



Quidway S5300 Series Ethernet Switches  
V100R002C02

## **Configuration Guide - QoS**

<b>Issue</b>	02
<b>Date</b>	2009-02-16
<b>Part Number</b>	

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

## Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <http://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

**Copyright © Huawei Technologies Co., Ltd. 2009. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

### Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

---

# Contents

---

<b>About This Document.....</b>	<b>1</b>
<b>1 QoS Configuration.....</b>	<b>1-1</b>
1.1 Introduction.....	1-3
1.1.1 QoS Overview.....	1-3
1.1.2 References.....	1-3
1.1.3 Logical Relationships Between Configuration Tasks.....	1-3
1.2 Configuring Traffic Policing and Re-marking.....	1-3
1.2.1 Establishing the Configuration Task.....	1-4
1.2.2 Setting Traffic Classification Rules.....	1-4
1.2.3 (Optional) Configuring Access Control Behaviors.....	1-6
1.2.4 (Optional) Configuring Traffic Policing.....	1-7
1.2.5 (Optional) Configuring Re-marking Behaviors.....	1-8
1.2.6 Creating and Applying a Traffic Policy.....	1-9
1.2.7 Checking the Configuration.....	1-10
1.3 Configuring Congestion Management.....	1-10
1.3.1 Establishing the Configuration Task.....	1-11
1.3.2 (Optional) Configuring the Mapping Between the Local Precedence and Queues.....	1-11
1.3.3 (Optional) Configuring PQ Scheduling.....	1-12
1.3.4 (Optional) Configuring DRR Scheduling.....	1-12
1.3.5 (Optional)Configuring PQ+DRR Scheduling.....	1-13
1.3.6 Configuring WRR Scheduling.....	1-13
1.3.7 (Optional) Configuring PQ+WRR Scheduling.....	1-14
1.3.8 (Optional) Configuring the Minimum Size of the Static Buffer.....	1-14
1.3.9 (Optional) Configuring the Maximum Number of Packets.....	1-14
1.3.10 Checking the Configuration.....	1-15
1.4 Configuring Congestion Avoidance.....	1-15
1.4.1 Establishing the Configuration Task.....	1-16
1.4.2 Setting SRED Parameters.....	1-16
1.4.3 Checking the Configuration.....	1-17
1.5 Configuring Traffic Shaping.....	1-17
1.5.1 Establishing the Configuration Task.....	1-17
1.5.2 Configuring Traffic Shaping for Queues on the Outbound Interface.....	1-18
1.5.3 Checking the Configuration.....	1-18

1.6 Configuring a Limit Rate on the Outbound Interface.....	1-18
1.6.1 Establishing the Configuration Task.....	1-18
1.6.2 Limiting the Rate of Traffic on the Outbound Interface.....	1-19
1.6.3 Checking the Configuration.....	1-19
1.7 Configuring Queue Statistics.....	1-19
1.7.1 Establishing the Configuration Task.....	1-19
1.7.2 Configuring Queue Statistics.....	1-20
1.7.3 Checking the Configuration.....	1-20
1.8 Configuring Trust DSCP.....	1-21
1.8.1 Establishing the Configuration Task.....	1-21
1.8.2 Configuring Trust DSCP.....	1-21
1.8.3 Checking the Configuration.....	1-22
1.9 Maintaining QoS.....	1-22
1.10 Configuration Examples.....	1-23

---

# Figures

**Figure 1-1** Diagram for configuring QoS.....1-24



---

# Tables

---

**Table 1-1** QoS for upstream traffic on inbound interfaces.....1-25

**Table 1-2** QoS for upstream traffic on outbound interfaces.....1-25

**Table 1-3** QoS for downstream traffic on each S-switch.....1-25



---

# About This Document

---

## Purpose

This document provides configuration procedures and examples for the QoS features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparations
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document helps you grasp the configuration procedures and application scenarios of the QoS features of the S-switch.

## Related Versions

The following table lists the product versions related to this document.

Product Name	Version
S5300	V100R002C02

## Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network administrators
- System maintenance engineers

# Organization






This document is organized as follows.

Chapter	Description
<a href="#">1 QoS Configuration</a>	This chapter describes the principle of class-based quality of service (QoS), and configuration procedures of traffic classification, re-marking, traffic policing, congestion management, congestion avoidance, queue statistics, and trust DSCP.

# Conventions

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>DANGER</b>	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.
 <b>CAUTION</b>	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 <b>TIP</b>	Indicates a tip that may help you address a problem or save your time.
 <b>NOTE</b>	Provides additional information to emphasize or supplement important points of the main text.

## General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
<b>Boldface</b>	Names of files, directories, folders, and users are in <b>Boldface</b> . For example, log in as user <b>Root</b> .
<i>Italic</i>	Book titles are in <i>Italics</i> .

Convention	Description
Courier New	Examples of information displayed on the screen are in Courier New.

## Command Conventions

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>boldface</b> .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x   y   ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[ x   y   ... ]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x   y   ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[ x   y   ... ] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Several or none is selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

## GUI Conventions

Convention	Description
<b>boldface</b>	Buttons, menus, parameters, tabs, windows, and dialog titles are in <b>boldface</b> . For example, click <b>OK</b> .
>	Multi-level menus are in <b>boldface</b> and separated by the ">" signs. For example, choose <b>File &gt; Create &gt; Folder</b> .

## Keyboard Operations

Convention	Description
<b>Key</b>	Press the key. For example, press <b>Enter</b> and press <b>Tab</b> .
<b>Key 1+Key 2</b>	Press the keys concurrently. For example, pressing <b>Ctrl+Alt+A</b> means the three keys should be pressed concurrently.
<b>Key 1, Key 2</b>	Press the keys in turn. For example, pressing <b>Alt, F</b> means the two keys should be pressed in turn.

## Mouse Operations

Convention	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

## Update History

Updates between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

### Updates in Issue 02 (2009-02-16)

Second commercial release. The document is updated as follows:

- Fixing bug
- Rewriting copyright statement
- Updating manual version

### Updates in Issue 01 (2008-12-26)

This is the first release.

# 1 QoS Configuration

---

## About This Chapter

This chapter describes the principle of class-based quality of service (QoS), and configuration procedures of traffic classification, re-marking, traffic policing, congestion management, congestion avoidance, queue statistics, and trust DSCP.

### [1.1 Introduction](#)

This section describes the basic concepts of QoS.

### [1.2 Configuring Traffic Policing and Re-marking](#)

This section describes how to configure QoS policies on the inbound interface, such as traffic classification, access control, re-marking, and traffic policing.

### [1.3 Configuring Congestion Management](#)

This section describes how to configure the mapping between a local precedence and a queue, queue scheduling mechanisms, the minimum size of the static buffer, and the maximum number of packets.

### [1.4 Configuring Congestion Avoidance](#)

This section describes how to configure the simple random early detection (SRED) to avoid congestion.

### [1.5 Configuring Traffic Shaping](#)

Configuring Traffic Shaping

### [1.6 Configuring a Limit Rate on the Outbound Interface](#)

This section describes how to limit the traffic rate on the outbound interface.

### [1.7 Configuring Queue Statistics](#)

This section describes how to configure queue statistics.

### [1.8 Configuring Trust DSCP](#)

This section describes how to configure trust DSCP.

### [1.9 Maintaining QoS](#)

This section describes how to clear the statistics on QoS and debug QoS.

### [1.10 Configuration Examples](#)

This section provides several configuration examples of QoS.

## 1.1 Introduction

This section describes the basic concepts of QoS.

[1.1.1 QoS Overview](#)

[1.1.2 References](#)

[1.1.3 Logical Relationships Between Configuration Tasks](#)

### 1.1.1 QoS Overview

#### Definition

QoS is a general assessment made about the service in several aspects, such as the bandwidth, delay, jitter, and packet loss ratio during the process of transmission.

#### Function

QoS is used to assess the ability of service provisioning supplied to meet customers' needs. In the Internet, QoS is used to assess the ability of the network to transmit packets.

### 1.1.2 References

For details about the QoS principle, refer to the *Quidway S5300 Series Ethernet Switches Feature Description*.

### 1.1.3 Logical Relationships Between Configuration Tasks

There is no strict logical relationship between configuration tasks.

## 1.2 Configuring Traffic Policing and Re-marking

This section describes how to configure QoS policies on the inbound interface, such as traffic classification, access control, re-marking, and traffic policing.

The procedures "[1.2.3 \(Optional\) Configuring Access Control Behaviors](#)", "[1.2.4 \(Optional\) Configuring Traffic Policing](#)", and "[1.2.5 \(Optional\) Configuring Re-marking Behaviors](#)" are optional and are not listed in sequence. First set rules for traffic classification, then set traffic policing or re-marking behaviors, and finally create and apply traffic policies.

[1.2.1 Establishing the Configuration Task](#)

[1.2.2 Setting Traffic Classification Rules](#)

[1.2.3 \(Optional\) Configuring Access Control Behaviors](#)

[1.2.4 \(Optional\) Configuring Traffic Policing](#)

[1.2.5 \(Optional\) Configuring Re-marking Behaviors](#)

[1.2.6 Creating and Applying a Traffic Policy](#)

### 1.2.7 Checking the Configuration

## 1.2.1 Establishing the Configuration Task

### Applicable Environment

It is necessary to define rules for traffic classification before offering class-based QoS. Traffic classification is implemented to provide differentiated service and must be associated with a certain traffic control or resource allocation behavior.

Depending on class-based QoS, the S-switch can provide access control and firewall functions. The S-switch can re-mark the destination medium access control (MAC) address of packets and change the original destination MAC address of the packets transmitted within the network to ensure the security of the packets.

In practice, you must select suitable behaviors according to the location and load status of traffic.

### Pre-configuration Tasks

Before configuring traffic policing and re-marking, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces

### Data Preparation

To configure traffic policing and re-marking, you need the following data.

No.	Data
1	Traffic classifier name, traffic behavior name, and traffic policy name
2	Destination MAC address, source MAC address, outbound interface, 802.1p priority, differentiated services code point (DSCP) value, virtual local area network (VLAN) ID
3	Access control list (ACL) rules
4	Re-marked value including the 802.1p priority, DSCP value, IP precedence, and local precedence
5	CIR, CBS, PIR, and PBS of traffic on the inbound interface

## 1.2.2 Setting Traffic Classification Rules

### Context

#### NOTE

In the traffic classifier view, there is no specified order among the matching rules. You can combine these rules.

## Setting Simple Traffic Classification Rules

### Context

Do as follows on the S-switch on which simple traffic classification rules need to be set.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic classifier** *class-name* command to create a traffic classifier and enter the traffic classifier view.
- Step 3** Run the **if-match** command to define a matching rule in traffic classification. The matching rules that can be defined are as follows:
- Run the **if-match 8021p** *802.Ip-precedence* command to define a rule to classify traffic based on the 802.1p priority in VLAN frames.
  - Run the **if-match acl** *acl-number* command to define a rule to classify traffic based on the ACL.
  - Run the **if-match cvlan-id** *cvlan-id* command to define a rule to classify traffic based on the IDs of inner VLAN tags in QinQ packets.
  - Run the **if-match cvlan-8021p** *802.Ip-precedence* command to define a rule to classify traffic based on the 802.1p priority in inner VLAN tags in QinQ packets.
  - Run the **if-match { destination-mac }** *mac-address* command to define a rule to classify traffic based on the destination MAC address.
  - Run the **if-match { source-mac }** *mac-address* command to define a rule to classify traffic based on the source MAC address.
  - Run the **if-match double-tag** command to define a rule to classify traffic based on QinQ packets.
  - Run the **if-match l2-protocol { arp | ip | mpls | rarp | protocol-value }** command to define a rule to classify traffic based on the protocol type field in the Ethernet frame header.
  - Run the **if-match outbound-interface** *interface-type interface-number* command to define a rule to classify traffic based on the outbound interface.
  - Run the **if-match vlan-id** *vlan-id* command to define a rule to classify traffic based on VLAN IDs in frames.
  - Run the **if-match discard** command to define a rule to classify traffic based on dropped packets.
  - Run the **if-match any** command to define a matching rule for classifying traffic based on all data packets.

Several matching rules can be defined in the same traffic classifier. The operation of all matching rules is AND.

#### NOTE

It is also possible that these rules are mutually exclusive and thus the applied traffic policies fail. Traffic classification rules for different protocols at the same network layer are mutually exclusive, for example, traffic classification rules for Layer 3 protocols are mutually exclusive.

----End

## Setting Complex Traffic Classification Rules

### Context

Do as follows on the S-switch on which complex traffic classification rules need to be set.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **acl [ number ] acl-number** command to create an ACL and enter the ACL view.

For detailed description of the ACL commands in this step and [Step 3](#), refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

**Step 3** Run the **rule** command to create a basic ACL rule or an advanced ACL rule. The procedures are as follows:

- To add a basic ACL rule, run the **rule [ rule-id ] { deny | permit } [ fragment | source { source-address source-wildcard | any } | time-range time-name ]\*** command.
- To create an advanced ACL rule, run the following command as required:
  - **rule [ rule-id ] { deny | permit } { protocol | gre | igmp | ip | ipinip | ospf } [ destination { destination-address destination-wildcard | any } | dscp dscp | fragment | precedence precedence | source { source-address source-wildcard | any } | time-range time-name | tos tos ]\***
  - **rule [ rule-id ] { deny | permit } { tcp | udp } [ destination { destination-address destination-wildcard | any } | destination-port operator port | fragment | precedence precedence | source { source-address source-wildcard | any } | source-port operator port | time-range time-name ]\***
  - **rule [ rule-id ] { deny | permit } icmp [ destination { destination-address destination-wildcard | any } | fragment | icmp-type icmp-type icmp-code | precedence precedence | source { source-address source-wildcard | any } | time-range time-name ]\***

#### NOTE

When the S-switch classifies traffic based on ACL rules, the **rule** commands are used only to classify traffic. The S-switch does not filter packets based on **permit** or **deny** in the commands.

The parameters related to Transfer Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) of an ACL rule are mutually exclusive to the rules based on Layer 3 protocols such as Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).

**Step 4** Run the **quit** command to return to the system view.

**Step 5** Run the **traffic classifier class-name** command to create a traffic classifier and enter the traffic classifier view.

**Step 6** Run the **if-match acl acl-number** command to define a rule to classify traffic based on the ACL.

----End

## 1.2.3 (Optional) Configuring Access Control Behaviors

## Context

Do as follows on the S-switch on which access control needs to be configured to control incoming packets.

### NOTE

The traffic action **deny** is exclusive to other traffic actions. Before the S-switch adds other traffic actions such as **remark** and **port-mirroring** in the traffic behavior, ensure that the current traffic actions do not include the traffic action **deny**. If the traffic action **deny** is already involved in the traffic behavior, perform the traffic action **permit** before adding other traffic actions.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic behavior** *behavior-name* command to create a traffic behavior and enter the traffic behavior view.
- Step 3** Deny or permit the traffic that matches the set rules to pass through by running the corresponding command.
- Run the **deny** command to deny the traffic that matches the set rules to pass through.
  - Run the **permit** command to permit the traffic that matches the set rules to pass through.

By default, the S-switch permits the traffic matching the rules to pass through.

----End

## Postrequisite

For a traffic classifier, configure the filtering behavior for permitting or denying packets to pass through, bind the traffic classifier to the traffic behavior in the policy, and then apply the policy on the inbound interface.

## 1.2.4 (Optional) Configuring Traffic Policing

### Context

Do as follows on the S-switch on which traffic policing needs to be configured.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic behavior** *behavior-name* command to create a traffic behavior and enter the traffic behavior view.
- Step 3** Run the **car** [**aggregation**] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-precedence* | **remark-dscp** { *dscp-name* | *dscp-value* } ] } ] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-precedence* | **remark-dscp** { *dscp-name* | *dscp-value* } ] } ] [**red** { **discard** | **pass** [**remark-8021p** *8021p-precedence* | **remark-dscp** { *dscp-name* | *dscp-value* } ] } ] command to configure a policy for committed access rate (CAR) traffic policing.

----End

## Postrequisite

After traffic policing is set, the S-switch starts to count packets that pass through the S-switch and discarded packets.

## 1.2.5 (Optional) Configuring Re-marking Behaviors

### Context

**NOTE**

The S-switch first judges whether to trust the 802.1p priority in packets, and then re-marks some fields of the traffic on demand.

### Configuring the S-switch to Trust the 802.1p Priority of Packets

#### Context

Do as follows on the S-switch that needs to be configured to trust the 802.1p priority of packets.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **trust 8021p** command to set the priority in packets received from this interface to trustable.

Each interface on the S-switch can judge whether to trust the priority in the packets. If the packets are trusted, they are forwarded normally; if not, the 802.1p priority is re-marked as 0.

----End

### Re-marking Priorities of Packets Based on Traffic Classification

#### Context

Do as follows on the S-switch on which priorities of packets need to be re-marked.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic behavior** *behavior-name* command to create a traffic behavior and enter the traffic behavior view.
- Step 3** Run the **remark** command to re-mark priorities in packets. You can re-mark the following priorities in packets:
  - Run the **remark 8021p** *8021p-precedence* command to re-mark the 802.1p priority of VLAN frames.
  - Run the **remark dscp** { *dscp-name* | *dscp-value* } command to re-mark the DSCP value of packets.

- Run the **remark ip-precedence** *ip-precedence* command to re-mark the IP precedence of packets.
- Run the **remark local-precedence** *local-precedence* command to re-mark the local precedence related to packets.
- Run the **remark vlan-id** *vlan-id* command to re-mark the VLAN ID in VLAN frames.
- Run the **remark cvlan-id** *cvlan-id* command to re-mark the inner VLAN ID in VLAN frames.
- Run the **remark destination-mac** *mac-address* command to re-mark the destination MAC address of packets.

 **NOTE**

You cannot re-mark the 802.1p priority and the local precedence in a traffic behavior at the same time.  
You cannot re-mark the DSCP value and IP precedence of packets at the same time.

At the edge of the network, the S-switch re-marks the priority in packets after it classifies the incoming traffic. The new marked priority alters the demand for QoS in the network. Inside the network, the S-switch trusts the priority in packets sent from upstream devices.

----End

## 1.2.6 Creating and Applying a Traffic Policy

### Context

Do as follows on the interface on which a traffic policy needs to be created and applied.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **traffic policy** *policy-name* command to define a traffic policy and enter the traffic policy view.
- Step 3** Run the **classifier** *class-name* **behavior** *behavior-name* command to bind a traffic behavior to a specified traffic classifier in the traffic policy.
- In the same traffic policy, you can configure several binding relationships between traffic classifiers and traffic behaviors and a traffic classifier can only be bound to a traffic behavior.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **interface** *interface-type* *interface-number* command to enter the interface view. Or Run the **vlan** *vlan-id* command to enter the VLAN view.
- Step 6** Run the **traffic-policy** *policy-name* { **inbound** | **outbound** } command to apply a traffic policy to an interface or a vlan.

In this step, the value of *policy-name* must be the same as the value of *policy-name* in [Step 2](#).

----End

## Postrequisite

Once a traffic policy is applied on an interface, you cannot randomly change the traffic policy, the related classifier or the behavior. If you want to change them, the traffic policy must be cancelled on the interface first.

## 1.2.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the behaviors defined by users.	<b>display traffic behavior user-defined</b> [ <i>behavior-name</i> ]
Check the classifiers defined by users.	<b>display traffic classifier user-defined</b> [ <i>class-name</i> ]
Check the policies defined by users.	<b>display traffic policy user-defined</b> [ <i>policy-name</i> [ <b>classifier</b> <i>class-name</i> ] ]
Check the current traffic policy applied on the interface, that is, display matching traffic classification rules or CAR statistics.	<b>display traffic policy interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [ <b>inbound</b> ]
Check complex traffic classification rules defined by users.	<b>display acl</b> { <b>all</b>   <i>acl-number</i> }

For details about the **display** command output, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

You can view the following types of information by running the **display traffic policy interface** command:

- To configure the device to start counting packets that match the traffic classification rules when the policy is applied, you must run the **count** command in the traffic behavior view. Take the time when the policy is applied as the statistics start time and collect statistics on matching traffic.
- To view the number of permitted and dropped packets after traffic policing, run the **car** command to perform CAR traffic policing on packets.

## 1.3 Configuring Congestion Management

This section describes how to configure the mapping between a local precedence and a queue, queue scheduling mechanisms, the minimum size of the static buffer, and the maximum number of packets.

### [1.3.1 Establishing the Configuration Task](#)

### [1.3.2 \(Optional\) Configuring the Mapping Between the Local Precedence and Queues](#)

### [1.3.3 \(Optional\) Configuring PQ Scheduling](#)

[1.3.4 \(Optional\) Configuring DRR Scheduling](#)

[1.3.5 \(Optional\) Configuring PQ+DRR Scheduling](#)

[1.3.6 Configuring WRR Scheduling](#)

[1.3.7 \(Optional\) Configuring PQ+WRR Scheduling](#)

[1.3.8 \(Optional\) Configuring the Minimum Size of the Static Buffer](#)

[1.3.9 \(Optional\) Configuring the Maximum Number of Packets](#)

[1.3.10 Checking the Configuration](#)

## 1.3.1 Establishing the Configuration Task

### Applicable Environment

When network congestion occurs, the S-switch must provide congestion management. The technique of congestion management can improve the usage of resources by scheduling queues.

To manage congestion better, you are recommended to adopt the same scheduling mode in the entire network.

### Pre-configuration Tasks

Before configuring congestion management, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces

### Data Preparation

To configure congestion management, you need the following data.

No.	Data
1	Mapping between the 802.1p priority of VLAN frames and the local precedence
2	Mode of queue scheduling
3	Weight of queues in deficit round robin (DRR) scheduling mode
4	Weight of queues in weighted round robin (WRR) scheduling mode
5	(Optional) Queue name
6	(Optional) Minimum size of the static buffer for a queue
7	(Optional) Maximum number of packets

## 1.3.2 (Optional) Configuring the Mapping Between the Local Precedence and Queues

## Context

Do as follows on the S-switch on which the mapping between the local precedence and queues needs to be configured.

## Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **qos local-precedence-queue-map** *local-precedence queue-index* command to configure the mapping between the local precedence and queues.

The mapping between the local precedence and queues takes effect only on the traffic on the inbound interface. That is, the S-switch puts traffic into queues based on the mapping.

----End

## 1.3.3 (Optional) Configuring PQ Scheduling

### Context

Do as follows on the interfaces on which the priority queuing (PQ) scheduling is required to manage congestion.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos pq** command to schedule queues in PQ mode.

----End

## 1.3.4 (Optional) Configuring DRR Scheduling

### Context

Do as follows on interfaces on which DRR scheduling is required to manage congestion.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos drr** command to schedule queues in DRR mode.

You can perform Step 4 only when the DRR mode is employed on the interface.

**Step 4** Run the **qos drr queue-index** *queue-index weight weight* command to set DRR scheduling weights for queues.

When forwarding a packet in a queue on an interface scheduled in DRR, the S-switch checks the length of the packet in the queue. If the packet length is greater than the maximum

transmission unit (MTU) forwarded by the interface, S-switch does not forward the packet in the queue but starts to forward packets in the next queue.

----End

## 1.3.5 (Optional)Configuring PQ+DRR Scheduling

### Context

Do as follows on interfaces on which PQ+DRR scheduling needs to be applied to manage congestion.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos drr** command to schedule queues in DRR mode.

You can perform Step 4 only when the DRR mode is employed on the interface.

**Step 4** Run the **qos drr queue-index** *queue-index* **weight 0** command to set DRR scheduling weights 0 for queues.

When DRR scheduling weights of all queues are 0s, all queues apply PQ scheduling. That is, the overall scheduling mode is PQ.

When DRR scheduling is applied and the weight of a queue is set to 0, the queue applies PQ scheduling and other queues apply DRR scheduling. That is, the overall scheduling mode is PQ+DRR.

----End

## 1.3.6 Configuring WRR Scheduling

### Context

Do as follows on the interfaces on which the WRR scheduling is required to manage congestion.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos wrr** command to set the scheduling mode to WRR.

Both the and support the WRR mode.

You can perform Step 4 only when the queue scheduling mode on the interface is WRR.

**Step 4** Run the **qos wrr queue-index** *queue-index* **weight** *weight* command to set WRR scheduling weights for queues.

Eight queues can be scheduled in WRR mode only when the WRR scheduling weights of all queues on the interface are not 0; otherwise, the queue with the scheduling weight 0 adopts the

PQ scheduling. That is, the eight queues adopt PQ+WRR scheduling. For how to configure PQ+WRR scheduling, see "[1.3.7 \(Optional\) Configuring PQ+WRR Scheduling](#)."

----End

## 1.3.7 (Optional) Configuring PQ+WRR Scheduling

### Context

Do as follows on interfaces on which PQ+WRR scheduling is required to manage congestion.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos wrr queue-index** *queue-index* **weight 0** command to set the WRR scheduling weight for the queue to 0. That is, the queue is scheduled in PQ mode.

When WRR weights of all queues are 0s, all queues apply PQ scheduling. That is, the overall scheduling mode is PQ.

When WRR scheduling is applied and the weight of a queue is set to 0, the queue applies PQ scheduling. That is, the overall scheduling mode is PQ+WRR.

----End

## 1.3.8 (Optional) Configuring the Minimum Size of the Static Buffer

### Context

Do as follows on the interface on which the minimum size of the static buffer for a queue needs to be specified.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.

**Step 3** Run the **qos queue** { *af1* | *af2* | *af3* | *af4* | *be* | *cs6* | *cs7* | *ef* } **static-cell** *cell-number* command to set the minimum size of the static buffer for a queue on an interface.

----End

## 1.3.9 (Optional) Configuring the Maximum Number of Packets

### Context

Do as follows on the interface on which the maximum number of packets in a specified queue needs to be specified.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **qos queue { af1 | af2 | af3 | af4 | be | cs6 | cs7 | ef } max-length packet-number** command to set the maximum number of packets in a specified queue on an interface.
- End

## 1.3.10 Checking the Configuration

### Prerequisite

The configurations of congestion management function are complete.

### Procedure

- Run the **display qos local-precedence-queue-map** command to check the mapping between the local precedence and queues.
- Run the **display qos static-cell** command to check the minimum size of the static buffer for an interface queue or all interface queues.
- Run the **display qos max-length** command to check the maximum number of packets in an interface queue or all interface queues.

----End

### Example

Run the **display qos static-cell** command to check the name of the interface, the name of the queue, and the minimum size of the static buffer. Take the following as an example:

```
<Quidway> system-view
[Quidway] display qos static-cell interface GigabitEthernet 0/0/1 queue be
Port          Queue   Static-cell (Cells)
-----
GigabitEthernet/0/1   be      12
```

## 1.4 Configuring Congestion Avoidance

This section describes how to configure the simple random early detection (SRED) to avoid congestion.

[1.4.1 Establishing the Configuration Task](#)

[1.4.2 Setting SRED Parameters](#)

[1.4.3 Checking the Configuration](#)

## 1.4.1 Establishing the Configuration Task

### Applicable Environment

To maximize throughput and utilization of resources and to minimize the number of discarded packets and delay of packets, the S-switch offers congestion avoidance based on SRED. The S-switch offers the SRED function to avoid congestion and prevent global TCP synchronization.

### Pre-configuration Tasks

Before configuring congestion avoidance, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces

### Data Preparation

To configure congestion avoidance, you need the following data.

No.	Data
1	SRED threshold and drop probability of red packets
2	SRED threshold and drop probability of yellow packets

## 1.4.2 Setting SRED Parameters

### Context

#### NOTE

When congestion avoidance based on the SRED is configured:

- A threshold for discarding red packets and the drop probability that are set for queues 0 to 4 take effect.
- A threshold for discarding yellow packets and the drop probability that are set for queues 0 to 4 do not take effect.
- A threshold for discarding yellow packets and the drop probability that are set for queues 5 to 7 take effect.
- A threshold for discarding red packets and the drop probability that are set for queues 5 to 7 do not take effect.

Do as follows on the interfaces on which SRED parameters need to be configured.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **qos sred queue-index queue-index red start-discard-point discard-probability discard-probability yellow start-discard-point discard-probability discard-probability** command to set the SRED threshold and drop probability of queues.

Each queue has its own SRED parameters to avoid congestion. Therefore, repeat performing this step for each queue.

On the inbound interface, the S-switch sets the drop precedence for the classified packets. On the outbound interface, the S-switch discards packets in each queue at a specific probability according to the drop precedence.

----End

## 1.4.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the SRED configurations of the queues on the outbound interface.	<b>display qos sred</b>

## 1.5 Configuring Traffic Shaping

Configuring Traffic Shaping

[1.5.1 Establishing the Configuration Task](#)

[1.5.2 Configuring Traffic Shaping for Queues on the Outbound Interface](#)

[1.5.3 Checking the Configuration](#)

### 1.5.1 Establishing the Configuration Task

#### Applicable Environment

When the rate of an interface on a downstream device is lower than the rate of an interface on an upstream device, traffic congestion may occur on the interface of the upstream device. In this case, you can configure traffic shaping for queues on the outbound interface of the upstream device and adjust the sending rate of the interface.

#### Pre-configuration Tasks

Before configuring the rate limit on the outbound interface, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces

#### Data Preparation

To configure traffic shaping, you need the following data.

No.	Data
1	Queue index
2	Shaping rate

## 1.5.2 Configuring Traffic Shaping for Queues on the Outbound Interface

### Context

Do as follows on the interface on which traffic shaping for queues on the outbound interface needs to be configured.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **qos queue { af1 | af2 | af3 | af4 | be | cs6 | cs7 | ef } cir cir-value pir pir-value [ cbs cbs-value pbs pbs-value ]** command to configure traffic shaping for queues on the outbound interface.

----End

## 1.5.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the traffic statistics on queues on the outbound interface.	<b>display current-configuration</b>

## 1.6 Configuring a Limit Rate on the Outbound Interface

This section describes how to limit the traffic rate on the outbound interface.

[1.6.1 Establishing the Configuration Task](#)

[1.6.2 Limiting the Rate of Traffic on the Outbound Interface](#)

[1.6.3 Checking the Configuration](#)

### 1.6.1 Establishing the Configuration Task

#### Applicable Environment

Before sending traffic from the interface, limit the traffic rate at the outbound interface. This function controls all outgoing packets

#### Pre-configuration Tasks

Before configuring a limit rate on the outbound interface, complete the following tasks:

- Configuring the physical parameters of interfaces
- Configuring the link layer attributes of interfaces

## Data Preparation

To configure a limit rate on the outbound interface, you need the following data.

No.	Data
1	CIR and CBS of the traffic on the outbound interface

## 1.6.2 Limiting the Rate of Traffic on the Outbound Interface

### Context

Do as follows on the interface on which the rate of outgoing traffic needs to be limited.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **qos lr circir cbs cbs** command to configure the rate of traffic on the outbound interface.
- End

## 1.6.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the limit rate on the outbound interface.	<b>display qos lr interface interface-type interface-number</b>

For details about the **display** command output, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

## 1.7 Configuring Queue Statistics

This section describes how to configure queue statistics.

[1.7.1 Establishing the Configuration Task](#)

[1.7.2 Configuring Queue Statistics](#)

[1.7.3 Checking the Configuration](#)

### 1.7.1 Establishing the Configuration Task

#### Applicable Environment

The S-switch counts the number of incoming packets or outgoing packets in the queues on the interface that receives or transmits packets.

## Pre-configuration Tasks

Before configuring queue statistics on the interface, complete the following tasks:

- Configuring physical parameters for the interface
- Configuring the data link layer for the interface

## Data Preparation

To configure queue statistics, you need the following data.

No.	Data
1	Queue index
2	Type and the number of the interface
3	Direction of the interface

## 1.7.2 Configuring Queue Statistics

### Context

Do as follows on the interface that needs to be configured with queue statistics.

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **port queue statistics enable queue-index queue-index inbound interface interface-type interface-number** command to enable traffic statistics on a specified queue at the inbound interface and set parameters. Or Run the **port queue statistics enable queue-index queue-index outbound interface interface-type interface-number [ from interface interface-type interface-number ]** command to enable traffic statistics on a specified queue at the outbound interface and set parameters.

----End

## 1.7.3 Checking the Configuration

### Prerequisite

The configurations of the queue statistics function are complete.

### Procedure

- Run the **display port queue statistics [ queue-index queue-index inbound interface interface-type interface-number ]** command to check traffic statistics on a specified inbound interface or a specified queue.
- Run the **display port queue statistics [ queue-index queue-index outbound interface interface-type interface-number [ from { interface interface-type interface-number |**

**all } ] ]** command to check traffic statistics on a specified outbound interface or a specified queue.

----End

## Example

Run the **display port queue statistics** command to check the interface name, the interface direction, the queue index and the number of packets. Take the following as an example:

```
<Quidway> display port queue statistics queue-index 7 inbound interface
gigabitethernet 0/0/1
ING-Port          EGR-Port  Direction  Queue  Count
-----
GigabitEthernet0/0/1  --      inbound    7      0
```

# 1.8 Configuring Trust DSCP

This section describes how to configure trust DSCP.

## 1.8.1 Establishing the Configuration Task

### 1.8.2 Configuring Trust DSCP

### 1.8.3 Checking the Configuration

## 1.8.1 Establishing the Configuration Task

### Applicable Environment

When an interface receives a packet, the interface determines the queue and the drop priority of the packet based on the DSCP value carried in the packet.

### Pre-configuration Tasks

Before configuring trust DSCP on the inbound interface, complete the following tasks:

- Configuring physical parameters for the interface
- Configuring the data link layer for the interface

### Data Preparation

To configure trust DSCP, you need the following data.

No.	Data
1	Type and the number of the interface

## 1.8.2 Configuring Trust DSCP

### Context

Do as follows on the interface that needs to be configured to trust DSCP values.

## Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **trust dscp** command to configure an interface to trust the DSCP value of a packet.
- Step 4** Run the **quit** command to quit the system view.
- Step 5** Run the **qos map-table { dscp-dot1p | dscp-dp | dscp-dscp }** command to enter the DSCP mapping table view.
- Step 6** Run the **input { input-value1 [ to input-value2 ]&<1-10> } output output-value** command to set the mapping in the DSCP table.

----End

## 1.8.3 Checking the Configuration

### Prerequisite

The configurations of the trust DSCP function are complete.

### Procedure

Run the **display qos map-table [ dscp-dot1p | dscp-dp | dscp-dscp ]** command to check the current DSCP mapping.

----End

### Example

Run the **display qos map-table** command to check DSCP-Dot1P, DSCP-DP, or DSCP-DSCP mapping. Take the following as an example:

```
<Quidway> system-view
[Quidway] display qos map-table
```

Input	DSCP	Dot1P	DP	DSCP
0		0	0	0
1		0	0	1
2		0	0	2
3		0	0	3
4		0	0	4
5		0	0	5
6		0	0	6
...				

## 1.9 Maintaining QoS

This section describes how to clear the statistics on QoS and debug QoS.

Currently, QoS supports only the function of clearing statistics.



## CAUTION

The QoS statistics cannot be restored after you clear them. Therefore, confirm the action before you run a command to clear the QoS statistics.

To clear the statistics about QoS, run the following **reset** commands in the user view.

Action	Command
Clear traffic statistics on a specified inbound interface or a specified queue.	<b>reset port queue statistics</b> [ <b>queue-index</b> <i>queue-index</i> <b>inbound interface</b> <i>interface-type interface-number</i> ]
Clear traffic statistics on a specified outbound interface or a specified queue.	<b>reset port queue statistics</b> [ <b>queue-index</b> <i>queue-index</i> <b>outbound interface</b> <i>interface-type interface-number</i> [ <b>from</b> { <b>interface</b> <i>interface-type interface-number</i>   <b>all</b> } ] ]
Clear the statistics on traffic.	<b>reset traffic policy statistics</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>vlan</b> <i>vlan-id</i> ]

## 1.10 Configuration Examples

This section provides several configuration examples of QoS.

### Networking Requirements

S-switch-A, S-switch-B, S-switch-C, and S-switch-D are connected to form a star Ethernet.

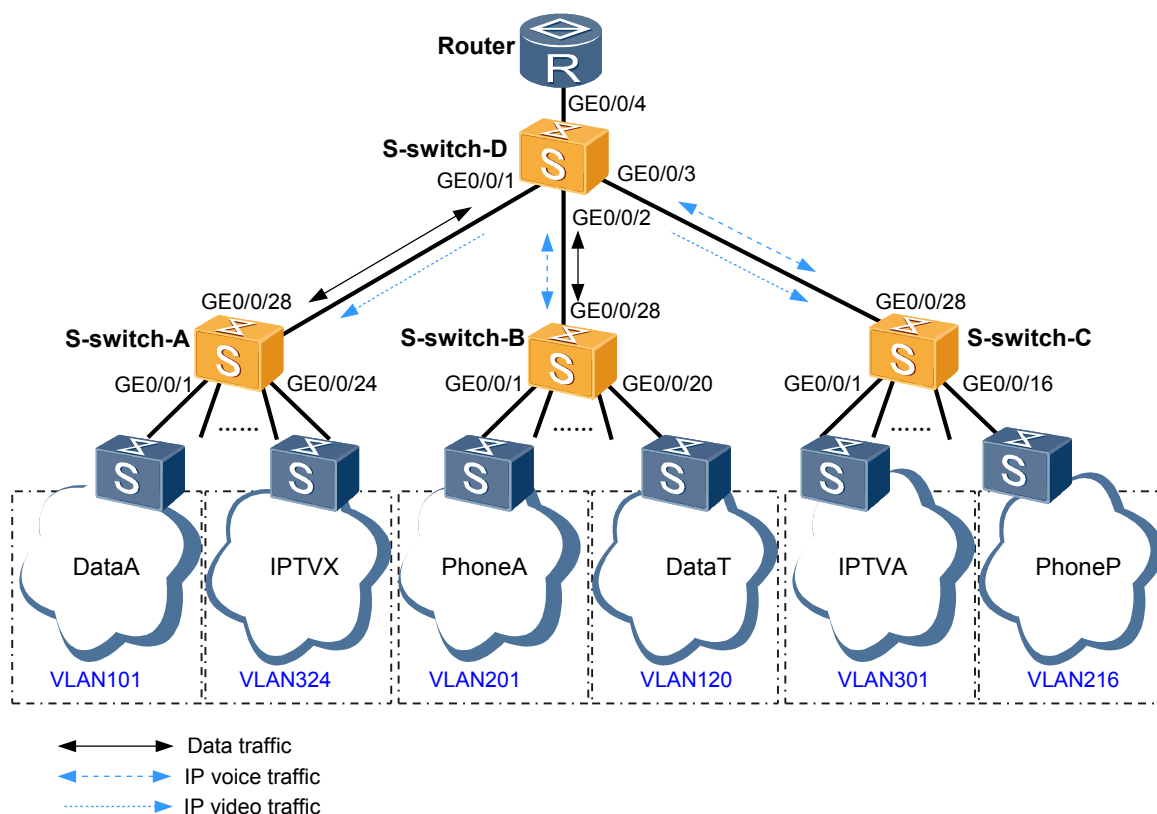
- Data users are on the networks Data A, Data B, ..., Data T that belong to VLAN 101, VLAN 102, ..., VLAN 120 respectively.
- Voice users are on the networks Phone A, Phone B, ..., Phone P that belong to VLAN 201, VLAN 202, ..., VLAN 216 respectively.
- Video users are on the networks IPTV A, IPTV B, ..., IPTV X that belong to VLAN 301, VLAN 302, ..., VLAN 324 respectively.

S-switch-A is connected to users in networks such as Data A and IPTV X. S-switch-B is connected to users in networks such as Phone A and Data T. S-switch-C is connected to users in networks such as IPTV A and Phone P.

Voice services and data services are both bidirectional. The upstream traffic of data services is less than that of the downstream traffic. The volume of upstream traffic and that of the downstream traffic of voice services are almost equal. Video services are mostly downstream traffic. Therefore, the upstream traffic can be neglected. In terms of the features, data and voice services must be guaranteed with bidirectional QoS. Video services, however, need QoS guarantee only for the downstream traffic.

The requirements for QoS in the entire network are as follows:

- In service flows, voice services and video services must be transmitted first, of which, voice services have a higher priority.
- In data streams, the data in Data A network has the highest priority.

**Figure 1-1** Diagram for configuring QoS

## Configuration Roadmap

Deploying QoS in the entire network concerns the whole system. Therefore, QoS capabilities of all devices in the network must be comprehensively considered. Suppose the Layer 3 network has good QoS capabilities; rate limit and congestion management for upstream traffic on the S-switch-D are provided; access control and traffic policing for downstream traffic are provided. This example involves only how to provide QoS between a user and the upstream S-switch-D.

### 1. Configuration roadmap for upstream traffic

The upstream traffic includes data and voice. Congestion may occur on the S-switch if the total volume of the incoming traffic exceeds that of the outgoing traffic. Configure QoS for data streams and voice streams on the S-switch as follows:

- Classify the traffic coming to S-switch-A, S-switch-B, and S-switch-C based on VLAN IDs, set CAR for the traffic to control the access, and then re-mark the 802.1p priority and DSCP priorities of data packets.
- Perform congestion management and congestion avoidance, and then limit the rate of traffic on outbound interfaces on S-switch-A, S-switch-B, and S-switch-C.

### 2. Configuration roadmap for downstream traffic

Downstream traffic includes data, voice, and video. On each S-switch, there is no congestion because the volume of incoming traffic is less than that of outgoing traffic. Do as follows on each S-switch:

- On S-switch-A, S-switch-B, and S-switch-C, limit rates of traffic on all outbound interfaces.

## Data Preparation

- QoS for upstream traffic on each S-switch

**Table 1-1** QoS for upstream traffic on inbound interfaces

Access Device	Traffic Source	Traffic Type	CIR (Mbit/s)	CBS (Byte)	PBS (Byte)	Re-marking Precedence
S-switch-A	Data A	Data	20000	200000	250000	4
S-switch-B	Phone A	Voice	60000	600000	650000	6
	Data T	Data	20000	200000	250000	2
S-switch-C	Phone P	Voice	60000	600000	650000	6

**Table 1-2** QoS for upstream traffic on outbound interfaces

Access Device	Traffic Source	Scheduling Mode	Limit Rate (Mbit/s)
S-switch-A	Data A	WRR	30
S-switch-B	Phone A	WRR	45
	Data T		
S-switch-C	Phone P	WRR	40

Set values of the global SRED parameters on each S-switch as follows:

- Set the S-switch to start discarding red packets when there are 500 red packets and set the drop probability to 1 (6.25%).
- Set the S-switch to start discarding yellow packets when there are 1000 red packets and set the drop probability to 4 (0.78125%).

- QoS for downstream traffic on each S-switch

The DSCP value of the packets from the upstream router is 2 in data packets, 6 in voice packets, and 5 in video packets.

**Table 1-3** QoS for downstream traffic on each S-switch

Access Device	Interface	Traffic Type	CIR (Mbit/s)	CBS (Byte)	Rate Limit (Mbit/s)
S-switch-A	GE 0/0/1	Data	-	-	30
	GE 0/0/24	Video	-	-	80

Access Device	Interface	Traffic Type	CIR (Mbit/s)	CBS (Byte)	Rate Limit (Mbit/s)
S-switch-B	GE 0/0/1	Voice	-	-	70
	GE 0/0/20	Data	-	-	20
S-switch-C	GE 0/0/1	Video	-	-	80
	GE 0/0/16	Voice	-	-	70

## Configuration Procedures

1. Bind interfaces to VLANs and assign IP addresses to VLAN interfaces on each S-switch (The configuration procedures are not mentioned here).
2. Set static routes between each S-switch and the router (The configuration procedures are not mentioned here).
3. Configure QoS for upstream services.

The following takes configuration procedures on S-switch-B as an example. Configuration procedures on S-switch-A, and S-switch-C are similar to those of S-switch-B.

# Classify the traffic based on VLAN IDs.

```
<S-switch-B> system-view
[S-switch-B] traffic classifier c201
[S-switch-B-classifier-c201] if-match vlan-id 201
[S-switch-B-classifier-c201] quit
[S-switch-B] traffic classifier c120
[S-switch-B-classifier-c120] if-match vlan-id 120
[S-switch-B-classifier-c120] quit
```

# Set access control and CAR rules, and then re-mark the priority of traffic. Set high drop precedence for data packets. Data packets on S-switch-A, S-switch-C, or S-switch-D do not need to be set with a high drop precedence.

```
[S-switch-B] traffic behavior b201
[S-switch-B-behavior-b201] permit
[S-switch-B-behavior-b201] car cir 600000 cbs 600000 pbs 650000
[S-switch-B-behavior-b201] remark 8021p 6
[S-switch-B-behavior-b201] remark dscp 6
[S-switch-B-behavior-b201] quit
[S-switch-B] traffic behavior b120
[S-switch-B-behavior-b120] permit
[S-switch-B-behavior-b120] car cir 20000 cbs 20000 pbs 250000
[S-switch-B-behavior-b120] remark 8021p 2
[S-switch-B-behavior-b120] remark dscp 2
[S-switch-B-behavior-b120] quit
```

# Create traffic polices, bind traffic classifications to traffic behaviors, and then apply traffic policies on inbound interfaces.

```
[S-switch-B] traffic policy p201
[S-switch-B-trafficpolicy-p201] classifier c201 behavior b201
[S-switch-B-trafficpolicy-p201] quit
[S-switch-B] interface gigabitethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] traffic-policy p201 inbound
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] traffic policy p120
[S-switch-B-trafficpolicy-p120] classifier c120 behavior b120
[S-switch-B-trafficpolicy-p120] quit
[S-switch-B] interface gigabitethernet 0/0/20
[S-switch-B-GigabitEthernet0/0/20] traffic-policy p120 inbound
[S-switch-B-GigabitEthernet0/0/20] quit
```

# Configure congestion management and set the WRR scheduling mode on GE 0/0/28.

```
[S-switch-B] interface gigabitethernet 0/0/28
[S-switch-B-GigabitEthernet0/0/28] qos wrr
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 0 weight 2
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 1 weight 2
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 2 weight 4
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 3 weight 6
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 4 weight 7
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 5 weight 8
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 6 weight 8
[S-switch-B-GigabitEthernet0/0/28] qos wrr queue-index 7 weight 8
[S-switch-B-GigabitEthernet0/0/28] quit

# Set global congestion avoidance on the outbound interface.

[S-switch-B] qos sred queue-index 0 red 500 discard-probability 1 yellow 1000
discard-probability 4
.....
[S-switch-B] qos sred queue-index 7 red 500 discard-probability 1 yellow 1000
discard-probability 4

# Run the display qos sred command to display global SRED configurations. The displayed
information is as follows:

[S-switch-B] display qos sred
Current sred configuration:
qos sred queue-index 0 red 500 discard-probability 1 yellow 1000 discard-
probability 4
.....

# Configure a limit rate on GE 0/0/28.

[S-switch-B] interface gigabitethernet 0/0/28
[S-switch-B-GigabitEthernet0/0/28] qos lr cir 45000 cbs 100000
[S-switch-B-GigabitEthernet0/0/28] quit

# Run the display qos lr interface command to display the limit rate on the outbound
interface. The displayed information is as follows:

[S-switch-B] display qos lr interface gigabitethernet 0/0/28
GigabitEthernet0/0/28 lr:
  cir: 45000 Kbps, cbs: 100000 Byte
```

#### 4. Configure QoS for downstream services.

The following takes configuration procedures on S-switch-B as an example. Configuration procedures on S-switch-A and S-switch-C are similar to those of S-switch-B.

# Configure limit rates on GigabitEthernet 0/0/1 and GigabitEthernet 0/0/20.

```
[S-switch-B] interface GigabitEthernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] qos lr cir 70000 cbs 150000
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface GigabitEthernet 0/0/20
[S-switch-B-GigabitEthernet0/0/20] qos lr cir 20000 cbs 500000
[S-switch-B-GigabitEthernet0/0/20] quit
```

# Verify the configuration. The following takes the configuration result on GigabitEthernet 0/0/20 as an example:

```
[S-switch-B] display qos lr interface GigabitEthernet 0/0/20
  cir: 20000 Kbps, cbs: 500000 Byte
```

## Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
qos sred queue-index 0 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 1 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 2 red 500 discard-probability 1 yellow 1000 discard-
```

```

probability 4
qos sred queue-index 3 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 4 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 5 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 6 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 7 red 500 discard-probability 1 yellow 1000 discard-
probability 4
#
traffic classifier c101
  if-match vlan-id 101
#
traffic behavior b101
  car cir 20000 pir 200000 cbs 200000 pbs 250000 green pass yellow pass red
discard
  remark 8021p 4
  remark dscp 2
#
traffic policy p101
  classifier c101 behavior b101
#
interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 101
  qos lr cir 30000 cbs 500000
  traffic-policy p101 inbound
#
interface GigabitEthernet0/0/24
  port trunk allow-pass vlan 324
  qos lr cir 80000 cbs 100000
  traffic-policy p101 inbound
#
interface GigabitEthernet0/0/28
  port trunk allow-pass vlan 101 324
  qos lr cir 30000 cbs 100000
  qos wrr queue-index 0 weight 2
  qos wrr queue-index 1 weight 2
  qos wrr queue-index 2 weight 4
  qos wrr queue-index 3 weight 6
  qos wrr queue-index 4 weight 7
  qos wrr queue-index 5 weight 8
  qos wrr queue-index 6 weight 8
  qos wrr queue-index 7 weight 8
#
return

```

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
qos sred queue-index 0 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 1 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 2 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 3 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 4 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 5 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 6 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 7 red 500 discard-probability 1 yellow 1000 discard-
probability 4
#
traffic classifier c120

```

```

    if-match vlan-id 120
traffic classifier c201
    if-match vlan-id 201
#
traffic behavior b120
    car cir 20000 pir 200000 cbs 200000 pbs 250000 green pass yellow pass red
discard
    remark 8021p 6
    remark dscp 6
traffic behavior b201
    car cir 60000 pir 600000 cbs 600000 pbs 650000 green pass yellow pass red
discard
    remark 8021p 2
    remark dscp 2
#
traffic policy p120
    classifier c120 behavior b120
traffic policy p201
    classifier c201 behavior b201
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 201
    qos lr cir 70000 cbs 150000
    traffic-policy p201 inbound
#
interface GigabitEthernet0/0/20
    port trunk allow-pass vlan 120
    qos lr cir 20000 cbs 500000
    traffic-policy p120 inbound
#
interface GigabitEthernet0/0/28
    port trunk allow-pass vlan 120 201
    qos lr cir 45000 cbs 100000
    qos wrr queue-index 0 weight 2
    qos wrr queue-index 1 weight 2
    qos wrr queue-index 2 weight 4
    qos wrr queue-index 3 weight 6
    qos wrr queue-index 4 weight 7
    qos wrr queue-index 5 weight 8
    qos wrr queue-index 6 weight 8
    qos wrr queue-index 7 weight 8
#
return

```

- Configuration file of S-switch-C

```

#
sysname S-switch-C
#
qos sred queue-index 0 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 1 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 2 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 3 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 4 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 5 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 6 red 500 discard-probability 1 yellow 1000 discard-
probability 4
qos sred queue-index 7 red 500 discard-probability 1 yellow 1000 discard-
probability 4
#
traffic classifier c216
    if-match vlan-id 216
#
traffic behavior b216

```

```
car cir 60000 pir 600000 cbs 600000 pbs 650000 green pass yellow pass red
discard
remark 8021p 6
remark dscp 6
#
traffic policy p216
classifier c216 behavior b216
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 301
qos lr cir 80000 cbs 100000
traffic-policy p216 inbound
#
interface GigabitEthernet0/0/16
port trunk allow-pass vlan 216
qos lr cir 70000 cbs 100000
traffic-policy p216 inbound
#
interface GigabitEthernet0/0/28
port trunk allow-pass vlan 216 301
qos lr cir 40000 cbs 100000
qos wrr queue-index 0 weight 2
qos wrr queue-index 1 weight 2
qos wrr queue-index 2 weight 4
qos wrr queue-index 3 weight 6
qos wrr queue-index 4 weight 7
qos wrr queue-index 5 weight 8
qos wrr queue-index 6 weight 8
qos wrr queue-index 7 weight 8
#
return
```