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.

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.

- IPv6 classification and marking are *not* supported on the Cisco RSP3 Module.

- You cannot configure QoS with empty class map and cannot attach a policy without any class map match condition.

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 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

Benefits of Marking Network Traffic

Table 1: Feature History

Feature Name	Release	Description
DSCP Preservation of MLDP Traffic	Cisco IOS XE Amsterdam 17.1.1	The Differentiated Services Code Point (DSCP) value does not change on both the uniform and pipe modes.

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.

    - 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.

- 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.

How to Mark 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.

This method is further described in the section that follows.

Method One 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 2: 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 **Note** set discard-class supports Layer 2 and Layer 3 on the Cisco RSP3 Module.	
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 Commands[1]	Traffic Attribute	Network Layer	Protocol
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 RSP3 Module.
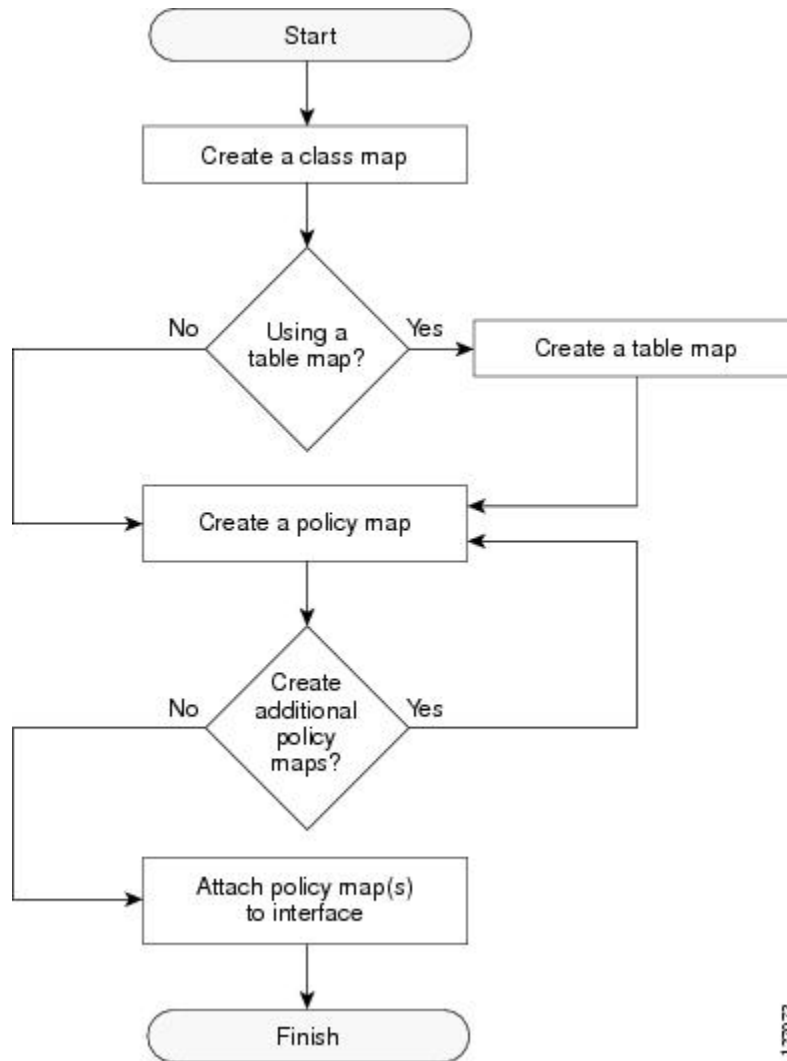
Note **set dscp** command is *not* supported on the Cisco RSP3 Module for L2 EFP configuration.

Traffic Marking Procedure Flowchart

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

Figure 1: Traffic Marking Procedure Flowchart

Method for Marking Traffic Attributes

You specify and mark the traffic attribute that you want to change by using a **set** command configured in a policy map.

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

Using a set Command

The table below lists the available **set** commands and the corresponding attribute. The table below also includes the network layer and the network protocol typically associated with the traffic attribute.

Table 3: set Commands and Corresponding Traffic Attribute, Network Layer, and Protocol

set Commands[2]	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 an input or 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

[2] Cisco set commands can vary by release. For more information, see the command documentation.

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 cos** command has been configured in the policy map (policy1) to mark the CoS value.

```
policy-map policy1
 class class1
  set cos 1
  end
```

For information on configuring a policy map, see the "Creating a Policy Map for Applying a QoS Feature to Network Traffic" section.

The final task is to attach the policy map to the interface. For information on attaching the policy map to the interface, see the "Attaching the Policy Map to an Interface" section.

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 4: 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.

How to Mark Network Traffic

Creating a Class Map for Marking Network Traffic

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 can only be attached as an output traffic policy.

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 .

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 co1
```

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.

- **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
```

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 co1
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
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*

Related Topic	Document Title
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