CONTENTS

CHAPTER 1

Marking Network Traffic

Finding Feature Information 1
Prerequisites for Marking Network Traffic 1
Restrictions for Marking Network Traffic 2
Information About Marking Network Traffic 2
  Purpose of Marking Network Traffic 2
  Benefits of Marking Network Traffic 2
  Two Methods for Marking Traffic Attributes 3
    Method One Using a set Command 4
    Traffic Marking Procedure Flowchart 5
  MQC and Network Traffic Marking 5
  Traffic Classification Compared with Traffic Marking 6
Table Maps 6
How to Mark Network Traffic 8
  Creating a Class Map for Marking Network Traffic 8
  Creating a Policy Map for Applying a QoS Feature to Network Traffic 9
  What to Do Next 10
  Attaching the Policy Map to an Interface, EFP or Xconnect 11
  Configuring Table Maps 12
  Using a Table Map under a Policy Map 14
Configuration Examples for Marking Network Traffic 17
  Example: Creating a Class Map for Marking Network Traffic 17
  Example Creating a Policy Map for Applying a QoS Feature to Network Traffic 17
  Example: Attaching a Traffic Policy to an Interface 17
Additional References for Marking Network Traffic 18
Feature Information for Marking Network Traffic 18

CHAPTER 2

Configuration to drop DEI / CFI traffic 21
CHAPTER 3
Classifying and Marking MPLS EXP 23
Finding Feature Information 23
Prerequisites for Classifying and Marking MPLS EXP 23
Restrictions for Classifying and Marking MPLS EXP 24
Information About Classifying and Marking MPLS EXP 24
Classifying and Marking MPLS EXP Overview 24
MPLS Experimental Field 25
Benefits of MPLS EXP Classification and Marking 25
How to Classify and Mark MPLS EXP 25
Classifying MPLS Encapsulated Packets 25
Marking MPLS EXP on All Imposed Labels 26
Marking MPLS EXP on Label Switched Packets 28
Configuring Conditional Marking 29
Configuration Examples for Classifying and Marking MPLS EXP 32
Example: Classifying MPLS Encapsulated Packets 32
Example: Marking MPLS EXP on All Imposed Labels 32
Example: Marking MPLS EXP on Label Switched Packets 33
Example: Configuring Conditional Marking 34
Additional References 34
Feature Information for Classifying and Marking MPLS EXP 35

CHAPTER 4
Configuration of an IPv6 Access Control List 37
Restrictions 37
Configuring IPv6 Access Control List 38
Creating an IPv6 Access List 38
Applying an IPv6 Access Control List to a Physical Interface 39
Example for Configuration of IPv6 ACL 40
Verifying the Configuration 40

CHAPTER 5
IPv6 QoS: MQC Packet Classification 43
Finding Feature Information 43
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information About IPv6 QoS: MQC Packet Classification</td>
<td>43</td>
</tr>
<tr>
<td>Implementation Strategy for QoS for IPv6</td>
<td>43</td>
</tr>
<tr>
<td>Packet Classification in IPv6</td>
<td>44</td>
</tr>
<tr>
<td>How to Configure IPv6 QoS: MQC Packet Classification</td>
<td>44</td>
</tr>
<tr>
<td>Classifying Traffic in IPv6 Networks</td>
<td>44</td>
</tr>
<tr>
<td>Using the Match Criteria to Manage IPv6 Traffic Flows</td>
<td>45</td>
</tr>
<tr>
<td>Confirming the Service Policy</td>
<td>46</td>
</tr>
<tr>
<td>Configuration Examples for IPv6 QoS: MQC Packet Classification</td>
<td>48</td>
</tr>
<tr>
<td>Example: Matching DSCP Value</td>
<td>48</td>
</tr>
<tr>
<td>Additional References</td>
<td>48</td>
</tr>
<tr>
<td>Feature Information for IPv6 QoS: MQC Packet Classification</td>
<td>50</td>
</tr>
</tbody>
</table>
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, page 1
- Prerequisites for Marking Network Traffic, page 1
- Restrictions for Marking Network Traffic, page 2
- Information About Marking Network Traffic, page 2
- Table Maps, page 6
- How to Mark Network Traffic, page 8
- Configuration Examples for Marking Network Traffic, page 17
- Additional References for Marking Network Traffic, page 18
- Feature Information for Marking Network Traffic, 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.

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 interface
- Multiregister 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 device. The device 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 IP precedence, which have 64 and 8, respectively.

  Note  The QoS group range is from 0 to 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 in
conjunction 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.
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>
<thead>
<tr>
<th><code>set</code> Commands¹</th>
<th>Traffic Attribute</th>
<th>Network Layer</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set cos</code></td>
<td>Layer 2 CoS value of the outgoing traffic</td>
<td>Layer 2</td>
<td>ATM, Frame Relay</td>
</tr>
<tr>
<td><code>set discard-class</code></td>
<td>discard-class value</td>
<td>Layer 2</td>
<td>ATM, Frame Relay</td>
</tr>
<tr>
<td><code>set dscp</code></td>
<td>DSCP value in the ToS byte</td>
<td>Layer 3</td>
<td>IP</td>
</tr>
<tr>
<td><code>set mpls experimental imposition</code></td>
<td>MPLS EXP field on all imposed label entries</td>
<td>Layer 3</td>
<td>MPLS</td>
</tr>
<tr>
<td><code>set mpls experimental topmost</code></td>
<td>MPLS EXP field value in the topmost label on either an input or an output interface</td>
<td>Layer 3</td>
<td>MPLS</td>
</tr>
<tr>
<td><code>set precedence</code></td>
<td>Precedence value in the packet header</td>
<td>Layer 3</td>
<td>IP</td>
</tr>
<tr>
<td><code>set qos-group</code></td>
<td>QoS group ID</td>
<td>Layer 3</td>
<td>IP, MPLS</td>
</tr>
</tbody>
</table>

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

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 atm-clp` command has been configured in the policy map (policy1) to mark the CLP attribute.

```
policy-map policy1
  class class1
    set atm-clp
  end
```

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

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

### 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, \textit{conform-action}, \textit{exceed-action} or \textit{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

SUMMARY STEPS

1. \texttt{enable}
2. \texttt{configure terminal}
3. \texttt{class-map class-map-name [match-all] match-any]
4. \texttt{match cos cos-value}
5. \texttt{end}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>\texttt{enable}</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>\texttt{Example:}</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>\texttt{configure terminal}</td>
<td></td>
</tr>
<tr>
<td>\texttt{Example:}</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.</td>
</tr>
<tr>
<td>\texttt{class-map class-map-name [match-all] match-any]}</td>
<td>Enter the class map name.</td>
</tr>
<tr>
<td>\texttt{Example:}</td>
<td>Router(config)# class-map class1</td>
</tr>
<tr>
<td>Step 4</td>
<td>Matches with Cos value.</td>
</tr>
<tr>
<td>\texttt{match cos cos-value}</td>
<td></td>
</tr>
</tbody>
</table>
## 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.

**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`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure  terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>policy-map  policy-map-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# policy-map policy1</td>
</tr>
</tbody>
</table>

| Step 4 | class  {class-name | class-default} |
|--------|--------------------------|
| **Example:** | Device(config-pmap)# class class1 |

<table>
<thead>
<tr>
<th>Step 5</th>
<th>set cos  cos-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-pmap-c)# set cos 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-pmap-c)# end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>show policy-map</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show policy-map</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>show policy-map  policy-map  class  class-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show policy-map policy1 class class1</td>
</tr>
</tbody>
</table>

### 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)*.

### SUMMARY STEPS

<table>
<thead>
<tr>
<th>Number</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>configure terminal</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>3.</td>
<td>service instance number ethernet [name]</td>
</tr>
<tr>
<td>4.</td>
<td>service-policy {input</td>
</tr>
<tr>
<td>5.</td>
<td>encapsulation {default</td>
</tr>
<tr>
<td>6.</td>
<td>bridge-domain bridge-id [split-horizon group group-id]</td>
</tr>
<tr>
<td>7.</td>
<td>end</td>
</tr>
</tbody>
</table>

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface gigabitethernet 0/3/6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>service instance number ethernet [name]</td>
<td>Configure an EFP (service instance) and enter service instance configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** | Router(config)# service instance 1 ethernet | • 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. |
| **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. |
### 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.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **table-map table-map-name**
4. **map from from-value to to-value**
5. **default {default-value | copy | ignore}**
6. **end**
7. **show table-map [table-map-name]**
8. **copy running-config startup-config**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> table-map table-map-name</td>
<td>Create a table map by entering a table-map name and entering table-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# table-map dscp-to-cos</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 4** map from *from-value* to *to-value*

**Example:**
```
Router(config-tablemap)# map from 1 to 1
```

**Purpose**
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
```

**Purpose**
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.

**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
```

**Purpose**
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.
SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class {class-name | class-default}
5. police {rate-bps | cir {cir-bps | percent percent}} [bc burst-bytes] [conform-action action] [pir pir-bps] [be be-bps]
6. conform-action action
7. exceed-action action
8. violate-action action
9. end
10. show policy-map policy-map

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map policy-map-name</td>
<td>Specifies the name of the policy map and enters policy-map configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# policy-map ingress</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> class {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example: Device(config-pmap)# class cos 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> police {rate-bps</td>
<td>cir {cir-bps</td>
</tr>
<tr>
<td>Example: Device(config-pmap-c)# police cir 1000000 bc 31250 pir 200000 be 62500</td>
<td></td>
</tr>
</tbody>
</table>

• 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).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• bc burst-bytes—(Optional) Specifies the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000.</td>
<td></td>
</tr>
<tr>
<td>• conform-action action— (Optional) Specifies action to take on packets that conform to the specified rate limit.</td>
<td></td>
</tr>
<tr>
<td>• pir pir-bps—(Optional) Specifies the peak information rate (PIR).</td>
<td></td>
</tr>
<tr>
<td>• be be-bps—(Optional) Specifies how much the pir can be exceeded, either as a bit rate or an amount of time at pir.</td>
<td></td>
</tr>
<tr>
<td>Note You must specify a value for pir before the device displays this argument.</td>
<td></td>
</tr>
<tr>
<td>Note cir percent percent option is not supported on the router.</td>
<td></td>
</tr>
</tbody>
</table>

**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:
Device(config-pmap-c-police)#
exceed-action transmit

Specifies action to take on packets that exceed the rate limit.

**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**

ded

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 configuring 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 configuring 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>MQC</td>
<td>“Applying QoS Features Using the MQC” module</td>
</tr>
<tr>
<td>Classifying network traffic</td>
<td>&quot;Classifying Network Traffic&quot; module</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marking Network Traffic</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>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).</td>
</tr>
</tbody>
</table>
CHAPTER 2

Configuration to drop DEI / CFI traffic

If Drop Eligible Indicator (DEI) bit is enabled in 802.1ad header or has Canonical Format Identifier (CFI) bit enabled in 802.1q header on an arriving packet, such packets will be dropped using QOS.

Restriction

Use platform acl drop-dei-1-packets command to filter DOT1Q and DOT1AD packets marked with CFI/DEI bits. The feature only matches the outermost tag and the matching on the inner tag is not supported.

• Finding Feature Information, page 21
• CLI commands used to configure DEI/CFI traffic behavior, page 21
• Verifying the DEI/CFI traffic configuration, page 22

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.

CLI commands used to configure DEI/CFI traffic behavior

To configure, you need to modify the behavior of the DEI traffic using the CLI commands:
To enable the behavior, use the following CLI command:

platform acl drop-dei-1-packets

To disable the behavior, use the following CLI command:

no platform acl drop-dei-1-packets
Verifying the DEI/CFI traffic configuration

Use the following commands to verify the DEI/CFI traffic configuration:

```text
show platform hardware pp active tcam utilization qos detail 0
Device# show platform hardware pp active tcam utilization qos detail 0
This displays TCAM usage of 8 extra entries when command enabled.
```
Classifying and Marking MPLS EXP

The QoS EXP Matching feature allows you to classify and mark network traffic by modifying the Multiprotocol Label Switching (MPLS) experimental bits (EXP) field in IP packets. This module contains conceptual information and the configuration tasks for classifying and marking network traffic using the MPLS EXP field.

- Finding Feature Information, page 23
- Prerequisites for Classifying and Marking MPLS EXP, page 23
- Restrictions for Classifying and Marking MPLS EXP, page 24
- Information About Classifying and Marking MPLS EXP, page 24
- How to Classify and Mark MPLS EXP, page 25
- Configuration Examples for Classifying and Marking MPLS EXP, page 32
- Additional References, page 34
- Feature Information for Classifying and Marking MPLS EXP, page 35

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 Classifying and Marking MPLS EXP

- The router must be configured as an MPLS provider edge (PE) or provider (P) router, which can include the configuration of a valid label protocol and underlying IP routing protocols.
Restrictions for Classifying and Marking MPLS EXP

- MPLS classification and marking can only occur in an operational MPLS Network.
- MPLS EXP classification and marking is supported on the main router interfaces for MPLS packet switching and imposition (simple IP imposition and Ethernet over MPLS (EoMPLS) imposition) and on Ethernet virtual circuits (EVCs) or Ethernet flow points (EFPs) for EoMPLS imposition.
- MPLS EXP classification or marking for bridged MPLS packets on EVCs or EFPs is not supported.
- MPLS EXP marking is supported only in the ingress direction.

**Note**
MPLS EXP marking is supported on both ingress and egress directions on the Cisco RSP3 Module.

- If a packet is classified by IP type of service (ToS) or class of service (CoS) at ingress, it cannot be reclassified by MPLS EXP at egress (imposition case). However, if a packet is classified by MPLS at ingress it can be reclassified by IP ToS, CoS, or Quality of Service (QoS) group at egress (disposition case).

**Note**
Quality of Service (QoS) group is the only egress classification supported on the Cisco RSP3 Module.

- If a packet is encapsulated in MPLS, the MPLS payload cannot be checked for other protocols such as IP for classification or marking. Only MPLS EXP marking affects packets encapsulated by MPLS.

Information About Classifying and Marking MPLS EXP

Classifying and Marking MPLS EXP Overview

The QoS EXP Matching feature allows you to organize network traffic by setting values for the MPLS EXP field in MPLS packets. By choosing different values for the MPLS EXP field, you can mark packets so that packets have the priority that they require during periods of congestion. Setting the MPLS EXP value allows you to:

- **Classify traffic**
  The classification process selects the traffic to be marked. Classification accomplishes this by partitioning traffic into multiple priority levels, or classes of service. Traffic classification is the primary component of class-based QoS provisioning. For more information, see the "Classifying Network Traffic" module.

- **Police and mark traffic**
  Policing causes traffic that exceeds the configured rate to be discarded or marked to a different drop level. Marking traffic is a way to identify packet flows to differentiate them. Packet marking allows you to partition your network into multiple priority levels or classes of service. For more information, see the "Marking Network Traffic" module.
MPLS Experimental Field

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header that you can use to define the QoS treatment (per-hop behavior) that a node should give to a packet. In an IP network, the DiffServ Code Point (DSCP) (a 6-bit field) defines a class and drop precedence. The EXP bits can be used to carry some of the information encoded in the IP DSCP and can also be used to encode the dropping precedence.

By default, Cisco IOS Software copies the three most significant bits of the DSCP or the IP precedence of the IP packet to the EXP field in the MPLS header. This action happens when the MPLS header is initially imposed on the IP packet. However, you can also set the EXP field by defining a mapping between the DSCP or IP precedence and the EXP bits. This mapping is configured using the `set mpls experimental` or `police` commands. For more information, see the "How to Classify and Mark MPLS EXP" section.

Benefits of MPLS EXP Classification and Marking

If a service provider does not want to modify the value of the IP precedence field in packets transported through the network, they can use the MPLS EXP field value to classify and mark IP packets.

**Note**
The MPLS EXP field value cannot be used to mark IP packets at disposition on the Cisco RSP3 Module.

By choosing different values for the MPLS EXP field, you can mark critical packets so that those packets have priority if network congestion occurs.

How to Classify and Mark MPLS EXP

Classifying MPLS Encapsulated Packets

**Note**
MPLS EXP topmost classification is not supported for bridged MPLS packets on Ethernet virtual circuits (EVC) or Ethernet flow points (EFP).

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `class-map [match-all | match-any] class-map-name`
4. `match mpls experimental topmost mpls-exp-value`
5. `end`
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
<tr>
<td>Example: Router(config)# class-map exp3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> match mpls experimental topmost mpls-exp-value</td>
<td>Specifies the match criteria.</td>
</tr>
<tr>
<td>Example: Router(config-cmap)# match mpls experimental topmost 3</td>
<td><strong>Note</strong> The <code>match mpls experimental topmost</code> command classifies traffic on the basis of the EXP value in the topmost label header.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-cmap)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Marking MPLS EXP on All Imposed Labels

Perform this task to set the value of the MPLS EXP field on all imposed label entries.

#### Before You Begin

The router supports MPLS EXP marking only in the ingress direction.

In typical configurations, marking MPLS packets at imposition is used with ingress classification on IP ToS or CoS fields. However, generic matching with the class default value is supported with other ingress attributes such as `vlan`.

**Note** For IP imposition marking, the IP precedence value is copied to the MPLS EXP value by default.
For EVC configuration, a policy map that performs matching based on the CoS and that sets the EXP imposition value should be used to copy CoS values to the EXP value.

The `set mpls experimental imposition` command works only on packets that have new or additional MPLS labels added to them.

Configure `set qos-group` command to mark MPLS EXP label. The `set mpls experimental imposition` command is not supported for xconnect/L2VPN on the Cisco RSP3 Module.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class class-map-name
5. set mpls experimental imposition mpls-exp-value
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map policy-map-name</td>
<td>Specifies the name of the policy map to be created and enters policy-map configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# policy-map mark-up-exp-2</td>
<td>• Enter the policy map name.</td>
</tr>
</tbody>
</table>
### Classifying and Marking MPLS EXP

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> class class-map-name</td>
<td>Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-pmap)# class prec012</td>
<td>Enter the class map name.</td>
</tr>
<tr>
<td><strong>Step 5</strong> set mpls experimental imposition mpls-exp-value</td>
<td>Sets the value of the MPLS EXP field on all imposed label entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-pmap-c)# set mpls experimental imposition 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-pmap-c)# end</td>
<td></td>
</tr>
</tbody>
</table>

#### Marking MPLS EXP on Label Switched Packets

Perform this task to set the MPLS EXP field on label switched packets.

**Before You Begin**

**Note** The set mpls experimental topmost command works only on packets that are already MPLS encapsulated.

**Note** The router supports MPLS EXP marking in the ingress direction only, and does not support MPLS EXP classification or marking for bridged MPLS packets on EVCs or EFPs.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. policy-map policy-map-name
4. class class-map-name
5. set mpls experimental topmost mpls-exp-value
6. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1     | `enable`          | Enables privileged EXEC mode.  
  * Enter your password if prompted.  
  * Example:  
  **Router> enable** |
| 2     | `configure terminal` | Enters global configuration mode.  
  * Example:  
  **Router# configure terminal** |
| 3     | `policy-map policy-map-name` | Specifies the name of the policy map to be created and enters policy-map configuration mode.  
  * Enter the policy map name.  
  * Example:  
  **Router(config)# policy-map mark-up-exp-2** |
| 4     | `class class-map-name` | 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.  
  * Example:  
  **Router(config-pmap)# class-map exp012** |
| 5     | `set mpls experimental topmost mpls-exp-value` | Sets the MPLS EXP field value in the topmost label on the output interface.  
  * Example:  
  **Router(config-pmap-c)# set mpls experimental topmost 2** |
| 6     | `end`             | (Optional) Returns to privileged EXEC mode.  
  * Example:  
  **Router(config-pmap-c)# end** |

## Configuring Conditional Marking

To conditionally set the value of the MPLS EXP field on all imposed label, perform the following task:
Before You Begin

Note: The `set-mpls-exp-topmost-transmit` action affects MPLS encapsulated packets only. The `set-mpls-exp-imposition-transmit` action affects any new labels that are added to the packet.

Note: The conditional marking is supported on the router in the ingress direction only.

Note: The following are not supported on the Cisco RSP3 Module:
- IPv6 ACL
- Conditional Marking

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class class-map-name`
5. `police cir bps bc pir bps be`
8. `violate-action drop`
9. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 | **policy-map** policy-map-name | Specifies the name of the policy map to be created and enters policy-map configuration mode.  
**Example:**  
Router(config)# policy-map ip2tag  
**Purpose**  
- Enter the policy map name. |
| Step 4 | **class** class-map-name | Creates a class map to be used for matching traffic to a specified class, and enters policy-map class configuration mode.  
**Example:**  
Router(config-pmap)# class iptcp  
**Purpose**  
- Enter the class map name. |
| Step 5 | **police** cir bps bc pir bps be | Defines a policer for classified traffic and enters policy-map class police configuration mode.  
**Example:**  
Router(config-pmap-c)# police cir 1000000 pir 2000000  
**Purpose**  
- Define the policer for classified traffic. |
| Step 6 | **conform-action** [set-mpls-exp-imposition-transmit mpls-exp-value | Defines the action to take on packets that conform to the values specified by the policer.  
**Example:**  
Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3  
**Purpose**  
- In this example, if the packet conforms to the committed information rate (cir) or is within the conform burst (bc) size, the MPLS EXP field is set to 3. |
| Step 7 | **exceed-action** [set-mpls-exp-imposition-transmit mpls-exp-value | Defines the action to take on packets that exceed the values specified by the policer.  
**Example:**  
Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2  
**Purpose**  
- In this example, if the packet exceeds the cir rate and the bc size, but is within the peak burst (be) size, the MPLS EXP field is set to 2. |
| Step 8 | **violate-action** drop | Defines the action to take on packets whose rate exceeds the peak information rate (pir) and is outside the bc and be ranges.  
**Example:**  
Router(config-pmap-c-police)# violate-action drop  
**Purpose**  
- You must specify the exceed action before you specify the violate action.  
- In this example, if the packet rate exceeds the pir rate and is outside the bc and be ranges, the packet is dropped. |
| Step 9 | **end** | (Optional) Returns to privileged EXEC mode.  
**Example:**  
Router(config-pmap-c-police)# end  
**Purpose**  
(Optional) Returns to privileged EXEC mode. |
Configuration Examples for Classifying and Marking MPLS EXP

Example: Classifying MPLS Encapsulated Packets

Defining an MPLS EXP Class Map
The following example defines a class map named exp3 that matches packets that contains MPLS experimental value 3:

```
Router(config)# class-map exp3
Router(config-cmap)# match mpls experimental topmost 3
Router(config-cmap)# exit
```

Defining a Policy Map and Applying the Policy Map to an Ingress Interface
The following example uses the class map created in the example above to define a policy map. This example also applies the policy map to a physical interface for ingress traffic.

```
Router(config)# policy-map change-exp-3-to-2
Router(config-pmap)# class exp3
Router(config-pmap-c)# set mpls experimental topmost 2
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input change-exp-3-to-2
Router(config-if)# exit
```

Defining a Policy Map and Applying the Policy Map to an Egress Interface
The following example uses the class map created in the example above to define a policy map. This example also applies the policy map to a physical interface for egress traffic.

```
Router(config)# policy-map WAN-out
Router(config-pmap)# class exp3
Router(config-pmap-c)# shape average 1000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy output WAN-out
Router(config-if)# exit
```

Example: Marking MPLS EXP on All Imposed Labels

Defining an MPLS EXP Imposition Policy Map
The following example defines a policy map that sets the MPLS EXP imposition value to 2 based on the IP precedence value of the forwarded packet:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map prec012
Router(config-cmap)# match ip prec 0 1 2
Router(config-cmap)# exit
Router(config)# policy-map mark-up-exp-2
```

QoS: Classification Configuration Guide (Cisco ASR 920 Series)
Router(config-pmap)# class prec012
Router(config-pmap-c)# set mpls experimental imposition 2
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Applying the MPLS EXP Imposition Policy Map to a Main Interface

The following example applies a policy map to Gigabit Ethernet interface 0/0/0:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input mark-up-exp-2
Router(config-if)# exit

Applying the MPLS EXP Imposition Policy Map to an EVC

The following example applies a policy map to the Ethernet Virtual Connection specified by the service instance command:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# xconnect 100.0.0.1 encapsulation mpls 100
Router(config-if-srv)# service-policy input mark-up-exp-2
Router(config-if-srv)# exit
Router(config-if)# exit

Example: Marking MPLS EXP on Label Switched Packets

Defining an MPLS EXP Label Switched Packets Policy Map

The following example defines a policy map that sets the MPLS EXP topmost value to 2 according to the MPLS EXP value of the forwarded packet:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map exp012
Router(config-cmap)# match mpls experimental topmost 0 1 2
Router(config-cmap)# exit
Router(config-cmap)# policy-map mark-up-exp-2
Router(config-pmap)# class exp012
Router(config-pmap-c)# set mpls experimental topmost 2
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Applying the MPLS EXP Label Switched Packets Policy Map to a Main Interface

The following example shows how to apply the policy map to a main interface:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy input mark-up-exp-2
Router(config-if)# exit
Example: Configuring Conditional Marking

The example in this section creates a policer for the `iptcp` class, which is part of the `ip2tag` policy map, and attaches the policy map to the Gigabit Ethernet interface.

```bash
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# police cir 1000000 pir 2000000
Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3
Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config-if)# interface GigabitEthernet 0/0/1
Router(config-if)# service-policy input ip2tag
```

Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>QoS commands</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>Classifying network traffic</td>
<td>&quot;Classifying Network Traffic&quot; module</td>
</tr>
<tr>
<td>Marking network traffic</td>
<td>“Marking Network Traffic” module</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported, and support for existing standards has not been modified.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Classifying and Marking MPLS EXP

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 4: Feature Information for Classifying and Marking MPLS EXP**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifying and Marking MPLS EXP</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>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).</td>
</tr>
</tbody>
</table>
CHAPTER 4

Configuration of an IPv6 Access Control List

IPv6 Access Control Lists (ACLs) determine what traffic is blocked and what traffic is forwarded at device interfaces. ACLs allow filtering based on source and destination addresses, inbound and outbound to a specific interface.

- **Restrictions**, page 37
- **Configuring IPv6 Access Control List**, page 38
- **Example for Configuration of IPv6 ACL**, page 40
- **Verifying the Configuration**, page 40

**Restrictions**

The following restrictions apply when configuring IPv6 ACLs:

- ACE-specific counters are not supported.
- Layer 3 IPv4 and IPv6 ACLs are not supported on same EVC.
- MAC ACLs are not supported on EFP or trunk EFP interfaces to which Layer 3 IPv4 or IPv6 ACLs are applied.
- Up to 500 ACEs per ACL or 1500 total ACEs are supported.
- Egress v4/v6 ACL on EVC is not supported.

The following ACE parameters are supported:

- Source address
- Destination address
- TCP ports
- UDP ports
- DSCP value
- ICMP
Other ACE parameters are not supported.

# Configuring IPv6 Access Control List

The sections below describe how to configure an IPv6 ACL on the Cisco ASR 903 Series Router:

## Before You Begin

## Creating an IPv6 Access List

### SUMMARY STEPS

1. `configure terminal`

2. `ipv6 access-list access-list-name`

3. `permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [port-number] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [port-number] [dscp value] [log] [log-input] [sequence value]`

4. `deny protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [port-number] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [port-number] [dscp value] [log] [log-input] [sequence value]`

5. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> ipv6 access-list access-list-name</td>
<td>Defines an IPv6 ACL, and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ipv6 access-list ipv6-acl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> permit protocol {source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-ipv6-acl)# permit 0-255 An IPv6 protocol number X:X::X::X IPv6 source address x:x::y X:X::X::X/0-128 IPv6 source prefix x:x::y/z ahp Authentication Header Protocol any Any source prefix esp Encapsulation Security Payload hhb Hop by Hop options header host A single source host</td>
<td></td>
</tr>
</tbody>
</table>
Step 4  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny protocol {source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
</tbody>
</table>

Example:


Step 5  

defy protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [port-number] | destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [port-number] | dscp value] | [log] | [log-input] | [sequence value] |

Sets deny conditions for the IPv6 ACL.

Step 5  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
</tbody>
</table>

---

**Applying an IPv6 Access Control List to a Physical Interface**

**Before You Begin**

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. ipv6 traffic-filter access-list-name {in | out}
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Step 3 | ipv6 traffic-filter *access-list-name [in | out]*
Example: Device(config)# ipv6 traffic-filter ipv6-acl
Step 4 | end

**Example for Configuration of IPv6 ACL**

```
Router(config)# ipv6 access-list ipv6_acl
Router(config-ipv6-acl)# permit tcp any any
Router(config-ipv6-acl)# permit udp any any
Router(config-ipv6-acl)# permit any any
Router(config-ipv6-acl)# hardware statistics
Router(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Router(config)# interface GigabitEthernet3/1/0
Router(config-if)# no ip address
Router(config-if)# negotiation auto
Router(config-if)# ipv6 address 2001:1::1/64
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 traffic-filter ipv6_acl in
Router(config-if)# exit
Router(config)# clear counters
Clear "show interface" counters on all interfaces [confirm]
Router#

! Verify the configurations.

Router# show running-config interface GigabitEthernet3/1/0

Building configuration...

Current configuration : 114 bytes

! interface GigabitEthernet3/1/0
no ip address
negotiation auto
ipv6 address 1001::1/64
ipv6 traffic-filter ipv6_acl in
```

**Verifying the Configuration**

You can use the following commands to verify your IPv6 ACL configuration on the Cisco ASR 903 Series Router:

- `show platform hardware pp active acl label label-number`—Displays ACL information for a given label.
• `show platform hardware pp active acl name acl-name`—Displays ACL information for a given ACL name.

• `show platform hardware pp active acl acl-name stats`—Displays statistics for a given IPv6 ACL.

• `show platform hardware pp active tcam utilization acl detail id`—Displays TCAM usage for a given IPv6 ACL.

Before You Begin
IPv6 QoS: MQC Packet Classification

- Finding Feature Information, page 43
- Information About IPv6 QoS: MQC Packet Classification, page 43
- How to Configure IPv6 QoS: MQC Packet Classification, page 44
- Configuration Examples for IPv6 QoS: MQC Packet Classification, page 48
- Additional References, page 48
- Feature Information for IPv6 QoS: MQC Packet Classification, page 50

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.

Information About IPv6 QoS: MQC Packet Classification

Implementation Strategy for QoS for IPv6

IPv6 packets are forwarded by paths that are different from those for IPv4. QoS features supported for IPv6 environments include packet classification, queueing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets. These features are available at both the process switching and Cisco Express Forwarding switching paths of IPv6.

All of the QoS features available for IPv6 environments are managed from the modular QoS command-line interface (MQC). The MQC allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.
To implement QoS in networks running IPv6, follow the same steps that you would follow to implement QoS in networks running only IPv4. At a very high level, the basic steps for implementing QoS are as follows:

- Know which applications in your network need QoS.
- Understand the characteristics of the applications so that you can make decisions about which QoS features would be appropriate.
- Know your network topology so that you know how link layer header sizes are affected by changes and forwarding.
- Create classes based on the criteria you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6, decide if you want to treat both of them the same way or treat them separately and specify match criteria accordingly. If you want to treat them the same, use match statements such as `match precedence`, `match dscp`, `set precedence`, and `set dscp`. If you want to treat them separately, add match criteria such as `match protocol ip` and `match protocol ipv6` in a match-all class map.
- Create a policy to mark each class.
- Work from the edge toward the core in applying QoS features.
- Build the policy to treat the traffic.
- Apply the policy.

### Packet Classification in IPv6

Packet classification is available with both process and Cisco Express Forwarding switching path. Classification can be based on IPv6 precedence, differentiated services control point (DSCP), and other IPv6 protocol-specific values that can be specified in IPv6 access lists in addition to other non-IPv6 protocol specific values such as COS, packet length, and QOS group. Once you determine which applications need QoS, you can create classes based on the characteristics of the applications. You can use a variety of match criteria to classify traffic. You can combine various match criteria to segregate, isolate, and differentiate traffic.

The enhancements to the modular QoS CLI (MQC) allow you to create matches on precedence, DSCP, and IPv6 access group values in both IPv4 and IPv6 packets. The `match` command allows matches to be made on DSCP values and precedence for both IPv4 and IPv6 packets.

### How to Configure IPv6 QoS: MQC Packet Classification

#### Classifying Traffic in IPv6 Networks

The `set cos` and `match cos` commands for 802.1Q (dot1Q) interfaces are supported only for packets that are switched by Cisco Express Forwarding. Packets that are process-switched, such as device-generated packets, are not marked when these options are used.
Using the Match Criteria to Manage IPv6 Traffic Flows

You can use multiple match statements. Depending on the type of class, you can specify whether to match all classes or any of the classes.

SUMMARY STEPS

1. enable
2. configure terminal
3. class-map \{class-name|class-default\}
4. Do one of the following:
   - match precedence precedence-value [precedence-value precedence-value]
   - match access-group name ipv6-access-group
   - match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables such as privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 class-map {class-name</td>
<td>class-default}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-pmap-c)# class cls1</td>
<td></td>
</tr>
<tr>
<td>Step 4 Do one of the following:</td>
<td>Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.</td>
</tr>
<tr>
<td></td>
<td>• match precedence precedence-value [precedence-value precedence-value]</td>
</tr>
<tr>
<td></td>
<td>• match access-group name ipv6-access-group</td>
</tr>
<tr>
<td></td>
<td>• match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]</td>
</tr>
</tbody>
</table>
Confirming the Service Policy

Ensure that the traffic flow matches the input or output parameter of the policy. For example, downloading a file from an FTP server generates congestion in the receive direction because the server sends large MTU-sized frames, and the client PC returns small acknowledgments (ACKs).

Before you begin this task, simulate congestion with an extended ping using a large ping size and a large number of pings. Also, try downloading a large file from an FTP server. The file constitutes "disturbing" data and fills the interface bandwidth.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number multipoint | point-to-point`
4. `ip address ip-address mask [secondary]`
5. `pvc [name] vpi / vci [ces | ilmi | qsaal | smds]`
6. `tx-ring-limit ring-limit`
7. `service-policy {input | output} policy-map-name`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router# configure terminal</code></td>
</tr>
<tr>
<td>3</td>
<td>`interface type number multipoint</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config)# interface gigabitethernet1/1/0 point-to-point</code></td>
</tr>
<tr>
<td>4</td>
<td><code>ip address ip-address mask [secondary]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if)# ip address 10.1.1.1 255.255.255.0</code></td>
</tr>
<tr>
<td>5</td>
<td>`pvc [name] vpi / vci [ces</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if)# pvc cisco 0/5</code></td>
</tr>
<tr>
<td>6</td>
<td><code>tx-ring-limit ring-limit</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if-atm-vc)# tx-ring-limit 10</code></td>
</tr>
<tr>
<td>7</td>
<td>`service-policy {input</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;<code>Router(config-if-atm-vc)# service-policy output policy9</code></td>
</tr>
</tbody>
</table>
**Example: Matching DSCP Value**

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface. In this example, the `match dscp` command includes the optional `ip` keyword, meaning that the match is for IPv4 packets only. The class map called ipdscp15 will evaluate all packets entering interface GigabitEthernet 1/0/0. If the packet is an IPv4 packet and has a DSCP value of 15, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)#
  class-map ipdscp15
Router(config-cmap)#
  match ip dscp 15
Router(config)#
  exit
```
```
Router(config)#
policy-map priority50
Router(config-pmap)#
  class ipdscp15
Router(config-pmap-c)#
  priority 50
Router(config-pmap-c)#
  exit
Router(config-pmap)#
  exit
```
```
Router(config)#
  service-policy input priority55
```

To match on IPv6 packets only, use the `match dscp` command without the `ip` keyword preceded by the `match protocol` command. Ensure that the class map has the `match-all` attribute (which is the default).

```
Router(config)#
  class-map ipdscp15
Router(config-cmap)#
  match protocol ipv6
Router(config-cmap)#
  match dscp 15
Router(config)#
  exit
```

To match packets on both IPv4 and IPv6 protocols, use the `match dscp` command:

```
Router(config)#
  class-map ipdscp15
Router(config-cmap)#
  match dscp 15
```

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 addressing and connectivity</td>
<td>IPv6 Configuration Guide</td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>IPv6 commands</td>
<td>Cisco IOS IPv6 Command Reference</td>
</tr>
<tr>
<td>Cisco IOS IPv6 features</td>
<td>Cisco IOS IPv6 Feature Mapping</td>
</tr>
<tr>
<td>Classifying Network Traffic</td>
<td>&quot;Classifying Network Traffic&quot; module</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFCs for IPv6</td>
<td>IPv6 RFCs</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for IPv6 QoS: MQC Packet Classification

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 5: Feature Information for IPv6 QoS: MQC Packet Classification

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 QoS: MQC Packet Classification</td>
<td>Cisco IOS XE Release 3.13.0S</td>
<td>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).</td>
</tr>
</tbody>
</table>