Marking Network Traffic

Marking network traffic allows you to set or modify the attributes for traffic (that is, packets) belonging to a specific class or category. When used in conjunction with network traffic classification, marking network traffic is the foundation for enabling many quality of service (QoS) features on your network. This module contains conceptual information and the configuration tasks for marking network traffic.

- Finding Feature Information, on page 1
- Prerequisites for Marking Network Traffic, on page 1
- Restrictions for Marking Network Traffic, on page 1
- Information About Marking Network Traffic, on page 2
- Table Maps, on page 6
- How to Mark Network Traffic, on page 8
- Configuration Examples for Marking Network Traffic, on page 16
- Additional References for Marking Network Traffic, on page 17
- Feature Information for Marking Network Traffic, on page 18

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Marking Network Traffic

In order to mark network traffic, Cisco Express Forwarding must be configured on both the interface receiving the traffic and the interface sending the traffic.

Restrictions for Marking Network Traffic

- Cos Marking is not supported for pop 0.

- You cannot configure QoS with empty class map and cannot attach a policy without any class map match condition.
- When fragment offset is set in the IP header, the system does not classify it as a L4 (TCP) header. The IP header is not subjected to the class-map that matches on the TCP or port combination. Hence, the traffic uses the class-default option.
- When a fragment offset is set in the IP reader, the network processor will not resolve the L4 header. Hence, the default L4 source or L4 destination port is assumed as '0'.

For information, see Quality of Service Configuration Guidelines (Cisco ASR 920 Series)

Information About Marking Network Traffic

Purpose of Marking Network Traffic

Traffic marking is a method used to identify certain traffic types for unique handling, effectively partitioning network traffic into different categories.

After the network traffic is organized into classes by traffic classification, traffic marking allows you to mark (that is, set or change) a value (attribute) for the traffic belonging to a specific class. For instance, you may want to change the class of service (CoS) value from 2 to 1 in one class, or you may want to change the differentiated services code point (DSCP) value from 3 to 2 in another class. In this module, these values are referred to as attributes.

Attributes that can be set and modified include the following:

- Discard-class value
- DSCP value in the type of service (ToS) byte
- MPLS EXP field value in the topmost label on an input or output interface
- Multiprotocol Label Switching (MPLS) experimental (EXP) field on all imposed label entries
- Precedence value in the packet header
- QoS group identifier (ID)
- ToS bits in the header of an IP packet

Note Set of MPLS EXP field value in the topmost label on output interface is *not* supported on the Cisco ASR 900 RSP3 Module.

Note Effective with Release 16.5.1, if the same table-mapping is applied on multiple interfaces, the MDT index is shared across these interfaces. Thus increased scaling of table-map is possible if table-mapping is reused.

For information on attributes that marking supports see, Quality of Service Configuration Guidelines for Cisco ASR 920 Series.

Benefits of Marking Network Traffic

Improved Network Performance

Traffic marking allows you to fine-tune the attributes for traffic on your network. This increased granularity helps single out traffic that requires special handling and, thus, helps to achieve optimal application performance.

Traffic marking allows you to determine how traffic will be treated, based on how the attributes for the network traffic are set. It allows you to segment network traffic into multiple priority levels or classes of service based on those attributes, as follows:

- The DSCP field (TAG to IP) value does not change in both the uniform mode and in pipe mode. This is applicable to both the Unicast and Multicast traffic scenario.
- Traffic marking is often used to set the IP precedence or IP DSCP values for traffic entering a network. Networking devices within your network can then use the newly marked IP precedence values to determine how traffic should be treated. For example, voice traffic can be marked with a particular IP precedence or DSCP, and a queueing mechanism can then be configured to put all packets of that mark into a priority queue.
- Traffic marking can be used to identify traffic for any class-based QoS feature (any feature available in policy-map class configuration mode, although some restrictions exist).
- Traffic marking can be used to assign traffic to a QoS group within a device. The device can use the QoS groups to determine how to prioritize traffic for transmission. The QoS group value is used for one of the two following reasons:
    - To leverage a large range of traffic classes. The QoS group value has 100 different individual markings, as opposed to DSCP and IP precedence, which have 64 and 8, respectively.

      Note The QoS group range is 0–7 on the Cisco RSP3 Module.

    - If changing the IP precedence or DSCP value is undesirable.
- If a packet (for instance, in a traffic flow) that needs to be marked to differentiate user-defined QoS services is leaving a device and entering a switch, the device can set the CoS value of the traffic, because the switch can process the Layer 2 CoS header marking. Alternatively, the Layer 2 CoS value of the traffic leaving a switch can be mapped to the Layer 3 IP or MPLS value.

  Note The mapping of Layer 2 CoS value of the traffic to the Layer 3 IP or MPLS value is *not* supported on the Cisco RSP3 Module.

- Weighted random early detection (WRED) uses precedence values or DSCP values to determine the probability that the traffic will be dropped. Therefore, the Precedence and DSCP can be used along with WRED.

Two Methods for Marking Traffic Attributes

There are two methods for specifying and marking traffic attributes:

- You can specify and mark the traffic attribute by using a **set** command.

  With this method, you configure individual **set** commands for the traffic attribute that you want to mark.

- You can specify and mark the traffic attribute by creating a mapping table (called a "table map").

  With this method, you configure the traffic attributes that you want to mark once in a table map and then the markings can be propagated throughout the network.

  These methods are further described in the sections that follow.

Mark Traffic Attributes Using a set Command

You specify the traffic attribute that you want to change with a **set**command configured in a policy map. The table below lists the available **set**commands and the corresponding attribute. The table also includes the network layer and the network protocol typically associated with the traffic attribute.

Table 1: set Commands and Corresponding Traffic Attribute, Network Layer, and Protocol

set Commands[1]	Traffic Attribute	Network Layer	Protocol
set cos	Layer 2 CoS value of the outgoing traffic	Layer 2	
set discard-class	discard-class value	Layer 2	
set dscp	DSCP value in the ToS byte	Layer 3	IP
set mpls experimental imposition	MPLS EXP field on all imposed label entries	Layer 3	MPLS
set mpls experimental topmost	MPLS EXP field value in the topmost label on either an input or an output interface	Layer 3	MPLS
set precedence	Precedence value in the packet header	Layer 3	IP
set qos-group	QoS group ID	Layer 3	IP, MPLS

[1] Cisco set commands can vary by release. For more information, see the command documentation for the Cisco release that you are using

Note The **set qos-group** can be used for L2 traffic on the Cisco ASR 900 RSP3 Module.

If you are using individual **set** commands, those **set** commands are specified in a policy map. The following is a sample policy map configured with one of the **set** commands listed in the table above. In this sample configuration, the **set dscp** command has been configured in the policy map (policy1).

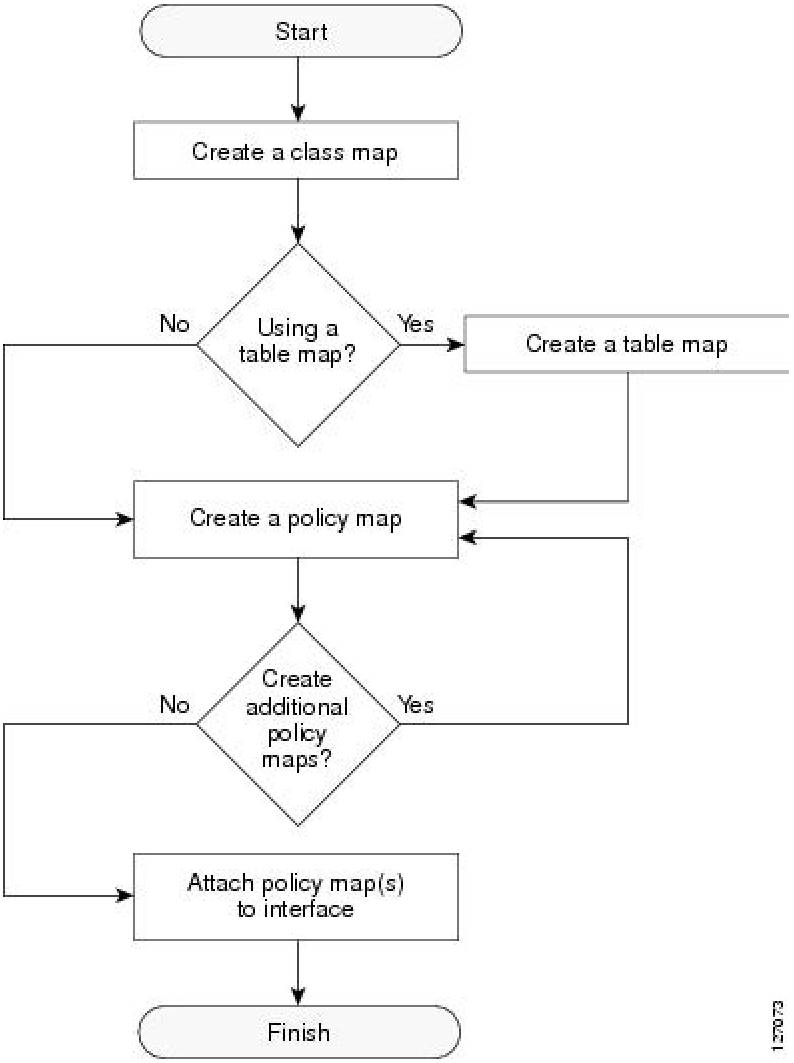
```
policy-map policy1
 class class1
```

```
set dscp 1
end
```

Traffic Marking Procedure Flowchart

The figure below illustrates the order of the procedures for configuring traffic marking.

Figure 1: Traffic Marking Procedure Flowchart



MQC and Network Traffic Marking

To configure network traffic marking, you use the Modular QoS CLI (MQC).

The MQC is a CLI structure that allows you to complete the following tasks:

- Specify the matching criteria used to define a traffic class.
- Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.

- Apply the policy actions specified in the policy map to an interface, EFP, Trunk EFP, or Xconect by using the **service-policy** command.

Traffic Classification Compared with Traffic Marking

Traffic classification and traffic marking are closely related and can be used together. Traffic marking can be viewed as an additional action, specified in a policy map, to be taken on a traffic class.

Traffic classification allows you to organize into traffic classes on the basis of whether the traffic matches specific criteria. For example, all traffic with a CoS value of 2 is grouped into one class, and traffic with a DSCP value of 3 is grouped into another class. The match criteria are user-defined.

After the traffic is organized into traffic classes, traffic marking allows you to mark (that is, set or change) an attribute for the traffic belonging to that specific class. For instance, you may want to change the CoS value from 2 to 1, or you may want to change the DSCP value from 3 to 2.

The match criteria used by traffic classification are specified by configuring a **match** command in a class map. The marking action taken by traffic marking is specified by configuring a **set** command in a policy map. These class maps and policy maps are configured using the MQC.

The table below compares the features of traffic classification and traffic marking.

Table 2: Traffic Classification Compared with Traffic Marking

Feature	Traffic Classification	Traffic Marking
Goal	Groups network traffic into specific traffic classes on the basis of whether the traffic matches the user-defined criterion.	After the network traffic is grouped into traffic classes, modifies the attributes for the traffic in a particular traffic class.
Configuration Mechanism	Uses class maps and policy maps in the MQC.	Uses class maps and policy maps in the MQC.
CLI	In a class map, uses **match** commands (for example, **match cos**) to define the traffic matching criteria.	Uses the traffic classes and matching criteria specified by traffic classification. In addition, uses **set** commands (for example, **set cos**) in a policy map to modify the attributes for the network traffic.

Table Maps

You can use table maps to manage a large number of traffic flows with a single command. Table-maps are supported only as part of a mark-down policer. Table maps are used only in input policy maps.

Table maps can be used to:

- Correlate specific CoS, DSCP, or IP precedence values to specific CoS, DSCP, or IP precedence values
- Mark down a CoS, DSCP, or IP precedence value
- Assign defaults for unmapped values

A table map includes one of these default actions:

- **default** *default-value*—applies a specific default value (0 to 63) for all unmapped values
- **default copy**—maps all unmapped values to the equivalent value in another qualifier
- **default ignore**—makes no changes for unmapped values

This example creates a table to map specific CoS values to DSCP values. The default command maps all unmapped CoS values to a DSCP value of 63.

```
Router(config)# table-map cos-dscp-tablemap
 Router(config-tablemap)# map from 5 to 46
 Router(config-tablemap)# map from 6 to 56
 Router(config-tablemap)# map from 7 to 57
 Router(config-tablemap)# default 63
 Router(config-tablemap)# exit
```

The router supports a maximum of 256 unique table maps. You can enter up to 64 different map from-to entries in a table map. These table maps are supported on the router:

- CoS to Precedence
- CoS to DSCP
- CoS to CoS
- CoS to EXP
- CoS to QoS-Group
- CoS to Discard-Class

- Precedence to CoS
- Precedence to DSCP
- Precedence to Precedence
- Precedence to EXP
- Precedence to QoS-Group
- Precedence to Discard-Class

- DSCP to Precedence
- DSCP to CoS
- DSCP to DSCP
- DSCP to EXP
- DSCP to QoS-Group
- DSCP to Discard-Class

Tunneling Cases (Layer 2 VPN or Layer 3 VPN):

- EXP to Precedence
- EXP to CoS

- EXP to DSCP
- EXP to EXP
- EXP to QoS-Group
- EXP to Discard-Class

Table-maps are only supported as part of a policer action, that is, **conform-action**, **exceed-action** or **violate-action** command in a police function.

Table maps are not supported in output policy maps. For more information, see the Configuring Table Maps, on page 12 section.

How to Mark Network Traffic

Creating a Class Map for Marking Network Traffic

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **class-map** *class-map-name* [**match-all**| **match-any**]

Example:

```
Router(config)# class-map class1
```

Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.

- Enter the class map name.

Step 4 **match cos** *cos-value*

Example:

```
Router (config)# match cos 1
```

Matches with Cos value.

cos-value: Sets the Cos Value. The valid values are 1 and 2.

Step 5 **end**

Example:

```
Router(config-cmap)# end
```

(Optional) Returns to privileged EXEC mode.

Creating a Policy Map for Applying a QoS Feature to Network Traffic

Before you begin

The following restrictions apply to creating a QoS policy map:

- A policy map containing the **set qos-group** command can only be attached as an input traffic policy. QoS group values are not usable for traffic leaving a device.
- A policy map containing the set cos command cannot be attached as an output traffic policy.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **policy-map** *policy-map-name*

Example:

```
Device(config)# policy-map policy1
```

Specifies the name of the policy map and enters policy-map configuration mode.

Step 4 **class** {*class-name* | **class-default**}

Example:

```
Device(config-pmap)# class class1
```

Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier.

Step 5 **set cos** *cos-value*

Example:

```
Device(config-pmap-c)# set cos 2
```

(Optional) Sets the CoS value in the type of service (ToS) byte.

Note The **set cos** command is an example of one of the **set** commands that can be used when marking traffic. Other **set** commands can be used. For a list of other **set** commands, see “Information About Marking Network Traffic”.

Step 6 **end**

Example:

```
Device(config-pmap-c)# end
```

Returns to privileged EXEC mode.

Step 7 **show policy-map**

Example:

```
Device# show policy-map
```

(Optional) Displays all configured policy maps.

Step 8 **show policy-map** *policy-map* **class** *class-name*

Example:

```
Device# show policy-map policy1 class class1
```

(Optional) Displays the configuration for the specified class of the specified policy map.

What to Do Next

Create and configure as many policy maps as you need for your network. To create and configure additional policy maps, repeat the steps in the “Creating a Policy Map for Applying a QoS Feature to Network Traffic” section. Then attach the policy maps to the appropriate interface, following the instructions in the “Attaching the Policy Map to an Interface” section.

Attaching the Policy Map to an Interface, EFP or Xconnect

Before you begin

Note Depending on the needs of your network, policy maps can be attached to targets that are supported. For information, see *Quality of Service Configuration Guidelines (Cisco ASR 920 Series)*.

Procedure

Step 1 **configure terminal**

Enter global configuration mode.

Example:

```
Router# configure terminal
```

Step 2 **interface** *interface-id*

Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.

Example:

```
Router(config)# interface gigabitethernet 0/3/6
```

Step 3 **service instance** *number* **ethernet** [*name*]

Configure an EFP (service instance) and enter service instance configuration) mode.

- The number is the EFP identifier, an integer from 1 to 4000.
- (Optional) **ethernet** name is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.

Example:

```
Rotuer(config)# service instance 1 ethernet
```

Step 4 **service-policy** {**input** | **output**} *policy-map-name*

Attaches the specified policy map to the input or output interfaces .

- *policy-map-name*: Specifies the policy map.

Example:

```
Router(config-if-srv)# service-policy input col
```

Step 5 **encapsulation** {**default** | **dot1q** | **priority-tagged** | **untagged**}

Configure encapsulation type for the service instance.

- **default**—Configure to match all unmatched packets.
- **dot1q**—Configure 802.1Q encapsulation. See *Table 1* for details about options for this keyword.
- **priority-tagged**—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.

- **untagged**—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.

Example:

```
Router(config-if-srv)# encapsulation dot1q 1
```

Step 6 **bridge-domain** *bridge-id* [**split-horizon group** *group-id*]

Configure the bridge domain ID. The range is from 1 to 4000.

You can use the **split-horizon** keyword to configure the port as a member of a split horizon group. The *group-id* range is from 0 to 2.

Example:

```
Router(config-if-srv)# bridge-domain 1
```

Step 7 **end**

Return to privileged EXEC mode.

Example:

```
Router(config-if-srv)# end
```

Configuration Example

```
Router(config)# interface gigabitethernet 0/3/6
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# service-policy input co1
Router(config-if-srv)# encapsulation dot1q 1
Router(config-if-srv)# bridge-domain 1
Router(config-if-srv)# end
```

Configuring Table Maps

Note these guidelines when configuring table maps:

- The router supports a maximum of 256 unique table maps.
- The maximum number of map statements within a table map is 64.
- Table maps cannot be marked using **set** commands. To mark table map, configure policer with 100% CIR.
- Table map marking cannot be done at interface or VLAN level.
- Multiple **set** table map marking transformations cannot be used for the same class. To mark table map, configure policer with 100% CIR.
- Ingress marking with and without table-map simultaneously under the same class cannot be done.
- Table maps cannot be used in output policy maps.
- Dynamic modification of the table map definition is not supported. To make changes to the table map, remove the table map from the policy map, make any necessary changes to the table map and then reconfigure it in the policy map.

- Dynamic addition, deletion or modification of the table-map to or from class-default in a physical level policy (pure class-default policy without other user-defined classes) is not supported.
- Dynamic addition, deletion or modification of policer containing table-map action in class-default in a class-level policy (policy-map that contains user-defined classes along with class-default) is not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**table-map** *table-map-name* **Example:** `Router(config)# table-map dscp-to-cos`	Create a table map by entering a table-map name and entering table-map configuration mode.
Step 4	**map from** *from-value* **to** *to-value* **Example:** `Router(config-tablemap)# map from 1 to 1`	Enters the mapping values to be included in the table. For example, if the table map is a DSCP-to-CoS table map, the from-value would be the DSCP value and the to_value would be the CoS value. Both ranges are from 0 to 63. Enter this command multiple times to include all the values that you want to map.

Step 5	**default** {*default-value* | **copy** | **ignore**}
	Example:
	`Router(config-tablemap)# default 4`
		Sets the default behavior for a value not found in the table map.
		- Enter a *default-value* to specify a certain value. For example, in a DSCP-to-CoS table map, this would be a specific CoS value to apply to all unmapped DSCP values. The range is from 0 to 63.
		- Enter **copy** to map unmapped values to an equivalent value. In a DSCP-to-CoS table map, this command maps all unmapped DSCP values to the equivalent CoS value.
		- Enter **ignore** to leave unmapped values unchanged. In a DSCP-to-CoS table map, the switch does not change the CoS value of unmapped DSCP values.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-tablemap)# end`
		(Optional) Returns to privileged EXEC mode.

Step 7	**show table-map** [*table-map-name*] **Example:** `Router(config)# show table-map dscp-to-cos`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Router(config)# copy running-config startup-config`	(Optional) Saves your entries in the configuration file. To delete a table map, use the **no table-map** *table-map-name* global configuration command.

Using a Table Map under a Policy Map

The following procedure uses a table map configured to map CoS to DSCP.

Before you begin

Table map must be configured. To configure a table map, see Configuring Table Maps, on page 12.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map ingress`	Specifies the name of the policy map and enters policy-map configuration mode.
Step 4	**class** {*class-name* | **class-default**} **Example:**	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier.

	Command or Action	Purpose
	`Device(config-pmap)# class cos 1`	
Step 5	**police** {*rate-bps* | **cir** {*cir-bps* | **percent** *percent*}} [**bc** *burst-bytes*] [**conform-action** *action*] [**pir** *pir-bps*] [**be** *be-bps*] **Example:** `Device(config-pmap-c)# police cir 1000000 bc 31250 pir 2000000 be 62500`	Configure a traffic policer based on the traffic rate or committed information rate (CIR). By default, no policer is defined. • *rate-bps*—Specifies average traffic rate in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed. • **cir**—Specifies a committed information rate (CIR). • *cir-bps*—Specifies a CIR in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed. • **bc** *burst-bytes*—(Optional) Specifies the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000. • **conform-action** *action*— (Optional) Specifies action to take on packets that conform to the specified rate limit. • **pir** *pir-bps*—(Optional) Specifies the peak information rate (PIR). • **be** *be-bps*—(Optional) Specifies how much the **pir** can be exceeded, either as a bit rate or an amount of time at **pir**. **Note** You must specify a value for **pir** before the device displays this argument. **Note** **cir percent** *percent* option is not supported on the router.
Step 6	**conform-action** *action* **Example:** `Device(config-pmap-c-police)# conform-action set-cos-transmit dscp table cos-dscp`	Specifies the action to take on packets that conform to the police rate limit and enters policy-map class police configuration mode.
Step 7	**exceed-action** *action* **Example:**	Specifies action to take on packets that exceed the rate limit.

	Command or Action	Purpose
	`Device(config-pmap-c-police)# exceed-action transmit`	
Step 8	**violate-action** *action* **Example:** `Device(config-pmap-c-police)# violate-action drop`	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes.

Step 9	**end**
	Example:
	`Device(config-pmap-c)# end`
		Returns to privileged EXEC mode.

Step 10	**show policy-map** *policy-map* **Example:** `Device# show policy-map ingress`	(Optional) Displays the configuration for the specified class of the specified policy map.

Configuration Examples for Marking Network Traffic

Example: Creating a Class Map for Marking Network Traffic

- The following is an example of configures a class map with using match-any .

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/3/6
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 1
Router(config-if-srv)# bridge-domain 1
Device(config)# class-map match-any class1
Device(config-cmap)# match cos 1
Device(config-cmap)# end
```

- The following is an example of configures a class map with using match-all .

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet0/3/6
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 1
Router(config-if-srv)# bridge-domain 1
Device(config)# class-map match-all class1
Device(config-cmap)# match cos 1
Device(config-cmap)# end
```

Example Creating a Policy Map for Applying a QoS Feature to Network Traffic

The following is an example of creating a policy map to be used for traffic classification.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
Router# exit
```

Example: Attaching a Traffic Policy to an Interface

The following example shows how to attach an existing traffic policy to an interface. After you define a traffic policy with the **policy-map** command, you can attach it to one or more interfaces by using the **service-policy** command in interface configuration mode. Although you can assign the same traffic policy to multiple interfaces, each interface can have only one traffic policy attached in the input direction and only one traffic policy attached in the output direction.

```
Router(config)# interface gigabitethernet0/3/6
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# service-policy input col
Router(config-if-srv)# encapsulation dot1q 1
Router(config-if-srv)# bridge-domain 1
Router(config-if)# service-policy input policy1
Router(config-if)# end
```

Additional References for Marking Network Traffic

Related Documents

Related Topic	Document Title
Cisco commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC	“Applying QoS Features Using the MQC” module
Classifying network traffic	“Classifying Network Traffic” module

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Marking Network Traffic

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Marking Network Traffic

Feature Name	Releases	Feature Information
Table Maps	Cisco IOS XE Release 3.14.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M) .
Marking Network Traffic	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).