Marking Network Traffic

Last Updated: December 8, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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.

Restrictions for Marking Network Traffic

Traffic marking can be configured on an interface, a subinterface, or an ATM permanent virtual circuit (PVC). Marking network traffic is not supported on the following interfaces:

- ATM switched virtual circuit (SVC)
- Fast EtherChannel
- PRI
- Tunnel

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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:

- Cell loss priority (CLP) bit
- CoS value of an outgoing packet
- Discard eligible (DE) bit setting in the address field of a Frame Relay frame
- Discard-class value
- DSCP value in the type of service (ToS) byte
- MPLS EXP field value in the topmost label on either an input or an 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

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:

- 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 router. The router can use the QoS groups to determine how to prioritize traffic for transmission. The QoS group value is usually 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 Precedence, which have 64 and 8, respectively.
  - If changing the Precedence or DSCP value is undesirable.
- If a packet (for instance, in a traffic flow) needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router 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.

Method for Marking Traffic Attributes

You 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.

- Using a set Command, page 3

Using a set Command

You specify the traffic attribute 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 below 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	ATM, Frame Relay
set discard-class	discard-class value	Layer 2	ATM, Frame Relay
set dscp	DSCP value in the ToS byte	Layer 3	IP
set fr-de	DE bit setting in the address field of a Frame Relay frame	Layer 2	Frame Relay
set ip tos (route-map)	ToS bits in the header of an IP packet	Layer 3	IP
set mpls experimental imposition	MPLS EXP field on all imposed label entries	Layer 3	MPLS

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

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

If you are using individual **set** commands, those **set** commands are specified in a policy map. The following is a sample of a 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.

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.

MQC and Network Traffic Marking

To configure network traffic marking, you use the Modular Quality of Service (QoS) Command-Line Interface (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, subinterface, or ATM PVC 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 DSCP value of 3 is grouped into another class. The match criterion is 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.

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

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 criterion.	Uses the traffic classes and matching criterion 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

Note The **match protocol** command is included in the steps below. The **match protocol** command is just an example of one of the **match** commands that can be used. See the command documentation for the Cisco IOS XE release that you are using for a complete list of **match** commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all** | **match-any**]
4. **match protocol** *protocol-name*
5. **end**

DETAILED STEPS

	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	**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 protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol ftp`	(Optional) Configures the match criterion for a class map on the basis of the specified protocol. **Note** The **match protocol** command is just an example of one of the **match** commands that can be used. The **match** commands vary by Cisco IOS XE release. See the command documentation for the Cisco IOS XE release that you are using for a complete list of **match** commands.
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

Note The **set cos** command is shown in the steps that follow. The **set cos** command is an example of a **set** command that can be used when marking traffic. Other **set** commands can be used. For a list of other **set** commands, see “Creating a Policy Map for Applying a QoS Feature to Network Traffic”.

The following restrictions apply to creating a QoS policy map:

- Before modifying the encapsulation type from IEEE 802.1 Q to ISL, or vice versa, on a subinterface, detach the policy map from the subinterface. After changing the encapsulation type, reattach the 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 router.
- A policy map containing the **set cos** command can only be attached as an output traffic policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set cos** *cos-value*
6. **end**
7. **show policy-map**
8. **show policy-map** *policy-map* **class** *class-name*
9. **exit**

DETAILED STEPS

	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	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map created earlier and enters policy-map configuration mode. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(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. • Enter the name of the class or enter the **class-default** keyword.

	Command or Action	Purpose
Step 5	**set cos** *cos-value* **Example:** `Router(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 "Creating a Policy Map for Applying a QoS Feature to Network Traffic".
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays all configured policy maps.
Step 8	**show policy-map** *policy-map* **class** *class-name* **Example:** `Router# show policy-map policy1 class class1`	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

• What to Do Next, page 8

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

Note Depending on the needs of your network, policy maps can be attached to an interface, a subinterface, or an ATM permanent virtual circuit (PVC).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds** | **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**} *policy-map-name*
7. **end**
8. **show policy-map interface** *type number*
9. **exit**

DETAILED STEPS

	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	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.

	Command or Action	Purpose
Step 4	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds** | **l2transport**] **Example:** `Router(config-if)# pvc cisco 0/16`	(Optional) Creates or assigns a name to an ATM permanent virtual circuit (PVC), specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode. • Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to Step 6 below.
Step 5	**exit** **Example:** `Router(config-atm-vc)# exit`	(Optional) Returns to interface configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC and you completed Step 4 above. If you are not attaching the policy map to an ATM PVC, advance to Step 6 below.
Step 6	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	Attaches a policy map to an input or output interface. • Enter the policy map name. **Note** Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show policy-map interface** *type number* **Example:** `Router# show policy-map interface serial4/0/0`	(Optional) Displays the traffic statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. • Enter the interface type and number.
Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Configuring QoS When Using IPsec VPNs

This task uses the **qos pre-classify** command to enable QoS preclassification for the packet. QoS preclassification is not supported for all fragmented packets. If a packet is fragmented, each fragment might received different preclassifications.

Note This task is required only if you are using IPsec Virtual Private Networks (VPNs). Otherwise, this task is not necessary. For information about IPsec VPNs, see the "Configuring Security for VPNs with IPsec" module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num*
4. **exit**
5. **interface** *type number* [**name-tag**]
6. **qos pre-classify**
7. **end**

DETAILED STEPS

	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	**crypto map** *map-name seq-num* **Example:** `Router(config)# crypto map mymap 10`	Enters crypto map configuration mode and creates or modifies a crypto map entry. • Enter the crypto map name and sequence number.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config-crypto-map)# exit`	Returns to global configuration mode.
Step 5	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.
Step 6	**qos pre-classify** **Example:** `Router(config-if)# qos pre-classify`	Enables QoS preclassification.
Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Marking Network Traffic

Example: Creating a Class Map for Marking Network Traffic

The following is an example of creating a class map to be used for marking network traffic. In this example, a class called class1 has been created. The traffic with a protocol type of ftp will be put in this class.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match protocol ftp
Router(config-cmap)# end
```

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

The following is an example of creating a policy map to be used for traffic marking. In this example, a policy map called policy1 has been created, and the **set dsc** command has been configured for class1.

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

Example: Attaching the Policy Map to an Interface

The following is an example of attaching the policy map to the interface. In this example, the policy map called policy1 has been attached in the input direction of the serial interface 4/0/0.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
```

Example: Configuring QoS When Using IPsec VPNs

The following is an example of configuring QoS when using IPsec VPNs. In this example, the **crypto map** command specifies the IPsec crypto map (mymap 10) to which the **qos pre-classify** command will be applied.

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10
Router(config-crypto-map)# qos pre-classify
Router(config-crypto-map)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS 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

Related Topic	Document Title
IPsec and VPNs	"Configuring Security for VPNs with IPsec" module

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

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	Software Releases	Feature Configuration Information
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
Class-Based Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	This feature was implemented on Cisco ASR 1000 Series Routers. This feature was integrated into Cisco IOS XE Software Release 2.2.
Frame Relay DE Bit Marking	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
IP DSCP marking for Frame-Relay PVC	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
QoS Group: Match and Set for Classification and Marking	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
QoS Packet Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.5S	This feature was implemented on Cisco ASR 1000 Series Routers. This feature was integrated into Cisco IOS XE Software Release 2.2. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
QoS: Traffic Pre-classification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.