Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(2)

November 20, 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

New and Changed Information

This chapter describes new and changed features in Release 4.0(4)SV1(2).

To find additional information, go to the following locations on Cisco.com.

- Configuration Guides
- Release Notes

The following table lists new and changed features and commands, and where they are documented.

Feature	Description	Changed in release	Where Documented
Configuration limits.	Added configuration limits for QoS policy-maps, QoS class-maps, and QoS interfaces.	4.0(4)SV1(2)	Chapter 7, "QoS Configuration Limits"

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(2)* and describes how to obtain related documentation.

Audience

This guide is for network administrators with the following experience and knowledge:

- An understanding of virtualization
- Using VMware tools to configure a vswitch

Note Knowledge of VMware vNetwork Distributed Switch is not a prerequisite.

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, “Overview”	Provides an overview of QoS features and lists supported RFPs.
Chapter 2, “Configuring QoS Classification”	Describes how to classify network traffic.
Chapter 3, “Configuring QoS Marking Policies”	Describes how to mark network traffic.
Chapter 4, “Configuring QoS Policing”	Describes how to police network traffic.
Chapter 5, “Monitoring QoS Statistics”	Describes how to enable and view QoS statistics.
Appendix 6, “DSCP and Precedence Values”	Provides the DSCP and precedence values used in QoS class maps and policy maps.
Appendix 7, “QoS Configuration Limits”	Provides information about limitations in configuring QoS.

Document Conventions

This publication uses the following conventions:

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
{ }	Elements in braces are required choices.
[ ]	Elements in square brackets are optional.
x | y | x	Alternative, mutually exclusive elements are separated by vertical bars.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or number sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Recommended Reading

Before configuring this feature in the Cisco Nexus 1000V, we recommend that you read and become familiar with the following documentation:

- *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(2)*
- *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*
- *Cisco VN-Link: Virtualization-Aware Networking* white paper

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Overview

This chapter describes the quality of service (QoS) features that you can use on Cisco Nexus 1000V to prevent traffic congestion in your network.

Information About Quality of Service

You can use QoS to provide the most desirable flow of traffic through a network. QoS allows you to classify your network traffic, police and prioritize the traffic flow, and provide congestion avoidance. Traffic is processed based on how you classify it and the QoS policies that you put in place.

You can implement a QoS policy using the following steps:

1. Define a traffic class by using the **class-map** command. For more information, see Chapter 2, "Configuring QoS Classification."
2. Create a traffic policy by using the **policy-map** command. A traffic policy defines how specific traffic is to be acted upon to improve the quality of service. For more information, see Chapter 3, "Configuring QoS Marking Policies."
3. Attach the traffic policy to an interface or port profile by using the **service-policy** command. For more information, see the "Creating Ingress and Egress Policies" section on page 3-10.
4. Police the traffic. For more information, see Chapter 4, "Configuring QoS Policing."

Traffic Classification and Marking

You can use traffic classification and marking to sort and modify traffic for the best quality of service. Table 1-1 describes these processes.

Table 1-1 Traffic Classification and Traffic Marking

QoS Method	Description	Command	Mechanism
Traffic Classification	Groups network traffic based on defined criteria.	**match**	class maps
Traffic Marking	Modifies traffic attributes by class.	**set**	policy maps

This section includes the following topics:

Traffic Classification

Traffic classification allows you to organize traffic (packets) into traffic classes or categories on the basis of whether the traffic matches the criteria you specify. The values used to classify traffic are called match criteria. When you define a traffic class, you can specify multiple match criteria, you can choose to not match on a particular criterion, or you can determine the traffic class by matching any or all criteria. For more information, see Chapter 2, "Configuring QoS Classification."

Traffic Marking

Marking is the process of assigning a priority and involves setting the fields, such as class of service or DSCP, in a packet. The traffic is then marked accordingly as it comes into the device on an ingress interface. The markings are used to treat the traffic as it leaves the device on the egress interface. For more information about configuring marking, see Chapter 3, "Configuring QoS Marking Policies."

Policing

Policing is the monitoring of data rates for a particular class of traffic. The Cisco Nexus 1000V can also monitor associated burst sizes.

Three conditions, are determined by the policer depending on the data rate parameters supplied: conform, exceed, or violate. You can configure only one action for each condition. When the data rate exceeds the user-supplied values, packets are either marked down or dropped.

You can define single-rate or dual-rate policers. Single-rate policers monitor the specified committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic.

For more information about configuring policing, see Chapter 4, "Configuring QoS Policing."

QoS Commands

QoS configuration commands are shown in Table 1-2.

Table 1-2 QoS Configuration Commands

Global Configuration Commands	Class Map QoS Configuration Command	Policy Map QoS Configuration Command	Interface or Port Profile Configuration Command	Policy Map Class QoS Configuration Command	Description
class-map	—	—	—	—	Defines a class map that represents a class of traffic.
table-map	—	—	—	—	Defines a table map that represents a mapping from one set of field values to another set of field values. You can reference a table map from a policy map.
policy-map	—	—	—	—	Defines a policy map that represents a set of policies to be applied to a set of class maps. Policy maps can reference table maps.
—	—	—	**service-policy**	—	Applies a specified policy map to input or output packets on interfaces configured as follows: • inherited from a port-profile[1] • port-channel • Ethernet • VEthernet
—	—	—	—	**police**	Defines the action to take regarding packet data rates.
—	**match**	—	—	—	Defines the criteria for a class map.
—	—	**set**	—	—	Defines the packet header values for a policy map.

1. For information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)*.

QoS Statistics

Statistics are maintained for each policy, class action, and match criteria per interface. For information about monitoring QoS statistics, see Chapter 5, "Monitoring QoS Statistics."

Default QoS Behavior

QoS has no default behavior. Policing and prioritization of traffic are only implemented when you apply a policy map to an interface. The only exception is that, by default, the CoS value for control and packet VLAN traffic is set to 6. This value can be overridden with an explicit QoS policy that is configured on the interface that carries the control and packet VLAN traffic.

However, when designing your QoS and ACL policies, note that access control lists (ACLs) that are referenced within a QoS policy are processed as follows as part of the QoS policy:

- QoS ingress processing follows ACL processing.
- QoS egress processing precedes ACL egress processing.

Supported RFCs

Table 1-3 lists RFCs that are supported by QoS.

Table 1-3 Supported RFCs

Number	Title
RFC 2475	Architecture for Differentiated Services
RFC 2697	A Single Rate Three Color Marker
RFC 2698	A Dual Rate Three Color Marker
RFC 3289	Management Information Base for the Differentiated Services Architecture
RFC 3550	RTP: A Transport Protocol for Real-Time Applications

High Availability Requirements for QoS Features

QoS recovers its previous state after a software restart, and it is able to switch over from the active supervisor to the standby supervisor without a loss of state.

CHAPTER 2

Configuring QoS Classification

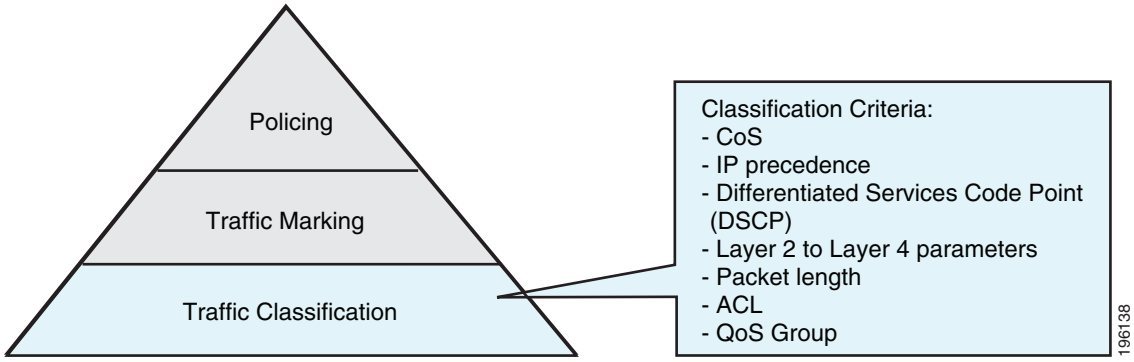
This chapter describes how to create and map classes of traffic for QoS on Cisco Nexus 1000V.

Information About Traffic Classes

Traffic classes are categories of traffic (packets) that are grouped on the basis of similarity. Such groups of traffic are called class maps. Classifying network traffic allows you to enable a quality of service (QoS) strategy in your network.

Figure 2-1 shows the criteria that you use to classify network traffic.

Figure 2-1 Criteria for Classifying Network Traffic



Identifying and categorizing network traffic into traffic classes (that is, classifying packets) enables you to handle different types of traffic by separating network traffic into different categories.

Classifying network traffic allows you to see the kinds of traffic you have and treat some types of traffic differently than others. Identifying and organizing network traffic allows you to allocate network resources to deliver the best performance for each type of traffic.

You can place network traffic with a specific IP precedence into one traffic class, while you place traffic with a specific differentiated services code point (DSCP) value into another traffic class. Each traffic class can be given a different QoS treatment, which you configure in a policy map later.

You define each class of traffic in a class map based upon criteria, such as the IP precedence or Class of Service (CoS). The allowable criteria for mapping classes of traffic is listed in Table 2-1. You can match the criteria to your traffic as follows:

- Matching all

- Matching or not matching one
- Matching or not matching multiple
- Matching or not matching another class map

Some of the criteria used in traffic class maps relates only to one direction of traffic—either ingress or egress. For example, the internal label QoS group has no meaning on ingress traffic because it has not yet been assigned a value.

Traffic that fails to match any traffic class in a QoS policy map is assigned to a default class of traffic called class-default. The class-default can be referenced in a QoS policy map to select this unmatched traffic.

Table 2-1 lists and describes the allowable criteria used for mapping traffic classes.

Table 2-1 Traffic Class Criteria

Class Criteria	Description
CoS	Class of service (CoS) field in the IEEE 802.1Q header.
IP precedence	Precedence value within the type of service (ToS) byte of the IP header. The IP precedence values are shown in the "IP Precedence Values" section on page 6-2.
Differentiated Services Code Point (DSCP)	DSCP value within the DIffServ field of the IP header. The standard DSCP values are listed in the "Commonly Used DSCP Values" section on page 6-1.
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 0 to 126.
Discard class	Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63.
ACL	IP access control list (ACL) or MAC ACL name. If you configure the class to match-all ACLs, no other match criteria, except the packet length, can be specified. If you configure the class to match-any ACL, you can match ACLs and any other match criteria.
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Applications that are using the Real-time Transport Protocol (RTP) are identified by UDP port number range.
Class map	Criteria that are specified in a named class-map object.

Prerequisites for Classification

Classification has the following prerequisites:

- You are logged in to the CLI in EXEC mode.

Guidelines and Limitations

Classification has the following guidelines and limitations:

- You can specify a maximum of 32 match criteria in a class map.
- You can configure a maximum of 64 classes for use in a single policy map, if no policers are configured.
- When you match on an ACL, the only other match that you can specify is the Layer 3 packet length in a match-all class.
- You can classify traffic on Layer 2 ports based on the port policy of the incoming packet.

Classifying Traffic

This section describes how to classify traffic:

Classifying ACL Traffic

You can classify traffic by matching packets based on existing access control lists (ACLs).

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- QoS does not use the permit-deny functions of ACLs. The **permit** and **deny** ACL keywords are ignored when matching.
- QoS does not support the **not** form of this command.
- If you configure the class to match-all ACLs, no other match criteria, except packet length, can be specified. If you configure the class to match-any ACL, you can match ACLs and any other match criteria.
- You are logged in to the CLI in EXEC mode.
- Tunneled IP packets are not matched unless the tunneling protocol is also IP, and then the match applies to the outer IP header and not the encapsulated IP header.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match access-group name** *acl_name*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
	
	Example:
	`n1000v(config)# class-map class_acl`
	`n1000v(config-cmap_qos)#`
		Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**match access-group name** *acl-name* **Example:** `n1000v(config-cmap-qos)# match access-group name my_acl`	Configures and saves the access group to match for this class in the running configuration. **Note** The **permit** and **deny** keywords are ignored when matching the ACL. **Note** The **not** form of this command is not supported.
Step 4	**show class-map** *class_map_name* **Example:** `n1000v(config-cmap-qos)# show class-map class_acl1`	Displays the class map configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-cmap-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Classifying DSCP Traffic

You can classify traffic based on the DSCP value in the DiffServ field of the IP header. The standard DSCP values are found in the "DSCP and Precedence Values" section on page 6-1.

Note Tunneled IP packets are not matched unless the tunneling protocol is also IP, and then the match applies to the outer IP header and not the encapsulated IP header.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **dscp** *dscp_list*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

`DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** n1000v(config)# class-map class_dscp n1000v(config-cmap-qos)#	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **dscp** *dscp_list* **Example:** n1000v(config-cmap-qos)# match dscp af21, af32	Configures the traffic class by matching packets that are based on *dscp-values*. The standard DSCP values are listed in the "DSCP and Precedence Values" section on page 6-1. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example:** n1000v(config-cmap-qos)# show class-map class_dscp	Displays the class map configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-cmap-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring IP Precedence Classification

You can classify traffic based on the precedence value in the type of service (ToS) byte field of the IP header. Precedence values can be found in the "DSCP and Precedence Values" section on page 6-1.

Note Tunneled IP packets are not matched unless the tunneling protocol is also IP, and then the match applies to the outer IP header and not the encapsulated IP header.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **precedence** *values*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

`DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** n1000v(config)# class-map class_ip_precedence n1000v(config-cmap-qos)#	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **precedence** *values* **Example:** n1000v(config-cmap-qos)# match precedence 1-2, 5-7	Configures the traffic class by matching packets that are based on *precedence-values*. Values are listed in the "DSCP and Precedence Values" section on page 6-1. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example**: n1000v(config-cmap-qos)# show class-map class_ip_precedence	Displays the class map configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-cmap-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring QoS Group Classification

You can classify traffic based on the value of the QoS group internal label, which is not part of the packet payload or any packet header. You can set the value of the QoS group within a policy map using the **set qos-group** command as described in the "Creating a QoS Group Policy" section on page 3-7.

Note You match on the QoS group only in egress policies because its value is undefined until you set it in an ingress policy.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **qos-group** *multi-range-qos-group-values*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
	
	Example:
	`n1000v(config)# class-map class_qos_group`
	`n1000v(config-cmap-qos)#`
		Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.
		
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**match** [**not**] **qos-group** *multi-range-qos-group-values* **Example:** `n1000v(config-cmap-qos)# match qos-group 4, 80-90`	Configures the traffic class by matching packets that are based on a list of QoS group values. Values can range from 0 to 126. The default QoS group value is 0. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example**: `n1000v(config-cmap-qos)# show class-map class_qos_group`	Displays the class map configuration for the specified traffic class name.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-cmap-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring Discard Class Classification

You can classify traffic based on the value of the discard class internal label, which is not part of the packet payload or any packet header. You can set the value of the discard class within a policy map using the **set discard-class** command as described in the "Creating a Discard Class Policy" section on page 3-8.

Note You match on the discard class only in egress policies because its value is undefined until you set it in an ingress policy.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **discard-class** *multi-range-discard-class-values*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
	
	Example:
	`n1000v(config)# class-map class_discard_class`
	`n1000v(config-cmap-qos)#`
		Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**match** [**not**] **discard-class** *multi-range-discard-class-values*
	
	Example:
	`n1000v(config-cmap-qos)# match discard-class 4, 60-62`
	`n1000v(config-cmap-qos)#`
		Configures the traffic class by matching packets that are based on the list of discard-class values. Values can range from 0 to 63. The default discard class value is 0. Use the **not** keyword to match on values that do not match the specified range.

Step 4	**show class-map** *class_map_name*
	
	Example:
	`n1000v(config-cmap-qos)# show class-map class_discard_class`
	`n1000v(config-cmap-qos)#`
		Displays the specified class map configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v(config-cmap-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring Layer 3 Packet Length Classification

You can classify Layer 3 traffic based on various packet lengths.

Note This feature is designed for IP packets only.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **packet length** *packet-length-list*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** n1000v(config)# class-map class_packet_length	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **packet length** *packet-length-list* **Example:** n1000v(config-cmap-qos)# match packet length 2000	Configures the traffic class by matching packets that are based on various packet lengths. Values can range from 1 to 9198. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example**: n1000v(config-cmap-qos)# show class-map class_packet_length n1000v(config-cmap-qos)#	Displays the specified class map configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-cmap-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring CoS Classification

You can classify traffic based on the class of service (CoS) in the IEEE 802.1Q header. This 3-bit field is defined in IEEE 802.1p to support QoS traffic classes. CoS is encoded in the high order 3 bits of the VLAN ID Tag field and is referred to as user_priority.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **cos** *cos-list*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** `n1000v(config)# class-map class_cos`	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **cos** *cos-list* **Example:** `n1000v(config-cmap-qos)# match cos 4, 5-6`	Configures the traffic class by matching packets that are based on the list of CoS values. Values can range from 0 to 7. Use the **not** keyword to match on values that do not match the specified range.

Step 4	**show class-map** *class_map_name*
	
	Example:
	`n1000v(config-cmap-qos)# show class-map class_cos`
	`n1000v(config-cmap-qos)#`
		Displays the specified class map configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v(config-cmap-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring IP RTP Classification

The IP Real-time Transport Protocol (RTP) is a transport protocol for real-time applications that transmits data such as audio or video and is defined by RFC 3550. Although RTP does not use a common TCP or UDP port, you typically configure RTP to use ports 16384 to 32767. UDP communications use an even port and the next higher odd port is used for RTP Control Protocol (RTCP) communications.

You can configure classification based on UDP port ranges, which are likely to target applications using RTP.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **ip rtp** *udp-port-values*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** n1000v(config)# class-map class_rtp n1000v(config-cmap-qos)#	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **ip rtp** *udp-port-values* **Example:** n1000v(config-cmap-qos)# match ip rtp 2000-2100, 4000-4100	Configures the traffic class by matching packets that are based on the range of lower and upper UDP port numbers, which is likely to target applications using RTP. Values can range from 2000 to 65535. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example**: n1000v(config-cmap-qos)# show class-map class_rtp	Displays the specified class map configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-cmap-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring Class Map Classification

You can classify traffic based on the match criteria in another class map.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- The referenced class map must be created prior to its reference.
- You can reference the same class map in multiple policies.
- You can configure only one level of nesting of class maps. You cannot reference a class map that references another class map.
- Before you delete a referenced class map, you should delete all references to that class map.
- To perform a logical OR with the class map that is specified in the **match class-map** command, use the **match-any** keyword. The **match-any** or **match-all** specification of the matched class map is ignored.
- To perform a logical AND with the class map that is specified in the **match class-map** command, use the **match-all** keyword. The **match-any** or **match-all** specification of the matched class map is ignored.

SUMMARY STEPS

1. **config t**
2. **class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name*
3. **match** [**not**] **class-map** *class_map_name*
4. **show class-map** *class_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**class-map** [**type qos**] [**match-any** | **match-all**] *class_map_name* **Example:** n1000v(config)# class-map class_class_map n1000v(config-cmap-qos)#	Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**match** [**not**] **class-map** *class_map_name* **Example:** n1000v(config-cmap-qos)# match class-map class_map3	Configures the traffic class by matching packets that are based on the match criteria in another class map. Because match-all is the default for the **class-map** command, the match criteria that is specified in class_map3 are ANDed with match criteria in class_class_map. Use the **not** keyword to match on values that do not match the specified range.
Step 4	**show class-map** *class_map_name* **Example:** n1000v(config-cmap-qos)# show class-map class_class_map	Displays the specified class map configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-cmap-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the Classification Configuration

To verify the classification configuration, use the commands in the following table:

Command	Description
show class-map *name*	Displays the class map configuration for all class maps or for a specified class map.
show ip access-lists *name*	Displays all IPv4 access control lists (ACLs) or a specific IPv4 ACL.

Configuration Example for QoS Classification

This example shows how to configure classification for the class map named *cmap1*, which matches DSCP traffic AF21 and AF32:

```
n1000v(config)# class-map type qos match-all cmap1
```

```
n1000v(config-cmap-qos)# match dscp af21 af32
n1000v(config-cmap-qos)# exit
n1000v(config)#
```

Feature History for QoS Classification

This section provides the QoS Classification release history.

Feature Name	Releases	Feature Information
QoS Classification	4.0	This feature was introduced.

CHAPTER 3

Configuring QoS Marking Policies

This chapter describes how to configure QoS marking policies on Cisco Nexus 1000V to prioritize network traffic.

Information About Policy Maps

Policy maps prioritize network traffic by class. You create policy maps to define how to treat each class of traffic so that it is prioritized for the best quality of service.

Marking is the process of marking packets, that is, changing one of the following in the packet for QoS purposes:

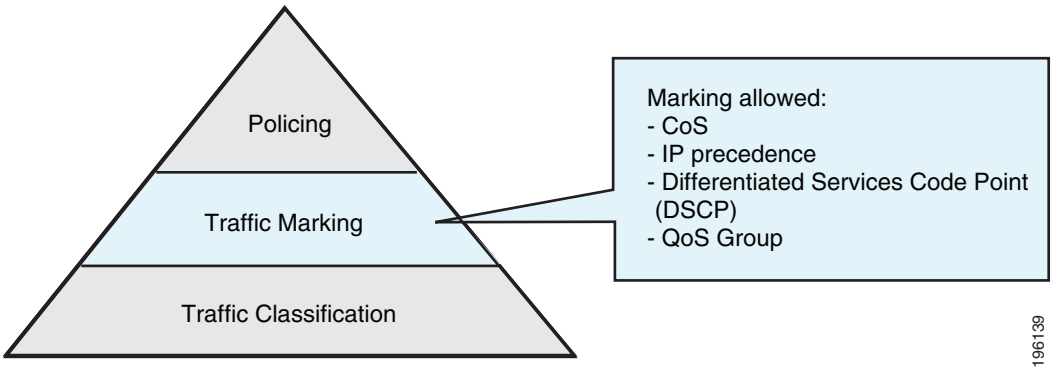
- Differentiated services code point (DSCP)
- Precedence
- CoS

You can map a traffic class to a DSCP, which is an indicator of the service level for a specified frame. The DSCP value ranges from 0 to 63, and the default is 0. A DSCP value of 46 is disallowed.

Service policies are specified using policy maps. Policy maps provide an ordered mapping of class maps to service levels. You can specify multiple class maps within a policy map, and map a class map to a high, medium, or low service level. The default priority is low. The policy map name is restricted to 63 alphanumeric characters.

The order of the class maps within a policy map is important to determine the order in which the frame is compared to class maps. The first matching class map has the corresponding priority marked in the frame.

Figure 3-1 Packet Fields Available for Marking



Marking is the setting of QoS information that is related to a packet. You can set the value of standard QoS fields IP precedence, DSCP and Class of Service (CoS), and internal labels that can be used in subsequent actions such as policing.

Once your traffic classes are defined, you can reference them in the policy map where you also define how they should be marked. We recommend that you keep the policy simple by using no more than four classes.

The fields available for marking are listed in Table 3-1.

Table 3-1 Fields That Can be Marked

Field	Description
DSCP	Layer 3 differentiated services code point (DSCP). **Note** If you mark DSCP, you cannot mark Discard Class.
IP precedence	Layer 3 IP precedence. **Note** IP precedence uses only the lower 3 bits of the type of service (ToS) field. The device overwrites the first 3 bits of the ToS field to 0.
CoS	Layer 2 class of service (CoS).
QoS group	Local QoS values that can be marked and matched as needed. The range is from 0 to 126.
Discard class	Local QoS values that can be matched and marked as needed. The range is from 0 to 63. **Note** If you mark Discard Class, you cannot mark DSCP.
Ingress and egress ports	The marking applies to incoming or outgoing packets.

For a single class, you can set operations on any two out of the following five fields: CoS, IP Precedence, DSCP, QoS Group, and Discard Class.

Unless noted as a restriction, you can mark both incoming and outgoing packets.

Prerequisites for QoS Marking Policies

Marking has the following prerequisites:

- You must have already classified your network traffic. For more information, see the "Configuring QoS Classification" section on page 2-1.
- You are already logged in to the CLI in EXEC mode.

Guidelines and Limitations

QoS policies have the following guidelines and limitations:

- The **set cos** command is applicable only to 802.1Q interfaces. So, although you can use the **set cos** command on an ingress interface, the setting is only applied if a packet eventually egresses an 802.1Q compliant interface.
- For a single class, you can set operations on any two out of the following five fields: CoS, IP Precedence, DSCP, QoS Group, and Discard Class.
- You can only use the **set qos-group** command in ingress policies.
- You can only use the **set discard-class** command in ingress policies.
- When designing your QoS and access control list (ACL) policies, note that ACLs referenced within a QoS policy are processed as follows as part of the QoS policy:
  - QoS ingress processing follows ACL processing.
  - QoS egress processing precedes ACL egress processing.

Creating QoS Marking Policies

This section describes how to create QoS policies for the Cisco Nexus 1000V.

Creating a DSCP Policy

You can create a policy that marks the DSCP value in the IP header packet to prioritize traffic in a particular class.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- DSCP is described in RFC 2475.
- You are logged in to the CLI in EXEC mode.
- If you use DSCP marking, you cannot use Discard Class marking (see the "Creating a Discard Class Policy" section on page 3-8).
- You can mark the DSCP field as a numeric value between 0 and 63 or as one of the commonly used values listed in the "DSCP and Precedence Values" section on page 6-1.

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set dscp** *value*
5. **show policy-map** *policy-map-name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name*
	
	Example:
	`n1000v(config)# policy-map policy1`
	`n1000v(config-pmap-qos)#`
		Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration.
		
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** `n1000v(config-pmap)# class class1`	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set dscp** *value* **Example:** `n1000v(config-pmap-c-qos)# set dscp af31`	Defines the DSCP value that should be used in all IP headers for the specified class and saves it in the running configuration. You can use a numeric value from 1 to 60 or one of the standard values from the "DSCP and Precedence Values" section on page 6-1. In this example, the standard value of af31 is used.
Step 5	**show policy-map** *policy_map_name* **Example:** `n1000v(config-pmap-c-qos)# show policy-map policy1`	Displays the policy map configuration for the specified map name.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-pmap-c-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating an IP Precedence Policy

You can mark IP Precedence to give priority to all packets in a particular traffic class.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Table 3-2 lists the RFC 791 precedence values from least to most important.

Table 3-2 Precedence Values

Value	Description
000 (0)	Routine or Best Effort
001 (1)	Priority
010 (2)	Immediate
011 (3)	Flash (mainly used for voice signaling or for video)
100 (4)	Flash Override
101 (5)	Critical (mainly used for voice RTP)
110 (6)	Internet
111 (7)	Network

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set precedence** *value*
5. **show policy-map** *policy-map-name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name*
	
	Example:
	`n1000v(config)# policy-map policy1`
	`n1000v(config-pmap-qos)#`
		Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration.
		
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

	Command	Purpose
Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** `n1000v(config-pmap-qos)# class class1`	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set precedence** *value* **Example:** `n1000v(config-pmap-c-qos)# set precedence 3`	Adds the precedence value that should be used in all packets for the specified traffic class. The change is saved in the running configuration. You can use a numeric value from 0 to 7, as show in Table 3-2.
Step 5	**show policy-map** *policy_map_name* **Example:** `n1000v(config-pmap-c-qos)# show policy-map policy1`	Displays the policy map configuration for the specified map name.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-pmap-c-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a Class of Service Policy

You can mark the CoS field in the IEEE 802.1Q header for all traffic in a specific class. If you mark this field in an ingress or egress policy, it will only be set when a packet egresses an IEEE 802.1Q-capable interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can set CoS in ingress and egress policies.

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set cos** *cos-value*
5. **show policy-map** *policy-map-name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name*
	
	Example:
	`n1000v(config)# policy-map policy1`
	`n1000v(config-pmap-qos)#`
		Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration.
		
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** `n1000v(config-pmap-qos)# class class1`	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set cos** *cos-value* **Example:** `n1000v(config-pmap-c-qos)# set cos 3`	Sets the CoS value to *cos-value*. The value can range from 0 to 7. You can use this command only in egress policies.
Step 5	**show policy-map** *policy_map_name* **Example**: `n1000v(config-pmap-c-qos)# show policy-map policy1`	Displays the policy map configuration for the specified map name.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-pmap-c-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a QoS Group Policy

You can mark the locally defined QoS group value.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You can mark the QoS group value only in ingress policies.
- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**

2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set qos-group** *qos-group-value*
5. **show policy-map** *policy-map-name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name*
	
	Example:
	`n1000v(config)# policy-map policy1`
	`n1000v(config-pmap-qos)#`
		Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration.
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3	**class** [**type qos**] {*class_map_name* | **class-default**}
	
	Example:
	`n1000v(config-pmap-qos)# class class1`
	`n1000v(config-pmap-c-qos)#`
		Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration.
		Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

Step 4	**set qos-group** *qos-group-value* **Example:** `n1000v(config-pmap-c-qos)# set qos-group 100`	Sets the QoS group value to *qos-group-value*. The value can range from 0 to 126.
Step 5	**show policy-map** *policy_map_name* **Example**: `n1000v(config-pmap-c-qos)# show policy-map policy1`	Displays the policy map configuration for the specified map name.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-pmap-c-qos)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating a Discard Class Policy

You can set a local internal label discard class policy.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- If you configure a local internal label discard class policy, you cannot create a DSCP policy. For more information about DSCP policies, see the "Creating a DSCP Policy" procedure on page 3-3.
- You can set a discard class only in ingress policies.
- To reference the local discard class in a policy or in traffic classification, use the **match discard-class** command.

  For more information, see the "Configuring Discard Class Classification" procedure on page 2-8.

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set discard-class** *discard-class-value*
5. **show policy-map** *policy-map-name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** n1000v(config)# policy-map policy1 n1000v(config-pmap-qos)#	Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

	Command	Purpose
Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** n1000v(config-pmap-qos)# class class1	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**set discard-class** *discard-class-value* **Example:** n1000v(config-pmap-c-qos)# set discard-class 40	Sets the discard class value to *discard-class-value*. The value can range from 0 to 63.
Step 5	**show policy-map** *policy_map_name* **Example**: n1000v(config-pmap-c-qos)# show policy-map policy1	Displays the policy map configuration for the specified map name.
Step 6	**copy running-config startup-config** **Example:** n1000v(config-pmap-c-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Creating Ingress and Egress Policies

You can attach a policy map to an interface or a port profile so that the marking instructions are applied to the ingress or egress packets.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- The interface or port profile have been created.
- The policy map that you want to use has been defined.

Note You can attach only one input policy and one output policy to an interface or port profile.

SUMMARY STEPS

1. **config t**
2. Enter one of the following commands:
   - **interface** *type number*
   - **port-profile** *name*
3. **service-policy** [**type qos**] {**input** | **output**} *policy-map-name* [**no-stats**]
4. **show policy-map** *policy_map_name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	Enter one of the following commands: • **interface** *type number* • **port-profile** *name* **Example:** n1000v(config)# interface ethernet 1/1 n1000v(config-if)#	Places you into Configuration mode for the specified Ethernet or vEthernet interface or port profile.
Step 3	**service-policy** [**type qos**] {**input** | **output**} *policy-map-name* [**no-stats**] **Example:** n1000v(config-if)# service-policy input policy1	(Optional) Attaches a policy map name that will be added to the input or output packets of the interface or port profile. **Note** You can attach only one input policy and one output policy to an interface or port profile.
Step 4	**show policy-map** *policy_map_name* **Example**: n1000v(config-if)# show policy-map policy1	Displays the policy map configuration for the specified map name.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to configure an ingress policy on an Ethernet interface:

```
n1000v# config t
n1000v(config)# interface ethernet 1/1
n1000v(config-if)# service-policy input policy1
n1000v(config-if)# show policy-map policy1


  Type qos policy-maps
  ====================

  policy-map type qos policy1
n1000v(config-if)# copy running-config startup-config
```

This example shows how to configure an ingress policy on a port profile:

```
n1000v# config t
n1000v(config)# port-profile accessprofile
n1000v(config-port-prof)# service-policy input policy1
n1000v(config-port-prof)# show policy-map policy1

  Type qos policy-maps
```

```
  ====================

  policy-map type qos policy1
n1000v(config-port-prof)# copy running-config startup-config
```

Marking the Port DSCP

You can mark the DSCP port for each class of traffic that is defined in a specified ingress or egress policy map.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- The default behavior is to preserve the DSCP value, or to trust DSCP. To make the port untrusted, change the DSCP value.
- Unless you configure a QoS policy and attach that policy to specified interfaces, the DSCP value is preserved.
- The class map that you want to use has been defined. See Chapter 2, "Configuring QoS Classification."

Note You can attach only one input policy and one output policy to an interface or port profile.

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **set dscp**-*value*
5. Repeat steps 3. and 4. for each class map that you want to create.
6. **exit**
7. **exit**
8. Enter one of the following commands:
   - **interface** *type number*
   - **port-profile** *name*
9. **service-policy** [**type qos**] {**input** | **output**} *policy-map-name* [**no-stats**]
10. **show policy-map** *policy_map_name*
11. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name*
	
	Example:
	`n1000v(config)# policy-map policy1`
	`n1000v(config-pmap-qos)#`
		Places you into policy map QoS configuration mode for the specified policy map and configures the map name in the running configuration.
		
		The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.

Step 3a	**class** [**type qos**] {*class_map_name* | **class-default**}
	
	Example:
	`n1000v(config-pmap)# class class1`
	`n1000v(config-pmap-c-qos)#`
		Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration.
		
		Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

Step 4b	**set dscp** *value* **Example:** `n1000v(config-pmap-c-qos)# set dscp af31`	Sets a DSCP value. Valid values are shown in the "DSCP and Precedence Values" section on page 6-1.
Step 5	Repeat Step 3 and Step 4 for each class map that you want to create.	

Step 6	**exit**
	
	Example:
	`n1000v(config-pmap-c-qos)# exit`
	`n1000v(config-pmap-qos)#`
		Returns you to policy map configuration mode.

Step 7	**exit**
	
	Example:
	`n1000v(config-pmap-qos)# exit`
	`n1000v(config)#`
		Returns you to global configuration mode.

	Command	Purpose

Step 8	Enter one of the following commands:
	• **interface** *type number*
	• **port-profile** *name*
	Example:
	`n1000v(config)# interface ethernet 1/1`
	`n1000v(config-if)#`
		Places you into the configuration mode for the specified Ethernet or vEthernet interface or port profile.

Step 9	**service-policy** [**type qos**] {**input** | **output**} *policy-map-name* [**no-stats**] **Example:** `n1000v(config-if)# service-policy input policy1`	(Optional) Attaches a policy map name that will be added to the input or output packets of the interface or port profile. **Note** You can attach only one input policy and one output policy to an interface or port profile.
Step 10	**show policy-map** *policy_map_name* **Example**: `n1000v(config-if)# show policy-map policy1`	Displays the policy map configuration for the specified map name.
Step 11	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to mark the DSCP port for each class of traffic defined in an ingress policy map on an Ethernet interface.

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap)# class class1
n1000v(config-pmap-c-qos)# set dscp af31
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# class class2
n1000v(config-pmap-c-qos)# set dscp af13
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# set dscp af22
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# exit
n1000v(config)# interface ethernet 1/1
n1000v(config-if)# service-policy input policy1
n1000v(config-if)# show policy-map policy1


  Type qos policy-maps
  ====================

  policy-map type qos policy1
    class  class1
      set dscp af31
    class  class2
      set dscp af13
    class  class-default
      set dscp af22
n1000v(config-if)# copy running-config startup-config
```

This example shows how to mark the DSCP port for each class of traffic defined in an ingress policy map on a port profile.

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class1
n1000v(config-pmap-c-qos)# set dscp af31
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# class class2
n1000v(config-pmap-c-qos)# set dscp af13
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# set dscp af22
n1000v(config-pmap-c-qos)# exit
n1000v(config-pmap-qos)# exit
n1000v(config)# port-profile accessprofile
n1000v(config-port-prof)# service-policy input policy1
n1000v(config-port-prof)# show policy-map policy1


  Type qos policy-maps
  ====================

  policy-map type qos policy1
    class  class1
      set dscp af31
    class  class2
      set dscp af13
    class  class-default
      set dscp af22
n1000v(config-port-prof)# copy running-config startup-config
```

Verifying the QoS Policy Configuration

To verify the QoS policy configuration, perform one of the following tasks:

Command	Description
show policy-map [**type qos**] [**name** *policy_map_name*]	Displays the policy map configuration.
show table-map *name*	Displays the table map configuration.

Configuration Example for QoS Marking Policies

This example shows how to display a specific policy-map policy:

```
n1000v(config)# show policy-map policy-ipacl
  Type qos policy-maps
  ====================
  policy-map type qos policy-ipacl
    class  class-ipacl
      set dscp 10
```

This example shows how to display policy maps for all interfaces:

```
n1000v# show policy-map interface brief

Interface/VLAN [Status]:INP QOS       OUT QOS       INP QUE       OUT QUE
================================================================================
Vethernet1      [Active]:              media
Vethernet10     [Active]:              media
Vethernet13     [Active]:web_policer
Vethernet15     [Active]:iperf
Vethernet16     [Active]:              iperf_policer
Vethernet17     [Active]:ixia_in       ixia_out
Vethernet18     [Active]:              media
Vethernet19     [Active]:iperf
Vethernet20     [Active]:              iperf_policer
Vethernet21     [Active]:netperf_polic

================================================================================
```

Feature History for QoS Marking Policies

This section provides the QoS marking policies release history.

Feature Name	Releases	Feature Information
QoS Marking Policies	4.0	This feature was introduced.
QoS Marking Policies	4.0(4)SV1(2)	DSCP and Discard Class are no longer mutually exclusive. For a single class, you can set operations on any two out of the following five fields: CoS, IP Precedence, DSCP, QoS Group, and Discard Class.

CHAPTER 4

Configuring QoS Policing

This chapter describes how to configure policing of traffic classes for Cisco Nexus 1000V.

Information About Policing

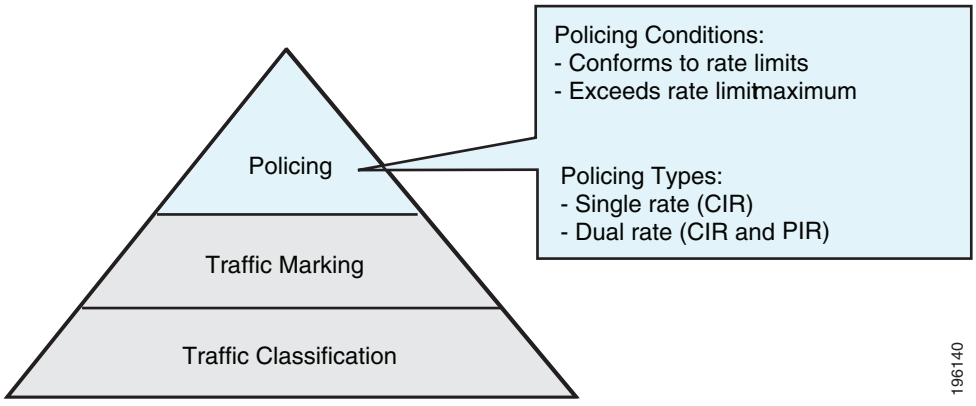
Policing is the monitoring of data rates for a particular class of traffic. The Cisco Nexus 1000V can also monitor associated burst sizes.

Three conditions, are determined by the policer depending on the data rate parameters supplied: conform (green), exceed (yellow), or violate (red). You can configure only one action for each condition. When the data rate exceeds the user-supplied values, packets are either marked down or dropped.

You can define single-rate or dual-rate policers. Single-rate policers monitor the specified committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic. Figure 4-1shows policing conditions and types.

For more information about policies, see RFC 2697, RFC 2698, and RFC 4115.

Figure 4-1 Policing Conditions and Types



The following conditions trigger actions by the policer depending on the defined data rate:

Condition	Color	Description	Policer Action (only one allowed per condition)
Conform	Green	The packet traffic data rate is within the defined boundaries.	The policer either transmits these packets as is, or changes the value in the header (DSCP, precedence, or CoS), and then transmits these packets.
Exceed	Yellow	The packet traffic data rate exceeds the defined boundary.	The policer can drop or mark down these packets.
Violate	Red	The packet traffic data rate violates the defined boundaries.	The policer can drop or mark down these packets.

Prerequisites for Policing

Policing has the following prerequisites:

- You must be familiar with RFC 2698.
- You are logged on to the CLI in EXEC mode.

Guidelines and Limitations

Use the following guideline to configure policing:

- Each module polices independently, which might affect a policer that is applied to traffic distributed across more than one module, such as in the case of a port channel interface.

Configuring Policing

You can configure a single- or dual-rate policer in the Cisco Nexus 1000V.

Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing

The type of policer that is created by the Cisco Nexus 1000V is based on a combination of the **police** command arguments described in Table 4-1.

Note Specify the identical value for **pir** and **cir** to configure 1-rate 3-color policing.

Table 4-1 Arguments to the Police Command

Argument	Description
cir	Committed information rate, or desired bandwidth, specified as a bit rate or a percentage of the link rate. Although a value for **cir** is required, the argument itself is optional. The range of values is from 1 to 80000000000; the range of policing values that are mathematically significant is 8000 to 80 Gbps.
percent	Specifies the rate as a percentage of the interface rate. The range of values is from 1 to 100%.
bc	Indication of how much the **cir** can be exceeded, either as a bit rate or an amount of time at **cir**. The default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes, and the Gigabit per second (gbps) rate is not supported for this parameter.
pir	Peak information rate, which is specified as a PIR bit rate or a percentage of the link rate. There is no default. The range of values is from 1 to 80000000000; the range of policing values that are mathematically significant is from 8000 to 80 Gbps. The range of percentage values is from 1 to 100%.
be	Indication of how much the **pir** can be exceeded, either as a bit rate or an amount of time at **pir**. When the **bc** value is not specified, the default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes, and the Gigabit per second (gbps) rate is not supported for this parameter. **Note** You must specify a value for **pir** before the device displays this argument.
conform	Single action to take if the traffic data rate is within bounds. The basic actions are transmit or one of the **set** commands listed in Table 4-4. The default is transmit.
exceed	Single action to take if the traffic data rate exceeds the specified boundaries. The basic actions are drop or markdown. The default is drop.
violate	Single action to take if the traffic data rate violates the configured rate values. The basic actions are drop or markdown. The default is drop.

Although all the arguments in Table 4-1 are optional, you must specify a value for **cir**. In this section, **cir** indicates what is its value but not necessarily the keyword itself. The combination of these arguments and the resulting policer types and actions are shown in Table 4-2.

Table 4-2 Policer Types and Actions

Police Arguments Present	Policer Type	Policer Action
cir, but not **pir**, **be**, or **violate**	1-rate, 2-color	≤**cir**, then **conform**; otherwise **violate**
cir and **pir**	1-rate, 3-color	≤**cir**, then **conform**; ≤**pir**, then **exceed**; otherwise **violate** **Note** You must specify identical values for **cir** and **pir**.
cir and **pir**	2-rate, 3-color	≤**cir**, then **conform**; ≤**pir**, then **exceed**; otherwise **violate**

The policer actions that you can specify are described in Table 4-3 and Table 4-4.

Table 4-3 Policer Actions for Exceed or Violate

Action	Description
drop	Drops the packet. This action is available only when the packet exceeds or violates the parameters.
set dscp dscp table {*cir-markdown-map* | *pir-markdown-map*}	Sets the specified fields from a table map and transmits the packet. For more information on the system-defined, or default table maps, see Chapter 3, "Configuring QoS Marking Policies." This is available only when the packet exceeds the parameters (use the cir-markdown-map) or violates the parameters (use the pir-markdown-map).

Table 4-4 Policer Actions for Conform

Action	Description
transmit	Transmits the packet. This action is available only when the packet conforms to the parameters.
set-prec-transmit	Sets the IP precedence field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-dscp-transmit	Sets the DSCP field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-cos-transmit	Sets the CoS field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-qos-transmit	Sets the QoS group internal label to specified value and transmits the packet. This action can be used only in input policies and is available only when the packet conforms to the parameters.
set-discard-class-transmit	Sets the discard-class internal label to a specified value and transmits the packet. This action can be used only in ingress policies and is available only when the packet conforms to the parameters.

Note The policer can only drop or mark down packets that exceed or violate the specified parameters. See Chapter 3, "Configuring QoS Marking Policies" for information on marking down packets.

The data rates that are used in the **police** command are described in Table 4-5.

Table 4-5 Data Rates for the police Command

Rate	Description
bps	Bits per second (default)
kbps	1,000 bits per seconds
mbps	1,000,000 bits per second
gbps	1,000,000,000 bits per second

Burst sizes that are used in the **police** command are described in Table 4-6.

Table 4-6 Burst Sizes for the police Command

Speed	Description
bytes	bytes
kbytes	1,000 bytes
mbytes	1,000,000 bytes
ms	milliseconds
us	microseconds

SUMMARY STEPS

Note You must specify the identical value for **pir** and **cir** to configure 1-rate, 3-color policing.

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]] [**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] {**conform** {**transmit** | **set-prec-transmit** | **set-dscp-transmit** | **set-cos-transmit** | **set-qos-transmit** | **set-discard-class-transmit**} [**exceed** {**drop** | **set dscp dscp table** {*cir-markdown-map*}} [**violate** {**drop** | **set dscp dscp table** {*pir-markdown-map*}}]}
5. **show policy-map** [**type qos**] [*policy-map-name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** n1000v(config)# policy-map policy1 n1000v(config-pmap-qos)#	Places you into policy map QoS configuration mode and creates or accesses the specified policy map. The *class_map_name* argument is an alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** n1000v(config-pmap-qos)# class class-default n1000v(config-pmap-c-qos)#	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

	Command	Purpose
Step 4	**police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]][**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] [**conform** {**transmit** | **set-prec-transmit** | **set-dscp-transmit** | **set-cos-transmit** | **set-qos-transmit** | **set-discard-class-transmit**} [**exceed** {**drop** | **set dscp dscp table** {*cir-markdown-map*}} [**violate** {**drop** | **set dscp dscp table** {*pir-markdown-map*}}]] **Example:** n1000v(config-pmap-c-qos)# police cir 256000 conform transmit violate set dscp dscp table pir-markdown-map n1000v(config-pmap-c-qos)#	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is ≤**cir**. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, then the **exceed** action is taken if the data rate ≤**pir**; otherwise the **violate** action is taken. The actions are described in Table 4-3 and Table 4-4. The data rates and link speeds are described in Table 4-5 and Table 4-6. **Note** You must specify identical values for **cir** and **pir.**
Step 5	**show policy-map** [**type qos**] [*policy-map-name*] **Example:** n1000v(config-pmap-c-qos)# show policy-map	(Optional) Displays information about all configured policy maps or a selected policy map of type QoS.
Step 6	**copy running-config startup-config** **Example:** n1000v(config-pmap-c-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to configure a 1-rate, 2-color policer that transmits if the data rate is within 200 milliseconds of traffic at 256000 bps and marks DSCP to the values that are configured in the table map if the data rate is violated:

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 conform transmit violate set dscp dscp table
pir-markdown-map
n1000v(config-pmap-c-qos)# show policy-map


  Type qos policy-maps
  ====================

  policy-map type qos policy1
    class  class1
      set dscp af31
    class  class2
      set dscp af13
    class  class-default
      set dscp af22
      police cir 256000 bps bc 200 ms conform transmit violate set dscp dscp tab
le pir-markdown-map
n1000v(config-pmap-c-qos)# copy running-config startup-config
```

This example shows how to configure a 1-rate, 3-color policer that transmits if the data rate is within 200 milliseconds of traffic at 256000 bps, and marks DSCP to the values that are configured in the table map if the data rate is violated:

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 pir 256000 conform transmit exceed
set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# show policy-map


  Type qos policy-maps
  ====================

  policy-map type qos policy1
    class  class1
      set dscp af31
    class  class2
      set dscp af13
    class  class-default
      set dscp af22
      police cir 256000 bps bc 200 ms pir 256000 bps be 200 ms conform transmit
exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# copy running-config startup-config
```

Configuring Ingress and Egress Policing

You can apply the policing instructions in a QoS policy map to ingress or egress packets by attaching that QoS policy map to an interface or port profile. To select ingress or egress, you specify either the **input** or **output** keyword in the **service-policy** command. For an example of how to use the **service-policy** command, see the "Creating Ingress and Egress Policies" procedure on page 3-10.

Configuring Markdown Policing

Markdown policing is the setting of a QoS field in a packet when traffic exceeds or violates the policed data rates. You can configure markdown policing by using the **set** commands for that are described in Table 4-3 and Table 4-4.

SUMMARY STEPS

1. **config t**
2. **policy-map** [**type qos**] [**match-first**] *policy-map-name*
3. **class** [**type qos**] {*class_map_name* | **class-default**}
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]] [**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] {**conform** *action* [**exceed** {**drop** | **set dscp dscp table** *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]]}}
5. **show policy-map** [**type qos**] [*policy-map-name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	**policy-map** [**type qos**] [**match-first**] *policy-map-name* **Example:** n1000v(config)# policy-map policy1 n1000v(config-pmap-qos)#	Creates or accesses the policy-map named *policy-map-name,* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	**class** [**type qos**] {*class_map_name* | **class-default**} **Example:** n1000v(config-pmap-qos)# class class-default n1000v(config-pmap-c-qos)#	Creates a reference to *class-map-name* and enters policy-map class QoS configuration mode for the specified class map. By default, the class is added to the end of the policy map. Changes are saved in the running configuration. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.
Step 4	**police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]] [**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] {**conform** *action* [**exceed** {**drop** | **set dscp dscp table** *cir-markdown-map*} [**violate** {**drop** | **set dscp dscp table** *pir-markdown-map*}]]}} **Example:** n1000v(config-pmap-c-qos)# police cir 256000 be 300 ms conform transmit exceed set dscp dscp table cir-markdown-map violate drop	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is ≤**cir**. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, then the **exceed** action is taken if the data rate ≤**pir**, and the **violate** action is taken otherwise. The actions are described in Table 4-3 and Table 4-4. The data rates and link speeds are described in Table 4-5 and Table 4-6.
Step 5	**show policy-map** [**type qos**] [*policy-map-name*] **Example:** n1000v(config-pmap-c-qos)# show policy-map	(Optional) Displays information about the policy map configuration.
Step 6	**copy running-config startup-config** **Example:** n1000v(config-pmap-c-qos)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows a 1-rate, 3-color policer that transmits if the data rate is within 300 milliseconds of traffic at 256000 bps; marks down DSCP using the system-defined table map if the data rate is within 300 milliseconds of traffic at 256000 bps; and drops packets otherwise:

```
n1000v# config t
n1000v(config)# policy-map policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police cir 256000 bps bc 300 ms pir 256000 conform transmit
exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# show policy-map policy1


  Type qos policy-maps
  ====================

  policy-map type qos policy1
    class  class-default
      police cir 256000 bps bc 300 ms pir 256000 bps be 300 ms conform transmit
exceed set dscp dscp table cir-markdown-map violate drop
n1000v(config-pmap-c-qos)# copy running-config startup-config
```

Verifying the Policing Configuration

To verify the policing configuration, perform the following task:

Command	Description
show policy-map	Displays information about policy maps and policing.

Configuration Example for QoS Policing

The following example shows how to configure a 1-rate, 2-color policer:

```
config t
  policy-map policy1
    class one_rate_2_color_policer
      police cir 256000 conform transmit violate drop
```

The following example shows how to configure a 1-rate, 2-color policer with DSCP mark down:

```
config t
  policy-map policy2
    class one_rate_2_color_policer_with_dscp_markdown
      police cir 256000 conform set-dscp-transmit af11 violate set dscp dscp table
pir-markdown-map
```

The following example shows how to configure a 1-rate, 3-color policer:

```
config t
```

```
  policy-map policy3
    class one_rate_3_color_policer
      police cir 256000 pir 256000 conform transmit exceed set dscp dscp table
cir-markdown-map violate drop
```

Feature History for QoS Policing

This section provides the QoS policing release history.

Feature Name	Releases	Feature Information
QoS Policing	4.0	This feature was introduced.

CHAPTER 5

Monitoring QoS Statistics

This chapter describes how to enable, display, and clear QoS statistics from the Cisco Nexus 1000V.

Information About QoS Statistics

Statistics are maintained for each policy, class action, and match criteria per interface. You can enable or disable the collection of statistics globally using the **[no] qos statistics** command. You can display statistics using the **show policy-map** interface command, and you can clear statistics based on an interface or policy map with the **clear qos statistics** command. Statistics are enabled by default and can be disabled globally.

Prerequisites for Monitoring QoS Statistics

Monitoring QoS statistics has the following prerequisites:

- You are logged in to the CLI in EXEC mode.

Enabling QoS Statistics

You can enable or disable QoS statistics for all interfaces on the device.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- By default, QoS statistics are enabled.

SUMMARY STEPS

1. **config t**
2. **qos statistics**
3. **show policy-map interface**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into global configuration mode.

Step 2	**qos statistics** **Example:** `n1000v(config)# qos statistics`	Enables QoS statistics on all interfaces.
Step 3	**show policy-map interface** **Example:** `n1000v(config)# show policy-map interface`	(Optional) Displays the status of the global statistics and the configured policy maps on all interfaces.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Displaying QoS Statistics

You can display QoS statistics for an interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You know the interface for which statistics are needed.

Note Statistics for individual interfaces are often the most useful.

SUMMARY STEPS

1. **show policy-map** [*policy-map-name* | **interface** [**brief** | **ethernet** *interface_number* | **output type qos** | **port-channel** *number* | **vethernet** *interface_number* | **input type qos**] | **type qos**]

DETAILED STEPS

	Command	Purpose
Step 1	**show policy-map** [*policy-map-name* | **interface** [**brief** | **ethernet** *interface_number* | **output type qos** | **port-channel** *number* | **vethernet** *interface_number* | **input type qos**] | **type qos**] **Example:** `n1000v# show policy-map interface ethernet 2/1`	Displays the specified statistics. To achieve the best result when your system has a large number of policies, use this command with specific arguments, such as specifying a particular interface or port channel. • Use the **interface** keyword with the following keywords to display the service policy on an interface: – **brief**—displays a brief report of all policies attached to interfaces. – **ethernet**—displays statistics for an Ethernet interface. – **input type qos**—displays statistics for QoS input policies. – **output type qos**—displays statistics for QoS output policies. – **port-channel**—displays statistics for a port channel interface. – **vethernet**—displays the statistics for a vEthernet interface. • Use the **type qos** keyword to display the type of policy map.

Clearing QoS Statistics

You can clear QoS statistics.

SUMMARY STEPS

1. **clear qos statistics [interface** {**ethernet** *interface_number* **| port-channel** *number* **| vethernet** *interface_number* **| output type qos | input type qos**}]

DETAILED STEPS

	Command	Purpose
Step 1	**clear qos statistics [interface** {**ethernet** *interface_number* | **port-channel** *number* | **vethernet** *interface_number* | **output type qos** | **input type qos**}] **Example:** n1000v# clear qos statistics type qos	Clears the specified QoS statistics.

Configuration Example for QoS Statistics

This example shows how to display statistics for policy maps that are configured on interfaces:

```
n1000v(config)# show policy-map interface


Global statistics status :   enabled

Vethernet3

  Service-policy (qos) input:   new-policy
    policy statistics status:   enabled

    Class-map (qos):   class-default (match-any)
      59610700 packets
      set prec 5

Vethernet5

  Service-policy (qos) output:   new-policer
    policy statistics status:   enabled

    Class-map (qos):   new-class (match-all)
      344661013 packets
      Match: precedence 5
      police cir 900 mbps bc 200 ms
        conformed 505953339796 bytes, 899924196 bps action: transmit
        violated 12285218014 bytes, 22283000 bps action: drop
```

This example shows how to display statistics for a specific IPv4 access control list (ACL):

```
n1000v(config)# show ip access-lists protoacl

IP access list protoacl
        statistics per-entry
        10 permit icmp 7.120.1.10/32 7.120.1.20/32
        20 permit tcp 7.120.1.10/32 7.120.1.20/32 dscp af11
        30 permit udp 7.120.1.10/32 7.120.1.20/32 precedence critical
        50 permit ip 7.120.1.20/32 7.120.1.10/32
        60 permit ip 7.120.1.20/32 7.120.1.10/32 dscp af11
        70 permit ip 7.120.1.20/32 7.120.1.10/32 precedence critical
```

This example shows how to display the status of the global statistics and the configured policy maps on a specific interface:

```
n1000v(config)# show policy-map interface vethernet 3
```

```
Global statistics status :   enabled

Vethernet3

  Service-policy (qos) input:   policy-protoacl
    policy statistics status:   enabled

    Class-map (qos):   class-protoacl (match-any)
      132 packets
      Match: access-group protoacl
        132 packets
      set qos-group 100
```

Additional References

This section provides additional information related to implementing system-level HA features.

Related Documents

Related Topic	Document Title
QoS Classification	"Configuring QoS Classification" section on page 2-1
QoS Policies and Marking	"Configuring QoS Marking Policies" section on page 3-1
QoS Overview	"Overview" section on page 1-1
QoS Policing	"Configuring QoS Policing" section on page 4-1
Configuring ACLs	*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(2)*
Cisco Nexus 1000V commands	*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-PROCESS-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No RFCs are supported by this feature	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature History for QoS Statistics

This section provides the QoS statistics release history.

Feature Name	Releases	Feature Information
QoS Statistics	4.0	This feature was introduced.

APPENDIX 6

DSCP and Precedence Values

This appendix provides the DSCP and precedence values used in QoS class maps and policy maps.

Commonly Used DSCP Values

Unless noted as a restriction, you can mark both incoming and outgoing packets.

Table 6-1 lists the commonly used DSCP values that are described in RFC 2475.

Table 6-1 Commonly Used DSCP Values

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2
011 000	24	CS3		3

Table 6-1 Commonly Used DSCP Values (continued)

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
100 000	32	CS4		4
101 000	40	CS5		5
110 000	48	CS6		6
111 000	56	CS7		7
000 000	0	Default		
101 110	46	EF		

IP Precedence Values

Table 6-2 lists the RFC 791 precedence values from least to most important.

Table 6-2 Precedence Values

Value	Description
000 (0)	Routine or Best Effort
001 (1)	Priority
010 (2)	Immediate
011 (3)	Flash (mainly used for voice signaling or for video)
100 (4)	Flash Override
101 (5)	Critical (mainly used for voice RTP)
110 (6)	Internet
111 (7)	Network

APPENDIX 7

QoS Configuration Limits

Table 7-1 shows the maximum configuration limits for QoS.

Table 7-1 QoS Maximum Configuration Limits

QoS feature	Maximum Limit
Match criteria per class-map	32
Class-maps per policy map	64
Class-maps per server	64 (with policers)
Policy-maps per server	16
Service Policies per server	128