

Comparing Class-Based Policing and Committed Access Rate

Contents

[Introduction](#)[Prerequisites](#)[Requirements](#)[Components Used](#)[Conventions](#)[What Is a Traffic Policer?](#)[Comparing CAR and Class-Based Policing](#)[Matching Criteria](#)[Conform and Exceed Actions](#)[RFC 2697 and the Violate Action](#)[Related Information](#)

Introduction

This document clarifies the differences between committed access rate (CAR), which is the Cisco legacy traffic policing feature, and class-based policing, which is the newer Cisco traffic policer. Class-based policing is implemented in the modular Quality of Service (QoS) command line interface (CLI) (MQC) by configuring a service policy. Class-based policing, also known as traffic policing, was introduced in Cisco IOS® Software 12.1(5)T.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to [Cisco Technical Tips Conventions](#).

What Is a Traffic Policer?

Traffic policing controls the maximum rate of traffic sent or received on an interface. Based on the results of the token bucket measurement, an action can be configured to mark packets and separate packets into multiple classes or levels of service.

Traffic policers provide two key benefits:

- **Bandwidth management through rate limiting** - Allows you to control the maximum rate of traffic sent or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped, or sent with a different priority.
- **Packet marking through IP precedence, QoS group, or DSCP value setting** - Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS).

Use traffic policing to set the IP precedence or differentiated services code point (DSCP) values for packets entering the network. Networking devices within your network can then use the adjusted IP Precedence values to determine how the traffic should be treated. For example, the VIP-Distributed Weighted Random Early Detection feature, as described in [Congestion Avoidance Overview](#), uses the IP precedence values to determine the probability that a packet will be dropped.

Comparing CAR and Class-Based Policing

Cisco recommends using the modular QoS CLI features when possible to implement quality of service in your network. Use class-based policing through the police command in a service policy to implement rate limiting without buffering or queuing. Avoid using CAR, for which no new features or functionality is planned. Cisco will continue to support CAR for existing implementations using this method.

This table lists the functional differences between class-based policing and CAR:

Function	Class-Based Policer	CAR

Enable method	Enabled within a service policy using the MQC	Enabled explicitly on an interface
Configuration command	police command in MQC	rate-limit command on an interface or subinterface
Classification (into traffic classes)	Required	Not required. Supports per-interface rate limiting for all IP traffic
Actions for conforming and non-conforming traffic	Three actions: conform, exceed, and violate	Two actions: conform and exceed <i>No violate action</i>
Token measurement method	Separate token buckets for burst-normal and burst-max	Single token bucket for burst-normal and burst-max
Support for Request for Comment (RFC) 2697	Yes, as of Cisco IOS Software Release 12.1(5)T	No

Note: See the [RFC 2697 and the Violate Action](#) section of this document for more information.

Matching Criteria

CAR and class-based policing support different packet header values on which you can match to classify your traffic. Traffic matching defines the process of identifying traffic for rate limiting and/or packet marking.

Packet Header Value	Support Level	
	Class-Based Policer	CAR
Incoming or outgoing interface	Yes	Yes
All IP traffic or IP packets matching a standard or extended access list	Yes	Yes
IP precedence value	Yes	Yes
DSCP	Yes	—

QoS group ID	Yes	Yes
MAC address	Yes	Yes
IP Real-Time Protocol (RTP) port numbers	Yes	—
Layer 2 CoS value	Yes	—
Predefined class-maps	Yes	—
MPLS experimental value	Yes	—
Network-based application recognition (NBAR) protocols	Yes	—

Conform and Exceed Actions



This table lists the supported actions for conforming and non-conforming traffic for each traffic-policing mechanism.

Action	Support Level	
	Class-Based Policer	CAR
continue	—	Yes
drop	Yes	Yes
set-clp-transmit	Yes	Yes
set-dscp-continue	—	Yes
set-dscp-transmit	Yes	Yes
set-frde-transmit	Yes	—
set-mpls-exp-continue	—	Yes
set-mpls-exp-transmit	Yes	Yes
set-prec-continue	—	Yes
set-prec-transmit	Yes	Yes
set-qos-continue	—	Yes
set-qos-transmit	Yes	Yes
transmit	Yes	Yes

As the above table illustrates, only CAR supports the continue action. This action configures the router to forward the packet to the next rate policy in a chain of rate-limit commands. CAR and class-based policing use different algorithms. Class-based policing uses algorithms based on RFCs 2697 and 2698 and does not need a continue statement. See the following section for more information.

RFC 2697 and the Violate Action

Unlike CAR, class-based policing uses the algorithms specified in the following two RFCs:

- [RFC 2697](#)  "A Single Rate Three Color Marker" - Cisco IOS Release 12.1(5)T
- [RFC 2698](#)  "A Two Rate Three Color Marker" - Cisco IOS Release 12.2(4)T

In addition, it is important to note that class-policing has used two algorithms depending on the Cisco IOS release. Cisco IOS Software Release 12.1(5)T introduced a new algorithm and support for a two-bucket policer using the violate action. The two-bucket mechanism represents a significant functional difference between CAR and class-based policing.

The token bucket algorithm provides users with three actions for each packet: a conform action, an exceed action, and a violate action. Traffic entering the interface with traffic policing configured is placed into one of these categories. Within these three categories, users can decide packet treatments. For instance, packets that conform can be configured to be transmitted; packets that exceed can be configured to be sent with a decreased priority; and packets that violate can be configured to be dropped.

When the violate-action option is specified, the token bucket algorithm uses separate token buckets for the conform and the exceed burst. The following example uses the token bucket algorithm with two token buckets.

```
policy-map POLICE
  class twobucket
    police 8000 1000 1000 conform-action transmit exceed-action
    set-dscp-transmit 4 violate-action drop

interface fastethernet 0/0
  service-policy output POLICE
```

Refer to the Feature Overview section in [Traffic Policing](#) for more information on configuring the violate action.

Related Information

- [Committed Access Rate](#)
- [Committed Access Rate White Paper](#)
- [Class-Based Policing](#)
- [QoS Support Page](#)
- [IP Routed Protocols Support Page](#)
- [IP Routing Support Page](#)
- [Technical Support - Cisco Systems](#)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).