color<K>|mode<K>|pri-base<K>||<K> }:
```

Command:

```
display early-drop
Early-drop is pri-base
Pri-base early-drop config:
```

Priority	Threshold
0	40
1	60
2	80
3	80
4	100
5	100
6	100
7	100

Color-base early-drop config:

Queue ID	WRED Profile Index
0	-
1	-
2	-
3	-
4	-
5	-
6	-
7	-

Pri-base early-drop mapping:

Priority	Queue ID	Mapping Class
0	0	0
1	1	0
2	2	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

To configure the color-based early drop, where,

- The early drop thresholds are set to 40% and 60% for 0-priority and 1-priority packets.
- The early drop thresholds are set to 80% for 2-priority and 3-priority packets.
- The early drop thresholds are set to 100% for 4-, 5-, 6-, and 7-priority packets.

Do as follows.

```
huawei(config)#early-drop mode color-base
huawei(config)#early-drop color yellow cos0 40 cos1 60 cos2 80 cos3 80 cos4 100 cos5 100 cos6 100
cos7 100
huawei(config)#display early-drop color yellow
{ <cr>||<K> }:
Command:
    display early-drop color yellow
Color-base early-drop config:
-----
Queue ID   Yellow Packet Threshold
-----
0           40
1           60
2           80
3           80
4           100
5           100
6           100
7           100
-----
```

To configure the color-based WRED early drop, where,

- All packet queues are bound to WRED profile 0.
- Green packets are not discarded; for yellow packets, the upper discard threshold is 80, that is, all yellow packets are discarded when the usage of the packet buffer exceeds 80%.

Do as follows.

```
huawei(config)#early-drop mode color-wred
huawei(config)#wred-profile index 0 green low-limit 100 high-limit 100 discard-probability 0 yellow
low-limit 80 high-limit 80 discard-probability 100
Command:
    wred-profile index 0 green low-limit 100 high-limit 100 discard-probab
ity 0 yellow low-limit 80 high-limit 80 discard-probability 100
huawei(config)#queue-wred queue0 0 queue1 0
queue2 0 queue3 0 queue4 0 queue5 0 queue6 0 queue7 0
Command:
    queue-wred queue0 0 queue1 0 queue2 0 queue3 0 queue4 0 queue5 0 queue
6 0 queue7 0
huawei(config)#display early-drop
{ <cr>|color<K>|mode<K>|pri-base<K>||<K> }:
Command:
    display early-drop
Early-drop is color-wred
Pri-base early-drop config:
-----
Priority    Threshold
-----
0           40
1           60
2           80
3           80
4           100
5           100
6           100
7           100
-----
```

Color-base early-drop config:

Queue ID	WRED Profile Index
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Pri-base early-drop mapping:

Priority	Queue ID	Mapping Class
0	0	0
1	1	0
2	2	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

15.10 Congestion Management

15.10.1 Introduction to Congestion Management

Definition

If packets arrive faster than they are forwarded on a port, traffic congestion occurs on the port. Congestion management is used to manage and control traffic congestion.

Congestion management is implemented using queuing techniques for transmitting packets out of a queue.

Purpose

When traffic congestion occurs on an outbound interface, a proper queue scheduling mechanism guarantees required QoS parameters (such as bandwidth, latency, and jitter) for a certain type of packets.

15.10.2 Basic Concepts of Congestion Management

Congestion management is implemented using queuing techniques. The MA5800 supports the following queuing techniques:

- Priority queuing (PQ)
- Deficit weighted round robin (DWRR)
- PQ+DWRR

The following table explains the basic concepts of congestion management.

Table 15-11 Basic concepts

Concept	Description	Remarks
PQ	In PQ, the strict priority scheduling algorithm is used. In this scheduling algorithm, eight priorities are defined. Packets with higher priorities are scheduled first.	Packets of important services are processed preferentially.
DWRR	In the Deficit WRR scheduling algorithm, packets are scheduled based on the assigned weights.	Specific QoS guarantees are provided for each queue.
PQ+DWRR	The combination of PQ+DWRR ensures that some of the packets with high priorities are scheduled first and the remaining packets are scheduled based on the specified weights.	This mechanism ensures effective transmission of services with high priorities. In the mean time, services with low priorities are scheduled in a timely manner when there is available bandwidth.
Enqueuing priority	The enqueuing priority of a packet determines the queue that the packet will enter.	There are several sources of the enqueuing priority for a packet and the priority value ranges from 0 to 7.
Queue buffering	The queue depth determines the queue's capability of processing burst packets. A larger buffering space means a better capability of processing burst packets and a lower chance to lose packets, but a larger delay in processing packets.	-

15.10.3 Implementation Principle of Congestion Management

The procedure before packets enter queues or when they are in queues is as follows:

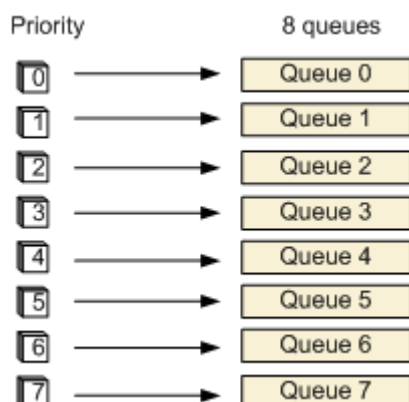
1. Traffic classification: For details, see the [implementation principle for traffic classification](#).
2. Enqueuing: Packets enter different queues based on the mapping between packet priorities and queues.
3. Scheduling: Schedules packets using a specific scheduling algorithm after the packets are enqueued.

Enqueuing

After priority processing, packets enter different queues based on the mapping between packet priorities and queues. By default, the mapping between packet priorities and queues is constant, as shown in [Figure 15-32](#).

The larger the queue ID, the higher the forwarding priority for packets in the queue. Among all the eight queues, queue 7 has the highest priority.

Figure 15-32 Default mapping between packet priorities and queues



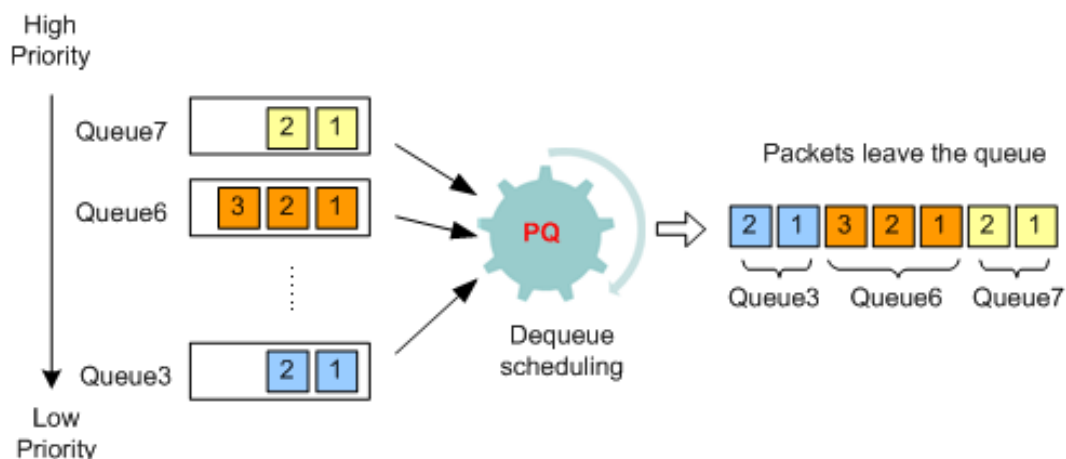
The system also supports a flexible mapping between packet priorities and queues. You can run the **cos-queue-map** command to map the 802.1p priority of the packet to any queue. That is, a queue can contain multiple 802.1p priorities or no 802.1p priorities.

The configuration of the mapping between packet priorities and queues takes effect globally. Generally, use the default value in the system and do not modify the parameters unless you have specific requirements.

Queue Scheduling: PQ

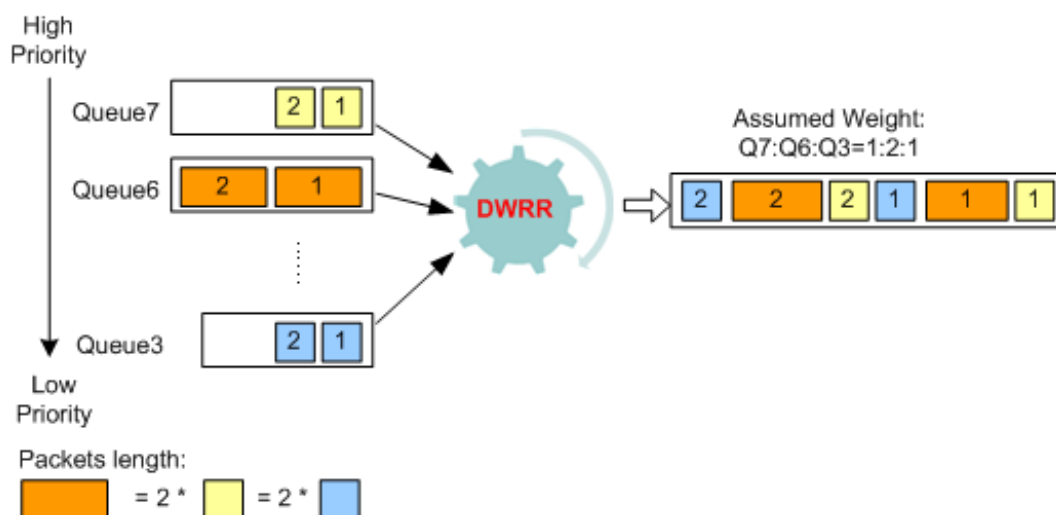
Priority queuing (PQ) queues are classified into high-priority queues, medium-priority queues, normal-priority queues, and low-priority queues in the descending priority order. As shown in [Figure 15-33](#), PQ allows the packets in a high-priority queue to exit the queue and be transmitted. After such a transmission is completed, PQ performs the same on all packets in a medium-priority queue, a normal-priority queue, and then a low-priority queue one by one.

In this way, packets in a queue with a higher priority precede packets in a queue with a lower priority and therefore are processed preferentially, even in case of congestion. This mechanism ensures that packets for critical services are processed first. Packets of non-critical services (such as email service) are processed only when the network has sufficient resources after critical services have been processed, thereby utilizing network resources efficiently.

Figure 15-33 PQ scheduling mechanism

Queue Scheduling: DWRR

Deficit weighted round robin (DWRR) is a weighted queue scheduling algorithm based on packet length in the unit of byte. DWRR schedules packets by byte. In DWRR, the quantum value indicates the bytes that can be scheduled in each round, and the deficit value indicates the total bytes that can be scheduled by each queue. If the deficit value of a queue is greater than the length of the packets located at the front end of the queue, these packets are scheduled and the length of these packets is subtracted from the deficit value. Packets in a queue can be scheduled if the deficit value is greater than or equal to 0. After packets are scheduled, the deficit value becomes negative. When the deficit value is greater than or equal to 0 again, packets can be scheduled, as shown in [Figure 15-34](#).

Figure 15-34 DWRR scheduling mechanism

DWRR scheduling prevents packets in low-priority queues from being starved out, that is, failing to be scheduled, and allows bandwidths to be allocated to packets

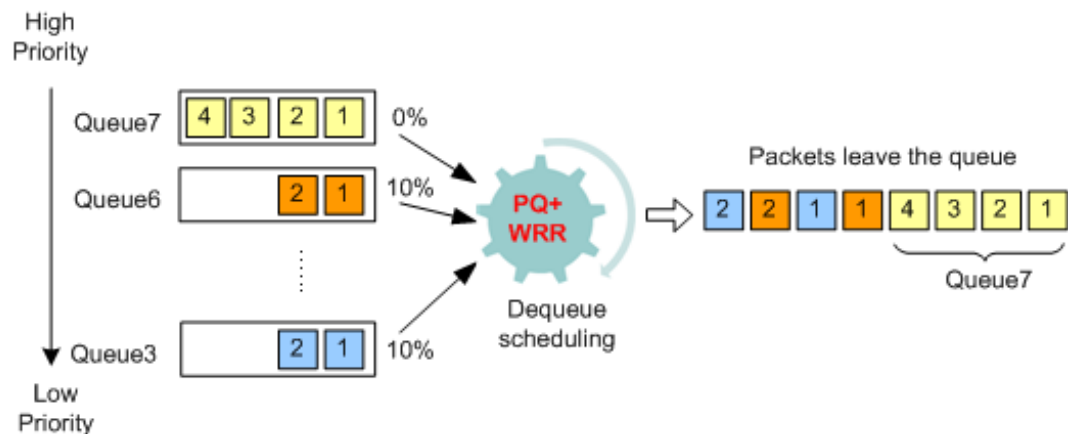
based on the weight ratio when the lengths of packets in different queues vary or change greatly.

Queue Scheduling: PQ+DWRR

PQ+DWRR is a combination of the PQ scheduling mode and DWRR scheduling mode. When the weight value of a queue is 0, the queue scheduling mode is PQ+DWRR. As shown in [Figure 15-35](#), in this mode, the system schedules the queues with the weight value 0 in the PQ mode, and then schedules other queues in the DWRR mode.

This scheduling mode is flexible. The services that must be guaranteed are scheduled in PQ mode, and the services with lower priorities are scheduled in DWRR mode when there is available bandwidth. In this way, services with higher priorities are ensured and those with lower priorities can obtain bandwidth whenever there is available bandwidth.

Figure 15-35 PQ+DWRR scheduling mechanism



15.10.4 Configuring the Congestion Management

Context

Congestion management contains the following content:

- Mapping between the queue and the 802.1p priority
- Queue depth
- Queue scheduling mode

And, the ultimate effect of the congestion management is determined by all of them.

Procedure

Step 1 Configure the mapping between the queue and the 802.1p priority.

The configuration of the mapping between priorities and queues takes effect globally. By default, 802.1p priorities and queues have a one-to-one mapping

relationship. Generally, use the default value in the system and do not customize the parameters unless you have specified requirements.

After the configuration, packets with different 802.1p priorities are mapped to the specified queues based on the configured mapping. This enhances the flexibility of mapping packets to queues.

1. Run the **cos-queue-map** command to configure the mapping between the 802.1p priority and the queue.
2. Run the **display cos-queue-map** command to query the mapping between the 802.1p priority and the queue.

Step 2 (Optional) Configure the queue depth.

By default, the queue depth of queue 0-7 is 13%, 6%, 13%, 13%, 12%, 12%, 25% and 6% respectively. Do not modify the value unless for special requirement.

Configure the queue depth (the queue buffer space) to re-allocate buffer space to the queues, therefore to improve the flexibility of QoS.

1. Run the **queue-buffer** command to set the buffer size percentage for packet queues of the service boards in the system.
2. Run the **display queue-buffer** command to query the buffer size percentage for queues of the service boards in the system.

Step 3 Configure the queue scheduling mode.

By default, the PQ mode is used. Properly set according to your actual requirements.

1. Run the **queue-scheduler** command to configure the queue scheduling mode.

NOTE

Range of *queue0-weight*: 0-100, 255, where 0 indicates that the strict PQ scheduling mode is used and 255 indicates that the queue is not used. The sum of the weight values of all queues must be 0 or 100.

2. Run the **display queue-scheduler** command to query the configuration of the queue scheduling mode.

----End

Example

Configure the queue scheduling mode to 3PQ+5DWRR. Where,

- Queues 5-7 adopt the PQ mode
- Queues 0-4 adopt the DWRR mode
- Queues 0-4 with the weights of 10, 30, 20, 20, and 20 respectively
- Other parameters use default settings

After that, packets with priority 5, 6, or 7 are scheduled in the PQ mode, and packets with other priority are scheduled in the DWRR mode.

```
huawei(config)#queue-scheduler wrr
{ queue0-weight<U><0,255> }:10
{ queue1-weight<U><0,255> }:30
{ queue2-weight<U><0,255> }:20
{ queue3-weight<U><0,255> }:20
```

```
{ queue4-weight<U><0,255> }:20
{ queue5-weight<U><0,255> }:0
{ queue6-weight<U><0,255> }:0
{ <cr>|queue7-weight<U><0,255> }:0
```

Command:

```
queue-scheduler wrr 10 30 20 20 20 0 0 0
```

huawei(config)#**display queue-scheduler**

Queue scheduler mode : WRR

Queue	Scheduler Mode	WRR Weight
0	WRR	10
1	WRR	30
2	WRR	20
3	WRR	20
4	WRR	20
5	PQ	--
6	PQ	--
7	PQ	--

15.11 ACL

Using the preset access control list (ACL) policy, the system permits or refuses data packets to pass.

15.11.1 Overview of ACL

Definition

The access control list (ACL) policy defines a series of matching rules, according to which the packets to be filtered are identified. The packets identified are permitted or refused to pass according to the preset rules.

ACL-based traffic filtering is a prerequisite for quality of service (QoS). ACL together with QoS improves system security.

Benefits

Mutual access between internal networks and communication between internal and external networks are primary requirements for enterprise networks. To ensure internal network security, a security policy is required to allow unauthorized users to access specified network resources so as to control access. With the ACL, network traffic can be filtered and network access is controlled.

After being bound to a QoS operation, the ACL helps to implement the following functions:

- Limiting network traffic and improving network performance
- Ensuring safe network access
- Determining which type of communication traffic to be forwarded or blocked on a port on the network device, such as a router or switch

Controlling packets on an access port when the ACL is used for packet-filtering ACL firewall, prohibiting unauthorized users from logging in to the system and ensuring device safety

15.11.2 Basic Concepts of ACL

ACL Type

The system supports IPv4 and IPv6 ACLs, that is, ACLv4 and ACLv6. ACLs include basic ACLs, advanced ACLs, link-layer ACLs, and user-defined ACLs.

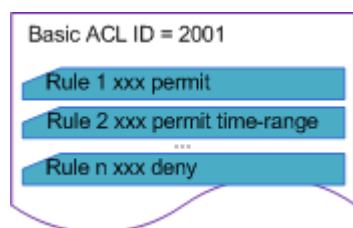
Table 15-12 ACL types

Type	Serial Number Range	Feature
Basic ACL	2000-2999	ACLv4: The rules of a basic ACL can be defined only according to the Layer 3 source IP address and the fragment field, for analyzing and processing data packets. ACLv6: The rules of a basic ACL can be defined only according to the Layer 3 source IP address and subnet prefix length, for analyzing and processing data packets.
Advanced ACL	3000-3999	Compared with a basic ACL, an advanced ACL allows for a wider scope of more accurate and flexible definition of the rules according to the following data packet information: • Source address • Destination address • IP bearer protocol types 0-255 (GRE, ICMP/ICMPv6, IP/IPv6, IPinIP, TCP, IPv6-ah, IPv6-esp, and OSPF) • TCP source port • TCP destination port • ICMP/ICMPv6 protocol type • ICMP/ICMPv6 code • Priority TOS/IP PRE/DSCP
Link-layer ACL	4000-4999	The rules of a link-layer ACL can be defined according to the following information: • Source MAC address • VLAN ID • Layer 2 protocol type • Destination MAC address • 802.1p priority

Type	Serial Number Range	Feature
User-defined ACL	5000-5999	The rules of a user-defined ACL can be defined according to any 32 bytes of the first 80 bytes in a Layer 2 frame. • IPoE matching: matches packets whose Ethernet packet header is IPv4-encapsulated, including untagged IP packets, one-tagged IP packets, and two-tagged IP packets. • Non-IPoE matching: matches IPv4 packets whose Ethernet packet header is not IP-encapsulated, that is non-IPoE IPv4 packets, including untagged, one-tagged, and two-tagged non-IPoE packets, or multi-tagged packets.

Rule

Rules are the main body of an ACL. An ACL can be composed of multiple rules, as shown in the following figure.



A rule has the following characteristics:

- Each rule belongs to an absolute ACL and is of the same type as the ACL.
- Each rule corresponds to a permit or deny action.
- Each rule can be configured with a time range in which the ACL takes effect.

15.11.3 ACL Rule Matching Sequence

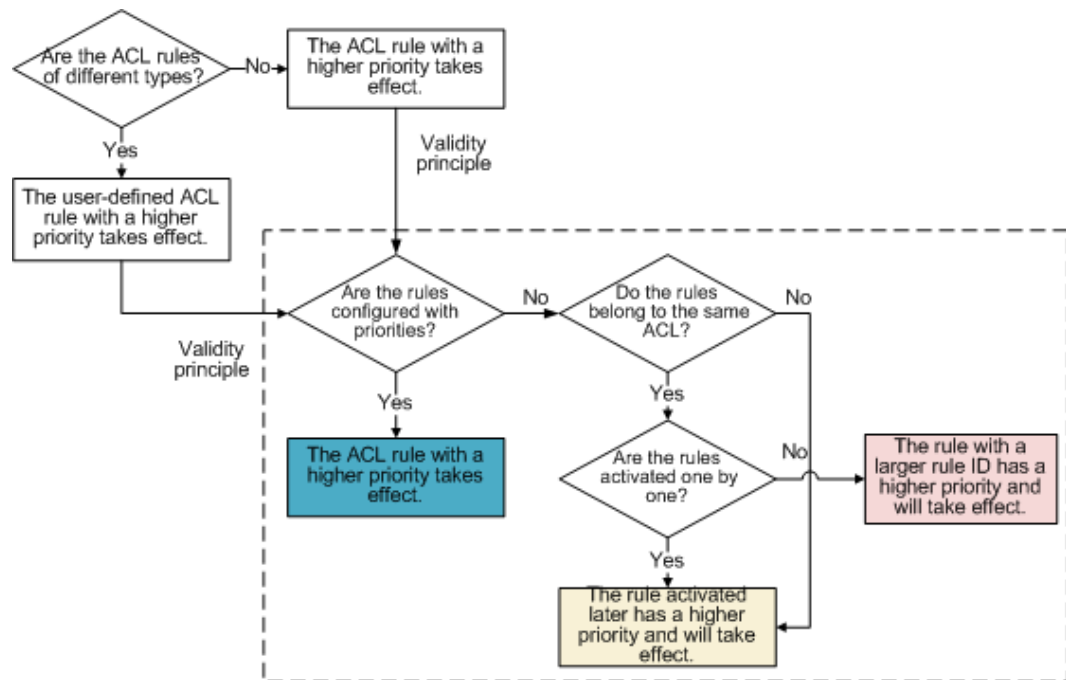
An ACL rule needs to be bound to a QoS policy so that it can take effect on a port. Two general ACL matching principles are provided as follows:

- An ACL rule is valid only when it is within the period of *time-range-name*.
- ACL rules are matched based on their priorities in a descending order; this process stops once a rule is matched.

Packets Matching Two or More ACL Rules

When packets reach a port, the system matches the packets with two or more ACL rules, as shown in [Figure 15-36](#).

Figure 15-36 Validity of ACL rules when packets match multiple ACL rules



When packets match two or more ACL rules:

- If ACL rules are of different types, the priority of a user-defined rule is higher than that of all non-user-defined rules. If the user-defined rule is used, the other rules may be invalid. Therefore, exercise caution when using this rule.
- If ACL rules are of the same type but configured with different priorities, the ACL rule of a higher priority will be valid.
- If ACL rules are of the same type and no priority is configured for these ACL rules, do as follows:
 - For rules of the same ACL, if they are activated at the same time, the rule with a larger *rule-id* has a higher priority.
 - For rules of the same ACL, if they are activated one by one, the rule activated later has a higher priority than the one activated earlier.
 - For rules belonging to different ACLs, the rule activated later has a higher priority than the one activated earlier.

In other cases:

- When both the Layer 3 ACL (basic ACL and advanced ACL) and the Layer 2 ACL (link-layer ACL) are issued, all rules use the priority that is configured for the Layer 2 ACL rule.
- When both the IPv6-based rule and the link-layer rule exist, the link-layer rule prevails even if a higher priority is configured for the IPv6-based rule.
- Among the rules issued to the routing interface or firewall, a rule with a smaller *rule-id* has a higher priority, regardless of the activation sequence or the configured priority. The rules are used to match the packets based on **rule-id** in an ascending order. Once the rule with a smaller **rule-id** matches

the packets, the rule matching stops, that is, other rules with a larger **rule-id** are invalid.

- When you run the **packet-filter** command to use an ACL and specify the **to-cpu** packet, the rules are matched based on priorities in a descending order; this process stops once a rule is matched. The matching sequence is irrelevant to whether the rule is a user-defined rule, an IPv6 rule, or a rule configured with a priority. Rules are matched based on the following principles only:
 - For rules of the same ACL, if they are activated at the same time, the rule with a larger *rule-id* has a higher priority.
 - For rules of the same ACL, if they are activated one by one, the rule activated later has a higher priority than the one activated earlier.
 - For rules belonging to different ACLs, if they are issued to the port from different ACLs, the rule activated later has a higher priority than the one activated earlier.

Packets Matching No ACL Rule

When no packet matches any rule in the ACL, the processing is as follows:

- For the ACL referenced by route interfaces or firewalls, if no packet matches any rule in the ACL, the traffic behavior will be performed, that is, the default operation is permit. You can run the **firewall default** command to configure the default operation for the firewall to **permit** or **deny**.

For example, when you run the **firewall packet-filter** command to filter out the packets that are about to pass the firewall, and the packet does not match any rule in the ACL, the packet is allowed to pass the firewall.

- For the ACL referenced by common ports, if no packet matches any rule in the ACL, no traffic behavior will be performed.

For example, when you run the **packet-filter** command to filter out the packets, and the packet does not match any rule in the ACL, the device will receive this packet. When you run the **traffic-limit** command to limit the traffic of packets that match the ACL rule and the packet does not match any rule in the ACL, the device only forwards the packet and does not perform the traffic limiting.

15.11.4 ACL Rule Matching Process

ACL Rule Matching Process

The system will match the inbound packets according to the defined ACL rules:

- If the packets match an ACL rule, they are performed with further QoS actions, including packet filtering, priority marking, rate limiting, traffic statistics measurement, packet redirection, and packet mirroring. After being processed using the preceding QoS actions, the packets are forwarded in the outbound direction.
- If the packets do not match an ACL rule, the packets are directly forwarded.

 NOTE

However, when the ACL rule is applied to the packet filtering firewall, the packets that do not match the ACL rule are processed according to the default firewall policy (run the **firewall default { permit | deny }** command to configure the default firewall policy). If the firewall default policy is deny, the packets will be discarded.

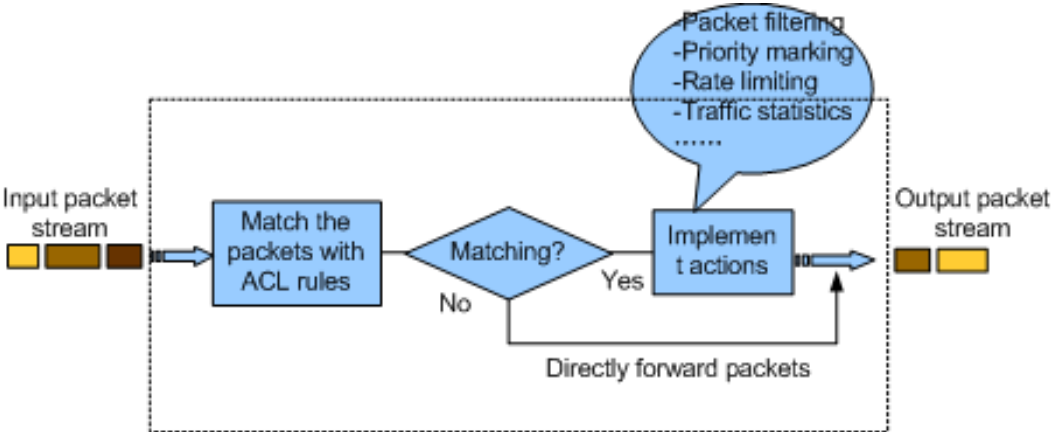
The following table lists the ACL-based QoS policies and relevant functions and configuration methods.

ACL-based QoS Policy	Function	Configuration Method
Packet filtering	Determines whether to discard packets or allow the packets to pass according to the matching result of the ACL rule (deny or permit).	Configuration command: packet-filter
Priority marking	Marks priorities for packets that match an ACL rule on a specified port or port list by type, such as ToS, DSCP, and 802.1p.	Configuration command: traffic-priority
Rate limiting	Limits the rate of packets that match an ACL rule on a specified port or port list. If traffic on a port exceeds the limit, the excessive packets will be discarded based on the trTCM algorithm or be configured with a new DSCP priority.	Configuration command: traffic-limit
Traffic statistics	Measures the packets that match an ACL rule on a specified port or port list in terms of packet number and byte.	Configuration command: traffic-statistic
Packet redirection	Redirects the packets that match an ACL rule on a specified port or port list to a new forwarding destination port (the original port is not used to forward packets that match an ACL rule).	Configuration command: traffic-redirect

ACL-based QoS Policy	Function	Configuration Method
Packet mirroring	Mirrors the packets that match an ACL rule on a specified port and copies the packets to other ports. If packets received or transmitted through a port need to be monitored during device maintenance or fault diagnosis, run the command to mirror packets to be monitored to other ports. NOTE Based on industry experience, the mirroring feature may involve obtaining personal data of users and the content of users' communications (the product does not save, parse, or process such information) for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.	Configuration command: traffic-mirror

Figure 15-37 illustrates ACL-based packet filtering and processing.

Figure 15-37 ACL-based packet filtering and processing



15.11.5 Matching Principle for the User-defined ACL Rule

The user-defined ACL rule is matched using any 32 bytes of the first 80 bytes of a Layer 2 data frame. The following describes the format of the Layer 2 data frame.

Format of the Layer 2 Data Frame

The following uses a Layer 2 IPv4 data frame as an example.

Figure 15-38 First 64 bytes of an IPv4 data frame

Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	AA	AA	AA	AA	AA	AA	BB	BB	BB	BB	BB	BB	CC	CC	CC	CC
	DD	DD	EE	FF	GG	GG	HH	HH	II	II	JJ	KK	LL	LL	MM	MM
	MM	MM	NN	NN	NN	NN	OO	OO	PP	PP	QQ	QQ	QQ	QQ	RR	RR
	RR	RR	SS	TT	UU	UU	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV

Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	AA	AA	AA	AA	AA	AA	BB	BB	BB	BB	BB	BB	CC	CC	CC	CC
	DD	DD	EE	FF	GG	GG	HH	HH	II	II	JJ	KK	LL	LL	MM	MM
	MM	MM	NN	NN	NN	NN	OO	OO	PP	PP	QQ	QQ	QQ	QQ	RR	RR
	RR	RR	SS	TT	UU	UU	VV	VV	VV	VV	VV	VV	VV	VV	VV	VV

shows the sequence of the first 64 bytes of the Layer 2 IPv4 data frame, in which:

- Different letters indicate different field values. For example, A refers to the destination MAC address and C refers to the Ethernet type+VLAN tag.
- The first letter of each letter group indicates the offset value of the field. For example, A indicates that the offset value is 0 and C indicates that the offset value is 12.

Table 15-13 lists the meaning and offset value of each letter.

Table 15-13 Meanings of letters and their offset values

Letter & Meaning	Offset Value	Letter & Meaning	Offset Value	Letter & Meaning	Offset Value
A: destination MAC address	0	I: flags	24	Q: serial number	42
B: source MAC address	6	J: time to live	26	R: acknowledgment field	46

Letter & Meaning	Offset Value	Letter & Meaning	Offset Value	Letter & Meaning	Offset Value
C: Ethernet type +VLAN tag	12	K: protocol ID ("6" represents TCP and "17" represents UDP)	27	S: IP header length and reserved bit	50
D: protocol type	16	L: IP checksum	28	T: reserved bit and flags bit	51
E: IP version number	18	M: source IP address	30	U: window size	52
F: service type	19	N: destination IP address	34	V: Others	54
G: length of the IP packet	20	O: TCP source port	38	-	-
H: ID	22	P: TCP destination port	40	-	-

 NOTE

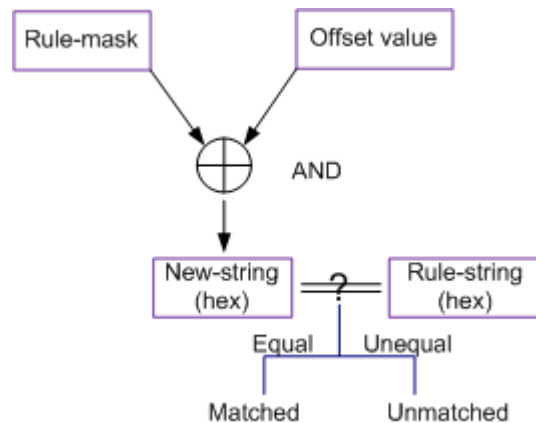
The offset value of each field is the offset value in data frame ETH II+VLAN tag.

Matching Principle

The user-defined ACL rule involves the following key concepts:

- rule-string: indicates the character string of the user-defined ACL rule. The character string is in hexadecimal notation. The number of characters in the string must be an even number ranging from 2 to 8.
- rule-mask: indicates the mask of the user-defined ACL rule. It is used to perform the logical AND operation with specified fields in the data packets.
- offset: indicates the offset. With the header of the packet as the reference point, it specifies a certain field in the Layer 2 data frame.

With the user-defined ACL rule, users can use rule-mask and offset to extract any 32 bytes of the first 80 bytes of a Layer 2 data frame and compare them with the rule-string so as to find the matched data frame. [Figure 15-39](#) shows the matching principle.

Figure 15-39 Matching principle for the user-defined ACL rule

15.11.6 Configuring Traffic Management Based on ACL Rules

The ACL can be used to implement flexible traffic classification according to user requirements. After traffic classification based on ACL rules is completed, you can perform QoS for the traffic streams.

15.11.6.1 Configuration Differences Between IPv4 ACLs and IPv6 ACLs

This topic describes differences regarding to configuration between IPv4 ACLs and IPv6 ACLs. It is recommended that you know well about how to configure IPv4 ACLs and then configure IPv6 ACLs based on their differences.

Configuration Differences

- The configuration differences between IPv4 ACLs and IPv6 ACLs are as follows:
 - IPv6 and IPv4 have different IP address formats and packet formats, so the **ipv6** parameter must be specified for configuring IPv6 basic ACLs and advanced ACLs. Use the **ipv6** parameter to choose between IPv4 ACLs and IPv6 ACLs.
 - IPv4 and IPv6 have the same link-layer packet encapsulation format, so configurations do not differentiate IPv6 link-layer ACLs and IPv4 link-layer ACLs.
 - Users define packets matching ACLs based on the packet type. IPv4 and IPv6 have the same packet command for user-defined ACLs, so configurations do not differentiate IPv6 user-defined ACLs and IPv4 user-defined ACLs. When user-defined ACLs are used for filtering packets, the protocol type of the packets must be the same as the protocol type of the ACL rules. If they are different, filtering may encounter errors.

15.11.6.2 Configuring an ACL Rule

Context

ACLs include:

- Basic ACL
- Advanced ACL
- Link-layer ACL
- User-defined ACL

For features of each type of ACL, see "[ACL Type](#)."

Because the ACL is flexible in use, Huawei provides the following suggestions on its configuration:

- It is recommended that you define a general rule, such as permit any or deny any, in each ACL, so that each packet has a matching traffic rule that determines to forward or filter the unspecified packet.
- The activated ACL rules share the hardware resources with the protocol modules, such as the Dynamic Host Configuration Protocol (DHCP) module and Internet Protocol over ATM (IPoA) module. In this case, the hardware resources are limited and may be insufficient. To prevent the failure to enable other service functions due to insufficient hardware resources, it is recommended that you enable the protocol module first and then activate ACL rules in the data configuration. If you fail to enable a protocol module, perform the following steps:
 - a. Check whether ACL rules occupy too many resources.
 - b. If ACL rules occupy too many resources, deactivate or delete the unimportant or temporarily unused ACL configurations, and then configure and enable the protocol module.

ACL-based applications can be classified to:

- Traffic management based on a single ACL rule (base mode)
- Traffic management based on a group of ACL rules (enhance mode)

For these 2 applications, the command **qos-acl mode** can be executed to switch the base and enhance modes. In these 2 modes, the method and commands of adding ACL sub-rules are the same. The configuration mode cannot be switched when:

- QoS is configured in the system.
- Remote TCP packet header obtaining and traffic burst detection are configured in the system.

Procedure

- Configure a basic ACL rule.

It is applicable to the scenario where the device needs to match packets by source IP address.

- a. (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

b. Create a basic ACL.

Run the **acl** command to create a basic ACL, and then enter the ACL mode. The serial number of a basic ACL ranges from 2000 to 2999.

c. Configure a basic ACL rule.

In the acl-basic mode, run the **rule** command to create a basic ACL rule. The parameters are as follows:

- *rule-id*: indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: indicates the keyword of the time range during which the ACL rule will take effect.

• Configure an advanced ACL rule.

It is applicable to the scenario where the device needs to match data packets by source IP address, destination IP address, type of protocol running over IP, and protocol feature, such as TCP source port, TCP destination port, and ICMP type of the data packets.

a. (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

b. Create an advanced ACL.

Run the **acl** command to create an advanced ACL, and then enter the acl-adv mode. The serial number of an advanced ACL ranges from 3000 to 3999.

c. Configure an advanced ACL rule.

In the acl-adv mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- *rule-id*: indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: indicates the keyword of the time range during which the ACL rule will take effect.

• Configure a link-layer ACL rule.

It is applicable to the scenario where the device needs to match packets by link-layer information such as source MAC address, source VLAN ID, Layer 2 protocol type, and destination MAC address.

- a. (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

- b. Create a link-layer ACL.

Run the **acl** command to create a link-layer ACL, and then enter the **acl-link** mode. The serial number of a link-layer ACL ranges from 4000 to 4999.

- c. Configure a link-layer ACL rule.

In the **acl-link** mode, run the **rule** command to create a link-layer ACL rule. The parameters are as follows:

- *rule-id*: indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: indicates the keyword for discarding the data packets that meet related conditions.
- **time-range**: indicates the keyword of the time range during which the ACL rule will take effect.

- Configure a user-defined ACL rule.

It is applicable to the scenario where the device needs to match packets by any 32 bytes of the first 80 bytes of a Layer 2 data frame.

Configuring a user-defined ACL requires a deep understanding of the Layer 2 data frame structure. Be sure to make a data plan according to the format of the Layer 2 data frame. Refer to "[15.11.5 Matching Principle for the User-defined ACL Rule](#)" for details.

- a. (Optional) Set a time range.

Run the **time-range** command to create a time range, which can be used when an ACL rule is created.

- b. Create a user-defined ACL.

Run the **acl** command to create a user-defined ACL, and then enter the **acl-user** mode. The serial number of a user-defined ACL ranges from 5000 to 5999.

- c. Configure a user-defined ACL rule.

In the **acl-user** mode, run the **rule** command to create an ACL rule. The parameters are as follows:

- *rule-id*: indicates the ACL rule ID. To create an ACL rule with a specified ID, use this parameter.
- **permit**: indicates the keyword for allowing the data packets that meet related conditions to pass.
- **deny**: indicates the keyword for discarding the data packets that meet related conditions.

- *rule-string*: indicates the character string of the user-defined ACL rule. The character string is in hexadecimal notation. The number of characters in the string must be an even number.
 - *rule-mask*: indicates the mask of the user-defined ACL rule. It is a positive mask, used to perform the AND operation with the data packets for extracting the information from the data packets.
 - *offset*: indicates the offset. With the header of the packet as the reference point, it specifies the byte from which the AND operation begins. Together with the rule mask, it extracts a character string from the packets.
 - **ipoe**: indicates that the Ethernet packet header encapsulates an IP packet, including untagged, single-tagged, and double-tagged IP packets.
 - **non-ipoe**: indicates that the Ethernet packet header encapsulates a non-IP packet, including the untagged, single-tagged, and double-tagged non-IP packets, or multi-tagged packets.
 - **time-range**: indicates the keyword of the time range during which the ACL rule will take effect.
- Perform traffic management based on ACL group.

When you need to apply an ACL group on a port, switch QoS ACL mode to enhance mode.

- a. Configure the QoS ACL mode.

Run the **qos-acl mode** command to set enhance mode.

- b. Create ACL and configure sub-rules. For details, see the preceding steps.
- c. Apply packet filtering and traffic limitation on ACL group-matched packets of a specified port.

----End

Example

To configure port 0/2/0 on the MA5800 to receive only the packets from address 10.2.2.2 from 00:00 to 12:00 on Fridays, and to discard the packets from other addresses, do as follows:

```
huawei(config)#time-range time1 00:00 to 12:00 fri
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule deny time-range time1
huawei(config-acl-basic-2000)#rule permit source 10.2.2.2 0.0.0.0 time-range time1
huawei(config-acl-basic-2000)#quit
huawei(config)#packet-filter inbound ip-group 2000 port 0/2/0
huawei(config)#save
```

Assuming that the service board of the MA5800 resides in slot 1 and belongs to a VLAN, and the IP address of the VLAN Layer 3 interface is 10.10.10.101, to prohibit the ICMP (such as ping) and telnet operations from the user side to the VLAN interface on the device, do as follows:

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 1 deny icmp destination 10.10.10.101 0
```

```
huawei(config-acl-adv-3001)rule 2 deny tcp destination 10.10.10.101 0 destination-port eq telnet
huawei(config-acl-adv-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/0
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/0
huawei(config)#save
```

NOTE

Configuration can be performed based on ACL group to achieve the same function.

```
huawei(config)#qos-acl mode enhance
huawei(config)#acl 3001
huawei(config-acl-adv-3001)rule 1 deny icmp destination 10.10.10.101 0
huawei(config-acl-adv-3001)rule 2 deny tcp destination 10.10.10.101 0 destination-port eq telnet
huawei(config-acl-adv-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule port 0/2/0
huawei(config)#save
```

Pay attention to the following during the configuration:

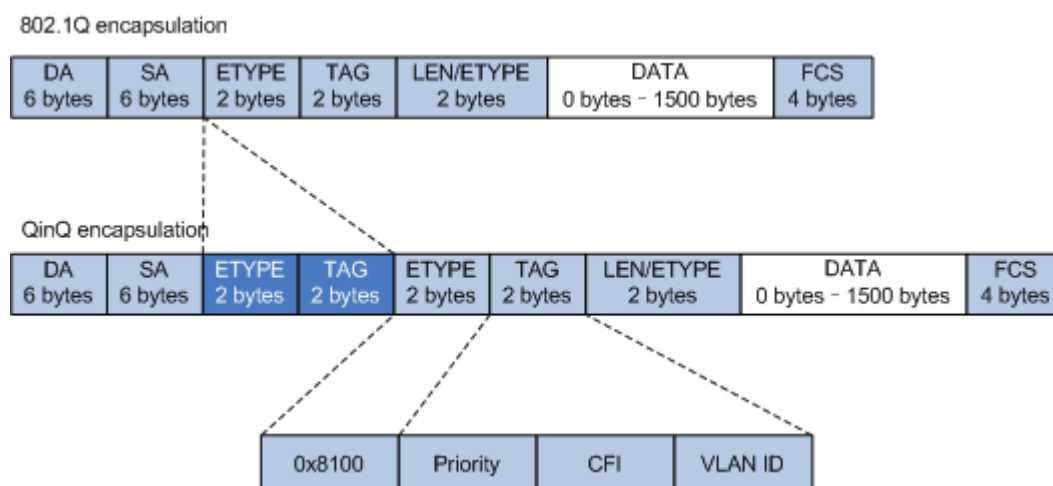
- If packets are filtered based on ACL group and parameter **ruleid** is not specified, all rules defined in ACL group are used to filter packets on a port.
- When a rule is added to or deleted from an ACL group, the action bound to this group is delivered or deleted. You do not need to configure this rule.

To create a link-layer ACL rule that allows data packets with protocol type 0x8863 (pppoe-control message), VLAN ID 12, CoS 1, source MAC address 00e0-fc00-2222, and destination MAC address 00e0-fc11-4141 to pass, do as follows:

```
huawei(config)#acl 4001
huawei(config-acl-link-4001)rule 1 permit type 0x8863 cos 1 source 12 00e0-fc00-2222 0000-0000-0000
destination 00e0-fc11-4141 0000-0000-0000
huawei(config-acl-link-4001)quit
huawei(config)#save
```

Assuming that the packet sent from port 0/2/0 to the MA5800 is the QinQ packet containing two VLAN tags, to change the CoS priority in the outer VLAN tag (VLAN ID: 10) to 5, do as follows:

Figure 15-40 QinQ packet format



```
huawei(config)#acl 5001
huawei(config-acl-user-5001)#rule 1 permit 8100 ffff 16
```

NOTE

The type value of a QinQ packet varies with vendors. Huawei adopts the default 0x8100. As shown in [Figure 15-40](#), the offset of this type value should be 16 bytes.

```
huawei(config-acl-user-5001)#rule 10 permit 0a ff 19
huawei(config-acl-user-5001)#quit
```

NOTE

"19" indicates the ADN operation after an offset of 19 bytes with the header of the packet as the base. "0a" refers to the value of the inner tag field of the QinQ packet. In this example, the second byte of the inner tag field is a part of the VLAN ID, which is exactly the value of the inner VLAN ID (VLAN 10).

```
huawei(config)#traffic-priority inbound user-group 5001 cos 5 port 0/2/0
```

15.11.6.3 Configuring ACL Matching for PPPoE Packets

This topic describes the format of PPPoE packets and how to match user-defined ACLs for various PPPoE packets.

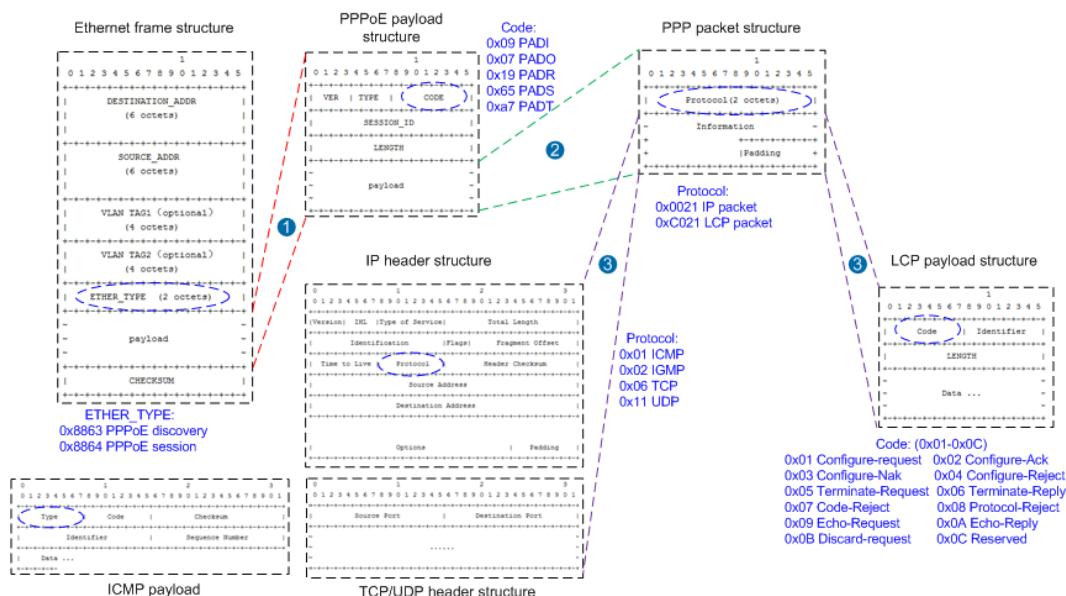
Prerequisites

You are familiar with the [15.11.5 Matching Principle for the User-defined ACL Rule](#).

Context

[Figure 15-41](#) shows the PPPoE packet format and offset value of each field.

Figure 15-41 PPPoE packet format and offset value of each field



Basic knowledge about PPPoE packets:

- In PPPoE-based data transmission, data packets are carried in the payload of ETH packets for transmission.

- The whole PPPoE-based transmission process has two stages: discovery (ETHER_TYPE = 0x8863) and session (ETHER_TYPE = 0x8864).
- In the discovery stage, there are four types of packets: PADI (code = 0x09), PADO (code = 0x07), PADR (code = 0x19), and PADS (code = 0x65).
- In the session stage, data is transmitted through PPP and PPP data is carried in the payload of PPPoE packets.
- PPP data frames can carry IP data packets (protocol = 0x0021) or LCP data packets (protocol = 0xC021).
- Based on the value of the protocol field in the IP header of IP data packets, the data transmission mode can be determined. The data transmission modes include:
 - 0x01 ICMP
 - 0x02 IGMP
 - 0x06 TCP
 - 0x11 UDP
- Based on the value (value range: 0x01-0x0C) of the code field of the LCP data packets, the packet encapsulation type can be determined.

Configuration Guideline

1. Determine the stage status of PPPoE packets, discovery or session.
2. Determine the protocol used to carry PPP packets, IP or LCP.
3. Determine the transmission mode (UDP, IGMP, or others) or encapsulation type of data packets.
4. Determine the offset value of each field.

Procedure

- **Match ACLs for PADI packets with a specified source MAC address and a single VLAN tag.**

As shown in [Figure 15-41](#), PADI packets contain the following information:

- Packets are in the discovery stage.
- Since the value of the ETHER_TYPE field of ETH packets is 0x8863, and packets carry only one single VLAN tag, the offset value is 16 (6 + 6 + 4 = 16).
- Since the value of the code field of PPPoE packets is 0x09, the offset value is 19 (16 + 2 + 1 = 19).

Based on the [15.11.5 Matching Principle for the User-defined ACL Rule](#), the corresponding ACLs can be determined.

Example: Run the following commands to match ACLs for PADI packets with the source MAC address of 0x00e0-fc00-4455 and a single VLAN tag:

```
huawei(config)#acl 5001
huawei((config-acl-user-5001))#rule permit 00e0fc00 FFFFFFFF 6 4455 FFFF 10 8863 FFFF 16 09 FF
19 non-ipo
```

- **Match ACLs for PPPoE echo-request packets with two VLAN tags.**

As shown in [Figure 15-41](#), PPPoE echo-request packets contain the following information:

- Packets are in the session stage and LCP is used for packet transmission.
- Since the value of the ETHER_TYPE field of ETH packets is 0x8864, and packets carry two VLAN tags, the offset value is 20 ($6 + 6 + 4 + 4 = 20$).
- Since the value of the protocol field of PPP packets is 0xC021, the offset value is 28 ($20 + 2 + 6 = 28$).
- Since the value of the code field of LCP packets is 0x09, the offset value is 30 ($28 + 2 = 30$).

Based on the [15.11.5 Matching Principle for the User-defined ACL Rule](#), the corresponding ACLs can be determined.

Example: Run the following commands to match ACLs for PPPoE echo-request packets with two VLAN tags:

```
huawei(config)#acl 5001
huawei((config-acl-user-5001))#rule permit 8864 FFFF 20 C021 FFFF 28 09 FF 30 non-ipoe
```

- **Match ACLs for packets with a specified inner VLAN ID and a specified UDP source port number.**

As shown in [Figure 15-41](#), the packets contain the following information:

- Packets are in the session stage and IP UDP is used for packet transmission.
- Since the value of the ETHER_TYPE field of ETH packets is 0x8864, and packets carry two VLAN tags, the offset value is 20 ($6 + 6 + 4 + 4 = 20$).
- Since the value of the protocol field of PPP packets is 0x0021, the offset value is 28 ($20 + 2 + 6 = 28$).
- Since the value of the protocol field in the IP header is 0x11, the offset value is 39 ($28 + 2 + 9 = 39$).
- Based on the UDP source port number, the offset value is 50 ($39 + 1 + 10 = 50$).

Based on the [15.11.5 Matching Principle for the User-defined ACL Rule](#), the corresponding ACLs can be determined.

Example: Run the following commands to match ACLs for PPPoE packets whose inner VLAN ID is 291 (0x123) and UDP source port number is 94 (0x5e):

```
huawei(config)#acl 5001
huawei((config-acl-user-5001))#rule permit 0123 0FFF 16 8864 FFFF 20 0021 FFFF 28 11 FF 39 5E FF 50 non-ipoe
```

- **Match ACLs for PPPoE-based PING (echo-request) packets with specified inner and outer VLAN IDs.**

As shown in [Figure 15-41](#), the packets contain the following information:

- Packets are in the session stage and IP ICMP is used for packet transmission.
- Since the value of the ETHER_TYPE field of ETH packets is 0x8864, and packets carry two VLAN tags, the offset value is 20 ($6 + 6 + 4 + 4 = 20$).
- Since the value of the protocol field of PPP packets is 0x0021, the offset value is 28 ($20 + 2 + 6 = 28$).
- Since the value of the protocol field in the IP header is 0x01, the offset value is 39 ($28 + 2 + 9 = 39$).

- Since the value of the type field in the ICMP header is 0x08, the offset value is 50 ($39 + 1 + 10 = 50$).

Based on the [15.11.5 Matching Principle for the User-defined ACL Rule](#), the corresponding ACLs can be determined.

Example: Run the following commands to match ACLs for PPPoE-based PING (echo-request) packets whose outer and inner VLAN IDs are 256 (0x100) and 291 (0x123) respectively.

```
huawei(config)#acl 5001
huawei((config-acl-user-5001))#rule permit 0100 0FFF 12 0123 0FFF 16 8864 FFFF 20 0021 FFFF
28 01 FF 39 08 FF 50 non-ipoe
```

----End

15.11.6.4 Controlling the Traffic Matching an ACL Rule

This topic describes how to control the traffic matching an ACL rule on a specified port, and process the traffic that exceeds the limit, such as adding the DSCP tag or dropping the packet directly.

Prerequisite

The [ACL and the rule of the ACL are configured](#), and the port for traffic limit is working in the normal state.

Context

- The traffic statistics are only effective for the permit rules of an ACL.
- The limited traffic must be an integer multiple of 64 Kbit/s.

Procedure

- Step 1** Run the **traffic-limit** command to control the traffic matching an ACL rule on a specified port.

Use the **target-rate** parameter to set the fixed maximum rate of the port, or use CAR parameters to set a rate for trTCM-based ports. The two rates cannot be set at a time. Run this command to set the action to be taken when the traffic received on the port exceeds the limited value. Two options are available:

- **drop**: Drop the traffic that exceeds the limited value.
- **remark-dscp value**: To set the DSCP priority for the traffic that exceeds the limited value, use this parameter.

- Step 2** Run the **display qos-info traffic-limit port** command to query the traffic limit information on the specified port.

----End

Example

To limit the traffic that matches ACL 2001 received on port 0/2/0 to 512 Kbit/s, and add the DSCP priority tag (af1) to packets that exceed the limit, do as follows:

```
huawei(config)#traffic-limit inbound ip-group 2001 512 exceed remark-dscp af1 port 0/2/0
// "af1" represents a dscp type: Assured Forwarding 1 service (10).
```

```
huawei(config)#display qos-info traffic-limit port 0/2/0
traffic-limit:
port 0/2/0:
Inbound:
Matches: Acl 2001 rule 5    running
Target rate: 512 Kbps
Exceed action: remark-dscp af1
```

15.11.6.5 Adding a Priority Tag to the Traffic Matching an ACL Rule

This topic describes how to add a priority tag to the traffic matching an ACL rule on a specified port so that the traffic can obtain the service that matches the specified priority. The priority tag type can be ToS, DSCP, or 802.1p.

Prerequisite

The [ACL and the rule of the ACL are configured](#), and the port for traffic limit is working in the normal state.

Context

- The traffic statistics are only valid to permit rules of an ACL.
- The ToS and the DSCP priorities are mutually exclusive. Therefore, they cannot be configured at the same time.

Procedure

- Step 1** Run the **traffic-priority** command to add a priority tag to the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-priority port** command to query the configured priority.

----End

Example

To add a priority tag to the traffic that matches ACL 2001 received on port 0/2/1, and the DSCP priority and local priority of the traffic are 10 (af1) and 0 respectively, do as follows:

```
huawei(config)#traffic-priority inbound ip-group 2001 dscp af1 local-precedence 0 port 0/2/1
huawei(config)#display qos-info traffic-priority port 0/2/1

traffic-priority:
port 0/2/1:
Inbound:
Matches: Acl 2001 rule 5    running
Priority action: dscp af1 local-precedence 0
```

15.11.6.6 Enabling the Statistics Collection of the Traffic Matching an ACL Rule

This topic describes how to enable the statistics collection of the traffic matching an ACL rule, analyzing and monitoring the traffic.

Prerequisite

The [ACL and the rule of the ACL are configured](#), and the port for traffic statistics is working in the normal state.

Procedure

- Step 1** Run the **traffic-statistic** command to enable the statistics collection of the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-statistic port** command to query the statistics information about the traffic matching an ACL rule on a specified port.

----End

Example

To enable the statistics collection of the traffic that matches ACL 2001 received on port 0/9/0, do as follows:

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/9/0
huawei(config)#display qos-info traffic-statistic port 0/9/0

traffic-statistic:
port 0/9/0:
Inbound:
Matches: Acl 2001 rule 5    running
         0 packet
```

15.11.6.7 Enabling the Mirroring of the Traffic Matching an ACL Rule

This topic describes how to mirror the traffic matching an ACL rule on a port to a specified port. Mirroring does not affect packet receipt and transmission on the mirroring source port. You can monitor the traffic of the mirroring source port by analyzing the traffic that passes the mirroring destination port.

Prerequisite

The [ACL and the rule of the ACL are configured](#), and the port for traffic mirroring is working in the normal state.

NOTE

Based on industry experience, the mirroring feature may involve obtaining personal data of users and the content of users' communications (the product does not save, parse, or process such information) for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

Context

- The traffic statistics are only valid to permit rules of an ACL.

- The destination mirroring port cannot be an aggregation port.
- The system supports only one mirroring destination port.

Procedure

- Step 1** Run the **traffic-mirror** command to enable the mirroring of the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-mirror port** command to query the mirroring information about the traffic matching an ACL rule on a specified port.

----End

Example

To mirror the traffic that matches ACL 2001 received on port 0/2/1 to port 0/9/0, do as follows:

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/2/1 to port 0/9/0
huawei(config)#display qos-info traffic-mirror port 0/2/1

traffic-mirror:
port 0/2/1:
Inbound:
Matches: Acl 2001 rule 5    running
Mirror to: port 0/9/0
```

15.11.6.8 Enabling the Redirection of the Traffic Matching an ACL Rule

This topic describes how to redirect the traffic matching an ACL rule on a specified port. After this operation is executed successfully, the original port does not forward the traffic matching the ACL rule, but the specified port forwards the traffic.

Prerequisites

The [ACL and the rule of the ACL are configured](#), and the port for redirection is working in the normal state.

Context

- The traffic statistics are only valid to permit rules of an ACL.
- Currently, the service ports support only redirection of the traffic matching the ACL rule to upstream ports. The upstream ports support only redirection of the traffic matching the ACL rule to ports on the board of the same type.

Procedure

- Step 1** Run the **traffic-redirect** command to redirect the traffic matching an ACL rule on a specified port.
- Step 2** Run the **display qos-info traffic-redirect port** command to query the redirection information about the traffic matching an ACL rule on a specified port.

----End

Example

To redirect the traffic that matches ACL 2001 received on port 0/9/0 to port 0/9/1, do as follows:

```
huawei(config)#traffic-redirect inbound ip-group 2001 port 0/9/0 to port 0/9/1
huawei(config)#display qos-info traffic-redirect port 0/9/0
traffic-redirect:
port 0/9/0:
Inbound:
Matches: Acl 2001 rule 5    running
Redirected to: port 0/9/1
```

15.12 ACLv6

This topic describes the aspects unique to access control list for IP version 6 (ACLv6), and the differences between ACLv6 and ACLv4. For details about the specifications and principles of ACLv6, see [15.11 ACL](#).

15.12.1 Comparison Between ACLv6 and ACLv4

On the MA5800, the application and the configuration processes of ACLv6 are the same as those of ACLv4, except the following differences regarding specifications and commands:

- ACLv4 supports segmented packets, while ACLv6 does not.
- IPv6 and IPv4 have different IP address formats and packet formats, so the **ipv6** parameter must be specified when you are configuring basic ACLs and advanced ACLs for IPv6. When the **ipv6** parameter is specified, the system supports both ACLv4 and ACLv6.
- Regarding user-defined ACLs, packets are matched based on the packet type defined by users. Because IPv4 and IPv6 have the same command format for specifying the packet type in user-defined ACLs, configurations do not differentiate between IPv6 user-defined ACLs and IPv4 user-defined ACLs. When user-defined ACLs are used for filtering packets, however, the protocol type of the packets must be matched against the protocol type specified in the ACL rules.

15.13 HQoS

Traditional quality of service (QoS) schedules traffic based on port. Hierarchical quality of service (HQoS) not only controls port traffic at a finer service granularity but also schedules traffic based on service priorities.

15.13.1 Overview of HQoS

Definition

Hierarchical quality of service (HQoS) is a technology that uses a multi-level scheduling mechanism to guarantee the bandwidth of various services for multiple users. It usually applies to Open Access networks.

The following HQoS scheduling models are available:

- The first level of HQoS guarantees the bandwidth of services for a user, and the second level guarantees the bandwidth of all users that use the same types of services.
- The first level of HQoS guarantees the bandwidth of services for a user, and the second level guarantees the bandwidth of all services for the user.

Background

In most scenarios, traditional QoS identifies service types on a network and provides services at different levels. As users and service types increase, traditional QoS faces the following challenges:

- Traditional QoS schedules traffic based on port bandwidth. Traffic management is therefore sensitive to the service level rather than users, which applies to traffic at the network core side rather than traffic at the service access side.
- Traditional QoS is unable to uniformly manage or hierarchically schedule various services or multiple users.

Purpose

HQoS controls traffic in a user-specific and service-specific manner, and therefore guarantees bandwidth of various services for multiple users. In addition, it provides the committed information rate (CIR) and peak information rate (PIR) of various services for each user.

Benefits

Benefits to carriers

Unlike traditional QoS which schedules traffic based on a port, HQoS implements QoS on a port at a finer granularity (users and service flows). Therefore, HQoS enables a carrier to guarantee QoS for enterprises and contracted users, provide guaranteed bandwidths and service packages for more users, and achieve higher profitability.

Benefits to users

HQoS ensures that the bandwidth designated for a user is not affected by other users.

15.13.2 Open Access of HQoS

Hierarchical quality of service (HQoS) mainly applies to Open Access networks. This topic describes the Open Access network model for better understanding of HQoS.

Definition and Benefits

Open Access provides a network business model that separates the physical bearer network from the service network. The infrastructure of an Open Access network, including passive infrastructure (optical fibers, equipment room premises, and cables) and active network devices, is built by a nation or an operator authorized

by the nation. Retail service providers (RSPs) directly lease bandwidth on the infrastructure network to provide service packages to end-users.

In the traditional model, an operator builds and operates its own network and delivers services to end-users. Unlike the traditional model, Open Access builds a layered network over which separate RSPs deliver their services.

Open Access brings the following benefits:

- Maximizes the freedom of choice for end users. End-users have more services to choose from and can even switch from one service provider to another without changing their home terminals (such as their ONTs).
- Lowers investment risks for RSPs. The business model of Open Access greatly shortens the cycle of return on investment (ROI). The traditional business model of operators, who usually have monopoly over their networks, requires an ROI cycle of 8-10 years. The Open Access business model shortens the ROI cycle to 1-2 years. Hence Open Access lowers the investment entrance level and risks for RSPs, and promotes competition and innovation.
- Opens up a wider arena for RSPs. RSPs no longer need to build the infrastructure network and are able to focus on innovation and competition of services and contents.

Open Access Modes

In a broad sense, there are two Open Access modes: the physical open access mode (LLU) and the bit stream open access mode.

- LLU Access Mode: This is a layer-one physical open access mode. In this mode, RSPs lease duct resources such as copper loops and optical fibers. One line cannot carry the services of multiple RSPs. To subscribe to services of different content providers (CPs), a user needs to apply for respective lines.
- Bit Stream Access Mode: In the bit stream access mode, RSPs are separated from the infrastructure network. RSPs purchase bandwidth on the infrastructure network and provide service packages to end-users.

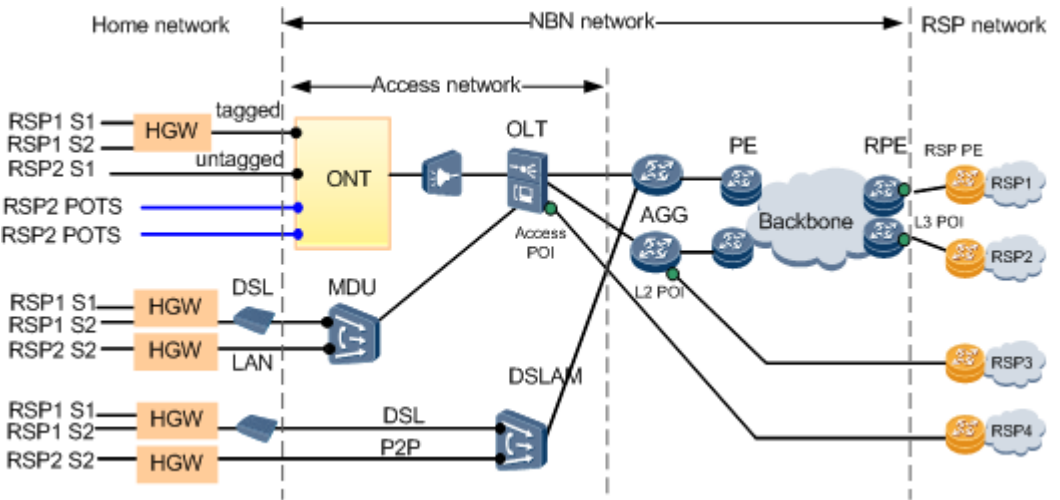
Wholesale is a special bit stream access mode. RSPs lease physical terminals, and one terminal belongs to one RSP. Wholesale allows for simpler terminal management.

The bit stream access mode presents multiple requirements and challenges to FTTx devices. Therefore, the following part of this document will focus on the bit stream access mode.

End-to-end Open Access network

Figure 15-42 shows an end-to-end Open Access network (Bit Stream Access Mode).

Figure 15-42 End-to-end Open Access network



Concept	Description
NBN	short for national broadband network. An NBN is usually constructed using the Open Access network model.
POI	short for point of interconnection. It is a point where a carrier network and retail service provider (RSP) network interconnects. Based on network layers, there are access POI, Layer 2 POI, and Layer 3 POI.

An end-to-end Open Access network consists of the RSP networks at both ends and the NBN open channel network in between. The NBN open channel network includes the ONT, OLT, and aggregation devices such as the user-end provider edge (UPE) and access aggregation gateway (AGG).

An RSP needs to purchase physical ports and logical bandwidth to access the NBN open channel network. The physical ports are the openings at both ends of the open channel.

- User network interfaces (UNIs). They are usually the ports on user-side devices, such as the ETH/POTS/Wi-Fi ports on an ONT, xDSL/LAN ports on a multi-dwelling unit (MDU), and xDSL/P2P ports on a digital subscriber line access multiplexer (DSLAM). UNIs connect upper-layer devices to user terminals or RSPs' home gateways.
- External network-to-network interfaces (ENNIs), also called point of interconnection (POI), are the interconnection points between an operator network and an RSP network. POIs can be the upstream GE or 10GE ports on an OLT, aggregation device, or backbone network device.

Because RSPs will share one physical network, the RSPs purchase logical bandwidth on the network and use the bandwidth as service channels to provision services to end-users. The logical bandwidth includes the bandwidth on the UNIs for access users and the aggregation bandwidth on the ENNIs. The logical bandwidth is expressed in the unit of bit/s.

Openness and fairness are two key points of a bit stream Open Access network. Openness means that an ONT on user side can be shared by multiple RSPs for

provisioning services. Also, on network side the ENNs can provide various openings to meet different network requirements. Fairness means that users of the same RSP can be isolated from each other, and RSPs can be isolated from each other, through HQoS.

15.13.3 Basic Concepts of HQoS

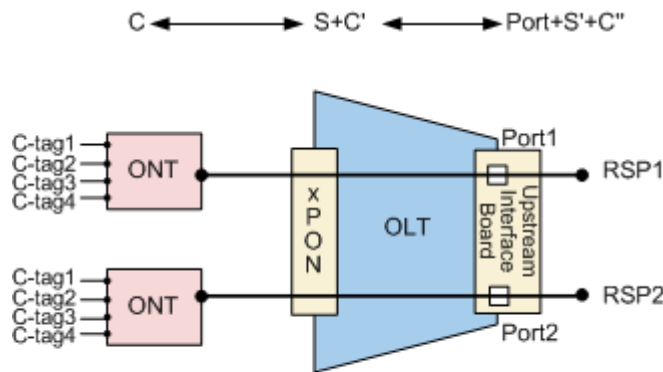
Concept	Description
HQoS user	A basic unit of bandwidth guarantee and traffic scheduling. Alternatively, a type of user service can also be a basic unit.
HQoS user group	A group of HQoS users. The committed information rate (CIR) of HQoS users is guaranteed by scheduling an HQoS user group.
Retail service provider (RSP)	Unlike carriers, RSPs focus on service content rather than infrastructure network construction. They lease bandwidth to quickly provision user services.
Open Access	A network construction mode that separates the physical bearer network from the service network. RSPs directly lease bandwidth on an infrastructure network where Open Access has been deployed to quickly provide service packages for customers.
CAR group	A combination of service flows for unified QoS control, with configurable parameters such as CIR and peak information rate (PIR). Generally, a CAR group is specified for limiting the rate of triple-play services of a specific household user.

15.13.4 HQoS Service Model (Based on Port+VLAN)

Figure 15-43 shows an HQoS service processing model based on the Port+VLAN. A Layer 2 leased line is used, between the ingress port on the optical network terminal (ONT) and the uplink port of the optical line terminal (OLT). On the line, services are forwarded based on S-VLAN+C-VLAN tags.

- The ONT attaches C-VLAN tags to services based on a port or service type to identify users.
- After receiving the services, the OLT translates the C-VLAN tags into C-VLAN' tags based on PON port information and adds S-VLAN tags to the services based on service types. The services are identified based on their S-VLAN+C-VLAN' tags.
- After services are forwarded to a port on the upstream interface board that is interconnected to an RSP network, the upstream interface board translates the S-VLAN+C-VLAN' tags into S-VLAN' +C-VLAN'' tags based on the RSP planning requirements configured on the port.

Figure 15-43 HQoS service model based on Port+VLAN



Note:
C, S, C', S', and C'' indicate different types of VLAN

The Layer 2 leased line can be considered as designated to an HQoS user with the following QoS requirements:

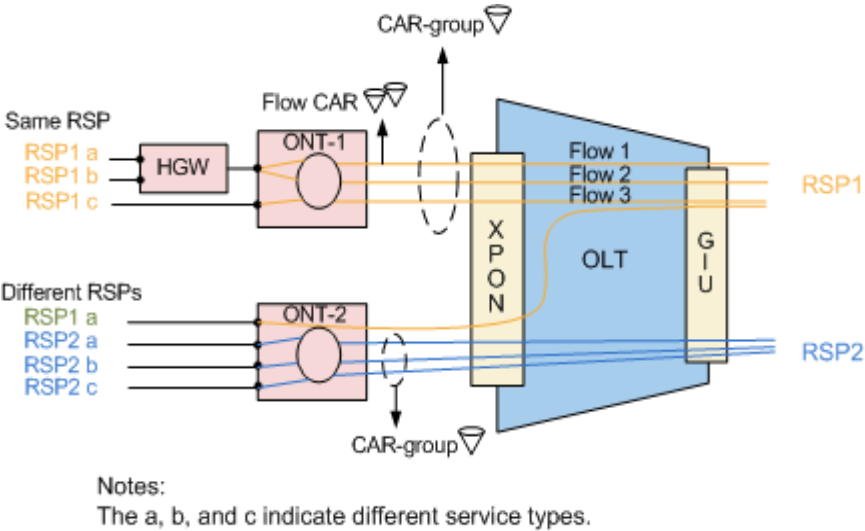
1. CIR can be ensured when network congestion occurs, and PIR can be ensured when the network is idle.
2. The services of the user occupy bandwidth based on service priorities. Specifically, services with a higher priority can preferentially occupy CIR and PIR resources.

15.13.5 HQoS Service Model (Based on a CAR Group)

Mode 1

- Installed at a user's home, an optical network terminal (ONT) can run services provided by one retail service provider or RSP (such as ONT-1 shown in the figure), or services provided by multiple RSPs (such as ONT-2 shown in the figure).
- On the ONT, triple play services are provisioned and each type of service is transmitted through one GEM port. On the optical line terminal (OLT), each type of service is mapped into one service flow.
- There is no limit on the VLAN tag translation mode. An S-VLAN+C-VLAN tagging mode, however, is recommended (the S-VLAN tag indicates an RSP while the C-VLAN tag indicates a service type).

Figure 15-44 HQoS service model based on a CAR group



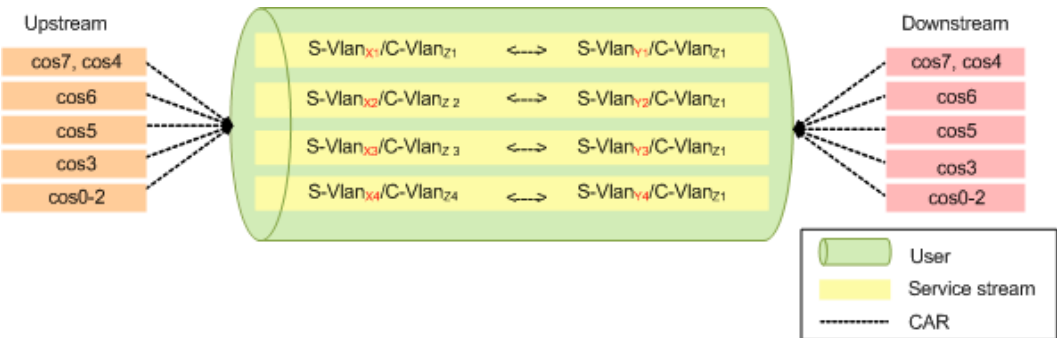
This HQoS service model can address the following QoS requirements:

1. For each type of service, CIR can be ensured when network congestion occurs, and PIR can be ensured when the network is idle.
2. When services are provided by only one RSP, the total user bandwidth can be limited.
3. When services are provided by multiple RSPs, the total lease bandwidth of each RSP can be limited.

Mode 2

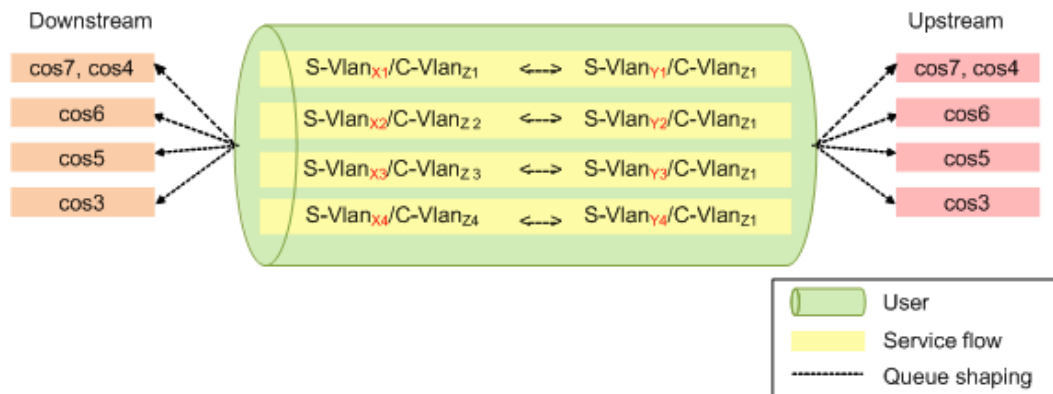
For RSP users leasing pipes, services can be flexibly deployed by configuring multi-level CAR groups on the OLT. As shown in [Figure 15-45](#), RSP users leasing pipes group service flows for level-1 rate limitation. Every group of service flows then can be grouped by priority for level-2 rate limitation (priority group CAR for service flows).

Figure 15-45 HQoS service model based on a CAR group



As shown in [Figure 15-46](#), subscriber shaping can be performed on the pipe for RSP users as the level-1 rate limitation and then queue shaping by priority as the level-2 rate limitation.

Figure 15-46 HQoS service model based on a CAR group

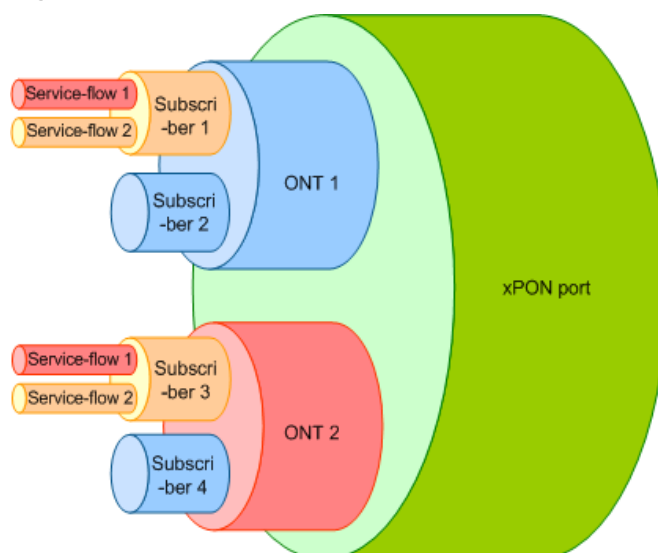


15.13.6 HQoS Service Model (xPON Board)

[Figure 15-47](#) shows the HQoS service model of an xPON board.

- One xPON port connects to multiple ONTs.
- One ONT connects to multiple users.
- One user is provisioned with multiple services.

Figure 15-47 HQoS service model (xPON board)



As shown in the figure, this model supports the specifications for HQoS:

- Rate limitation on every user and every service

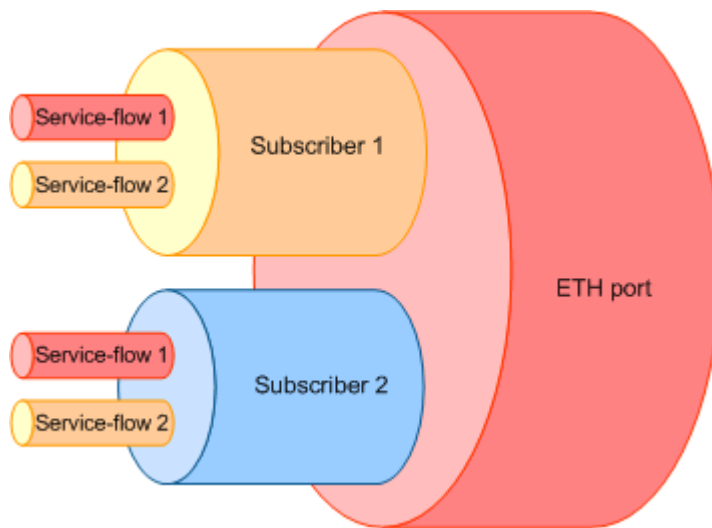
- Bandwidth scheduling between multiple services of every user
- Rate limitation on every user
- Bandwidth scheduling on every ONT
- Rate limitation on every ONT
- Scheduling between multiple ONTs connected to every xPON port

15.13.7 HQoS Service Model (P2P Board)

Figure 15-48 shows the HQoS service model of a P2P board.

- An Ethernet port connects to multiple users.
- One user is provisioned with multiple services.

Figure 15-48 HQoS service model (P2P board)



As shown in the figure, this model supports the specifications for HQoS:

- Rate limitation on every user and every service
- Packet scheduling between multiple services of every user
- Rate limitation on every user
- Packet scheduling between multiple users connected to every Ethernet port

15.13.8 Implementation Principle of HQoS

15.13.8.1 Implementation Principle of HQoS based on Port+VLAN

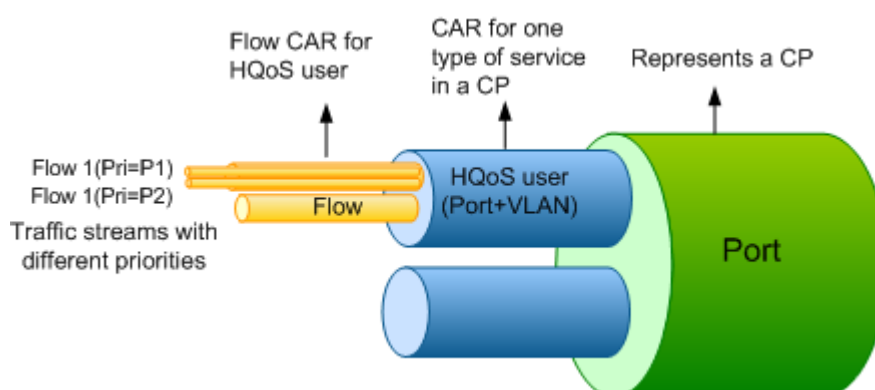
Implementation Model of HQoS based on Port+VLAN

Figure 15-49 shows an implementation model of HQoS based on Port+VLAN. In the model, each HQoS user is mapped to one Layer 2 service flow.

The core of the implementation principle of HQoS based on Port+VLAN is a two-level service rate limitation mechanism on the upstream interface board. The following describes the mechanism:

1. The committed access rate (CAR) is limited for an HQoS user, and the service packets are marked with colors based on committed information rate (CIR) and peak information rate (PIR). If priority-based CAR is enabled (with CAR thresholds configured), packets with a higher priority will be marked green and transmitted.
2. Color-based CAR is performed on an HQoS user group (a type of service provided by an RSP and identified by port+VLAN tags). In this manner, the bandwidth for a type of service can be ensured among the total leased RSP bandwidth, HQoS users can be isolated from each other, the CIR can be ensured for the services of HQoS users, and the PIR can also be ensured if bandwidth resources are sufficient.

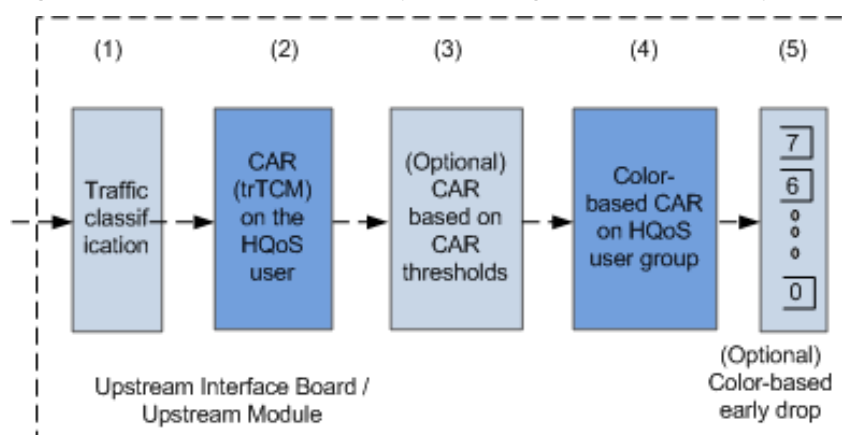
Figure 15-49 Implementation model of HQoS based on Port+VLAN



Implementation Solution

Figure 15-50 shows the implementation solution of HQoS based on port+VLAN on an upstream board.

Figure 15-50 Procedure for implementing HQoS based on port+VLAN

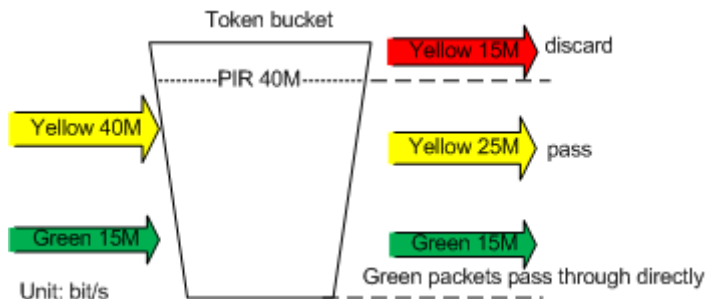


The following describes how HQoS is implemented using the upstream interface board:

1. The upstream board performs traffic classification on received packets.
On an optical line terminal (OLT), each HQoS user is mapped to one Layer 2 service flow. When a service packet from the uplink direction enters the OLT, the upstream board on the OLT performs traffic classification on it based on related packet parameters and determines the HQoS user to which the service packet belongs.
 - On the network-to-network interface (NNI) side (or an uplink port of the upstream board), traffic classification can be performed based on port+S-VLAN+C-VLAN' tags.
 - On the user-to-network interface (UNI) side, traffic classification can be performed based on S-VLAN+C-VLAN' tags.For detailed principles of traffic classification, see [Implementation Principle of Traffic Classification](#).
2. The upstream board performs CAR on the HQoS user (flow CAR) using a two rate three color marker (trTCM) algorithm.
The traffic profile bound to the Layer 2 service flow (that is, the HQoS user) is used for CAR. Specifically, a packet is marked with a color based on the CIR and PIR.
 - If the packet rate is lower than or equal to the CIR, the upstream board will mark the packet green (and will transmit it).
 - If the packet rate is higher than the CIR, but is lower than or equal to the PIR, the upstream board will mark the packet yellow (and will transmit it).
 - If the packet rate is higher than the PIR, the upstream board will directly drop the packet.For detailed principles of the trTCM algorithm, see [Dual-Token Bucket \(trTCM\) Principle](#).
3. (Optional) The upstream board performs flow CAR based on CAR thresholds, and marks user packets with colors based on packet priorities (configurable through the **car-threshold** command).
The upstream board marks the packets of the HQoS user with colors based on the CIR and PIR settings. (If an enhanced trTCM algorithm is used, thresholds for 4 priorities will be supported.) A packet will be marked green if the packet rate is lower than the CIR, or yellow if the packet rate is between the CIR and the PIR, or will be directly dropped if the packet rate is higher than the PIR. When marking packets with colors, the upstream board also differentiates packet priorities. Packets with a higher priority can preferentially use the CIR and PIR bandwidth specified for the HQoS user.
For detailed principles of packet color marking based on CAR thresholds, see [Enhanced trTCM: Marking Packet with Color Based on CAR Thresholds](#).
4. The upstream board performs CAR on HQoS user groups (group CAR) based on packet colors (configurable through the **car-port portid vlan** command).
As shown in [Figure 15-51](#), CAR is performed on yellow packets and green packets that have been identified in step 2. Specifically,
 - a. Green packets will be transmitted.
 - b. All yellow packets can be transmitted if their rate is within the remaining bandwidth (Remaining bandwidth = PIR - Rate of green packets).

- c. If the rate of yellow packets exceeds the remaining bandwidth, some yellow packets can be transmitted using the remaining bandwidth while the excessive yellow packets will be dropped.

Figure 15-51 CAR on yellow packets and green packets



5. (Optional) The upstream board performs color-based early drop on an egress port.

On the egress port, the upstream board puts all HQoS users into the same priority queue. The queue deploys a strict priority-based scheduling policy, and color-based early drop will be performed based on the queue. When the rate of yellow packets reaches the specific drop threshold, yellow packets will be dropped to ensure low latency of green packets. Note that the drop threshold is 50% for yellow packets and 100% for green packets. The two drop thresholds cannot be modified manually.

To put HQoS users into one priority queue, the following configuration methods can be used:

- In fiber to the building (FTTB) scenarios where both S-VLAN and double C-VLAN tags are attached to packets, the outer S-VLAN tags of HQoS users can be set to a specific priority so that all HQoS users can be in the same queue based on the priority.
- In fiber to home (FTTH) scenarios where packets are single-tagged, all priorities of single tags can be mapped into one port queue.

For details on color-based early drop, see [Color-based Early Drop](#).

15.13.8.2 Implementation Principle of CAR-Group-based HQoS

Implementation Model of CAR-Group-based HQoS

A CAR group is a combination of traffic streams for unified QoS control, with configurable parameters such as CIR and PIR. One of its typical applications is for multiple services (IPTV, Internet access, and voice services) of home users. Using the CAR group, QoS based on the home user instead of based on each service is implemented.

Figure 15-52 illustrates the model of CAR-group-based HQoS supported by the MA5800.

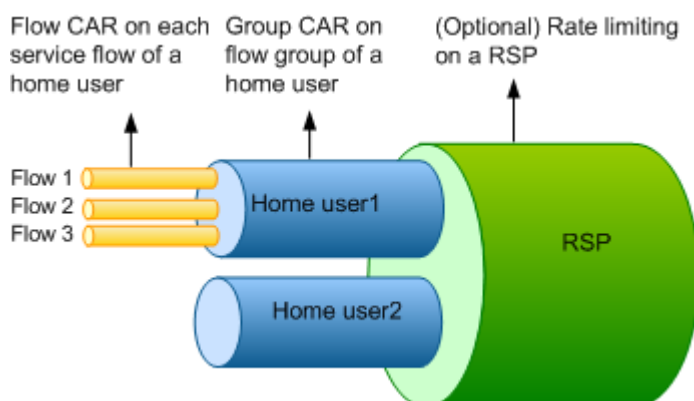
HQoS based on a CAR group implements two-level CAR for services:

1. The first level performs flow CAR on various service flows of a home user.
2. The second level performs group CAR on flow groups of home users.

If required, a level of CAR can be performed specifically for retail service providers (RSPs).

For example, the two-level CAR can achieve the following settings: limiting a user's Internet access rate, multicast service rate, and voice service rate to 2 Mbit/s, 4 Mbit/s, and 128 Kbit/s respectively, and at the same time limiting the total bandwidth of the user to 5 Mbit/s.

Figure 15-52 Implementation model of CAR-group-based HQoS

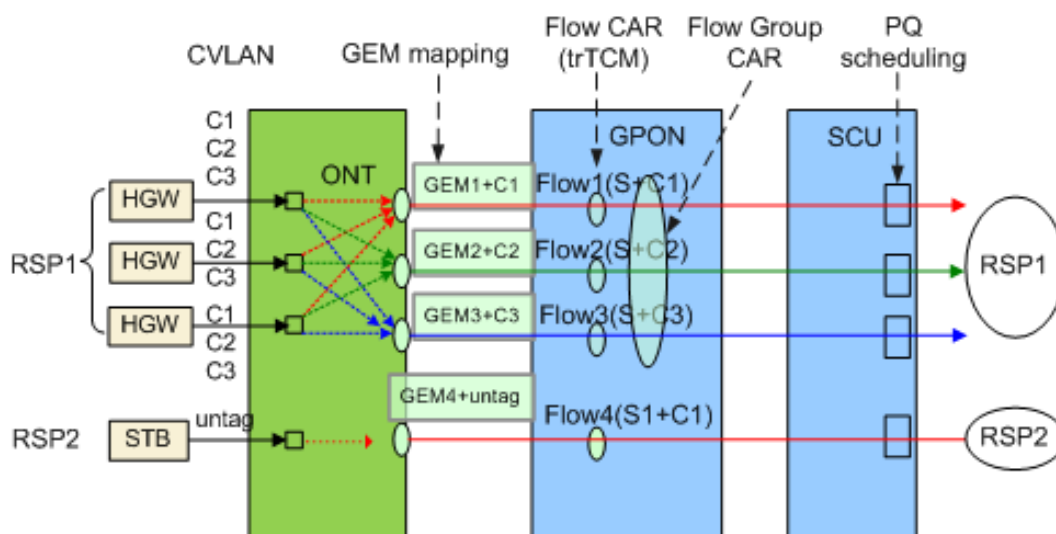


Implementation Solution

Figure 15-53 shows how HQoS is implemented based on a CAR group in the uplink direction.

In the downlink direction, a reverse process is performed. This topic only describes the implementation process in the uplink direction.

Figure 15-53 Flowchart for implementing HQoS based on a CAR group (in the uplink direction)



RSP: retail service provider

HGW: home gateway

STB: set-top box

GEM: G-PON encapsulation method

trTCM: two rate three color marker

-

Table 15-14 Implementation principle of HQoS based on a CAR group in the uplink direction

Subject	Operation	Result
HGW	Identifies different types of services provided by the same RSP based on C-VLAN tags. In Figure 15-53 , C1, C2, and C3 indicate different service types.	It receives various types of services and identifies them based on the C-VLAN tags of service packets.
ONT	Maps each type of service into one GEM port based on VLAN tags. In the figure, services tagged as C1 are mapped to GEM port 1 while services tagged as C2 are mapped to GEM port 2.	It identifies various service packets based on GEM port+C-VLAN tags.
	Binds each GEM port to one T-CONT. Performs priority queuing (PQ) on T-CONTs. (To prevent queuing differences, the class of service, or CoS, must have been uniformly configured.)	Guarantees the uplink bandwidth of each type of service on a T-CONT.

Subject	Operation	Result
Service board of the OLT	Performs traffic classification and priority processing. Each GEM port+C-VLAN tag identifies one service flow. The priority of the service flow can be configured (if the user-side priority is not trusted), or directly duplicated from the user-side priority (if the user-side priority is trusted). Performs two-level CAR: 1. Flow CAR (rate limiting on each service flow) using the trTCM algorithm. For details, see Traffic Policing Classification: Classification Based on Service Flows. 2. Group CAR (rate limiting on all service flow groups provided by the same RSP) based on the packet color.	It identifies service flows through traffic classification, preparing for CAR. Flow CAR is based on the packet color that is marked based on the CIR and PIR. A packet is marked green (and will be transmitted) if the packet rate is lower than the CIR, is marked yellow (and will be transmitted) if the packet rate is higher than the CIR but is lower than or equal to the PIR, or is dropped if the packet rate is higher than the PIR. Group CAR is implemented using a single-token leaky bucket mechanism. With the single-token leaky bucket mechanism, drop thresholds can be set for different priorities of yellow packets to ensure that yellow packets with a higher priority can be preferentially transmitted. (The drop thresholds are the half of the CAR thresholds set using the CAR-threshold command). NOTE The PIR of a flow group must be higher than or equal to the sum of the CIRs of all flows. The two-level CAR mechanism guarantees the QoS for each type of service and for all services of a home user.
Uplink port of the OLT	Prevents congestion using a color-based early drop mechanism. Schedules queues (PQ scheduling) based on priorities.	The color-based early drop mechanism ensures that all green packets of a priority are transmitted. PQ scheduling ensures that packets with a higher priority preferentially occupy bandwidth resources.

 NOTE

One traffic stream can belong to only one group; one group can contain a maximum of eight service flows; all service flows of a group should belong to the same xPON port.

15.13.8.3 HQoS Implementation Principle on an xPON Board

HQoS on an xPON board supports the following scenarios:

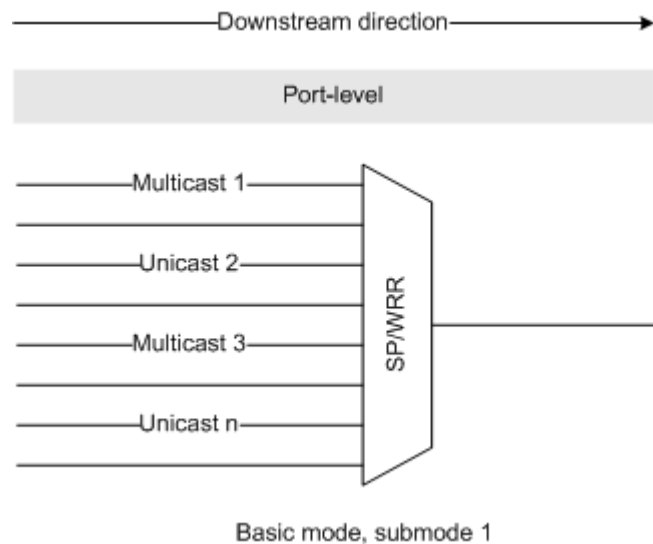
- Basic application
- Bandwidth priority
- Service priority

The following describes HQoS implementation principles in these 3 scenarios.

Basic Application Scenario

The basic mode inherits QoS functions on an xPON board. This mode has 2 sub-modes. [Figure 15-54](#) shows the HQoS implementation principle in sub-mode 1 of the basic mode.

Figure 15-54 Sub-mode 1 of basic mode

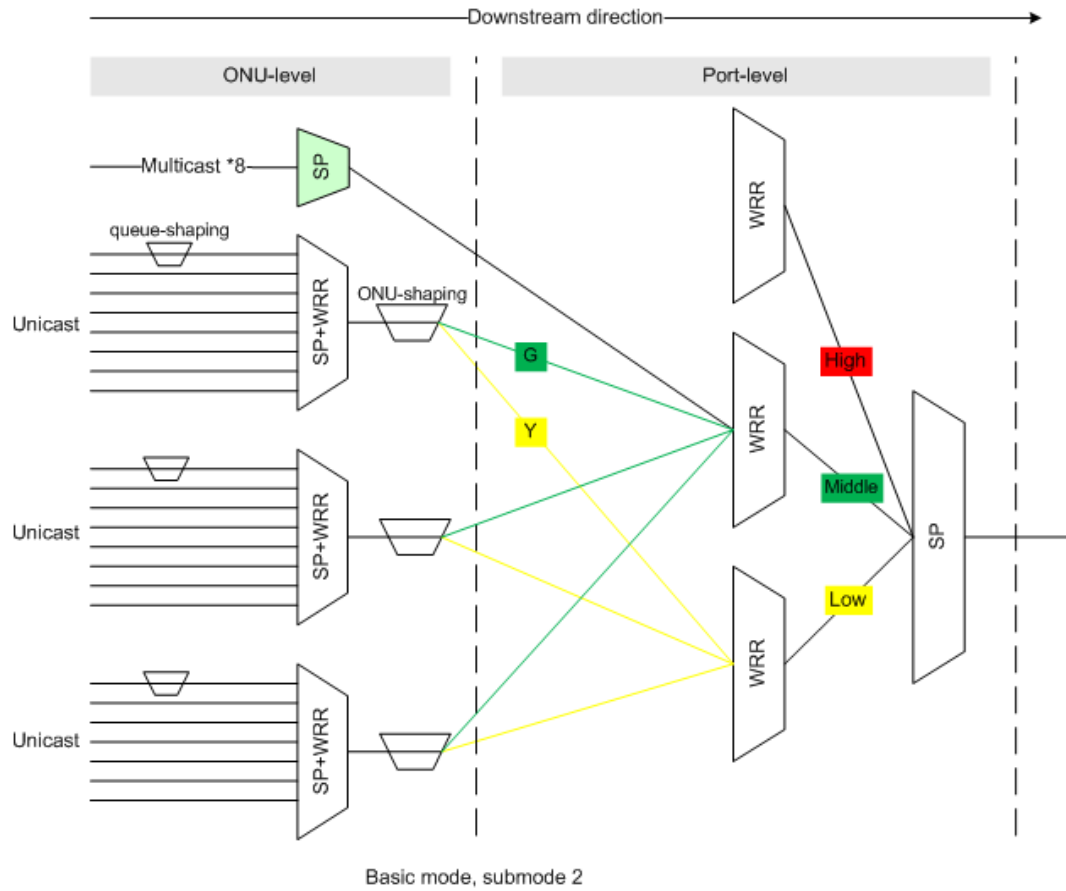


As shown in the figure, HQoS in this mode features the following:

- User unicast and multicast packets are enqueued on the PON port and are scheduled by SP and WRR by queue priorities.

When an xPON port has onu-shaping or queue-shaping, the HQoS mode is automatically switched to sub-mode 2 of the basic mode, as shown in [Figure 15-55](#).

Figure 15-55 Sub-mode 2 of basic mode

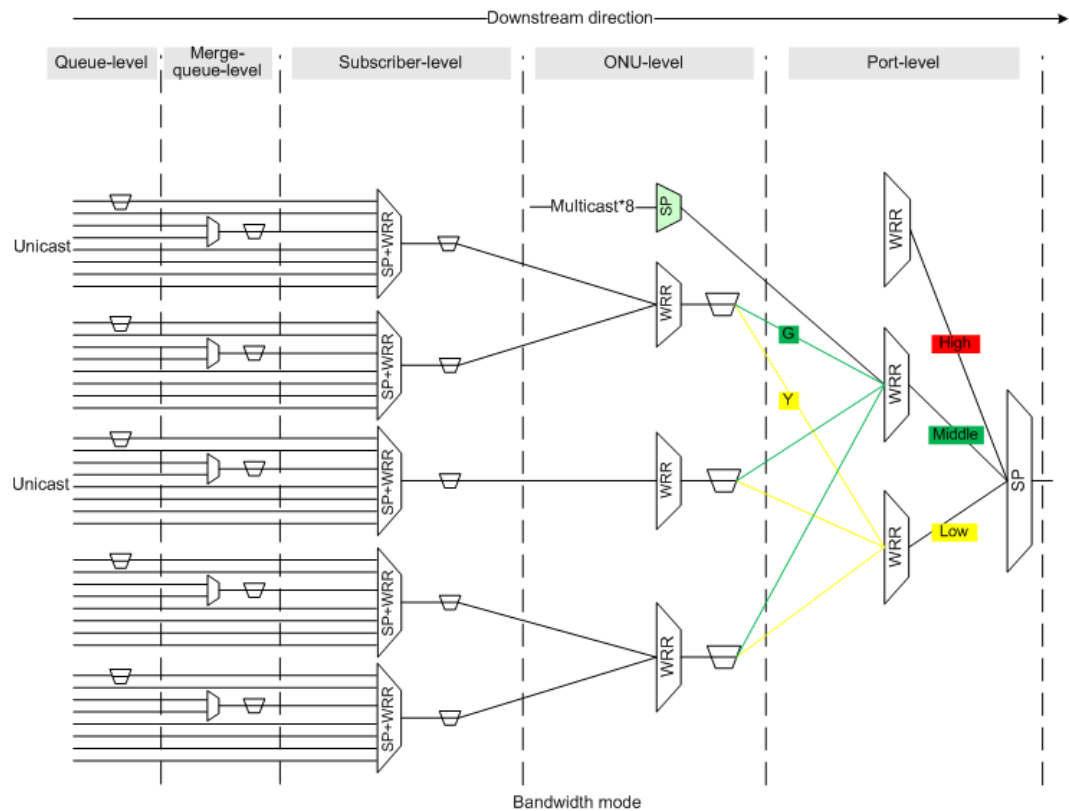


HQoS in this mode features the following:

- Multicast packets are enqueued on multicast queues.
- Unicast packets are enqueued on 8 priority queues of the ONU.
- Multicast duplication packets and unicast packets are scheduled by SP.
- 8 priority queues inside an ONU are scheduled by SP and WRR.
- Every ONU supports 8 queue shapers with only valid PIR.
- Every ONU supports a shaper with valid CIR and PIR.

Bandwidth Priority Scenario

In the bandwidth priority mode, the system preferentially assures bandwidths at all hierarchies for fair user usage, as shown in [Figure 15-56](#).

Figure 15-56 Bandwidth priority mode

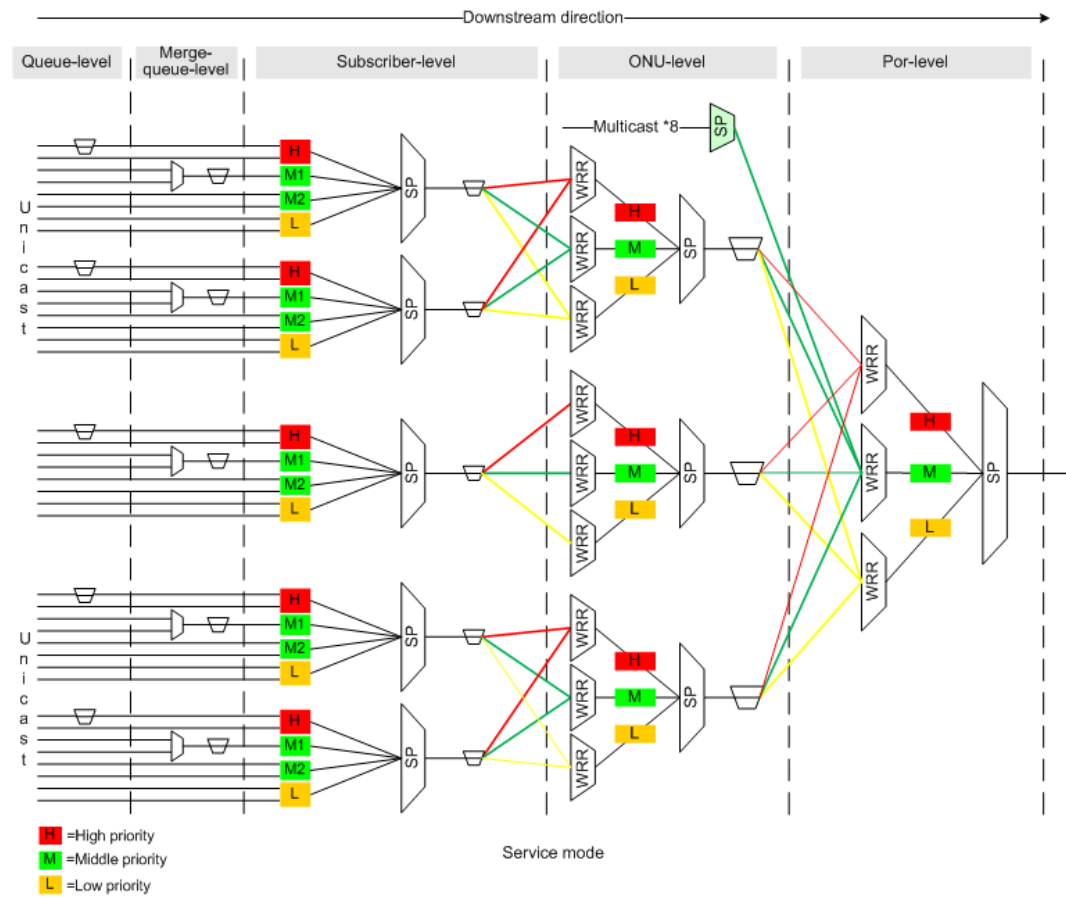
HQoS in this mode features the following:

- Multicast packets are enqueued on multicast queues.
- Unicast packets are enqueued on 8 priority queues.
- (Multicast duplication packets, ONU CIR, and) yellow ONU packets are scheduled by SP on a PON port.
- Every ONU supports a shaper with valid CIR and PIR. Between ONUs, CIRs are scheduled by RR and EIRs (PIR-CIR) are scheduled by WRR (weights are calculated by EIR or obtained from the traffic profile).
- Users under an ONU are scheduled by WRR. Between users, CIRs are scheduled by RR and EIRs (PIR-CIR) are scheduled by WRR (weights are calculated by EIR or obtained from the traffic profile).
- Every user supports a shaper with valid CIR and PIR.
- Every user supports a merged queue shaper with only valid PIR.
- 8 priority queues inside users are scheduled by SP and WRR.
- 8 priority queues for users support queue shaper with only valid PIR.

Service Priority Scenario

In the service priority scenario, the system preferentially assures services with higher priorities for service scheduling, as shown in [Figure 15-57](#).

Figure 15-57 Service priority mode



HQoS in this mode features the following:

- Multicast packets are enqueued on multicast queues.
- Unicast packets are enqueued on 8 priority queues.
- Packets with high priority, (multicast duplication packets and packets with medium priority, and) packets with low priority are scheduled by SP on a PON port.
- Every ONU supports a shaper with valid CIR and PIR.
- Packets having the same priority of different ONUs are scheduled by WRR.
- Packets having the same priority of different users under ONUs are scheduled by WRR (weights are calculated by PIR). Priorities high, medium, and low are supported for priority groups.
- Every user supports a shaper with only valid PIR.
- Every user supports a merged queue shaper with only valid PIR.
- 8 priority queues for users are scheduled by SP.
- 8 priority queues for users support queue shaper with only valid PIR.

15.13.8.4 HQoS Implementation Principle on a P2P Board

HQoS on a P2P board supports the following scenarios:

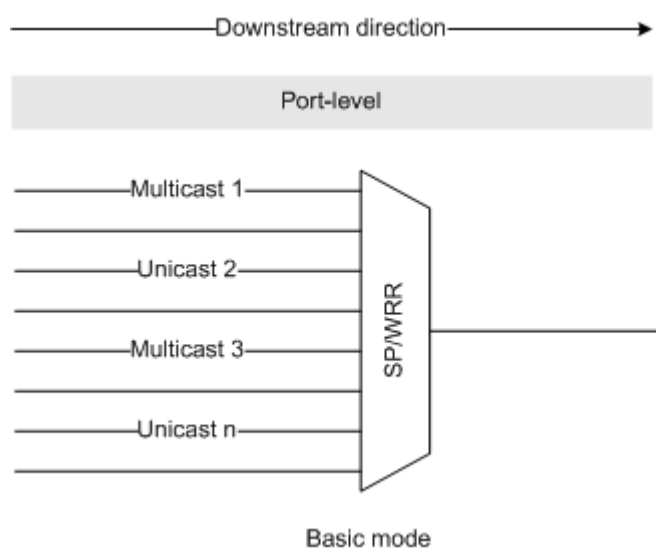
- Basic application
- Bandwidth priority
- Service priority

The following describes HQoS implementation principles in these 3 scenarios.

Basic Application Scenario

The basic mode inherits QoS functions on a P2P board. [Figure 15-58](#) shows the HQoS implementation principle in the basic mode.

Figure 15-58 Basic mode



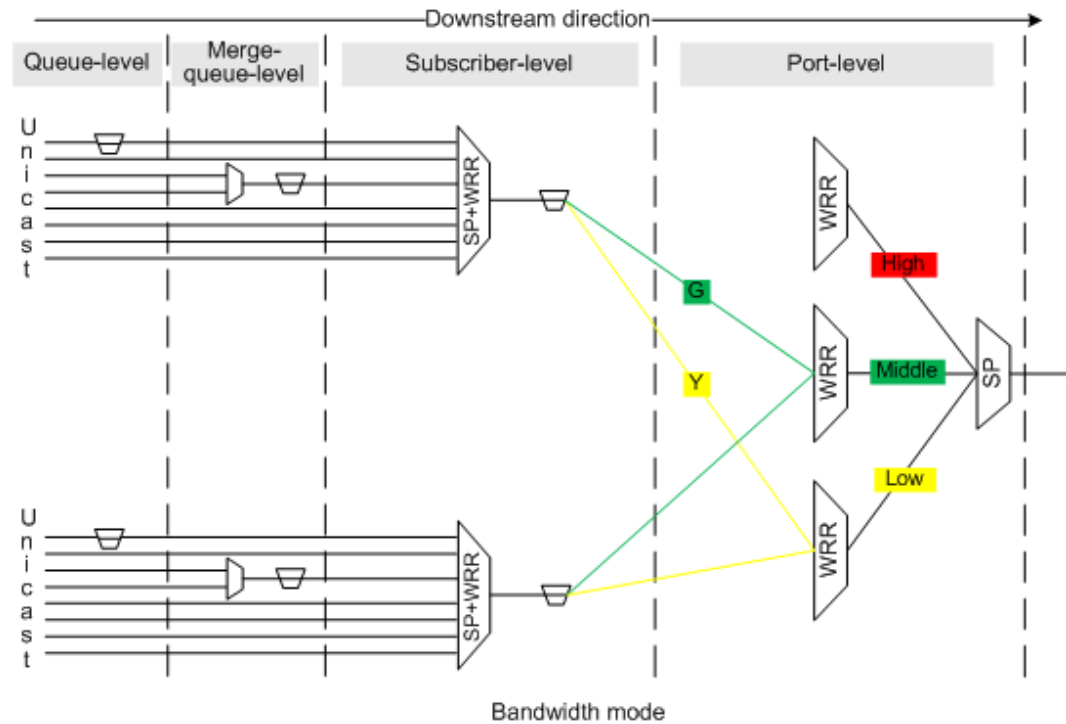
As shown in the figure, HQoS in this mode features the following:

- User unicast and multicast packets are enqueued on the Ethernet port and are scheduled by SP and WRR by queue priorities.

Bandwidth Priority Scenario

In the bandwidth priority mode, the system preferentially assures bandwidths at all hierarchies for fair usage between users, as shown in [Figure 15-59](#).

Figure 15-59 Bandwidth priority mode

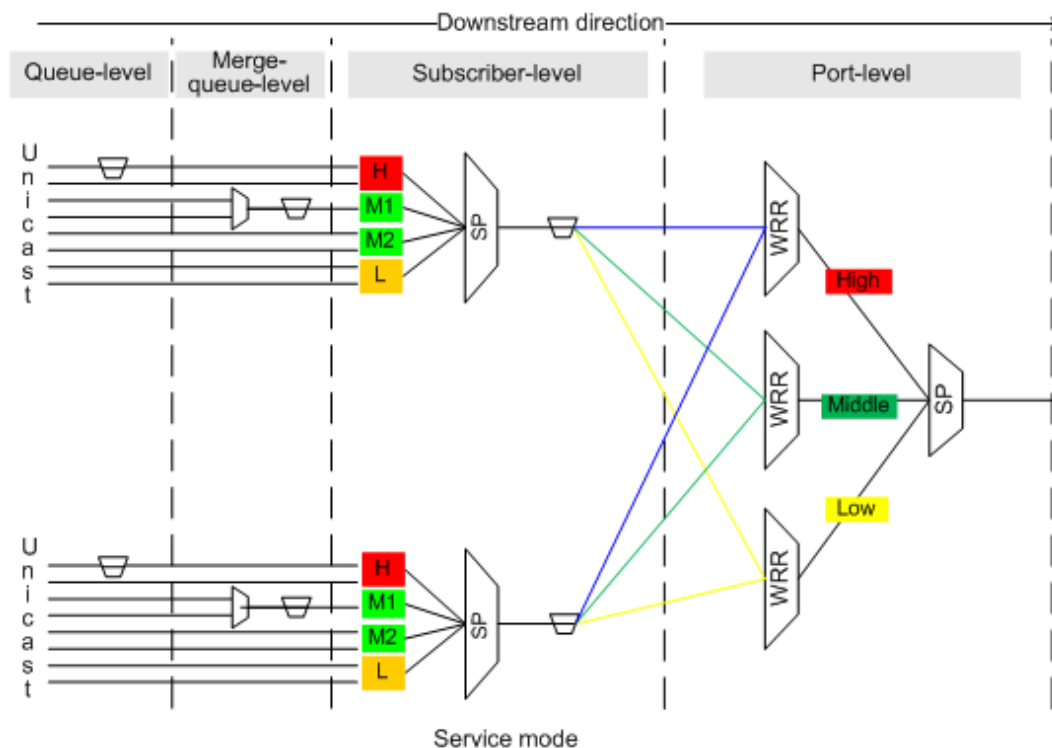


HQoS in this mode features the following:

- Unicast packets are enqueued on 8 priority queues.
- Green and yellow packets are scheduled by SP on an Ethernet port.
- Every user supports a shaper with valid CIR and PIR. Green packets with CIR are scheduled between users by RR and yellow packets with EIR (PIR-CIR) are scheduled between users by WRR (weights are calculated by EIR).
- Every user supports a merged queue shaper with only valid PIR.
- 8 priority queues inside users are scheduled by SP and WRR.
- 8 priority queues for users support queue shaper with only valid PIR.

Service Priority Scenario

In the service priority scenario, the system preferentially assures services with higher priorities for service scheduling, as shown in [Figure 15-60](#).

Figure 15-60 Service priority mode

HQoS in this mode features the following:

- Unicast packets are enqueued on 8 priority queues.
- Packets with high, medium, and low priorities are scheduled by SP on an Ethernet port.
- Every user supports a shaper with only valid PIR.
- Every user supports a merged queue shaper with only valid PIR.
- 8 priority queues for users are scheduled by SP.
- 8 priority queues for users support queue shaper with only valid PIR.

15.13.9 Networking Application of HQoS

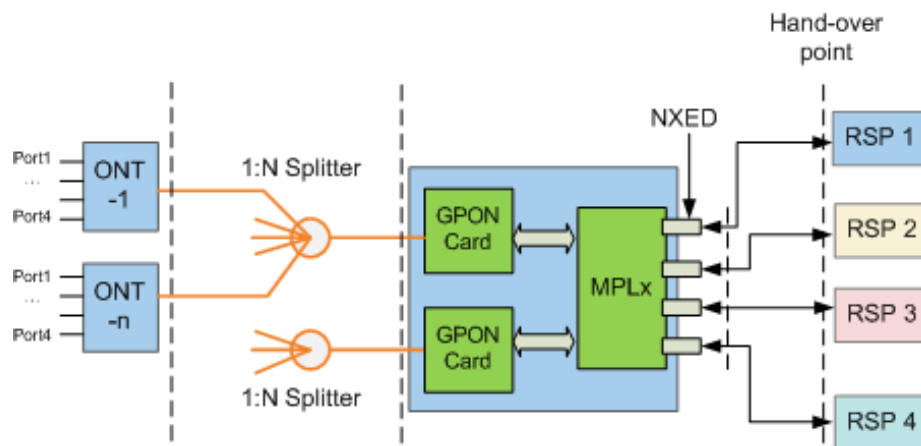
Networking Application of HQoS based on Port+VLAN

Figure 15-61 shows typical networking of hierarchical quality of service (HQoS) based on Port+VLAN. When Open Access is deployed, the carrier is only responsible for the network between the optical line terminal (OLT) and optical network terminal or ONT (including the ODN), while retail service providers (RSPs) are responsible for devices connected to the OLT and home area devices (an ONT provides 4 Ethernet UNI interfaces and each interface can be connected to one home device). The carrier network and RSP network are therefore interconnected at the uplink interface of the OLT.

Generally, RSPs use different physical uplink interfaces. Sometimes, one RSP may use multiple physical uplink interfaces. If required, link convergence can be used to converge multiple uplink ports into one logical channel.

Since RSPs use different physical interfaces, each RSP can use all VLAN IDs, and duplicated VLAN IDs can be used for different RSPs.

Figure 15-61 Networking application of HQoS based on Port+VLAN



With the preceding networking, services that a carrier provides for RSPs cover the following types and the services address the following requirements:

- Voice services with symmetric uplink and downlink bandwidth, with CIR, but without PIR (voice services have the highest priority)
- Data services with symmetric uplink and downlink bandwidth, with CIR, but without PIR
- Data services with asymmetric uplink and downlink bandwidth (usually downlink bandwidth is far higher than the uplink bandwidth), with downlink PIR but without uplink PIR
- An ONT user port can carry traffic with multiple priorities:
 - Packets with a higher priority can preferentially occupy CIR resources. If there are remaining CIR resources, packets with a lower priority can be processed.
 - If the packet rate exceeds the CIR, packets with a higher priority can preferentially occupy PIR resources.
 - If there are remaining PIR resources, packets with a lower priority can be processed.
- For each type of data service, the CIR must be guaranteed. If required, PIR resources can be used in a certain proportion according to the network congestion status.

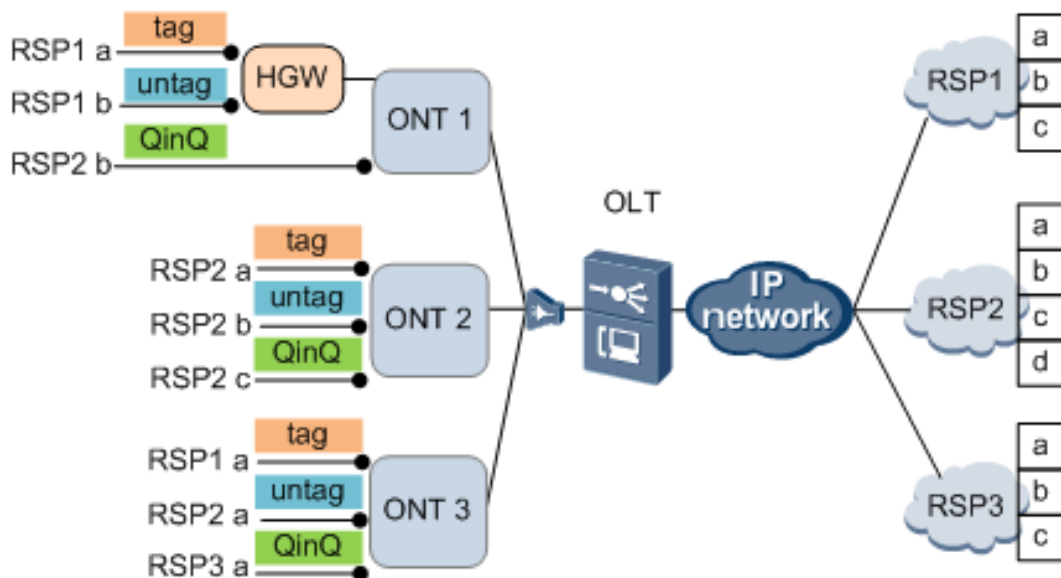
The preceding requirements can be well addressed by HQoS based on Port+VLAN.

Networking Application of CAR-Group-based HQoS

As shown in [Figure 15-62](#), users under the same ONT may belong to different RSPs. Different services of the same user are mapped to different service flows on

the OLT. Given that different service CIRs/PIRs are guaranteed, the total bandwidth of each RSP needs to be ensured and each service should be allowed to occupy the total bandwidth when a burst occurs in the traffic. To put it simply, rate limitation needs to be performed on the RSP. To do so, a group based on all service flows of an RSP can be created, and then the total bandwidth of a user can be limited by limiting the bandwidth of the group. Such is a typical application of CAR group.

Figure 15-62 Networking application of HQoS based on a CAR group

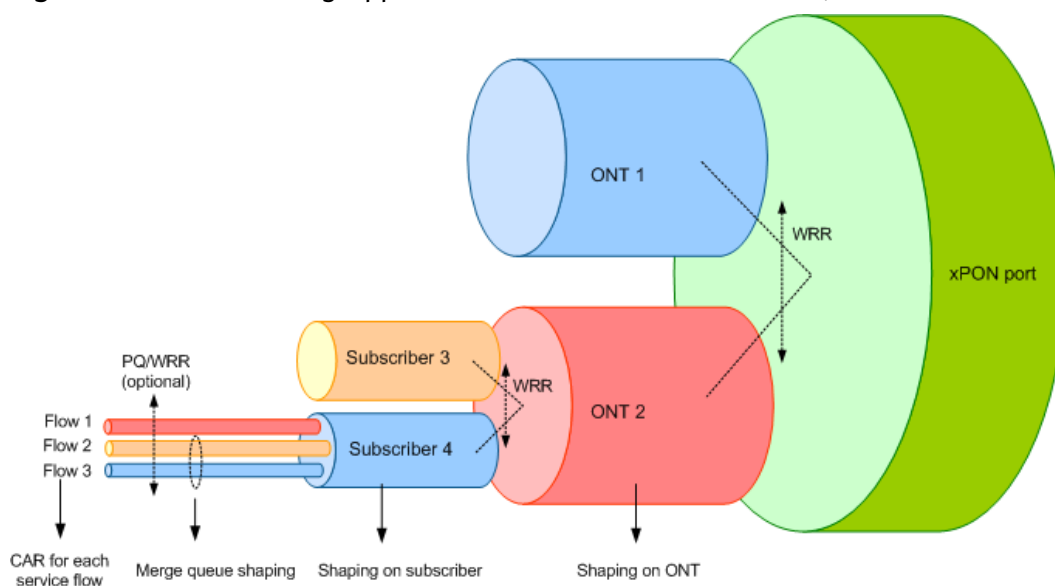


Networking Application of xPON-board-based HQoS

Figure 15-63 shows an HQoS application in the bandwidth priority mode of an xPON port. One xPON port connects to multiple ONTs, every ONT connects to multiple users, and every user is provisioned with multiple services. In this scenario, the bandwidth priority mode is used to ensure bandwidths of services at different hierarchies.

- CIR and EIR (PIR-CIR) permitted on different ONTs are allocated by preset weights.
- CIR and EIR (PIR-CIR) permitted by different users on an ONT are allocated by preset weights.
- WRR scheduling is used between users and between ONTs.

This application preferentially ensures user bandwidths for fair usage between users. It is applicable to the scenario in which the user priority is not a sensitive factor. In this case, when a network congestion occurs, the bandwidth plays an important role and users who subscribe to higher bandwidths have the high scheduling weight.

Figure 15-63 Networking Application of xPON-board-based HQoS

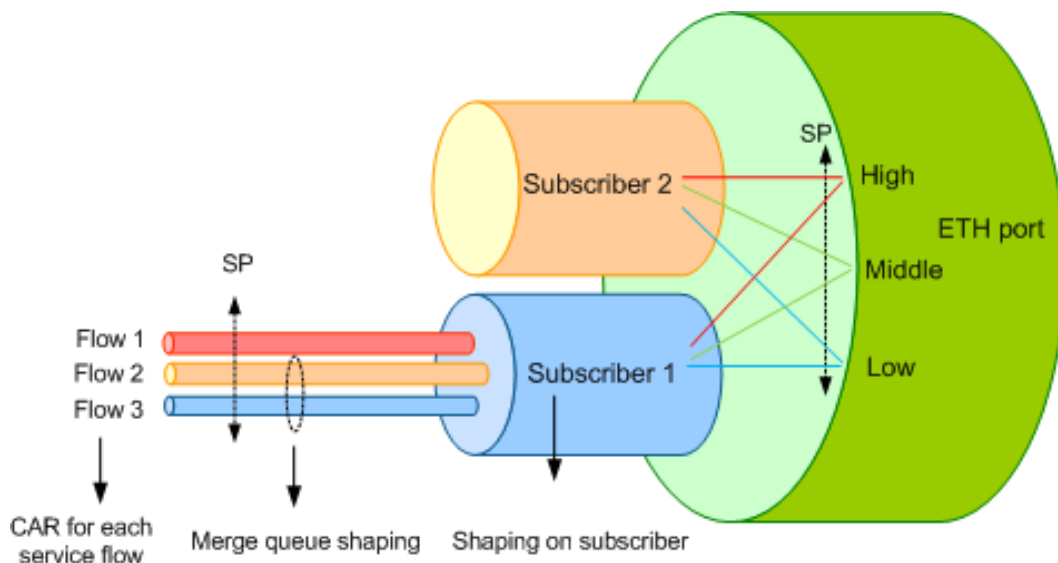
Networking application of P2P-board-based HQoS

Figure 15-64 shows an HQoS application in the service priority mode of an Ethernet port. An Ethernet port connects to multiple users and every user is provisioned with multiple services. In this scenario, the service priority mode is used to ensure services with higher priority for service scheduling.

- 8 priority queues inside users are scheduled by SP.
- Packets with different priorities between users are scheduled by SP.

This application preferentially ensures services with higher priority for service scheduling. It is applicable to the scenario in which the user priority is a sensitive factor. In this case, when a network congestion occurs, the service priority plays an important role and services with higher priority are scheduled first.

Figure 15-64 Networking application of P2P-board-based HQoS



15.13.10 Reference Standards and Protocols of HQoS

The following lists the reference standards and protocols of this feature:

RFC2698: A Two Rate Three Color Marker

15.13.11 Configuring HQoS

The hierarchical QoS (HQoS) is a QoS technology that controls user traffic on a port with finer granularity and also schedules services of a user based on the service priority. This topic describes the configuration of HQoS.

15.13.11.1 Configuring HQoS Based on Port+VLAN

This topic describes how to configure the Port+VLAN-based HQoS to ensure different CIRs and PIRs for data with different priorities in the private line services (that is, data with a higher priority preferentially occupies the bandwidth).

Prerequisites

[Networking Application of HQoS based on Port+VLAN](#) is configured.

Context

Configuration method:

1. Configure a traffic profile.
2. Use the traffic profile to limit the rate of service flows for HQoS users.
3. Limit the rate of HQoS users based on the CAR threshold and mark colors of packets having different priorities.

4. Limit rates of HQoS user groups (port+SVLAN) based on colors.

Precaution:

HQoS is implemented through user configurations. Rate limitation on HQoS user groups is implemented using the single leaky bucket algorithm and bound TrTCM traffic profile. In the configured traffic profile, CIR = PIR; otherwise, PIR prevails for rate limitation. Ensure that $PIR \geq \text{Total CIR bandwidths of all HQoS users}$.

Procedure

Step 1 Configure a traffic profile.

Run the **traffic table ip** command to configure the CIR and PIR of a service, and priority copy policy and enqueueing policy of packets.

Step 2 Configure rate limitation on Layer 2 service flows (HQoS).

Run the **service-port** command to configure an HQoS user and use the traffic profile to limit the rate of this user.

Step 3 Limit the rate of the HQoS user based on the CAR threshold and mark packet colors.

Run the **car-threshold profile** command to configure drop thresholds for packets having different priorities and mark yellow and green for packets.

Step 4 Limit the rate of an HQoS user group based on port+VLAN.

Run the **car-port portid vlan** command to specify a traffic profile to limit the rate of an HQoS user group.

NOTE

An HQoS user group can be considered as a collection of users on a specified port within a specified VLAN range.

- **inbound ip-traffic-table-index**: Sets the traffic profile index for the packet from the outside of the device to the inside of the device.
- **outbound ip-traffic-table-index**: Sets the traffic profile index for the packet from the inside of the device to the outside of the device.

Step 5 Query the configuration results.

1. Run the **display traffic table ip** command to query the traffic profile configurations.
2. Run the **display service-port** command to query the HQoS user configurations.
3. Run the **display car-threshold profile** command to query drop thresholds for packets having different priorities.
4. Run the **display car-port** command to query rate limitation configurations of an HQoS user group.

----End

Example

In an open access network, a retail service provider (RSP) leases lines and bandwidths of a carrier and uses upstream port 0/2/0 on the upstream board to provide the following data service package for FTTH users:

- Assured bandwidth 4 Mbit/s, symmetric upstream and downstream bandwidths, and permitted burst bandwidth 6 Mbit/s.
- User-side VLAN 20, network-side VLAN 100, trust user-side priority, and queue scheduling in egress queues by packet priorities.
- Priorities 0, 3, and 6 for the data service, and packets having the higher priority preferentially use the assured bandwidth and burst bandwidth.
- Packets having the lower priorities are dropped first when a congestion occurs on a port. Drop thresholds for packets having priorities 0, 3, and 6 are 12%, 50%, and 100%.
- Total upstream bandwidth of the data service on the port is 50 Mbit/s and no burst bandwidth is permitted; total downstream bandwidth is 200 Mbit/s and the permitted burst bandwidth is 250 Mbit/s.

Configure HQoS in this scenario:

```
//Configures the traffic profile for the data service of residential users by the RSP.
huawei(config)#car-threshold profile 0 cos0 12 cos3 50 cos6 100
huawei(config)#traffic table ip index 8 cir 4096 pir 6144 priority user-cos 0 priority-policy tag-In-Package

//Configures the traffic profile for an RSP leased port by the carrier.
huawei(config)#traffic table ip index 9 cir 51200 car-threshold profile 0 priority user-cos priority-policy tag-In-Package //Indicates the downstream traffic profile.
huawei(config)#traffic table ip index 10 cir 204800 pir 256000 car-threshold profile 0 priority user-cos priority-policy tag-In-Package //Indicates the upstream traffic profile.

//Indicates an HQoS user (Layer 2 service flow).
huawei(config)#service-port 1 vlan 100 eth 0/2/0 multi-service user-vlan 20 rx-cttr 8 tx-cttr 8
huawei(config)#interface eth 0/2
huawei(config-if-eth-0/2)#car-port 0 vlan 100 inbound 10 outbound 9
```

After the configuration:

- Assured bandwidth 4 Mbit/s for the user when a network congestion occurs; burst bandwidth 6 Mbit/s for the user when the network is idle.
- Packets having different priorities share the bandwidth and packets are dropped from ones having the lower priorities when a network congestion occurs.
- Total bandwidth of the data service provided on the leased port by an RSP is at the most of the bandwidth allocated by the carrier.

15.13.11.2 Configuring HQoS Based on CAR Group

This topic describes how to configure HQoS based on CAR group for ensuring the bandwidth of each service of a user and the total bandwidth of the user.

Prerequisites

HQoS networking based CAR-Group is configured.

Context

Configuration method:

1. Configure a traffic profile.
2. Use the traffic profile to limit the rate of various service flows for the same user.
3. All the user's service flows are added to a service flow group and rate limitation is performed

Precaution:

HQoS is implemented through user configurations. Rate limitation on CAR-group is implemented using the single leaky bucket algorithm and bound TrTCM traffic profile. In the configured traffic profile, CIR = PIR; otherwise, PIR prevails for rate limitation. Ensure that PIR in CAR-group $\geq$ Total CIR bandwidths of all service flows.

Procedure

Step 1 Configure a traffic profile.

Run the **traffic table ip** command to configure the CIR/PIR of a service/service group, priority copy policy, and enqueueing policy of packets.

Step 2 Configure rate limitation on service flows of a user.

Run the **service-port** command to configure different service flows for a user and use the traffic profile to limit the rate of the service flows.

Step 3 Configure CAR for an HQoS user group.

1. Create a CAR-group.

Run the **car-group** command to create a CAR group for a service port and bind a traffic profile to the CAR group.

2. Add a service port to the CAR group.

In the global config mode, run the **car-group add-member service-port** command to add a service port to the CAR group. Bandwidth of service ports in this CAR group is limited by that of the traffic profile bound to the CAR group.

NOTE

An HQoS user group can be considered as a collection of users whose port IDs and VLAN IDs are within the port+VLAN range specified by this command.

Step 4 Query the configuration results.

1. Run the **display traffic table ip** command to query the traffic profile configurations.
2. Run the **display service-port** command to query the configuration of the user's service flow.
3. Run the **display car-group** to query the configuration of the CAR group.

----End

Example

In an open access network, a retail service provider (RSP) leases lines and bandwidths of a carrier to provide the following data service packages for FTTH users:

- Internet, voice, and video services are provided through the same GPON ONT.
- User-side VLANs of the Internet, voice, and video services are 10, 20, and 30 respectively. The network-side VLANs are 100, 200, and 300.
- Different services have different bandwidth and priority requirements.
 - The downstream assured bandwidth of the Internet service is 2 Mbit/s, the burst bandwidth is 4 Mbit/s, the upstream assured bandwidth is 512 Kbit/s, and no burst bandwidth exists. The priority is 0.
 - The assured upstream and downstream bandwidths of the voice service are 512 Kbit/s and no burst bandwidth exists. The priority is 7.
 - The assured upstream and downstream bandwidths of the video service are 4 Mbit/s and the burst bandwidth is 6 Mbit/s. The priority is 4.
- The total upstream and downstream bandwidths of the home users are limited to 6 Mbit/s and 8 Mbit/s respectively.

Configure HQoS in this scenario:

```
//Traffic profile
huawei(config)#traffic table ip index 8 cir 512 priority 0 priority-policy tag-In-Package //Upstream
Internet service
huawei(config)#traffic table ip index 9 cir 2048 pir 4096 priority 0 priority-policy tag-In-Package //
Downstream Internet service
huawei(config)#traffic table ip index 10 cir 512 priority 7 priority-policy tag-In-Package //Upstream
and downstream voice service
huawei(config)#traffic table ip index 11 cir 4096 pir 6144 priority 4 priority-policy tag-In-Package //
Upstream and downstream video service
huawei(config)#traffic table ip index 20 cir 6144 priority user-cos 0 priority-policy tag-In-Package //
Total upstream bandwidth
huawei(config)#traffic table ip index 21 cir 8192 priority user-cos 0 priority-policy tag-In-Package //
Total downstream bandwidth
//Internet service flow
huawei(config)#service-port 1 vlan 100 gpon 0/1/1 ont 1 gemport 1 multi-service user-vlan 10 rx-cttr
9 tx-cttr 8
//Voice service flow
huawei(config)#service-port 2 vlan 200 gpon 0/1/1 ont 1 gemport 2 multi-service user-vlan 20 rx-cttr
10 tx-cttr 10
//Video service flow
huawei(config)#service-port 3 vlan 300 gpon 0/1/1 ont 1 gemport 3 multi-service user-vlan 30 rx-cttr
11 tx-cttr 11
CAR for an HQoS user group
huawei(config)#car-group 1 inbound traffic-table index 20 outbound traffic-table index 21
huawei(config)#car-group 1 add-member service-port 1-3
```

After the configuration:

- The bandwidth of each service of the user can be guaranteed. When the network is idle, the Internet and video service can obtain certain burst bandwidth.
- The overall bandwidth of the user is guaranteed.

15.13.11.3 Configuring HQoS for an xPON Board

In an xPON access scenario, select a proper HQoS mode according to actual QoS requirements.

Context

xPON boards support HQoS applications in the following exclusive scenarios:

- Basic application scenario: Inherits the original QoS function. It is the default mode.
- Bandwidth priority scenario: The system preferentially assures bandwidths at all hierarchies for fair user usage.
- Service priority scenario: The system preferentially assures services with higher priorities for service scheduling.
- Slice priority scenario: The system preferentially assures slices are scheduled according to their priorities.

For detailed application scenarios, see [15.13.8.3 HQoS Implementation Principle on an xPON Board](#).

Procedure

- **Configure HQoS in a basic application scenario.**
 - a. In xPON mode, run the **hqos mode basic** command to set the HQoS mode of an xPON board to basic.
 - b. Run the **display hqos mode** command to query the HQoS mode of a board.
- **Configure HQoS in a bandwidth priority scenario.**
 - a. Set the HQoS mode to **bandwidth**.

In xPON mode, run the **hqos mode bandwidth** command to set the HQoS mode of an xPON board to bandwidth priority.
 - b. Configure rate limitation on an ONT.

Run the **traffic-limit ont** command to limit the traffic of downstream packets on a specified ONT.
 - c. Configure the HQoS user profile and its attributes.
 - i. Run the **subscriber profile** command to create an HQoS user profile.
 - ii. Run the **subscriber shaping** command to limit the rate of an HQoS user.
 - d. (Optional) Configure the merged queue profile of HQoS users and its attributes.
 - i. Run the **merge queue profile** command to create a merged queue profile and bind queues.
 - ii. Run the **merge queue bind** command to bind a merged queue profile.
 - iii. Run the **merge queue shaping** command to set rate limitation on the merged queue.
 - e. Add an HQoS user and limit the rate of this user.
 - i. Run the **subscriber add** command to bind a user to the HQoS user profile and limit the rate of this user.
 - ii. Run the **subscriber member add** command to add a service port as an HQoS user.

- f. Query the configuration.
 - Run the **display hqos mode** command to query the HQoS mode of a board.
 - Run the **display subscriber** command to query the HQoS user information.
 - (Optional) Run the **display merge queue profile** command to query the merged queue information about an HQoS user.
- **Configure HQoS in a service priority scenario.**

 NOTE

HQoS configuration in this scenario is the same as that in the bandwidth priority scenario. The only difference is that HQoS mode in this scenario is set to **service**.

- a. Set the HQoS mode to **service**.
In xPON mode, run the **hqos mode service** command to set the HQoS mode of an xPON board to service priority.
- b. Configure rate limitation on an ONT.
Run the **traffic-limit ont** command to limit the traffic of downstream packets on a specified ONT.
- c. Configure the HQoS user profile and its attributes.
 - i. Run the **subscriber profile** command to create an HQoS user profile.
 - ii. Run the **subscriber shaping** command to limit the rate of an HQoS user.
- d. (Optional) Configure the merged queue profile of HQoS users and its attributes.
 - i. Run the **merge queue profile** command to create a merged queue profile and bind queues.
 - ii. Run the **merge queue bind** command to bind a merged queue profile.
 - iii. Run the **merge queue shaping** command to set rate limitation on the merged queue.
- e. Add an HQoS user and limit the rate of this user.
 - i. Run the **subscriber add** command to bind a user to the HQoS user profile and limit the rate of this user.
 - ii. Run the **subscriber member add** command to add a service port as an HQoS user.
- f. Query the configuration.
 - Run the **display hqos mode** command to query the HQoS mode of a board.
 - Run the **display subscriber** command to query the HQoS user information.
 - (Optional) Run the **display merge queue profile** command to query the merged queue information about an HQoS user.

----End

Example

The following is an example of the configurations used to plan 3 ONTs under GPON port 0/1/0:

- Set the bandwidth priority mode.
- Configure a user for ONT 1 (ONT ID 1).
 - Configure 2 service flows: the rate of one service flow with index 100 and priority 4 is limited to 600 Mbit/s and that of the other one with index 101 and priority 0 is limited to 150 Mbit/s.
 - Limit the shaping rate of users to 800 Mbit/s (traffic profile index 10, CIR 400 Mbit/s, and PIR 800 Mbit/s).
 - Limit the shaping rate of ONT 1 to 1 Gbit/s (traffic profile index 11, CIR 400 Mbit/s, and PIR 1 Gbit/s).
- Configure ONT 2 (ONT ID 2) in the same way as ONT 1 (the indexes of the two service flows are 102 and 103).
- Configure 2 users for ONT 3 (ONT ID 3) under 2 GE ports on the ONT.
 - Configure 2 service flows for user 1 (ID 2): the rate of one service flow with index 102 and priority 4 is limited to 600 Mbit/s and that of the other one with index 103 and priority 0 is limited to 150 Mbit/s.
 - Limit the shaping rate of user 1 to 800 Mbit/s (traffic profile index 12, CIR 600 Mbit/s, and PIR 800 Mbit/s).
 - Configure 2 service flows for user 2 (ID 3): the rate of one service flow with index 104 and priority 4 is limited to 600 Mbit/s and that of the other one with index 105 and priority 0 is limited to 150 Mbit/s.
 - Limit the shaping rate of user 2 to 1 Gbit/s (CIR 400 Mbit/s and PIR 1 Gbit/s).
 - Limit the shaping rate of ONT 3 to 2 Gbit/s (traffic profile index 13, CIR 1.2 Gbit/s, and PIR 2 Gbit/s).

The configuration procedures are as follows:

```
//Configure the HQoS mode.
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#hqos mode bandwidth
huawei(config-if-gpon-0/1)#quit

//Configure the traffic profile.
huawei(config)#traffic table ip index 10 cir 409600 pir 819600 priority user-cos 0 priority-policy tag-In-package
huawei(config)#traffic table ip index 11 cir 409600 pir 1024000 priority user-cos 0 priority-policy tag-In-package
huawei(config)#traffic table ip index 12 cir 614400 pir 819600 priority user-cos 0 priority-policy tag-In-package
huawei(config)#traffic table ip index 13 cir 1228800 pir 2048000 priority user-cos 0 priority-policy tag-In-package

//Configure the profile for HQoS users under ONT 1 and ONT 2.
huawei(config)#subscriber profile profile-id 1
huawei(config-subscriber-profile-1)#subscriber shaping outbound traffic-table index 10
huawei(config-subscriber-profile-1)#quit

//Add HQoS users under ONT 1 and ONT 2.
huawei(config)#subscriber add 0/1/0 ont 1 1 profile-id 1
huawei(config)#subscriber member add 0/1/0 ont 1 1 service-port 100
huawei(config)#subscriber member add 0/1/0 ont 1 1 service-port 101
huawei(config)#subscriber add 0/1/0 ont 2 1 profile-id 1
```

```
huawei(config)#subscriber member add 0/1/0 ont 2 1 service-port 102
huawei(config)#subscriber member add 0/1/0 ont 2 1 service-port 103

//Limit rates of ONT 1 and ONT 2.
huawei(config)#traffic-limit ont 0/1/0 1 down-stream traffic-table index 11
huawei(config)#traffic-limit ont 0/1/0 2 down-stream traffic-table index 11

//Configure the profile for HQoS user 1 under ONT 3.
huawei(config)#subscriber profile profile-id 2
huawei(config-subscriber-profile-2)#subscriber shaping outbound traffic-table index 12
huawei(config-subscriber-profile-2)#quit

//Add HQoS user 1 under ONT 3.
huawei(config)#subscriber add 0/1/0 ont 3 2 profile-id 2
huawei(config)#subscriber member add 0/1/0 ont 2 2 service-port 102
huawei(config)#subscriber member add 0/1/0 ont 2 2 service-port 103

//Configure the profile for HQoS 2 under ONT 3.
huawei(config)#subscriber profile profile-id 3
huawei(config-subscriber-profile-3)#subscriber shaping outbound traffic-table index 11
huawei(config-subscriber-profile-3)#quit

//Add HQoS user 3 under ONT 3.
huawei(config)#subscriber add 0/1/0 ont 3 3 profile-id 3
huawei(config)#subscriber member add 0/1/0 ont 3 3 service-port 104
huawei(config)#subscriber member add 0/1/0 ont 3 3 service-port 105

//Limit the rate of ONT 3.
huawei(config)#traffic-limit ont 0/1/0 3 down-stream traffic-table index 13
```

Follow-up Procedure

Expected results:

- The CIR ratio of ONT 1, ONT 2, and ONT 3 is 1:1:3, and the total CIR of these 3 ONTs is 2.0 Gbit/s, which does not exceed the downstream bandwidth of a PON port.
- The EIR (PIR-CIR) ratio of ONT 1, ONT 2, and ONT 3 is 3:3:4, and the remaining bandwidth of a PON port can be used by EIR.
- ONT 1 permits bandwidth about 550 Mbit/s, containing CIR 400 Mbit/s for packets with priority 4 and EIR 150 Mbit/s for packets with priority 4.
- ONT 2 permits bandwidth about 550 Mbit/s, containing CIR 400 Mbit/s for packets with priority 4 and EIR 150 Mbit/s for packets with priority 4.
- ONT 3 permits bandwidth about 1400 Mbit/s:
 - The CIR ratio of user 1 and user 2 is 6:4 and EIR ratio is 1:3.
 - Packet bandwidth of user 1 is 700 Mbit/s, containing CIR 600 Mbit/s for packets with priority 4 and EIR 100 Mbit/s for packets with priority 0.
 - Packet bandwidth of user 2 is 700 Mbit/s, containing CIR 400 Mbit/s for packets with priority 4 and EIR 300 Mbit/s for packets with priority 4 (200 Mbit/s) and with priority 0 (100 Mbit/s).

15.13.11.4 Configuring HQoS for a P2P Board

In a P2P access scenario, select a proper HQoS mode according to actual QoS requirements.

Context

P2P boards support HQoS applications in the following exclusive scenarios:

- Basic application scenario: Inherits the original QoS function. It is the default mode.
- Bandwidth priority scenario: The system preferentially assures bandwidths at all hierarchies for fair user usage.
- Service priority scenario: The system preferentially assures services with higher priorities for service scheduling.

For detailed application scenarios, see [15.13.8.4 HQoS Implementation Principle on a P2P Board](#).

Procedure

- **Configure HQoS in a basic application scenario.**
 - a. In ETH mode, run the **hqos mode basic** command to set the HQoS mode of an P2P board to basic.
 - b. Run the **display hqos mode** command to query the HQoS mode of a board.
- **Configure HQoS in a bandwidth priority scenario.**
 - a. Set the HQoS mode to **bandwidth**.

In ETH mode, run the **hqos mode bandwidth** command to set the HQoS mode of an P2P board to bandwidth priority.
 - b. Configure rate limitation for an Ethernet port.

The **line-rate** command is used to limit the traffic rate of a specified Ethernet port.
 - c. Configure the HQoS user profile and its attributes.
 - i. Run the **subscriber profile** command to create an HQoS user profile.
 - ii. Run the **subscriber shaping** command to limit the rate of an HQoS user.
 - d. (Optional) Configure the merged queue profile of HQoS users and its attributes.
 - i. Run the **merge queue profile** command to create a merged queue profile and bind queues.
 - ii. Run the **merge queue bind** command to bind a merged queue profile.
 - iii. Run the **merge queue shaping** command to set rate limitation on the merged queue.
 - e. Add an HQoS user and limit the rate of this user.
 - i. Run the **subscriber add** command to bind a user to the HQoS user profile and limit the rate of this user.
 - ii. Run the **subscriber member add** command to add a service port as an HQoS user.
 - f. Query the configuration.

- Run the **display hqos mode** command to query the HQoS mode of a board.
 - Run the **display subscriber** command to query the HQoS user information.
 - (Optional) Run the **display merge queue profile** command to query the queue group information about an HQoS user.
- **Configure HQoS in a service priority scenario.**

 NOTE

HQoS configuration in this scenario is the same as that in the bandwidth priority scenario. The only difference is that HQoS mode in this scenario is set to **service**.

- a. Set the HQoS mode to **service**.

In ETH mode, run the **hqos mode service** command to set the HQoS mode of an P2P board to service priority.

- b. Configure rate limitation for an Ethernet port.

The **line-rate** command is used to limit the traffic rate of a specified Ethernet port.

- c. Configure the HQoS user profile and its attributes.
 - i. Run the **subscriber profile** command to create an HQoS user profile.
 - ii. Run the **subscriber shaping** command to limit the rate of an HQoS user.
- d. (Optional) Configure the merged queue profile of HQoS users and its attributes.
 - i. Run the **merge queue profile** command to create a merged queue profile and bind queues.
 - ii. Run the **merge queue bind** command to bind a merged queue profile.
 - iii. Run the **merge queue shaping** command to set rate limitation on the merged queue.
- e. Add an HQoS user and limit the rate of this user.
 - i. Run the **subscriber add** command to bind a user to the HQoS user profile and limit the rate of this user.
 - ii. Run the **subscriber member add** command to add a service port as an HQoS user.
- f. Query the configuration.
 - Run the **display hqos mode** command to query the HQoS mode of a board.
 - Run the **display subscriber** command to query the HQoS user information.
 - (Optional) Run the **display merge queue profile** command to query the queue group information about an HQoS user.

----End

Example

The following is an example of the configurations used to plan 2 users under port 0/2/0 on the P2P board:

- Set the service priority mode.
- Limit the rate in the outbound direction of the port to 800 Mbit/s.
- Configure 3 service flows for user 1 (ID 1): the rate of one service flow with index 100 and priority 5 is limited to 300 Mbit/s, one with index 101 and priority 4 is limited to 250 Mbit/s, and one with index 102 and priority 0 is limited to 100 Mbit/s.
- Limit the shaping rate of user 1 to 600 Mbit/s (traffic profile index 10, CIR 400 Mbit/s, and PIR 600 Mbit/s).
- Limit the merged rate on queues 4 and 5 of user 1 to 500 Mbit/s (traffic profile index 11, CIR 300 Mbit/s, and PIR 500 Mbit/s).
- Configure 2 service flows for user 2 (ID 2): the rate of one service flow with index 103 and priority 5 is limited to 300 Mbit/s and that of the other one with index 104 and priority 4 is limited to 250 Mbit/s.
- Limit the shaping rate of user 2 to 400 Mbit/s (traffic profile index 12, CIR 300 Mbit/s, and PIR 400 Mbit/s).

The configuration procedures are as follows:

```
//Configure the HQoS mode.
huawei(config)#interface gpon 0/2
huawei(config-if-eth-0/2)#hqos mode service
  This operation will reset the board, which may take several minutes. Are you
sure to continue ? (y/n)[n]:y
huawei(config-if-eth-0/2)#quit

//Configure the traffic profile.
huawei(config)#traffic table ip index 10 cir 409600 pir 614400 priority user-cos 0 priority-policy tag-In-
package
huawei(config)#traffic table ip index 11 cir 307200 pir 512000 priority user-cos 0 priority-policy tag-In-
package
huawei(config)#traffic table ip index 12 cir 307200 pir 409600 priority user-cos 0 priority-policy tag-In-
package

//Configure the profile for HQoS user 1.
huawei(config)#subscriber profile profile-id 1
huawei(config-subscriber-profile-1)#subscriber shaping outbound traffic-table index 10
huawei(config-subscriber-profile-1)#merge queue bind profile 3 //Binds the default profile 3 and uses
queues 4 and 5.
huawei(config-subscriber-profile-1)#merge queue shaping outbound traffic-table index 11
huawei(config-subscriber-profile-1)#quit

//Configure the profile for HQoS user 2.
huawei(config)#subscriber profile profile-id 2
huawei(config-subscriber-profile-2)#subscriber shaping outbound traffic-table index 12
huawei(config-subscriber-profile-2)#quit

//Add HQoS user 1.
huawei(config)#subscriber add 0/2/0 1 profile-id 1
huawei(config)#subscriber member add 0/2/0 1 service-port 100
huawei(config)#subscriber member add 0/2/0 1 service-port 101
huawei(config)#subscriber member add 0/2/0 1 service-port 102

//Add HQoS user 2.
huawei(config)#subscriber add 0/2/0 2 profile-id 2
huawei(config)#subscriber member add 0/2/0 2 service-port 103
huawei(config)#subscriber member add 0/2/0 2 service-port 104
```

```
//Limit the rate of Ethernet port 0/2/0.  
huawei(config)#line-rate outbound 819200
```

15.14 End-to-End QoS

15.14.1 FTTH End-to-End QoS Policy

The FTTH end-to-end (E2E) QoS solution uses the differentiated service (DiffServ) model. In this solution, QoS parameters are carried in each packet header to ensure QoS guarantees. The following describes upstream and downstream FTTH E2E QoS applications.

Upstream E2E QoS

Upstream E2E QoS is shown in the [Figure 15-65](#) and [Table 15-15](#).

1. QoS policy on the ONT.
 - a. An ONT classifies traffic based on user ports or user-side VLAN IDs to distinguish services.
 - b. Re-marks the 802.1p priority for service packets.
 - c. Based on packet priorities, the ONT arranges packets into different priority queues by using PQ scheduling. This ensures that services with higher QoS requirements are forwarded preferentially.
 - d. Limits the upstream traffic on user-side ports. (optional).
2. QoS policy on the OLT.
 - a. Classifies traffic based on VLAN IDs and the 802.1p priority
 - b. Trusts the user-side priority or re-marks the 802.1p priority for service packets.
 - c. Implements priority scheduling and congestion management based on the 802.1p priority.
 - d. Implements DBA to limit the ONUs upstream bandwidth.
 - e. (Optional) limits upstream traffic bandwidth based on service flows.
3. The layer 2 metropolitan area network (MAN) between the OLT and the BRAS/service router (SR) implements priority scheduling based on the 802.1p priority of service packets.
4. Traffic classification is enabled on the ingress of the BRAS/SR to identify 802.1p values of different packets and re-mark packets according to the upper network.
 - When the upper-layer network is a native IP Layer 3 network, the BRAS/SR maps the 802.1p priority to the ToS/DSCP value in the IP header.
 - When the upper-layer network is an MPLS VPN, the BRAS/SR maps the 802.1p priority to MPLS EXP.(Optional) The BRAS/SR can also limit bandwidth for upstream user traffic based on service flows.

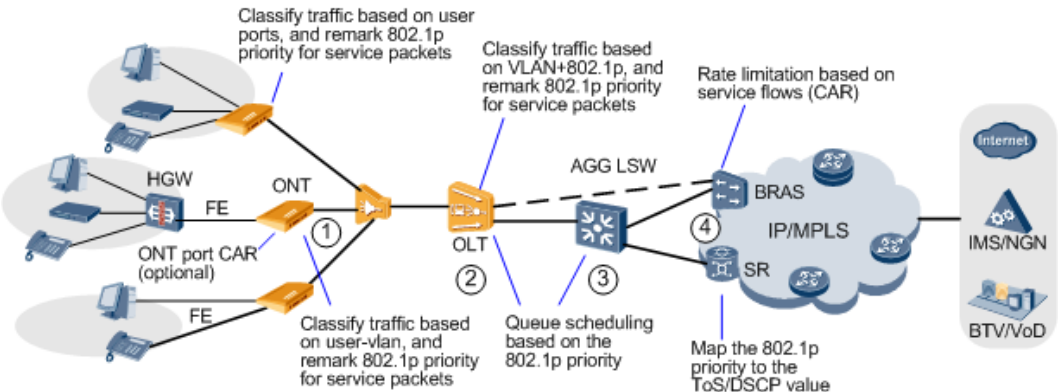
5. Upper-level networks of the BRAS/SR implement traffic classification, congestion management, and congestion avoidance based on ToS/DSCP in the IP header or the MPLS EXP priority.

Table 15-15 Upstream E2E QoS policy

Device	QoS policy			
	Traffic classification	Priority processing	Traffic policing	Queue scheduling
ONT	- Based on user ports - Based on user-side VLAN IDs	Re-marks the 802.1p priority	(Optional) Limits the upstream traffic on user-side ports.	PQ schedule based on 802.1p priority
OLT	VLAN +802.1p priority	- Trusts the user-side priority - Re-marks the 802.1p priority	Implements DBA to limit the ONUs upstream bandwidth. (Optional) Limits upstream traffic bandwidth based on service flows.	PQ schedule based on 802.1p priority
L2 MAN	N/A	N/A	N/A	PQ schedule based on 802.1p priority of service packets

Device	QoS policy			
	Traffic classification	Priority processing	Traffic policing	Queue scheduling
BRAS /SR	Based on VLAN	- Maps the 802.1p priority to the ToS/DSCP value in the IP header when upper-layer is IP L3 network. - Maps the 802.1p priority to MPLS EXP when upper-layer is MPLS VPN.	(Optional) Limits bandwidth for upstream user traffic based on service flows.	N/A
L3 network (IP/MPLS)	IP network: based on ToS/DSCP MPLS network: based on MPLS EXP	Trusts priority of packets	N/A	PQ

Figure 15-65 FTTH E2E QoS networking



Downstream E2E QoS

Downstream E2E QoS is shown in the [Figure 15-65](#) and [Table 15-16](#).

1. The packets of the IPTV, VoIP, and broadband Internet services are assigned different DSCP/MPLS EXP values based on priority requirements using related egress switches or provider edge (PE) devices. Core networks and backbone networks perform priority-based queue scheduling according to DSCP/MPLS EXP.
2. (Optional) Downstream packets are transmitted to edge BRAS/SR of the Layer 3 network through core networks and backbone networks. The BRAS/SR maps IP DSCP or MPLS EXP of packets to the VLAN 802.1p priority. The BRAS/SR can also limit bandwidth for downstream user traffic based on service flows.
 - For broadband Internet services in PPPoE mode, the BRAS controls the access bandwidth of each broadband user based on the rate authorized by the RADIUS server. For example, the rate can be 512 Kbit/s, 1 Mbit/s, or 2 Mbit/s.
 - Due to traffic jitter of the server or network, queue shaping is necessary for IPTV services on service routers.
3. Metropolitan networks and Layer 2 access networks downstream to the BRAS/SR implement priority scheduling based on the packet 802.1p priority.
4. (Optional) The OLT classifies traffic based on VLAN IDs and the 802.1p priority, and it trusts the network-side priority or re-marks the 802.1p priority for service packets. It implements priority scheduling and congestion management based on the 802.1p priority. It can limit downstream traffic bandwidth based on service flows.
5. (Optional) The ONT trusts the network-layer 802.1p priority and implements priority scheduling based on the 802.1p priority. The ONT can also limit downstream traffic bandwidth based on user-side ports.

Table 15-16 Downstream E2E QoS policy

Device	QoS policy			
	Traffic classification	Priority processing	Traffic policing	Queue scheduling
L3 network (IP/MPLS)	N/A	Assign different priority values based on service types and networks. - IP network: assign different IP ToS/DSCP value - MPLS network: assign different MPLS EXP value	N/A	PQ
BRAS/SR	N/A	- Maps the ToS/DSCP value to 802.1p priority when upper-layer is IP L3 network. - Maps the MPLS EXP to 802.1p priority when upper-layer is MPLS network.	(Optional) Limits bandwidth for downstream user traffic based on service flows. - HSI service in PPPoE mode: CAR - IPTV service: queue shaping	N/A
L2 MAN	N/A	N/A	N/A	PQ schedule based on 802.1p priority of service packets
OLT	VLAN +802.1p priority	- Trusts the network-layer 802.1p priority - Re-marks 802.1p priority	(Optional) Limits downstream traffic bandwidth based on service flows.	PQ schedule based on 802.1p priority

Device	QoS policy			
	Traffic classification	Priority processing	Traffic policing	Queue scheduling
ONT	N/A	Trusts the network-layer 802.1p priority	(Optional) Limits downstream traffic bandwidth based on user-side ports.	PQ schedule based on 802.1p priority

15.14.2 FTTB/FTTC End-to-End QoS Policy

The FTTB/FTTC E2E QoS solution uses the DiffServ model. In this solution, QoS parameters are carried in each packet header to ensure QoS guarantees. The following describes upstream and downstream E2E QoS applications for FTTB/FTTC.

Upstream E2E QoS

Figure 15-66 shows the upstream E2E QoS.

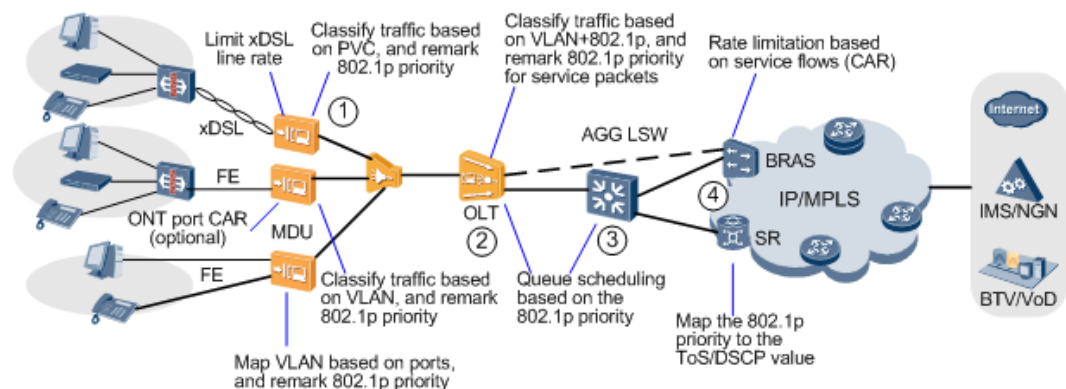
- QoS policy on the MDU.
 - An MDU classifies traffic based on the user port or user-side VLAN IDs/PVC (xDSL access) to distinguish services
 - Re-marks the 802.1p priority for service packets.
 - Based on packet priorities, the MDU arranges packets into different priority queues by using PQ scheduling. This operation ensures that services with high QoS are forwarded preferentially.
 - (Optional) Limits the upstream traffic on user-side ports.
- QoS policy on the OLT.
 - Classifies traffic based on VLAN IDs and the 802.1p priority
 - Trusts the user-side priority or re-marks the 802.1p priority for service packets.
 - Implements priority scheduling and congestion management based on the 802.1p priority.
 - Implements DBA to limit the ONUs upstream bandwidth.
 - (Optional) Limits upstream traffic bandwidth based on service flows.
- The layer 2 metropolitan area network (MAN) between the OLT and the BRAS/service router (SR) implements priority scheduling based on the 802.1p priority of service packets.
- Traffic classification is enabled on the ingress of the BRAS/SR to identify 802.1p values of different packets and re-mark packets according to the upper network.

- When the upper-layer network is a native IP Layer 3 network, the BRAS/SR maps the 802.1p priority to the ToS/DSCP value in the IP header.
- When the upper-layer network is an MPLS VPN, the BRAS/SR maps the 802.1p priority to MPLS EXP.

(Optional) The BRAS/SR can also limit bandwidth for upstream user traffic based on service flows

5. Upper-level networks of the BRAS/SR implement traffic classification, congestion management, and congestion avoidance based on ToS/DSCP in the IP header or the MPLS EXP priority.

Figure 15-66 FTTB/FTTC E2E QoS networking



Downstream E2E QoS

Figure 15-66 shows the downstream E2E QoS.

1. The packets of the IPTV, VoIP, and broadband Internet services are assigned different DSCP/MPLS EXP values based on priority requirements using related egress switches or provider edge (PE) devices. Core networks and backbone networks perform priority-based queue scheduling according to DSCP/MPLS EXP.
2. (Optional) Downstream packets are transmitted to edge BRAS/SR of the Layer 3 network through core networks and backbone networks. The BRAS/SR maps IP DSCP or MPLS EXP of packets to the VLAN 802.1p priority. The BRAS/SR can also limit bandwidth for downstream user traffic based on service flows.
 - For broadband Internet services in PPPoE mode, the BRAS controls the access bandwidth of each broadband user based on the rate authorized by the RADIUS server. For example, the rate can be 512 Kbit/s, 1 Mbit/s, or 2 Mbit/s.
 - Due to traffic jitter of the server or network, queue shaping is necessary for IPTV services on service routers.
3. Metropolitan networks and Layer 2 access networks downstream to the BRAS/SR implement priority scheduling based on the packet 802.1p priority.
4. (Optional) The OLT classifies traffic based on VLAN IDs and the 802.1p priority, and it trusts the network-side priority or re-marks the 802.1p priority for service packets. It implements priority scheduling and congestion

management based on the 802.1p priority. It can limit downstream traffic bandwidth based on service flows.

5. (Optional) The MDU trusts the network-layer 802.1p priority and implements priority scheduling based on the 802.1p priority. The user-side port on the MDU limits bandwidth for downstream traffic.

15.14.3 QoS Solution for FTTH

Basic Principles of QoS for FTTH

1. The ingress (upstream port on ONT/downstream port on OLT) of an FTTx access network classifies traffic and re-marks the 802.1p priority for packets. The access device (MA5800) implements congestion control in PQ scheduling mode based on the 802.1p priority.
2. Service packets on an ONT are differentiated based on VLAN IDs.
 - In a GPON system, GEM port mapping is implemented based on VLAN IDs to specify whether different traffic packets are transmitted to different GEM ports or to the same GEM port. Each ONT uses a T-CONT.
3. DBA profiles are configured based on users' bandwidth types. During service provisioning, relevant DBA profiles are selected based on the bandwidth types that users apply for. The recommended DBA type is type 3 (assured bandwidth+maximum bandwidth). Upstream priority of the T-CONT for an ONT follows 802.1p-based priority scheduling.
4. It is recommended to use the same VLAN configuration for all ONTs and implement VLAN translation on the OLT. This operation ensures that the same type of ONTs having the same bandwidth types use the same line profile and service profile.
5. It is recommended to limit service flow bandwidth on the BRAS or service router (SR) but not on the access device.

 NOTE

The ONT can be configured to limit bandwidth for user-side ports, and the OLT can be configured to rate limit service flows based on traffic profiles.

Recommended QoS Plan for FTTH

The following table provides details about the recommended QoS plan for FTTH with respect to traffic classification, priority marking, and queue scheduling policies.

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

 NOTE

The service priorities in this table are recommended values only. Configure the service priorities according to the operator's actual network plan.

The following table provides details about the recommended QoS plan for FTTH with respect to traffic policing and DBA policies.

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port (only for GPON)	11 [Remark 1]	12	13	14
TCONT (only for GPON)	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is greater than or equal to the maximum bandwidth that users apply.			

Items	Management service	Internet access service	VoIP service	IPTV service
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	No rate limit			
Rate limit on ONU downstream port	No rate limit			

Remark 1: GEM port values depend on the planning of the service provider. Generally, however, use different GEM ports for different services.

Remark 2: [Table 15-17](#) shows the reference service bandwidth of each service for each user.

Table 15-17 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the service package.	Determined based on the service package.	Available bandwidth of Internet access service = Committed bandwidth of the service package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 Kbit/s	200 Kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (standard definition program)	—	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture (PiP) information, 10% of the assured bandwidth for burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires only a little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be ignored.
IPTV service (high definition program)	—	9.7 Mbit/s per channel	

Note:

- If the BRAS does not support rate limitation, OLTs can limit the rate for service flows by using traffic profiles.
- Different service packets on the ONT are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) can correspond to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to an OLT PON port and the fixed bandwidth of OMCI management channel should be smaller than the GPON upstream bandwidth. Some bandwidth must be reserved for future service expansion.

15.14.4 QoS Solution for FTTB/FTTC

Basic Principles of QoS for FTTB/FTTC

1. Plan different CoS priorities for different services. The advised priority order is as follows: management packets > VoIP > IPTV > HSI.
2. Classify traffic and re-mark 802.1p priority on the ingress (upstream port on MDU/downstream port on OLT) on the FTTx network. Implement congestion control based on 802.1p priority in PQ scheduling mode on the internal access network (MDU/OLT). For packets transmitted downstream from the network side of the OLT, the priority can be trusted. The priority does not need to be re-marked.
3. Service packets on MDUs are distinguished by 802.1p priority.

- GEM port mapping is implemented in a GPON system based on 802.1p, so that different service packets enter different GEM ports. Each GEM port (each service) can correspond to a T-CONT or all GEM ports share a T-CONT.

NOTE

T-CONT 0 is still used exclusively for OMCI management.

4. DBA planning:
 - GPON MDUs sharing one T-CONT: Set different DBA profiles for different MDU types on the OLT, and then choose corresponding DBA profiles in the service pre-provisioning phase based on the MDU type. Type 3 (assured bandwidth+maximum bandwidth) is recommended for a DBA profile. The T-CONT upstream priority for MDUs is based on 802.1p priority.
 - GPON MDUs using multiple T-CONTs: Allocate different DBA profiles for T-CONTs of each service.
5. Bandwidth limit: It is recommended to implement bandwidth limit of user service flows on the BRAS/SR, not on the access network. MDUs can be configured to limit the bandwidth on the user-side ports; MDUs/OLTs can be configured to limit the rate of service flows based on traffic profiles.
6. For xDSL access, an MxU supports bandwidth limit on physical links using the xDSL link traffic profile. Bandwidth limit on xDSL link is based on the fact that the channels on user-side ports do not differentiate multiple service PVCs. It is recommended that you differentiate services on the modem for users with large upstream traffic so that QoS can be ensured.

Recommended QoS Plan for FTTB/FTTC

The following table provides details about the recommended QoS plan for FTTB/FTTC with respect to traffic classification, priority marking, and queue scheduling policies.

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	MDU Queue ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Internet access service	0	PQ	0	0	0

Note

- Different service packets are distinguished by different VLAN IDs. GEM ports are mapped based on 802.1p priorities for the GPON system.
- Service priorities in this table are for reference only. Configure the service priorities according to the operator's actual network plan.

The following table provides details about the recommended QoS plan for FTTB/FTTC with respect to traffic policing and DBA policies.

Items	Management service	Internet access service	VoIP service	IPTV service
GEM port (only for GPON)	11 [Remark 1]	12	13	14
T-CONT (only for GPON)	All services share a T-CONT.			
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)			
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is greater than or equal to the maximum bandwidth that users apply.			
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	Set ONU port rate limit or xDSL line rate limit as required. [Remark 2]			
Rate limit on ONU downstream port	Set ONU port rate limit or xDSL line rate limit as required. [Remark 2]			

Remark 1: GEM port values depend on the planning of the service provider. Generally, however, use different GEM ports for different services.

Remark 2: [Table 15-18](#) shows the reference service bandwidth of each service for each user.

Table 15-18 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service	Determined based on the service package.	Determined based on the service package.	Available bandwidth of Internet access service = Committed bandwidth of the service package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 Kbit/s	200 Kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth varies with the coding format. This bandwidth is calculated for two POTS ports.
IPTV service (common program)	/	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture (PiP) information, 10% of the assured bandwidth for burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires a little bandwidth and can be ignored.
IPTV service (high definition program)	/	9.7 Mbit/s per channel	

Note

- It is recommended to configure rate limitation on the BRAS or SR, not on the OLTs or MDUs. If the BRAS does not support rate limit, OLTs can limit rates on service flows using traffic profiles.
- Different service packets of MDUs are distinguished by 802.1p priorities and are mapped to GEM ports based on 802.1p priorities so that packets are transmitted to different GEM ports. Each GEM port (each service) can correspond to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to an OLT PON port and the fixed bandwidth of OMCI management channel should be smaller than the GPON upstream bandwidth. Some bandwidth must be reserved for future service expansion.