# QoS: Classification Configuration Guide, Cisco IOS Release 15S

**First Published:** November 26, 2012

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

# CONTENTS

CHAPTER 1

# IPv6 Quality of Service

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.



# 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 at the end of this module.

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 Quality of Service

## 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, queuing, 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 that are 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 that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, 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 the 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 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 Quality of Service

## 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.

# Specifying Marking Criteria for IPv6 Packets

Perform this task to establish the match criteria to be used to match packets for classifying network traffic.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. Do one of the following:
   - **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
   - **set** [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy map** *policy-map-name*<br><br>**Example:**<br>`Device(config)# policy map policy1` | Creates a policy map using the specified name and enters QoS policy-map configuration mode.<br>• Enter the name of the policy map that you want to create. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Device(config-pmap)# class class-default` | Specifies the treatment for traffic of a specified class (or the default class) and enters QoS policy-map class configuration mode. |
| **Step 5** | Do one of the following:<br>• **set precedence** {*precedence-value* \| *from-field* [**table** *table-map-name*]} | Sets the precedence value and the DSCP value based on the CoS value (and action) defined in the specified table map. Both precedence and DSCP cannot be changed in the same packets. |

| | Command or Action | Purpose |
|---|---|---|
| | • **set** [**ip**] **dscp**{*dscp-value* \| *from-field* [**table** *table-map-name*]}<br><br>**Example:**<br>`Device(config-pmap-c)#`<br>`set precedence cos table table-map1`<br><br>**Example:**<br>`Device(config-pmap-c)#`<br>`set dscp cos table table-map1` | |

# 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 dscp-value*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables such as privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** {*class-name*\| **class-default**}<br><br>**Example:**<br><br>`Router(config-pmap-c)# class clsl` | Creates the specified class and enters QoS class-map configuration mode. |
| **Step 4** | Do one of the following:<br>• **match precedence** *precedence-value* [*precedence-value precedence-value*]<br>• **match access-group name** *ipv6-access-group*<br>• **match [ip] dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*<br><br>**Example:**<br><br>`Router(config-pmap-c)#`<br><br>`match precedence 5`<br><br>**Example:**<br><br>`Router(config-pmap-c)# match ip dscp 15` | Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.<br>or<br>Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class.<br>or<br>Identifies a specific IP DSCP value as a match criterion. |

# Configuration Examples for IPv6 Quality of Service

## Example: Verifying Cisco Express Forwarding Switching

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0. Use this command to verify that Cisco Express Forwarding switching is enabled for policy decisions to occur. Notice that the display shows that Cisco Express Forwarding switching is enabled.

```
Router# show cef interface Ethernet 1/0 detail

Ethernet1/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 10.2.61.8/24
```

```
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is Ethernet1/0
  Fast switching type 1, interface type 5
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A82 (0x48001A82)
  IP MTU 1500
```

# Example: Verifying Packet Marking Criteria

The following example shows how to use the **match precedence** command to manage IPv6 traffic flows:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-m c1
Device(config-cmap)# match precedence 5
Device(config-cmap)# end
Device#
Device(config)# policy p1
Device(config-pmap)# class c1
Device(config-pmap-c)# police 10000 conform set-prec-trans 4
```

To verify that packet marking is working as expected, use the **show policy** command. The output of this command shows a difference between the number of total packets and the number of packets marked.

```
Device# show policy p1
  Policy Map p1
    Class c1
      police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface serial 4/1
Device(config-if)# service out p1
Device(config-if)# end
Device# show policy interface s4/1
 Serial4/1
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: precedence 5
      police:
        10000 bps, 1500 limit, 1500 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 4
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps violate 0 bps
    Class-map: class-default (match-any)
      10 packets, 1486 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

During periods of transmit congestion at the outgoing interface, packets arrive faster than the interface can send them. It is helpful to know how to interpret the output of the **show policy-map interface** command, which is useful for monitoring the results of a service policy created with Cisco's MQC.

Congestion typically occurs when a fast ingress interface feeds a relatively slow egress interface. Functionally, congestion is defined as filling the transmit ring on the interface (a ring is a special buffer control structure). Every interface supports a pair of rings: a receive ring for receiving packets and a transmit ring for sending

packets. The size of the rings varies with the interface controller and with the bandwidth of the interface or virtual circuit (VC). As in the following example, use the **show atm vc** *vcd* command to display the value of the transmit ring on a PA-A3 ATM port adapter.

```
Device# show atm vc 3

ATM5/0.2: VCD: 3, VPI: 2, VCI: 2
VBR-NRT, PeakRate: 30000, Average Rate: 20000, Burst Cells: 94
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20, VCmode: 0x0
OAM frequency: 0 second(s)
PA TxRingLimit: 10
InARP frequency: 15 minutes(s)
Transmit priority 2
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

Cisco software (also referred to as the Layer 3 processor) and the interface driver use the transmit ring when moving packets to the physical media. The two processors collaborate in the following way:

- The interface sends packets according to the interface rate or a shaped rate.
- The interface maintains a hardware queue or transmit ring, where it stores the packets waiting for transmission onto the physical wire.
- When the hardware queue or transmit ring fills, the interface provides explicit back pressure to the Layer 3 processor system. It notifies the Layer 3 processor to stop dequeuing packets to the interface's transmit ring because the transmit ring is full. The Layer 3 processor now stores the excess packets in the Layer 3 queues.
- When the interface sends the packets on the transmit ring and empties the ring, it once again has sufficient buffers available to store the packets. It releases the back pressure, and the Layer 3 processor dequeues new packets to the interface.

The most important aspect of this communication system is that the interface recognizes that its transmit ring is full and throttles the receipt of new packets from the Layer 3 processor system. Thus, when the interface is congested, the drop decision is moved from a random, last-in, first-dropped decision in the first in, first out (FIFO) queue of the transmit ring to a differentiated decision based on IP-level service policies implemented by the Layer 3 processor.

Service policies apply only to packets stored in the Layer 3 queues. The table below illustrates which packets sit in the Layer 3 queue. Locally generated packets are always process-switched and are delivered first to the Layer 3 queue before being passed on to the interface driver. Fast-switched and CEF-switched packets are delivered directly to the transmit ring and sit in the L3 queue only when the transmit ring is full.

***Table 1: Packet Types and the Layer 3 Queue***

| Packet Type | Congestion | Noncongestion |
|---|---|---|
| Locally generated packets, including Telnet packets and pings | Yes | Yes |
| Other packets that are process-switched | Yes | Yes |

| Packet Type | Congestion | Noncongestion |
|---|---|---|
| Packets that are CEF or fast-switched | Yes | No |

The following example shows these guidelines applied to the **show policy-map interface** command output.

```
Device# show policy-map interface atm 1/0.1

ATM1/0.1: VC 0/100 -
 Service-policy output: cbwfq (1283)
   Class-map: A (match-all) (1285/2)
     28621 packets, 7098008 bytes

     5 minute offered rate 10000 bps, drop rate 0 bps
     Match: access-group 101 (1289)
     Weighted Fair Queueing
       Output Queue: Conversation 73
       Bandwidth 500 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 28621/7098008

       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: B (match-all) (1301/4)

     2058 packets, 148176 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: access-group 103 (1305)
     Weighted Fair Queueing
       Output Queue: Conversation 75
       Bandwidth 50 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: class-default (match-any) (1309/0)
     19 packets, 968 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1313)
```

The table below defines counters that appear in the example.

***Table 2: Packet Counters from show policy-map interface Output***

| Counter | Explanation |
|---|---|
| 28621 packets, 7098008 bytes | The number of packets matching the criteria of the class. This counter increments whether or not the interface is congested. |
| (pkts matched/bytes matched) 28621/709800 | The number of packets matching the criteria of the class when the interface was congested. In other words, the interface's transmit ring was full, and the driver and the L3 processor system worked together to queue the excess packets in the L3 queues, where the service policy applies. Packets that are process switched always go through the L3 queuing system and therefore increment the "packets matched" counter. |
| Class-map: B (match-all) (1301/4) | These numbers define an internal ID used with the CISCO-CLASS-BASED-QOS-MIB. |

| Counter | Explanation |
|---|---|
| 5 minute offered rate 0 bps, drop rate 0 bps | Use the **load-interval** command to change this value and make it a more instantaneous value. The lowest value is 30 seconds; however, statistics displayed in the **show policy-map interface** command output are updated every 10 seconds. Because the command effectively provides a snapshot at a specific moment, the statistics may not reflect a temporary change in queue size. |

Without congestion, there is no need to queue any excess packets. When congestion occurs, packets, including CEF and fast-switched packets, might go into the Layer 3 queue. If you use congestion management features, packets accumulating at an interface are queued until the interface is free to send them; they are then scheduled according to their assigned priority and the queueing mechanism configured for the interface.

Normally, the packets counter is much larger than the packets matched counter. If the values of the two counters are nearly equal, then the interface is receiving a large number of process-switched packets or is heavily congested. Both of these conditions should be investigated to ensure optimal packet forwarding.

Devices allocate conversation numbers for the queues that are created when the service policy is applied. The following example shows the queues and related information.

```
Device# show policy-map interface s1/0.1 dlci 100

      Serial1/0.1: DLCI 100 -
      output : mypolicy
       Class voice
        Weighted Fair Queueing
            Strict Priority
            Output Queue: Conversation 72

              Bandwidth 16 (kbps) Packets Matched 0
             (pkts discards/bytes discards) 0/0
       Class immediate-data
        Weighted Fair Queueing
            Output Queue: Conversation 73

              Bandwidth 60 (%) Packets Matched 0
              (pkts discards/bytes discards/tail drops) 0/0/0
              mean queue depth: 0
              drops: class  random   tail     min-th   max-th   mark-prob
                     0      0        0        64       128      1/10
                     1      0        0        71       128      1/10
                     2      0        0        78       128      1/10
                     3      0        0        85       128      1/10
                     4      0        0        92       128      1/10
                     5      0        0        99       128      1/10
                     6      0        0        106      128      1/10
                     7      0        0        113      128      1/10
                     rsvp   0        0        120      128      1/10
       Class priority-data
        Weighted Fair Queueing
            Output Queue: Conversation 74

              Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
              (pkts discards/bytes discards/tail drops) 0/0/0
       Class class-default
        Weighted Fair Queueing
            Flow Based Fair Queueing
            Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
```

Information reported for each class includes the following:

- Class definition
- Queueing method applied
- Output queue conversation number
- Bandwidth used
- Number of packets discarded
- Number of bytes discarded
- Number of packets dropped

The **class-default** class is the default class to which traffic is directed, if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map. The **fair-queue** command allows you to specify the number of dynamic queues into which IP flows are sorted and classified. Alternately, devices allocate a default number of queues derived from the bandwidth on the interface or VC. Supported values in either case are a power of two, in a range from 16 to 4096.

The table below lists the default values for interfaces and for ATM permanent virtual circuits (PVCs).

***Table 3: Default Number of Dynamic Queues as a Function of Interface Bandwidth***

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 64 kbps | 16 |
| More than 64 kbps and less than or equal to 128 kbps | 32 |
| More than 128 kbps and less than or equal to 256 kbps | 64 |
| More than 256 kbps and less than or equal to 512 kbps | 128 |
| More than 512 kbps | 256 |

The table below lists the default number of dynamic queues in relation to ATM PVC bandwidth.

***Table 4: Default Number of Dynamic Queues as a Function of ATM PVC Bandwidth***

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 128 kbps | 16 |
| More than 128 kbps and less than or equal to 512 kbps | 32 |
| More than 512 kbps and less than or equal to 2000 kbps | 64 |

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| More than 2000 kbps and less than or equal to 8000 kbps | 128 |
| More than 8000 kbps | 256 |

Based on the number of reserved queues for WFQ, Cisco software assigns a conversation or queue number as shown in the table below.

***Table 5: Conversation Numbers Assigned to Queues***

| Number | Type of Traffic |
|---|---|
| 1 to 256 | General flow-based traffic queues. Traffic that does not match to a user-created class will match to class-default and one of the flow-based queues. |
| 257 to 263 | Reserved for Cisco Discovery Protocol and for packets marked with an internal high-priority flag. |
| 264 | Reserved queue for the priority class (classes configured with the **priority** command). Look for the "Strict Priority" value for the class in the **show policy-map** interface output. The priority queue uses a conversation ID equal to the number of dynamic queues, plus 8. |
| 265 and higher | Queues for user-created classes. |

# 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 Fast Ethernet 1/0. 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)#
interface fa1/0
Router(config-if)#
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

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IPv6 commands | Cisco IOS IPv6 Command Reference |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |
| Classifying Network Traffic | “Classifying Network Traffic” module |
| Marking Network Traffic | “Marking Network Traffic” module |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 2474 | *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* |
| RFC 2475 | *An Architecture for Differentiated Services Framework* |
| RFC 2597 | *Assured Forwarding PHB* |
| RFC 2598 | *An Expedited Forwarding PHB* |
| RFC 2697 | *A Single Rate Three Color Marker* |
| RFC 2698 | *A Two Rate Three Color Marker* |
| RFCs for IPv6 | IPv6 RFCs |

### MIBs

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

### 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 IPv6 Quality of Service

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 6: Feature Information for IPv6 Quality of Service***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 Quality of Service | 12.2(13)T<br>12.3<br>12.2(50)SG<br>3.2.0SG<br>15.0(2)SG<br>12.2(33)SRA<br>12.2(18)SXE<br>Cisco IOS XE Release 2.1 | QoS features supported for IPv6 environments include packet classification, queueing, traffic shaping, WRED, class-based packet marking, and policing of IPv6 packets.<br>The following commands were introduced or modified: **match dscp**, **match precedence**, **set dscp**, **set precedence**.<br>The following commands were introduced or modified: **match access-group name**, **match dscp**, **match precedence**, **set dscp**, **set precedence**. |

CHAPTER 2

# IPv6 QoS: MQC Packet Marking/Remarking



## 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 at the end of this module.

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 Marking/Remarking

### 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, queuing, 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 that are 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 that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, 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.

## Policies and Class-Based Packet Marking in IPv6 Networks

You can create a policy to mark each class of traffic with appropriate priority values, using either DSCP or precedence. Class-based marking allows you to set the IPv6 precedence and DSCP values for traffic management. The traffic is marked as it enters the router on the ingress interface. The markings are used to treat the traffic (forward, queue) as it leaves the router on the egress interface. Always mark and treat the traffic as close as possible to its source.

## Traffic Policing in IPv6 Environments

Congestion management for IPv6 is similar to IPv4, and the commands used to configure queueing and traffic shaping features for IPv6 environments are the same commands as those used for IPv4. Traffic shaping allows you to limit the packet dequeue rate by holding additional packets in the queues and forwarding them as specified by parameters configured for traffic shaping features. Traffic shaping uses flow-based queueing by default. CBWFQ can be used to classify and prioritize the packets. Class-based policer and generic traffic shaping (GTS) or Frame Relay traffic shaping (FRTS) can be used for conditioning and policing traffic.

# How to Specify IPv6 QoS: MQC Packet Marking/Remarking

## Specifying Marking Criteria for IPv6 Packets

Perform this task to establish the match criteria to be used to match packets for classifying network traffic.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. Do one of the following:
   - **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
   - **set** [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy map** *policy-map-name*<br><br>**Example:**<br>`Device(config)# policy map policy1` | Creates a policy map using the specified name and enters QoS policy-map configuration mode.<br>• Enter the name of the policy map that you want to create. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Device(config-pmap)# class class-default` | Specifies the treatment for traffic of a specified class (or the default class) and enters QoS policy-map class configuration mode. |
| **Step 5** | Do one of the following:<br>• **set precedence** {*precedence-value* \| *from-field* [**table** *table-map-name*]}<br>• **set** [**ip**] **dscp** {*dscp-value* \| *from-field* [**table** *table-map-name*]} | Sets the precedence value and the DSCP value based on the CoS value (and action) defined in the specified table map. Both precedence and DSCP cannot be changed in the same packets. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-pmap-c)# set precedence cos table table-map1`<br><br>**Example:**<br>`Device(config-pmap-c)# set dscp cos table table-map1` | |

# Configuration Examples for IPv6 QoS: MQC Packet Marking/Remarking

## Example: Verifying Packet Marking Criteria

The following example shows how to use the **match precedence** command to manage IPv6 traffic flows:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-m c1
Device(config-cmap)# match precedence 5
Device(config-cmap)# end
Device#
Device(config)# policy p1
Device(config-pmap)# class c1
Device(config-pmap-c)# police 10000 conform set-prec-trans 4
```

To verify that packet marking is working as expected, use the **show policy** command. The output of this command shows a difference between the number of total packets and the number of packets marked.

```
Device# show policy p1
  Policy Map p1
    Class c1
      police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface serial 4/1
Device(config-if)# service out p1
Device(config-if)# end
Device# show policy interface s4/1
 Serial4/1
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: precedence 5
      police:
        10000 bps, 1500 limit, 1500 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 4
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps violate 0 bps
```

```
    Class-map: class-default (match-any)
      10 packets, 1486 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

During periods of transmit congestion at the outgoing interface, packets arrive faster than the interface can send them. It is helpful to know how to interpret the output of the **show policy-map interface** command, which is useful for monitoring the results of a service policy created with Cisco's MQC.

Congestion typically occurs when a fast ingress interface feeds a relatively slow egress interface. Functionally, congestion is defined as filling the transmit ring on the interface (a ring is a special buffer control structure). Every interface supports a pair of rings: a receive ring for receiving packets and a transmit ring for sending packets. The size of the rings varies with the interface controller and with the bandwidth of the interface or virtual circuit (VC). As in the following example, use the **show atm vc** *vcd* command to display the value of the transmit ring on a PA-A3 ATM port adapter.

```
Device# show atm vc 3

ATM5/0.2: VCD: 3, VPI: 2, VCI: 2
VBR-NRT, PeakRate: 30000, Average Rate: 20000, Burst Cells: 94
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20, VCmode: 0x0
OAM frequency: 0 second(s)
PA TxRingLimit: 10
InARP frequency: 15 minutes(s)
Transmit priority 2
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

Cisco software (also referred to as the Layer 3 processor) and the interface driver use the transmit ring when moving packets to the physical media. The two processors collaborate in the following way:

- The interface sends packets according to the interface rate or a shaped rate.
- The interface maintains a hardware queue or transmit ring, where it stores the packets waiting for transmission onto the physical wire.
- When the hardware queue or transmit ring fills, the interface provides explicit back pressure to the Layer 3 processor system. It notifies the Layer 3 processor to stop dequeuing packets to the interface's transmit ring because the transmit ring is full. The Layer 3 processor now stores the excess packets in the Layer 3 queues.
- When the interface sends the packets on the transmit ring and empties the ring, it once again has sufficient buffers available to store the packets. It releases the back pressure, and the Layer 3 processor dequeues new packets to the interface.

The most important aspect of this communication system is that the interface recognizes that its transmit ring is full and throttles the receipt of new packets from the Layer 3 processor system. Thus, when the interface is congested, the drop decision is moved from a random, last-in, first-dropped decision in the first in, first out (FIFO) queue of the transmit ring to a differentiated decision based on IP-level service policies implemented by the Layer 3 processor.

Service policies apply only to packets stored in the Layer 3 queues. The table below illustrates which packets sit in the Layer 3 queue. Locally generated packets are always process-switched and are delivered first to the Layer 3 queue before being passed on to the interface driver. Fast-switched and CEF-switched packets are delivered directly to the transmit ring and sit in the L3 queue only when the transmit ring is full.

*Table 7: Packet Types and the Layer 3 Queue*

| Packet Type | Congestion | Noncongestion |
|---|---|---|
| Locally generated packets, including Telnet packets and pings | Yes | Yes |
| Other packets that are process-switched | Yes | Yes |
| Packets that are CEF or fast-switched | Yes | No |

The following example shows these guidelines applied to the **show policy-map interface** command output.

```
Device# show policy-map interface atm 1/0.1

ATM1/0.1: VC 0/100 -
 Service-policy output: cbwfq (1283)
   Class-map: A (match-all) (1285/2)
     28621 packets, 7098008 bytes

     5 minute offered rate 10000 bps, drop rate 0 bps
     Match: access-group 101 (1289)
     Weighted Fair Queueing
       Output Queue: Conversation 73
       Bandwidth 500 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 28621/7098008

       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: B (match-all) (1301/4)

     2058 packets, 148176 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: access-group 103 (1305)
     Weighted Fair Queueing
       Output Queue: Conversation 75
       Bandwidth 50 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: class-default (match-any) (1309/0)
     19 packets, 968 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1313)
```

The table below defines counters that appear in the example.

*Table 8: Packet Counters from show policy-map interface Output*

| Counter | Explanation |
|---|---|
| 28621 packets, 7098008 bytes | The number of packets matching the criteria of the class. This counter increments whether or not the interface is congested. |

| Counter | Explanation |
|---|---|
| (pkts matched/bytes matched) 28621/709800 | The number of packets matching the criteria of the class when the interface was congested. In other words, the interface's transmit ring was full, and the driver and the L3 processor system worked together to queue the excess packets in the L3 queues, where the service policy applies. Packets that are process switched always go through the L3 queuing system and therefore increment the "packets matched" counter. |
| Class-map: B (match-all) (1301/4) | These numbers define an internal ID used with the CISCO-CLASS-BASED-QOS-MIB. |
| 5 minute offered rate 0 bps, drop rate 0 bps | Use the **load-interval** command to change this value and make it a more instantaneous value. The lowest value is 30 seconds; however, statistics displayed in the **show policy-map interface** command output are updated every 10 seconds. Because the command effectively provides a snapshot at a specific moment, the statistics may not reflect a temporary change in queue size. |

Without congestion, there is no need to queue any excess packets. When congestion occurs, packets, including CEF and fast-switched packets, might go into the Layer 3 queue. If you use congestion management features, packets accumulating at an interface are queued until the interface is free to send them; they are then scheduled according to their assigned priority and the queueing mechanism configured for the interface.

Normally, the packets counter is much larger than the packets matched counter. If the values of the two counters are nearly equal, then the interface is receiving a large number of process-switched packets or is heavily congested. Both of these conditions should be investigated to ensure optimal packet forwarding.

Devices allocate conversation numbers for the queues that are created when the service policy is applied. The following example shows the queues and related information.

```
Device# show policy-map interface s1/0.1 dlci 100

      Serial1/0.1: DLCI 100 -
      output : mypolicy
       Class voice
        Weighted Fair Queueing
            Strict Priority
            Output Queue: Conversation 72

              Bandwidth 16 (kbps) Packets Matched 0
             (pkts discards/bytes discards) 0/0
       Class immediate-data
        Weighted Fair Queueing
            Output Queue: Conversation 73

              Bandwidth 60 (%) Packets Matched 0
              (pkts discards/bytes discards/tail drops) 0/0/0
              mean queue depth: 0
              drops: class  random   tail     min-th   max-th   mark-prob
                     0      0        0        64       128      1/10
                     1      0        0        71       128      1/10
```

```
                2      0        0        78       128      1/10
                3      0        0        85       128      1/10
                4      0        0        92       128      1/10
                5      0        0        99       128      1/10
                6      0        0        106      128      1/10
                7      0        0        113      128      1/10
                rsvp   0        0        120      128      1/10
Class priority-data
 Weighted Fair Queueing
     Output Queue: Conversation 74

       Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
       (pkts discards/bytes discards/tail drops) 0/0/0
Class class-default
 Weighted Fair Queueing
     Flow Based Fair Queueing
     Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
```

Information reported for each class includes the following:

- Class definition
- Queueing method applied
- Output queue conversation number
- Bandwidth used
- Number of packets discarded
- Number of bytes discarded
- Number of packets dropped

The **class-default** class is the default class to which traffic is directed, if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map. The **fair-queue** command allows you to specify the number of dynamic queues into which IP flows are sorted and classified. Alternately, devices allocate a default number of queues derived from the bandwidth on the interface or VC. Supported values in either case are a power of two, in a range from 16 to 4096.

The table below lists the default values for interfaces and for ATM permanent virtual circuits (PVCs).

***Table 9: Default Number of Dynamic Queues as a Function of Interface Bandwidth***

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 64 kbps | 16 |
| More than 64 kbps and less than or equal to 128 kbps | 32 |
| More than 128 kbps and less than or equal to 256 kbps | 64 |
| More than 256 kbps and less than or equal to 512 kbps | 128 |
| More than 512 kbps | 256 |

The table below lists the default number of dynamic queues in relation to ATM PVC bandwidth.

*Table 10: Default Number of Dynamic Queues as a Function of ATM PVC Bandwidth*

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 128 kbps | 16 |
| More than 128 kbps and less than or equal to 512 kbps | 32 |
| More than 512 kbps and less than or equal to 2000 kbps | 64 |
| More than 2000 kbps and less than or equal to 8000 kbps | 128 |
| More than 8000 kbps | 256 |

Based on the number of reserved queues for WFQ, Cisco software assigns a conversation or queue number as shown in the table below.

*Table 11: Conversation Numbers Assigned to Queues*

| Number | Type of Traffic |
|---|---|
| 1 to 256 | General flow-based traffic queues. Traffic that does not match to a user-created class will match to class-default and one of the flow-based queues. |
| 257 to 263 | Reserved for Cisco Discovery Protocol and for packets marked with an internal high-priority flag. |
| 264 | Reserved queue for the priority class (classes configured with the **priority** command). Look for the "Strict Priority" value for the class in the **show policy-map** interface output. The priority queue uses a conversation ID equal to the number of dynamic queues, plus 8. |
| 265 and higher | Queues for user-created classes. |

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IPv6 commands | Cisco IOS IPv6 Command Reference |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |
| Marking Network Traffic | "Marking Network Traffic" module |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | IPv6 RFCs |

### MIBs

| MIB | MIBs Link |
|---|---|
| | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### 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 IPv6 QoS: MQC Packet Marking/Remarking

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 12: Feature Information for IPv6 QoS: MQC Packet Marking/Remarking***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 QoS: MQC Packet Marking/Remarking | 12.0(28)S<br>12.2(33)SRA<br>12.2(18)SXE2<br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | Class-based marking allows you to set the IPv6 precedence and DSCP values for traffic management. |

CHAPTER 3

# IPv6 QoS: MQC Packet Classification



## 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 at the end of this module.

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, queuing, 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 that are 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 that you establish for your network. In particular, if the same network is also carrying IPv4 traffic along with IPv6 traffic, 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 the 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 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 dscp-value*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** {*class-name*| **class-default**}<br><br>**Example:**<br>`Router(config-pmap-c)# class clsl` | Creates the specified class and enters QoS class-map configuration mode. |
| **Step 4** | Do one of the following:<br>• **match precedence** *precedence-value* [*precedence-value precedence-value*]<br>• **match access-group name** *ipv6-access-group*<br>• **match [ip] dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value* | Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.<br>or<br>Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class.<br>or<br>Identifies a specific IP DSCP value as a match criterion. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config-pmap-c)#`<br>`match precedence 5`<br><br>**Example:**<br>`Router(config-pmap-c)# match ip dscp 15` | |

# 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* **multipoint** \| **point-to-point**<br><br>**Example:**<br><br>`Router(config)# interface ethernet1/1 point-to-point` | Enters interface configuration mode. |
| **Step 4** | **ip address ip-address mask** [*secondary*]<br><br>**Example:**<br><br>`Router(config-if)# ip address 10.1.1.1 255.255.255.0` | Specifies the IP address of the interface you want to test. |
| **Step 5** | **pvc** [*name*] *vpi* / *vci* [**ces** \| **ilmi** \| **qsaal** \| **smds**]<br><br>**Example:**<br><br>`Router(config-if)#`<br><br>`pvc cisco 0/5` | Creates or assigns a name to an ATM PVC, optionally specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode. |
| **Step 6** | **tx-ring-limit** *ring-limit*<br><br>**Example:**<br><br>`Router(config-if-atm-vc)# tx-ring-limit 10` | Reduces the size of the transmit ring of the interface. Lowering this value accelerates the use of the QoS in the Cisco IOS software.<br><br>• Specify the ring limit as the number of packets for 2600 and 3600 series routers, or as the number of memory particles for 7200 and 7500 series routers. |
| **Step 7** | **service-policy** {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Router(config-if-atm-vc)# service-policy output policy9` | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.<br><br>• The packets-matched counter is a part of queueing feature and is available only on service policies attached in output direction. |

# Configuration Examples for IPv6 QoS: MQC Packet Classification

## 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 Fast Ethernet 1/0. 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)#
interface fa1/0
Router(config-if)#
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

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IPv6 commands | Cisco IOS IPv6 Command Reference |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |
| Classifying Network Traffic | "Classifying Network Traffic" module |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### 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 releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### 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 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 13: Feature Information for IPv6 QoS: MQC Packet Classification***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 QoS: MQC Packet Classification | 12.2(33)SRA<br>12.2(18)SXE2<br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | The modular QoS CLI allows you to define traffic classes, create and configure traffic policies, and then attach those traffic policies to interfaces.<br>The following commands were introduced or modified: **match access-group name**, **match dscp**, **match precedence**, **set dscp**, **set precedence**. |

CHAPTER 4

# Packet Classification Based on Layer 3 Packet Length

This feature provides the added capability of matching and classifying traffic on the basis of the Layer 3 packet length in the IP header. The Layer 3 packet length is the IP datagram length plus the IP header length. This new match criterion supplements the other match criteria, such as the IP precedence, the differentiated services code point (DSCP) value, and the class of service (CoS).



## 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 at the end of this module.

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 Packet Classification Based on Layer 3 Packet Length

When configuring this feature, you must first create a policy map (sometimes referred to as a service policy or a traffic policy) using the Modular QoS Command-Line Interface (CLI) (MQC). Therefore, you should be familiar with the procedure for creating a policy map using the MQC.

For more information about creating a policy map (traffic policy) using the MQC, see the "Applying QoS Features Using the MQC" module.

# Restrictions for Packet Classification Based on Layer 3 Packet Length

- This feature is intended for use with IP packets only.
- This feature considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 overhead.

# Information About Packet Classification Based on Layer 3 Packet Length

## MQC and Packet Classification Based on Layer 3 Packet Length

Use the MQC to enable packet classification based on Layer 3 packet length. The MQC is a CLI that allows you to create traffic policies, enable a QoS feature (such as packet classification), and attach these policies to interfaces.

In the MQC, the **class-map** command is used to define a traffic class (which is then associated with a traffic policy). The purpose of a traffic class is to classify traffic.

The MQC consists of the following three processes:

- Defining a traffic class with the **class-map** command.
- Creating a traffic policy by associating the traffic class with one or more QoS features (using the **policy-map** command).
- Attaching the traffic policy to the interface with the**service-policy** command.

A traffic class contains three major elements: a name, a series of **match** commands, and, if more than one **match** command exists in the traffic class, an instruction on how to evaluate these **match** commands. The traffic class is named in the **class-map** command line; for example, if you enter the**class-mapcisco**command while configuring the traffic class in the CLI, the traffic class would be named "cisco".

The**match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified

criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

# How to Configure Packet Classification Based on Layer 3 Packet Length

## Configuring the Class Map to Match on Layer 3 Packet Length

Class maps can be used to classify packets into groups that can then receive specific QoS features. For example, class maps can be configured to match packets on the basis of one or more user-specified criteria (for example, the DSCP value or access list number). In this procedure, the class map is configured to match on the Layer 3 packet length.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match packet length** {**max***maximum-length-value* [**min***minimum-length-value*] | **min***minimum-length-value* [**max***maximum-length-value*]}
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** *class-map-name*<br><br>**Example:**<br>`Router(config)# class-map class1` | Specifies the name of the class map to be created and enters class-map configuration mode.<br>• Enter the class map name. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **match packet length** {**max***maximum-length-value* [**min***minimum-length-value*] \| **min***minimum-length-value* [**max***maximum-length-value*]}<br><br>**Example:**<br><br>`Router(config-cmap)# match packet length min 100 max 300` | Configures the class map to match traffic on the basis of the Layer 3 packet length.<br><br>• Enter the Layer 3 packet length in bytes. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Router(config-cmap)# end` | (Optional) Exits class-map configuration mode and returns to privileged EXEC mode. |

# Attaching the Policy Map to an Interface

### Before You Begin

Before attaching the policy map to an interface, the policy map must be created using the MQC.

## SUMMARY STEPS

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

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br><br>**Example:**<br><br>`Device(config)# interface serial4/0/0` | Configures an interface (or subinterface) type and enters interface configuration mode |
| **Step 4** | **pvc** [*name*] *vpi*/*vci* [**ilmi** \| **qsaal** \| **smds**]<br><br>**Example:**<br><br>`Device(config-if)# pvc cisco 0/16 ilmi` | (Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode.<br><br>**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, skip this step. |
| **Step 5** | **service-policy** {**input**\| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Device(config-if)# service-policy input policy1`<br><br>**Example:**<br><br>`Device(config-if-atm-vc)# service-policy input policy1` | Specifies the name of the policy map to be attached to either the input or output direction of the interface.<br><br>**Note** Policy maps can be configured on ingress or egress devices. They can also be attached in the input or output direction of an interface. The direction (input or output) and the device (ingress or egress) to which the policy map should be attached vary according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the device and the interface direction that are appropriate for your network configuration. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Device(config-if)# end`<br><br>**Example:**<br><br>`Device(config-if-atm-vc)# end` | (Optional) Exits interface configuration or ATM VC configuration mode and returns to privileged EXEC mode. |

# Verifying the Layer 3 Packet Length Classification Configuration

## SUMMARY STEPS

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map interface** *interface-name* [**vc** [*vpi*/] *vci*] [**dlci***dlci*] [**input**\| **output**]
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show class-map** [*class-map-name*]<br><br>**Example:**<br>`Router# show class-map class1` | (Optional) Displays all information about a class map, including the match criterion.<br>• Enter the class map name. |
| **Step 3** | **show policy-map interface** *interface-name* [**vc** [*vpi/*] *vci*] [**dlci***dlci*] [**input**\| **output**]<br><br>**Example:**<br>`Router# show policy-map interface serial4/0/0` | (Optional) Displays the packet 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.<br>• Enter the interface name. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Router# exit` | (Optional) Exits privileged EXEC mode. |

## Troubleshooting Tips

The commands in the Verifying the Layer 3 Packet Length Classification Configuration section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or that the feature is not functioning as expected, perform these operations:

If the configuration is not the one that you intended, perform the following operations:

- Use the **showrunning-config** command and analyze the output of the command.
- If the policy map does not appear in the output of the **showrunning-config** command, enable the **loggingconsole** command.
- Attach the policy map to the interface again.

If the packets are not being matched correctly (for example, the packet counters are not incrementing correctly), perform the following operations:

- Run the **showpolicy-map**command and analyze the output of the command.
- Run the **showrunning-config** command and analyze the output of the command.

- Use the **showpolicy-mapinterface** command and analyze the output of the command. Check the the following:
  - If a policy map applies queueing, and the packets are matching the correct class, but you see unexpected results, compare the number of packets in the queue with the number of packets matched.
  - If the interface is congested, and only a small number of packets are being matched, check the tuning of the tx ring and evaluate whether queueing is happening on the tx ring. To do this, use the **showcontrollers** command and look at the value of the tx count in the output.

# Configuration Examples for Packet Classification Based on Layer 3 Packet Length

## Example Configuring the Layer 3 Packet Length as a Match Criterion

In the following example, a class map called "class 1" has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes are viewed as meeting the match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class map class1
Router(config-cmap)# match packet length min 100 max 300
```

## Example Verifying the Layer 3 Packet Length Setting

Use either the **showclass-map** command or the **showpolicy-mapinterface** command to verify the setting of the Layer 3 packet length value used as a match criterion for the class map and the policy map. The following section begins with sample output of the **showclass-map**command and concludes with sample output of the **showpolicy-mapinterface** command.

The sample output of the **showclass-map** command shows the defined class map and the specified match criterion. In the following example, a class map called "class1" is defined. The Layer 3 packet length has been specified as a match criterion for the class. Packets with a Layer 3 length of between 100 bytes and 300 bytes belong to class1.

```
Router# show class-map
class-map match-all class1
    match packet length min 100 max 300
```

The sample output of the **showpolicy-mapinterface** command displays the statistics for FastEthernet interface 4/1/1, to which a service policy called "mypolicy" is attached. The configuration for the policy map called "mypolicy" is given below.

```
Router(config)# policy-map mypolicy
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface fastethernet4/1/1
Router(config-if)# service-policy input mypolicy
```

The following are the statistics for the policy map called "mypolicy" attached to FastEthernet interface 4/1/1. These statistics confirm that matching on the Layer 3 packet length has been configured as a match criterion.

```
Router# show policy-map interface
 FastEthernet4/1/1
 FastEthernet4/1/1
  Service-policy input: mypolicy
    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

# 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 and information about attaching policy maps to interfaces | "Applying QoS Features Using the MQC" module |
| Additional match criteria that can be used for packet classification | "Classifying Network Traffic" module |
| Marking network traffic | "Marking Network Traffic" module |

### Standards

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

### MIBs

| MIB | MIBs Link |
|---|---|
| • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB<br>• CISCO-CLASS-BASED-QOS-MIB | 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:<br>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 Packet Classification Based on Layer 3 Packet Length

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 14: Feature Information for Packet Classification Based on Layer 3 Packet Length*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Packet Classification Based on Layer 3 Packet Length | 12.2(13)T<br>12.2(18)SXE<br>Cisco IOS XE Release 2.2 | This feature provides the added capability of matching and classifying traffic on the basis of the Layer 3 packet length in the IP header.<br>In Release 12.2(13)T, this feature was introduced.<br>This feature was integrated into Cisco IOS Release 12.2(18)SXE.<br>This feature was integrated into Cisco IOS XE Release 2.2.<br>The following commands were introduced or modified: **matchpacketlength** (class-map), **showclass-map**, **showpolicy-mapinterface**. |

CHAPTER 5

# Configuring Committed Access Rate

This module describes the tasks for configuring committed access rate (CAR) and distributed CAR (DCAR).

**Note** In Cisco IOS Release 12.2 SR, CAR is not supported on the Cisco 7600 series router.

For complete conceptual information about these features, see the "Classification Overview"module and the "Policing and Shaping Overview" module.

For a complete description of the CAR commands in this module, see the Cisco IOS Quality of Service Solutions Command Reference. To locate documentation of other commands that appear in this module, use the command reference master index or search online.

**Note** CAR and DCAR can only be used with IP traffic. Non-IP traffic is not rate limited. CAR and DCAR can be configured on an interface or subinterface. However, CAR and DCAR are not supported on the Fast EtherChannel, tunnel, or PRI interfaces, nor on any interface that does not support Cisco Express Forwarding (CEF). CEF must be enabled on the interface before you configure CAR or DCAR. CAR is not supported for Internetwork Packet Exchange (IPX) packets.

# 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 at the end of this module.

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.

# Committed Access Rate Configuration Task List

The CAR and DCAR services limit the input or output transmission rate on an interface or subinterface based on a flexible set of criteria. CAR is often configured on interfaces at the edge of a network to limit traffic into or out of the network.

CAR can rate limit traffic based on certain matching criteria, such as incoming interface, IP precedence, or IP access list. You configure the actions that CAR will take when traffic conforms to or exceeds the rate limit.

You can set CAR rate policies that are associated with one of the following:

- All IP traffic
- IP precedence
- MAC address
- IP access list, both standard and extended. Matching to IP access lists is more processor-intensive than matching based on other criteria.

Each interface can have multiple CAR policies, corresponding to different types of traffic. For example, low priority traffic may be limited to a lower rate than high-priority traffic. With multiple rate policies, the router examines each policy in the order entered until the packet matches. If a match is not found, the default action is to send.

The rate policies can be independent; each rate policy deals with a different type of traffic. Alternatively, rate policies can be cascading; a packet can be compared to multiple different rate policies in succession. You can configure up to 100 rate policies on a subinterface.

**Note** Because of the linear search for the matching rate-limit statement, the CPU load increases with the number of rate policies.

Basic CAR and DCAR functionality requires that the following criteria be defined:

- Packet direction, incoming or outgoing.
- An average rate, determined by a long-term average of the transmission rate. Traffic that falls under this rate will always conform.
- A normal burst size, which determines how large traffic bursts can be before some traffic is considered to exceed the rate limit.

- An excess burst size (Be). Traffic that falls between the normal burst size and the Excess Burst size exceeds the rate limit with a probability that increases as the burst size increases. CAR propagates bursts. It does no smoothing or shaping of traffic.

***Table 15: Rate-Limit Command Action Keywords***

| Keyword | Description |
|---|---|
| **continue** | Evaluates the next **rate-limit** command. |
| **drop** | Drops the packet. |
| **set-prec-continue** *new-prec* | Sets the IP Precedence and evaluates the next **rate-limit** command. |
| **set-prec-transmit** *new-prec* | Sets the IP Precedence and sends the packet. |
| **transmit** | Sends the packet. |

# IP Precedence or MAC Address

Use the **access-list rate-limit** command to classify packets using either IP Precedence or MAC addresses. You can then apply CAR policies using the **rate-limit** command to individual rate-limited access lists. Packets with different IP precedences or MAC addresses are treated differently by the CAR service. See the section Example Rate Limiting in an IXP, on page 51 for an example of how to configure a CAR policy using MAC addresses.

# IP Access List

Use the **access-list** command to define CAR policy based on an access list. The *acl-index* argument is an access list number. Use a number from 1 to 99 to classify packets by precedence or precedence mask. Use a number from 100 to 199 to classify by MAC address.

**Note** If an access list is not present, the **rate-limit** command will act as if no access list is defined and all traffic will be rate limited accordingly.

When you configure DCAR on Cisco 7000 series routers with RSP7000 or Cisco 7500 series routers with a VIP2-40 or greater interface processor, you can classify packets by group, to allow you to partition your network into multiple priority levels or classes of service. This classification is achieved by setting IP precedences based on different criteria for use by other QoS features such as Weighted Random Early Detection (WRED) or weighted fair queueing (WFQ).

# Configuring CAR and DCAR for All IP Traffic

## SUMMARY STEPS

1. Router(config)# **interface***interface-type interface-number*
2. Router(config-if)# **rate-limit** {**input** | **output**} *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **interface***interface-type interface-number* | Specifies the interface or subinterface. This command puts the router in interface configuration mode. |
| **Step 2** | Router(config-if)# **rate-limit** {**input** \| **output**} *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* | Specifies a basic CAR policy for allConfiguring CAR and DCAR for All IP Traffic, on page 48ef"> Table 1 for a description of conform and exceed *action* keywords. |

# Configuring CAR and DCAR Policies

## SUMMARY STEPS

1. Router(config-if)# **interface** *interface-type interface-number*
2. Router(config-if)# **rate-limit** {**input** | **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*
3. Router(config-if) **exit**
4. Router(config)# **access-list rate-limit** *acl-index* {*precedence* | *mac-address*| **mask** *prec-mask*}
5. Do one of the following:
   - Router(config)# **access-list** *acl-index* {**deny** | **permit**} *source*[*source-wildcard*]
   - Router(config)# **access-list** *acl-index* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config-if)# **interface** *interface-type interface-number* | Specifies the interface or subinterface. This command puts the router in interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Router(config-if)# **rate-limit** {**input** \| **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* | Specifies the rate policy for each particular class of traffic. See Configuring CAR and DCAR Policies, on page 48 for a description of the **rate-limit** command action keywords. Repeat this command for each different class of traffic. |
| **Step 3** | Router(config-if) **exit** | (Optional) Returns to global configuration mode.<br>**Note** This change in configuration mode is needed only if you complete optional Configuring CAR and DCAR Policies or Configuring CAR and DCAR Policies. |
| **Step 4** | Router(config)# **access-list rate-limit** *acl-index* {*precedence* \| *mac-address*\| **mask** *prec-mask*} | (Optional) Specifies a rate-limited access list. Repeat this command if you wish to specify a new access list. |
| **Step 5** | Do one of the following:<br>• Router(config)# **access-list** *acl-index* {**deny** \| **permit**} *source*[*source-wildcard*]<br>• Router(config)# **access-list** *acl-index* {**deny** \| **permit**} *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] | (Optional) Specifies a standard or extended access list. Repeat this command to further configure the access list or specify a new access list. |

# Configuring a Class-Based DCAR Policy

## SUMMARY STEPS

1. Router(config-if)# **interface** *interface-type interface-number*
2. Router(config-if)# **rate-limit** {**input** | **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action*
3. Router(config-if)# **random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator*
4. Do one of the following:
   - Router(config-if)# **access-list** *acl-index* {**deny** | **permit**} *source*[*source-wildcard*]
   - Router(config-if)# **access-list** *acl-index* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*] [**tos** *tos*] [**log**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config-if)# **interface** *interface-type interface-number* | Specifies the interface or subinterface. This command puts the router in interface configuration mode. |
| **Step 2** | Router(config-if)# **rate-limit** {**input** \| **output**} [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* | Specifies the rate policy for each particular class of traffic. See Configuring a Class-Based DCAR Policy, on page 49 for a description of the **rate-limit** command action keywords. Repeat this command for each different class of traffic. |
| **Step 3** | Router(config-if)# **random-detect precedence** *precedence min-threshold max-threshold mark-prob-denominator* | Configures WRED and specifies parameters for packets with specific IP Precedence. |
| **Step 4** | Do one of the following:<br>• Router(config-if)# **access-list** *acl-index* {**deny** \| **permit**} *source*[*source-wildcard*]<br>• Router(config-if)# **access-list** *acl-index* {**deny** \| **permit**} *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*] [**tos** *tos*] [**log**] | (Optional) Specifies a standard or extended access list. Repeat this command to further configure the access list or specify a new access list. |

# Monitoring CAR and DCAR

| Command | Purpose |
|---|---|
| `Router#` **show access-lists** | Displays the contents of current IP and rate-limited access lists. |
| `Router#` **show access-lists rate-limit** [*access-list-number*] | Displays information about rate-limited access lists. |
| `Router#` **show interfaces** [*interface-type interface-number*] **rate-limit** | Displays information about an interface configured for CAR. |

# CAR and DCAR Configuration Examples

## Example Subrate IP Services

The following example illustrates how to configure a basic CAR policy that allows all IP traffic. In the example, the network operator delivers a physical T3 link to the customer, but offers a less expensive 15 Mbps subrate service. The customer pays only for the subrate bandwidth, which can be upgraded with additional access bandwidth based on demand. The CAR policy limits the traffic rate available to the customer and delivered to the network to the agreed upon rate limit, plus the ability to temporarily burst over the limit.

```
interface hssi 0/0/0
rate-limit output 15000000 2812500 5625000 conform-action transmit exceed-action drop
ip address 10.1.0.9 255.255.255.0
```

## Example Input and Output Rate Limiting on an Interface

In this example, a customer is connected to an Internet service provider (ISP) by a T3 link. The ISP wants to rate limit transmissions from the customer to 15 Mbps of the 45 Mbps. In addition, the customer is allowed to send bursts of 2,812,500 bytes. All packets exceeding this limit are dropped. The following commands are configured on the High-Speed Serial Interface (HSSI) of the ISP connected to the customer:

```
interface Hssi0/0/0
 description 45Mbps to R1
 rate-limit input 15000000 2812500 2812500 conform-action transmit exceed-action drop
 ip address 200.200.14.250 255.255.255.252
 rate-limit output 15000000 2812500 2812500 conform-action transmit exceed-action drop
```

The following sample output shows how to verify the configuration and monitor CAR statistics using the **show interfaces rate-limit** command:

```
Router# show interfaces hssi 0/0/0 rate-limit
Hssi0/0/0 45Mbps to R1
 Input
  matches: all traffic
   params: 15000000 bps, 2812500 limit, 2812500 extended limit
   conformed 8 packets, 428 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 8680ms ago, current burst: 0 bytes
   last cleared 00:03:59 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 15000000 bps, 2812500 limit, 2812500 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 8680ms ago, current burst: 0 bytes
   last cleared 00:03:59 ago, conformed 0 bps, exceeded 0 bps
```

## Example Rate Limiting in an IXP

The following example uses rate limiting to control traffic in an Internet Exchange Point (IXP). Because an IXP comprises many neighbors around an FDDI ring, MAC address rate-limited access lists are used to control traffic from a particular ISP. Traffic from one ISP (at MAC address 00e0.34b0.7777) is compared to a rate

limit of 80 Mbps of the 100 Mbps available on the FDDI connection. Traffic that conforms to this rate is sent. Nonconforming traffic is dropped.

```
interface Fddi2/1/0
 rate-limit input access-group rate-limit 100 80000000 15000000 30000000 conform-action
transmit exceed-action drop
 ip address 200.200.6.1 255.255.255.0
!
access-list rate-limit 100 00e0.34b0.7777
```

The following sample output shows how to verify the configuration and monitor the CAR statistics using the **show interfaces rate-limit** command:

```
Router# show interfaces fddi2/1/0 rate-limit
Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 15000000 limit, 30000000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
```

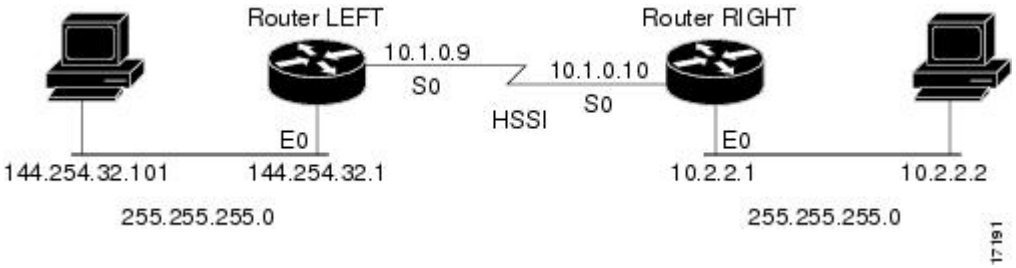
# Example Rate Limiting by Access List

The following example shows how CAR can be used to limit the rate by application to ensure capacity for other traffic including mission-critical applications:

- All World Wide Web traffic is sent. However, the IP precedence for Web traffic that conforms to the first rate policy is set to 5. For nonconforming Web traffic, the IP precedence is set to 0 (best effort).
- File Transfer Protocol (FTP) traffic is sent with an IP precedence of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped.
- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 15,000 bytes and an Excess Burst size of 30,000 bytes. Traffic that conforms is sent with an IP precedence of 5. Traffic that does not conform is dropped.

The figure below illustrates the configuration. Notice that two access lists are created to classify the Web and FTP traffic so that they can be handled separately by CAR.

***Figure 1: Rate Limiting by Access List***




### Router LEFT Configuration

```
interface Hssi0/0/0
description 45Mbps to R2
rate-limit output access-group 101 20000000 3750000 7500000 conform-action set-prec-
```

```
transmit 5 exceed-action set-prec-transmit 0
rate-limit output access-group 102 10000000 1875000 3750000 conform-action
set-prec-transmit 5 exceed-action drop
rate-limit output 8000000 1500000 3000000 conform-action set-prec-transmit 5
exceed-action drop
ip address 10.1.0.9 255.255.255.0
!
access-list 101 permit tcp any any eq www
access-list 102 permit tcp any any eq ftp
```

The following sample output shows how to verify the configuration and monitor CAR statistics using the **show interfaces rate-limit** command:

```
Router# show interfaces hssi 0/0/0 rate-limit
Hssi0/0/0 45Mbps to R2
 Input
  matches: access-group 101
   params: 20000000 bps, 3750000 limit, 7500000 extended limit
   conformed 3 packets, 189 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 309100ms ago, current burst: 0 bytes
   last cleared 00:08:00 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 102
   params: 10000000 bps, 1875000 limit, 3750000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 19522612ms ago, current burst: 0 bytes
   last cleared 00:07:18 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 8000000 bps, 1500000 limit, 3000000 extended limit
   conformed 5 packets, 315 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: drop
   last packet: 9632ms ago, current burst: 0 bytes
   last cleared 00:05:43 ago, conformed 0 bps, exceeded 0 bps
```

CHAPTER 6

# 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

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 at the end of this module.

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

•
•
•
•

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

## 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.
  - 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.

# 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.

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 16: set Commands and Corresponding Traffic Attribute, Network Layer, and Protocol***

| set Commands[1] | Traffic Attribute | Network Layer | Protocol |
|---|---|---|---|
| | | | |
| **set cos** | Layer 2 CoS value of the outgoing traffic | Layer 2 | |

| set Commands[1] | Traffic Attribute | Network Layer | Protocol |
|---|---|---|---|
| **set discard-class** | discard-class value | Layer 2 | |
| **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 | |
| **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 |
| **set mpls experimental topmost** | MPLS EXP field value in the topmost label on either an input or an output interface | Layer 3 | MPLS |
| **set precedence** | Precedence value in the packet header | Layer 3 | IP |
| **set qos-group** | QoS group ID | Layer 3 | IP, MPLS |

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

## Method Two Using a Table Map

You can create a table map that can be used to mark traffic attributes. A table map is a kind of two-way conversion chart that lists and maps one traffic attribute to another. A table map supports a many-to-one type of conversion and mapping scheme. The table map establishes a to-from relationship for the traffic attributes and defines the change to be made to the attribute. That is, an attribute is set *to* one value that is taken *from* another value. The values are based on the specific attribute being changed. For instance, the Precedence attribute can be a number from 0 to 7, while the DSCP attribute can be a number from 0 to 63.

The following is a sample table map configuration:

```
table-map table-map1
map from 0 to 1
map from 2 to 3
exit
```

The table below lists the traffic attributes for which a to-from relationship can be established using the table map.

*Table 17: Traffic Attributes for Which a To-From Relationship Can Be Established*

| The "To" Attribute | The "From" Attribute |
|---|---|
| Precedence | CoS |
| | QoS group |
| DSCP | CoS |
| | QoS group |
| CoS | Precedence |
| | DSCP |
| QoS group | Precedence |
| | DSCP |
| | MPLS EXP topmost |
| MPLS EXP topmost | QoS group |
| MPLS EXP imposition | Precedence |
| | DSCP |

Once the table map is created, you configure a policy map to use the table map. In the policy map, you specify the table map name and the attributes to be mapped by using the **table** keyword and the *table-map-name* argument with one of the commands listed in the table below.

*Table 18: Commands Used in Policy Maps to Map Attributes*

| Command Used in Policy Maps | Maps These Attributes |
|---|---|
| **set cos dscp table** *table-map-name* | CoS to DSCP |
| **set cos precedence table** *table-map-name* | CoS to Precedence |
| **set dscp cos table** *table-map-name* | DSCP to CoS |
| **set dscp qos-group table** *table-map-name* | DSCP to qos-group |
| **set mpls experimental imposition dscp table** *table-map-name* | MPLS EXP imposition to DSCP |
| **set mpls experimental imposition precedence table** *table-map-name* | MPLS EXP imposition to precedence |

| Command Used in Policy Maps | Maps These Attributes |
|---|---|
| **set mpls experimental topmost qos-group table** *table-map-name* | MPLS EXP topmost to QoS-group |
| **set precedence cos table** *table-map-name* | Precedence to CoS |
| **set precedence qos-group table** *table-map-name* | Precedence to QoS-group |
| **set qos-group dscp table** *table-map-name* | QoS-group to DSCP |
| **set qos-group mpls exp topmost table** *table-map-name* | QoS-group to MPLS EXP topmost |
| **set qos-group precedence table** *table-map-name* | QoS-group to Precedence |

The following is an example of a policy map (policy2) configured to use the table map (table-map1) created earlier:

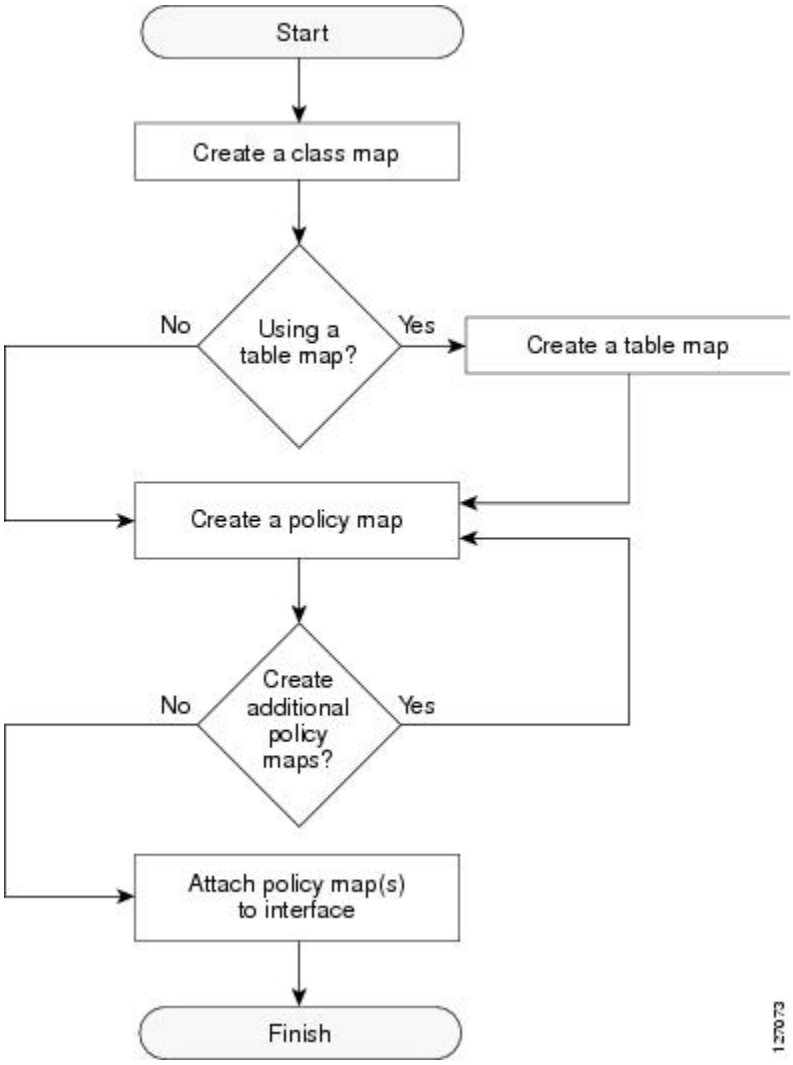
```
policy map policy2
class class-default
set cos dscp table table-map1
exit
```

In this example, a mapping relationship was created between the CoS attribute and the DSCP attribute as defined in the table map.

## Traffic Marking Procedure Flowchart

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

***Figure 2: Traffic Marking Procedure Flowchart***




# Method for Marking Traffic Attributes

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

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

## Using a set Command

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

***Table 19: set Commands and Corresponding Traffic Attribute, Network Layer, and Protocol***

| set Commands[2] | Traffic Attribute | Network Layer | Protocol |
|---|---|---|---|
| **set cos** | Layer 2 CoS value of the outgoing traffic | Layer 2 | 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 |
| **set mpls experimental topmost** | MPLS EXP field value in the topmost label on an input or output interface | Layer 3 | MPLS |
| **set precedence** | Precedence value in the packet header | Layer 3 | IP |
| **set qos-group** | QoS group ID | Layer 3 | IP, MPLS |

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

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

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

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

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

# MQC and Network Traffic Marking

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

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

- Specify the matching criteria used to define a traffic class.
- Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.
- Apply the policy actions specified in the policy map to an interface, 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 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 20: Traffic Classification Compared with Traffic Marking***

| Feature | Traffic Classification | Traffic Marking |
|---|---|---|
| Goal | Groups network traffic into specific traffic classes on the basis of whether the traffic matches the user-defined criterion. | After the network traffic is grouped into traffic classes, modifies the attributes for the traffic in a particular traffic class. |
| Configuration Mechanism | Uses class maps and policy maps in the MQC. | Uses class maps and policy maps in the MQC. |
| CLI | In a class map, uses **match** commands (for example, **match cos**) to define the traffic matching criteria. | Uses the traffic classes and matching criteria specified by traffic classification.<br>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 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**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** *class-map-name* [**match-all** \| **match-any**]<br><br>**Example:**<br>`Device(config)# class-map class1` | Creates a class map to be used for matching traffic to a specified class and enters class-map configuration mode. |
| **Step 4** | **match protocol** *protocol-name*<br><br>**Example:**<br>`Device(config-cmap)# match protocol ftp` | (Optional) Configures the match criterion for a class map on the basis of the specified protocol.<br>**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 release. See the command documentation for a complete list of **match** commands. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **end**<br><br>**Example:**<br>`Device(config-cmap)# end` | (Optional) Returns to privileged EXEC mode. |

# Creating a Table Map for Marking Network Traffic

**Note** If you are not using a table map, skip this procedure and advance to the "Creating a Policy Map for Applying a QoS Feature to Network Traffic".

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **table-map** *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-action-or-value*]
4. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **table-map** *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-action-or-value*]<br><br>**Example:** | Creates a table map using the specified name and enters tablemap configuration mode.<br>• Enter the name of the table map you want to create.<br>• Enter each value mapping on a separate line. Enter as many separate lines as needed for the values you want to map. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# table-map table-map1 map from 2 to 1` | • The **default** keyword and *default-action-or-value* argument set the default value (or action) to be used if a value is not explicitly designated. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-tablemap)#`<br>`end` | (Optional) Exits tablemap configuration mode and returns to privileged EXEC mode. |

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

### Before You Begin

The following restrictions apply to creating a QoS policy map:

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

## 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br>**Example:**<br>`Device(config)# policy-map policy1` | Specifies the name of the policy map and enters policy-map configuration mode. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br>**Example:**<br>`Device(config-pmap)# class class1` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. |
| **Step 5** | **set cos** *cos-value*<br>**Example:**<br>`Device(config-pmap-c)# set cos 2` | (Optional) Sets the CoS value in the type of service (ToS) byte.<br>**Note** The **set cos** command is an example of one of the **set** commands that can be used when marking traffic. Other **set** commands can be used. For a list of other **set** commands, see "Information About Marking Network Traffic". |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-pmap-c)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show policy-map**<br>**Example:**<br>`Device# show policy-map` | (Optional) Displays all configured policy maps. |
| **Step 8** | **show policy-map** *policy-map* **class** *class-name*<br>**Example:**<br>`Device# show policy-map policy1 class class1` | (Optional) Displays the configuration for the specified class of the specified policy map. |

## What to Do Next

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

# Attaching the Policy Map to an Interface

**Note**

### 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*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br><br>**Example:**<br>`Device(config)# interface serial4/0/0` | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **pvc** [*name*] *vpi*/*vci* [**ilmi** \| **qsaal** \| **smds** \| **l2transport**]<br><br>**Example:**<br><br>`Device(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.<br><br>**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**<br><br>**Example:**<br><br>`Device(config-atm-vc)# exit` | (Optional) Returns to interface configuration mode.<br><br>**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*<br><br>**Example:**<br><br>`Device(config-if)# service-policy input policy1` | Attaches a policy map to an input or output interface.<br><br>**Note** Policy maps can be configured on ingress or egress devices. They can also be attached in the input or output direction of an interface. The direction (input or output) and the device (ingress or egress) to which the policy map should be attached vary according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the device and the interface direction that are appropriate for your network configuration. |
| **Step 7** | **end**<br><br>**Example:**<br><br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show policy-map interface** *type number*<br><br>**Example:**<br><br>`Device# 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. |

# 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. Ttraffic with a protocol type of FTP will be put in this class.

```
Device> enable
Device# configure terminal
```

```
Device(config)# class-map class1
Device(config-cmap)# match protocol ftp
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. In this example, a policy map called policy1 has been created, and the **bandwidth** command has been configured for class1. The **bandwidth** command configures the QoS feature CBWFQ.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router#
show policy-map policy1 class class1
Router# exit
```

**Note** This example uses the **bandwidth** command. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.

## 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 to the serial interface 4/0/0.

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

# Additional References for Marking Network Traffic

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco commands | Cisco IOS Master Commands List, All Releases |
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS Quality of Service Solutions Command Reference* |
| MQC | "Applying QoS Features Using the MQC" module |

| Related Topic | Document Title |
|---|---|
| Classifying network traffic | "Classifying Network Traffic" module |

### Technical Assistance

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

# Feature Information for Marking Network Traffic

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

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

***Table 21: Feature Information for Marking Network Traffic***

| Feature Name | Software Releases | Feature Configuration Information |
|---|---|---|
| Class-Based Marking | 12.2(2)T<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 2.2<br>Cisco IOS XE Release 3.2SE | The Class-Based Packet Marking feature provides a user-friendly command-line interface (CLI) for efficient packet marking by which users can differentiate packets.<br>This feature was implemented on Cisco ASR 1000 Series Routers.<br>This feature was integrated into Cisco IOS XE Release 2.2. |

| Feature Name | Software Releases | Feature Configuration Information |
|---|---|---|
| Enhanced Packet Marking | 12.2(13)T | The Enhanced Packet Marking feature allows you to map and convert the marking of a packet from one value to another by using a kind of conversion chart called a table map. The table map establishes an equivalency from one value to another. For example, the table map can map and convert the class of service (CoS) value of a packet to the precedence value of the packet. This value mapping can be propagated for use on the network, as needed. |
| QoS Packet Marking | 12.2(8)T<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 2.2<br>Cisco IOS XE Release 3.5S | The QoS Packet Marking feature allows you to mark packets by setting the IP precedence bit or the IP differentiated services code point (DSCP) in the Type of Service (ToS) byte, and to associate a local QoS group value with a packet.<br>This feature was implemented on Cisco ASR 1000 Series Routers.<br>This feature was integrated into Cisco IOS XE Software Release 2.2.<br>In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. |
| IP DSCP marking for Frame-Relay PVC | 12.2(15)T<br>Cisco IOS XE Release 2.1 | This feature was implemented on Cisco ASR 1000 Series Routers. |
| PXF Based Frame Relay DE Bit Marking | 12.2(31)SB2<br>15.0(1)S | PXF Based Frame Relay DE Bit Marking was integrated into the Cisco IOS Release 15.0(1)S release. |

CHAPTER 7

# Classifying Network Traffic

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying 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 classifying network traffic.



# 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 at the end of this module.

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 Classifying Network Traffic

## Purpose of Classifying Network Traffic

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling other QoS features such as traffic shaping and traffic policing on your network.

The goal of network traffic classification is to group traffic based on user-defined criteria so that the resulting groups of network traffic can then be subjected to specific QoS treatments. The QoS treatments might include faster forwarding by intermediate routers and switches or reduced probability of the traffic being dropped due to lack of buffering resources.

Identifying and categorizing network traffic into traffic classes (that is, classifying packets) enables distinct handling for different types of traffic, effectively separating network traffic into different categories. This classification can be associated with a variety of match criteria such as the IP Precedence value, differentiated services code point (DSCP) value, class of service (CoS) value, source and destination MAC addresses, input interface, or protocol type. You classify network traffic by using class maps and policy maps with the Modular Quality of Service Command-Line Interface (MQC). For example, you can configure class maps and policy maps to classify network traffic on the basis of the QoS group, Frame Relay DLCI number, Layer 3 packet length, or other criteria that you specify.

# Benefits of Classifying Network Traffic

Classifying network traffic allows you to see what kinds of traffic you have, organize the various kinds of network traffic into traffic classes, and treat some types of traffic differently than others. Identifying and organizing network traffic is the foundation for applying the appropriate QoS feature to that traffic, enabling you to allocate network resources to deliver optimal performance for different types of traffic. For example, high-priority network traffic or traffic matching specific criteria can be singled out for special handling, and thus, help to achieve peak application performance.

# MQC and Network Traffic Classification

To configure network traffic classification, you use the Modular Quality of Service Command-Line Interface (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 permanent virtual circuit (PVC) by using the **service-policy** command.

# Network Traffic Classification match Commands and Match Criteria

Network traffic classification allows you to group or categorize traffic on the basis of whether the traffic meets one or more specific criteria. For example, network traffic with a specific IP precedence can be placed into one traffic class, while traffic with a specific DSCP value can be placed into another traffic class. The network traffic within that traffic class can be given the appropriate QoS treatment, which you can configure in a policy map later.

You specify the criteria used to classify traffic with a **match** command. The table below lists the available **match** commands and the corresponding match criterion.

*Table 22: match Commands and Corresponding Match Criterion*

| match Commands[3] | Match Criterion |
|---|---|
| **match access group** | Access control list (ACL) number |
| **match any** | Any match criteria |
| **match atm clp** | ATM cell loss priority (CLP) |
| **match class-map** | Traffic class name |
| **match cos** | Layer 2 class of service (CoS) value |
| **match destination-address mac** | MAC address |
| **match discard-class** | Discard class value |
| **match dscp** | DSCP value |
| **match field** | Fields defined in the protocol header description files (PHDFs) |
| **match fr-de** | Frame Relay discard eligibility (DE) bit setting |
| **match fr-dlci** | Frame Relay data-link connection identifier (DLCI) number |
| **match input-interface** | Input interface name |
| **match ip rtp** | Real-Time Transport Protocol (RTP) port |
| **match mpls experimental** | Multiprotocol Label Switching (MPLS) experimental (EXP) value |
| **match mpls experimental topmost** | MPLS EXP value in the topmost label |
| **match not** | Single match criterion value to use as an unsuccessful match criterion |
| **match packet length (class-map)** | Layer 3 packet length in the IP header |
| **match port-type** | Port type |
| **match precedence** | IP precedence values |
| **match protocol** | Protocol type |
| **match protocol (NBAR)** | Protocol type known to network-based application recognition (NBAR) |

| match Commands[3] | Match Criterion |
|---|---|
| **match protocol citrix** | Citrix protocol |
| **match protocol fasttrack** | FastTrack peer-to-peer traffic |
| **match protocol gnutella** | Gnutella peer-to-peer traffic |
| **match protocol http** | Hypertext Transfer Protocol |
| **match protocol rtp** | RTP traffic |
| **match qos-group** | QoS group value |
| **match source-address mac** | Source Media Access Control (MAC) address |
| **match start** | Datagram header (Layer 2) or the network header (Layer 3) |
| **match tag (class-map)** | Tag type of class map |
| **match vlan (QoS)** | Layer 2 virtual local-area network (VLAN) identification number |

3 Cisco match commands can vary by release and platform. For more information, see the command documentation for the Cisco release and platform that you are using.

# 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 23: Traffic Classification Compared with Traffic Marking*

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

# How to Classify Network Traffic

## Creating a Class Map for Classifying Network Traffic

**Note** In the following task, the **matchfr-dlci**command is shown in Step 4. The **matchfr-dlci**command matches traffic on the basis of the Frame Relay DLCI number. The **matchfr-dlci**command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see the Network Traffic Classification match Commands and Match Criteria section.

### SUMMARY STEPS

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

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** *class-map-name* [**match-all**\| **match-any**]<br>**Example:**<br>`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.<br>• Enter the class map name. |
| **Step 4** | **match fr-dlci** *dlci-number*<br>**Example:**<br>`Router(config-cmap)# match fr-dlci 500` | (Optional) Specifies the match criteria in a class map.<br>**Note** The **matchfr-dlci** command classifies traffic on the basis of the Frame Relay DLCI number. The **matchfr-dlci**command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see the Network Traffic Classification match Commands and Match Criteria section. |
| **Step 5** | **end**<br>**Example:**<br>`Router(config-cmap)# end` | (Optional) Returns to privileged EXEC mode. |

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

**Note** In the following task, the **bandwidth** command is shown at Creating a Policy Map for Applying a QoS Feature to Network Traffic. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature you want to use.

**Note** Configuring bandwidth on policies that have the class-default class is supported on physical interfaces such as Gigabit Ethernet (GigE), Serial, Mobile Location Protocol (MLP), and Multilink Frame-Relay (MFR).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*}
6. **end**
7. **show policy-map**
8. 
9. **show policy-map** *policy-map* **class** *class-name*
10. Router# show policy-map
11. 
12. Router# show policy-map policy1 class class1
13. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br><br>**Example:**<br><br>`Router(config)# policy-map policy1` | Specifies the name of the policy map to be created and enters policy-map configuration mode.<br><br>• Enter the policy map name. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br><br>`Router(config-pmap)# class class1` | Specifies the name of the class and enters policy-map class configuration mode. This class is associated with the class map created earlier.<br><br>• Enter the name of the class or enter the **class-default**keyword. |
| **Step 5** | **bandwidth** {*bandwidth-kbps*\| **remaining percent** *percentage*\| **percent** *percentage*} | (Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config-pmap-c)# bandwidth percent 50` | • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth.<br>**Note** The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use. |
| **Step 6** | **end**<br>**Example:**<br>`Router(config-pmap-c)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show policy-map** | (Optional) Displays all configured policy maps. |
| **Step 8** | | or |
| **Step 9** | **show policy-map** *policy-map* **class** *class-name*<br>**Example:** | (Optional) Displays the configuration for the specified class of the specified policy map.<br>• Enter the policy map name and the class name. |
| **Step 10** | Router# show policy-map | |
| **Step 11** | | |
| **Step 12** | Router# show policy-map policy1 class class1 | |
| **Step 13** | **exit**<br>**Example:**<br>`Router# exit` | (Optional) Exits privileged EXEC mode. |

## 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 PVC.

**Note** A policy with the command **match fr-dlic** can only be attached to a Frame Relay main interface with point-to-point connections.

## 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number* [**name-tag**]<br><br>**Example:**<br>`Router(config)# interface serial4/0/0` | Configures an interface type and enters interface configuration mode.<br>• Enter the interface type and number. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **pvc** [*name*] *vpi*/*vci* [**ilmi**\|**qsaal**\|**smds**\|**l2transport**]<br><br>**Example:**<br><br>`Router(config-if)# pvc cisco 0/16` | (Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode.<br><br>• Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier.<br><br>**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 Attaching the Policy Map to an Interface. |
| **Step 5** | **exit**<br><br>**Example:**<br><br>`Router(config-atm-vc)# exit` | (Optional) Returns to interface configuration mode.<br><br>**Note** This step is required only if you are attaching the policy map to an ATM PVC and you completed Attaching the Policy Map to an Interface. If you are not attaching the policy map to an ATM PVC, advance to Attaching the Policy Map to an Interface. |
| **Step 6** | **service-policy** {**input** \| **output**}*policy-map-name*<br><br>**Example:**<br><br>`Router(config-if)# service-policy input policy1` | Attaches a policy map to an input or output interface.<br><br>• Enter the policy map name.<br><br>**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**<br><br>**Example:**<br><br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show policy-map interface** *type number*<br><br>**Example:**<br><br>`Router# show policy-map interface serial4/0/0` | (Optional) Displays the traffic statistics of all traffic classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.<br><br>• Enter the type and number. |
| **Step 9** | **exit**<br><br>**Example:**<br><br>`Router# exit` | (Optional) Exits privileged EXEC mode. |

# Configuration Examples for Classifying Network Traffic

## Example Creating a Class Map for Classifying Network Traffic

The following is an example of creating a class map to be used for traffic classification. In this example, a traffic class called class1 has been created. Traffic with a Frame Relay DLCI value of 500 will be put in this traffic class.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
Router(config-cmap)# end
```

**Note** This example uses the **matchfr-dlci** command. The **matchfr-dlci** command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see Network Traffic Classification match Commands and Match Criteria.

A policy with match fr-dlic can only be attached to a Frame Relay main interface with point-to-point connections.

## 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. In this example, a policy map called policy1 has been created, and the **bandwidth** command has been configured for class1. The **bandwidth** command configures the QoS feature CBWFQ.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router#
show policy-map policy1 class class1
Router# exit
```

**Note** This example uses the **bandwidth** command. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.

# Example Attaching the Policy Map to an Interface

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

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
Router#
show policy-map interface serial4/0/0
Router# 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 |
| Marking network traffic | "Marking Network Traffic" module |
| IPsec and VPNs | "Configuring Security for VPNs with IPsec" module |
| NBAR | "Classifying Network Traffic Using NBAR" module |
| IPv6 QoS | “IPv6 Quality of Service” module |
| IPv6 MQC Packet Classification | “IPv6 QoS: MQC Packet Classification” 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:<br>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 Classifying 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 24: Feature Information for Classifying Network Traffic*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Packet Classification Using Frame Relay DLCI Number | 12.2(13)T<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 3.12 | The Packet Classification Using the Frame Relay DLCI Number feature allows customers to match and classify traffic based on the Frame Relay data-link connection identifier (DLCI) number associated with a packet. This new match criteria is in addition to the other match criteria, such as the IP Precedence, differentiated services code point (DSCP) value, class of service (CoS), currently available.<br>The following commands were added or modified:**matchfr-dlci** |
| QoS: Local Traffic Matching Through MQC | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| QoS: Match ATM CLP | Cisco IOS XE Release 2.3 | The QoS: Match ATM CLP features allows you to classify traffic on the basis of the ATM cell loss priority (CLP) value.<br>The following command was introduced or modified: **matchatm-clp**. |
| QoS: MPLS EXP Bit Traffic Classification | Cisco IOS XE Release 2.3 | The QoS: MPLS EXP Bit Traffic Classification feature allows you to classify traffic on the basis of the Multiprotocol Label Switching (MPLS) experimental (EXP) value.<br>The following command was introduced or modified: **matchmplsexperimental**. |

CHAPTER 8

# QoS Tunnel Marking for GRE Tunnels

The QoS Tunnel Marking for GRE Tunnels feature introduces the capability to define and control the quality of service (QoS) for both incoming and outgoing customer traffic on the provider edge (PE) router in a service provider network.



## 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 at the end of this module.

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 QoS Tunnel Marking for GRE Tunnels

- You must determine the topology and interfaces that need to be configured to mark incoming and outgoing traffic.

# Restrictions for QoS Tunnel Marking for GRE Tunnels

- GRE tunnel marking is not supported on the following paths:
  - IPsec tunnels
  - Multiprotocol Label Switching over generic routing encapsulation (MPLSoGRE)
  - Layer 2 Tunneling Protocol (L2TP)

# Information About QoS Tunnel Marking for GRE Tunnels

## GRE Definition

Generic routing encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

## GRE Tunnel Marking Overview

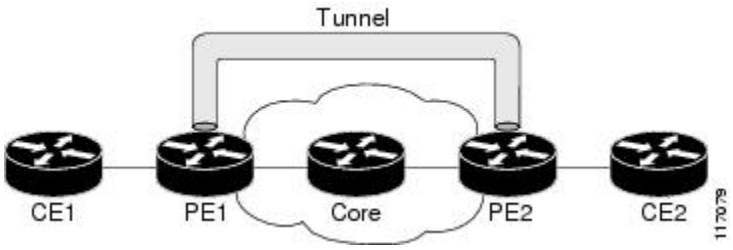
The QoS Tunnel Marking for GRE Tunnels feature allows you to define and control QoS for incoming and outgoing customer traffic on the PE router in a service provider (SP) network. This feature lets you set (mark) either the IP precedence value or the differentiated services code point (DSCP) value in the header of an GRE tunneled packet. GRE tunnel marking can be implemented by a QoS marking command, such as **set ip** {**dscp** | **precedence**} [**tunnel**], and it can also be implemented in QoS traffic policing. This feature reduces administrative overhead previously required to control customer bandwidth by allowing you to mark the GRE tunnel header on the tunnel interface on the PE routers.

**Note** The **set ip** {**dscp** | **precedence**} [**tunnel**] command is equivalent to the **set** {**dscp** | **precedence**} [**tunnel**] command.

The figure below shows traffic being received from the CE1 router through the incoming interface on the PE1 router on which tunnel marking occurs. The traffic is encapsulated (tunneled), and the tunnel header is marked on the PE1 router. The marked packets travel (tunnel) through the core and are decapsulated automatically on the exit interface of the PE2 router. This feature is designed to simplify classifying customer edge (CE)

traffic and is configured only in the service provider network. This process is transparent to the customer sites. The CE1 and CE2 routers exist as a single network.

***Figure 3: Tunnel Marking***




# GRE Tunnel Marking and the MQC

Before you can configure tunnel marking for GRE tunnels, you must first configure a class map and a policy map and then attach that policy map to the appropriate interface. These three tasks can be accomplished by using the MQC.

For information on using the MQC, see the "Applying QoS Features Using the MQC" module.

# GRE Tunnel Marking and DSCP or IP Precedence Values

GRE tunnel marking is configured with the **set ip precedence tunnel** or **set ip dscp tunnel** command on PE routers that carry incoming traffic from customer sites. GRE tunnel marking allows you to mark the header of a GRE tunnel by setting a DSCP value from 0 to 63 or an IP precedence value from 0 to 7 to control GRE tunnel traffic bandwidth and priority.

GRE traffic can also be marked under traffic policing with the **set-dscp-tunnel-transmit** and the **set-prec-tunnel-transmit** actions (or keywords) of the **police** command. The tunnel marking value is from 0 to 63 for the **set-dscp-tunnel-transmit** actions and from 0 to 7 for the **set-prec-tunnel-transmit** command. Under traffic policing, tunnel marking can be applied with conform, exceed, and violate action statements, allowing you to automatically apply a different value for traffic that does not conform to the expected traffic rate.

After the tunnel header is marked, GRE traffic is carried through the tunnel and across the service provider network. This traffic is decapsulated on the interface of the PE router that carries the outgoing traffic to the other customer site. The configuration of GRE tunnel marking is transparent to customer sites. All internal configuration is preserved.

There is a different between the **set ip precedence** and **set ip dscp** commands and the **set ip precedence tunnel** and **set ip dscp tunnel** commands:

- The **set ip precedence** and **set ip dscp** commands are used to set the IP precedence value or DSCP value in the header of an IP packet.
- The **set ip precedence tunnel** and **set ip dscp tunnel** commands are used to set (mark) the IP precedence value or DSCP value in the tunnel header that encapsulates the GRE traffic.
- The **set ip precedence tunnel** and **set ip dscp tunnel** commands have no effect on egress traffic that is not encapsulated in a GRE tunnel.

# Benefits of GRE Tunnel Marking

GRE tunnel marking provides a simple mechanism to control the bandwidth of customer GRE traffic. The QoS Tunnel Marking for GRE Tunnels feature is configured entirely within the service provider network and on interfaces that carry incoming and outgoing traffic on the PE routers.

## GRE Tunnel Marking and Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS). If you use traffic policing in your network, you can also implement the GRE tunnel marking feature with the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** action (or keyword) of the **police** command in policy-map class configuration mode. Under traffic policing, tunnel marking can be applied with conform, exceed, and violate action statements, allowing you to apply a different value automatically for traffic that does not conform to the expected traffic rate.

## GRE Tunnel Marking Values

The range of the tunnel marking values for the **set ip dscp tunnel** and **set-dscp-tunnel-transmit** commands is from 0 to 63, and the range of values for the **set ip precedence tunnel** and **set-prec-tunnel-transmit** commands is from 0 to 7.

# How to Configure Tunnel Marking for GRE Tunnels

# Configuring a Class Map

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match ip precedence** *precedence-value*
5. **exit**
6. **class-map** [**match-all** | **match-any**] *class-map-name*
7. **match ip dscp** *dscp-value*
8. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** [**match-all** \| **match-any**] *class-map-name*<br>**Example:**<br>`Router(config)# class-map match-any MATCH_PREC` | Specifies the name of the class map to be created and enters QoS class map configuration mode.<br>• The class map defines the criteria to use to differentiate the traffic. For example, you can use the class map to differentiate voice traffic from data traffic, based on a series of match criteria defined using the **match** command.<br>**Note** If the **match-all** or **match-any** keyword is not specified, traffic must match all the match criteria to be classified as part of the traffic class. |
| **Step 4** | **match ip precedence** *precedence-value*<br>**Example:**<br>`Router(config-cmap)# match ip precedence 0` | Enables packet matching on the basis of the IP precedence values you specify.<br>**Note** You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. |
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-cmap)# exit` | Returns to global configuration mode. |
| **Step 6** | **class-map** [**match-all** \| **match-any**] *class-map-name*<br>**Example:**<br>`Router(config)# class-map match-any MATCH_DSCP` | Specifies the name of the class map to be created and enters QoS class map configuration mode. |
| **Step 7** | **match ip dscp** *dscp-value*<br>**Example:**<br>`Router(config-cmap)# match ip dscp 0` | Enables packet matching on the basis of the DSCP values you specify.<br>• This command is used by the class map to identify a specific DSCP value marking on a packet.<br>• The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **end**<br><br>**Example:**<br>`Router(config-cmap)# end` | (Optional) Returns to privileged EXEC mode. |

# Creating a Policy Map

Perform this task to create a tunnel marking policy marp and apply the map to a specific interface.

## SUMMARY STEPS

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

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map** *policy-map-name*<br><br>**Example:**<br>`Router(config)# policy-map TUNNEL_MARKING` | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters QoS policy-map configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br><br>`Router(config-pmap)# class MATCH_PREC` | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.<br><br>• Enters policy-map class configuration mode. |
| **Step 5** | **set ip precedence tunnel** *precedence-value*<br><br>**Example:**<br><br>`Router(config-pmap-c)# set ip precedence tunnel 3` | Sets the IP precedence value in the tunnel header of a GRE-tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 7 when IP precedence is configured. |
| **Step 6** | **exit**<br><br>**Example:**<br><br>`Router(config-pmap-c)# exit` | Returns to QoS policy-map configuration mode. |
| **Step 7** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br><br>`Router(config-pmap)# class MATCH_DSCP` | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.<br><br>• Enters policy-map class configuration mode. |
| **Step 8** | **set ip dscp tunnel** *dscp-value*<br><br>**Example:**<br><br>`Router(config-pmap-c)# set ip dscp tunnel 3` | Sets the differentiated services code point (DSCP) value in the tunnel header of a GRE-tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 63 when DSCP is configured. |
| **Step 9** | **end**<br><br>**Example:**<br><br>`Router(config-pmap-c)# end` | (Optional) Returns to privileged EXEC mode. |

# Attaching the Policy Map to an Interface or a VC

Policy maps can be attached to main interfaces, subinterfaces, or ATM permanent virtual circuits (PVCs). Policy maps are attached to interfaces by using the **service-policy** command and specifying either the **input** or **output** keyword to indicate the direction of the interface.

**Note** Tunnel marking policy can be applied on Ingress or Egress direction. A tunnel marking policy can be applied as an ingress policy on the ingress physical interface of a Service Provider Edge (SPE) router or as an egress policy on a tunnel interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service-policy** {**input** | **output**} *policy-map-name*
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br><br>`Router(config)# interface GigabitEthernet 0/0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **service-policy** {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Router(config-if)# service-policy input TUNNEL_MARKING` | Specifies the name of the policy map to be attached to the input or output direction of the interface.<br><br>• 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 vary according your network configuration. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Returns to privileged EXEC mode. |

# Verifying the Configuration of Tunnel Marking for GRE Tunnels

Use the **show** commands in this procedure to view the GRE tunnel marking configuration settings. The **show** commands are optional and can be entered in any order.

### SUMMARY STEPS

1. **enable**
2. **show policy-map interface** *interface-name*
3. **show policy-map** *policy-map*
4. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **show policy-map interface** *interface-name*<br><br>**Example:**<br><br>`Router# show policy-map interface GigabitEthernet0/0/1` | (Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface. |
| **Step 3** | **show policy-map** *policy-map*<br><br>**Example:**<br><br>`Router# show policy-map TUNNEL_MARKING` | (Optional) Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **Step 4** | **exit**<br><br>**Example:**<br><br>`Router# exit` | (Optional) Returns to user EXEC mode. |

## Troubleshooting Tips

If you find that the configuration is not functioning as expected, perform these operations to troubleshoot the configuration:

- Use the **show running-config** command and analyze the output of the command.
- If the policy map does not appear in the output of the **show running-config** command, enable the **logging console** command.
- Attach the policy map to the interface again.

# Configuration Examples for QoS Tunnel Marking for GRE Tunnels

## Example: Configuring Tunnel Marking for GRE Tunnels

The following is an example of a GRE tunnel marking configuration. In this example, a class map called "MATCH_PREC" has been configured to match traffic based on the DSCP value.

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_DSCP
Router(config-cmap)# match ip dscp 0
Router(config-cmap)# end
```

In the following part of the example configuration, a policy map called "TUNNEL_MARKING" has been created and the **set ip dscp tunnel** command has been configured in the policy map. You could use the **set ip precedence tunnel** command instead of the **set ip dscp tunnel** command if you do not use DSCP in your network.

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class MATCH_DSCP
Router(config-pmap-c)# set ip dscp tunnel 3
Router(config-pmap-c)# end
```

**Note** The following part of the example configuration is not required to configure this feature if you use the **set ip dscp tunnel** or **set ip precedence tunnel** commands to enable GRE tunnel marking. This example shows how GRE tunnel marking can be enabled under traffic policing.

In the following part of the example configuration, the policy map called "TUNNEL_MARKING" has been created and traffic policing has also been configured by using the **police** command and specifying the appropriate policing actions. The **set-dscp-tunnel-transmit** command can be used instead of the **set-prec-tunnel-transmit** command if you use DSCP in your network.

```
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action
 set-prec-tunnel-transmit 0
Router(config-pmap-c)# end
```

In the following part of the example configuration, the policy map is attached to GigabitEthernet interface 0/0/1 in the inbound (input) direction by specifying the **input** keyword of the **service-policy** command:

```
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# service-policy input TUNNEL_MARKING
Router(config-if)# end
```

In the final part of the example configuration, the policy map is attached to tunnel interface 0 in the outbound (output) direction using the **output** keyword of the **service-policy** command:

```
Router(config)# interface Tunnel 0
Router(config-if)# service-policy output TUNNEL_MARKING
Router(config-if)# end
```

# Example: Verifying the Tunnel Marking for GRE Tunnels Configuration

This section contains sample output from the **show policy-map interface** and the **show policy-map** commands. The output from these commands can be used to verify and monitor the feature configuration in your network.

The following is sample output from the **show policy-map interface** command. In this sample output:

- The character string “ip dscp tunnel 3” indicates that GRE tunnel marking has been configured to set the DSCP value in the header of a GRE-tunneled packet.
- The character string “ip precedence tunnel 3” indicates that GRE tunnel marking has been configured to set the precedence value in the header of a GRE-tunneled packet.

```
Router# show policy-map interface GigabitEthernet0/0/1
 Service-policy input: TUNNEL_MARKING

    Class-map: MATCH_PREC (match-any)
      22 packets, 7722 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      QoS Set
        ip precedence tunnel 3
          Marker statistics: Disabled

    Class-map: MATCH_DSCP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp default (0)
      QoS Set
        ip dscp tunnel 3
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      107 packets, 8658 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

The following is sample output from the **show policy-map** command. In this sample output, the character string “ip precedence tunnel 3” indicates that the GRE tunnel marking feature has been configured to set the IP precedence value in the header of an GRE-tunneled packet.

```
Router# show policy-map

Policy Map TUNNEL_MARKING
    Class MATCH_PREC
      set ip precedence tunnel 3
    Class MATCH_DSCP
      set ip dscp tunnel 3
```

# 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 |
| Tunnel marking for Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnels | "QoS: Tunnel Marking for L2TPv3 Tunnels" module |
| DSCP | "Overview of DiffServ for Quality of Service" module |

### Standards

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

### MIBs

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

### RFCs

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

### 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 QoS Tunnel Marking for GRE Tunnels

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 25: Feature Information for QoS Tunnel Marking for GRE Tunnels***

| Feature Name | Releases | Feature Information |
|---|---|---|
| QoS Tunnel Marking for GRE Tunnels | Cisco IOS XE Release 3.5S | The QoS Tunnel Marking for GRE Tunnels feature introduces the capability to define and control the QoS for incoming customer traffic on the PE router in a service provider network.<br><br>The following commands were introduced or modified: **match atm-clp**, **match cos**, **match fr-de**, **police**, **police (two rates)**, **set ip dscp tunnel**, **set ip precedence tunnel**, **show policy-map**, **show policy-map interface**. |

CHAPTER 9

# Class-Based Ethernet CoS Matching and Marking

The Class-Based Ethernet CoS Matching and Marking (801.1p and ISL CoS) feature allows you to mark and match packets using Class of Service (CoS) values.



## 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 at the end of this module.

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 Class-Based Ethernet CoS Matching and Marking

When configuring this feature, you must first create a policy map (sometimes referred to as a service policy or a traffic policy) using the Modular QoS Command-Line Interface (CLI) (MQC). Therefore, you should be familiar with the procedure for creating a policy map using the MQC.

For more information about creating a policy map (traffic policy) using the MQC, see the “Applying QoS Features Using the MQC” module.

# Information About Class-Based Ethernet CoS Matching and Marking

## Layer 2 CoS Values

Layer 2 (L2) Class of Service (CoS) values are relevant for IEEE 802.1Q and Interswitch Link (ISL) types of frames. The Class-based Ethernet CoS Matching and Marking feature extends Cisco software capabilities to match packets by looking at the CoS value of the packet and marking packets with user-defined CoS values. This feature can be used for L2 CoS to L3 Terms of Service (TOS) mapping. CoS matching and marking can be configured via the Cisco Modular QoS CLI framework.

# How to Configure Class-Based Ethernet CoS Matching and Marking

## Configuring Class-Based Ethernet CoS Matching

In the following task, classes named voice and video-and-data are created to classify traffic based on the CoS values. The classes are configured in the CoS-based-treatment policy map, and the service policy is attached to all packets leaving Gigabit Ethernet interface 1/0/1.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match cos** *cos-value*
5. **exit**
6. **class-map** *class-map-name*
7. **match cos** *cos-value*
8. **exit**
9. **policy-map** *policy-map-name*
10. **class** {*class-name* | **class-default**}
11. **priority level** *level*
12. **exit**
13. **class** {*class-name* | **class-default**}
14. **bandwidth remaining percent** *percentage*
15. **exit**
16. **exit**
17. **interface** *type number*
18. **service-policy** {**input**| **output**} *policy-map-name*
19. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map** *class-map-name*<br><br>**Example:**<br>`Device(config)# class-map voice` | Specifies the name of the class map to be created and enters class-map configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **match cos** *cos-value*<br><br>**Example:**<br>`Device(config-cmap)# match cos 7` | Configures the class map to match traffic on the basis of the CoS value. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Device(config-cmap)# exit` | (Optional) Exits class-map configuration mode. |
| **Step 6** | **class-map** *class-map-name*<br><br>**Example:**<br>`Device(config)# class-map video-and-data` | Specifies the name of the class map to be created and enters class-map configuration mode.<br>• Enter the class map name. |
| **Step 7** | **match cos** *cos-value*<br><br>**Example:**<br>`Device(config-cmap)# match cos 5` | Configures the class map to match traffic on the basis of the CoS value. |
| **Step 8** | **exit**<br><br>**Example:**<br>`Device(config-cmap)# exit` | (Optional) Exits class-map configuration mode. |
| **Step 9** | **policy-map** *policy-map-name*<br><br>**Example:**<br>`Device(config)# policy-map cos-based-treatment` | Specifies the name of the policy map created earlier and enters policy-map configuration mode. |
| **Step 10** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Device(config-pmap)# class voice` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. |
| **Step 11** | **priority level** *level*<br><br>**Example:**<br>`Device(config-pmap-c)# priority level 1` | Specifies the level of the priority service. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **exit**<br><br>**Example:**<br><br>`Device(config-pmap-c)# exit` | (Optional) Exits policy-map class configuration mode. |
| **Step 13** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br><br>`Device(config-pmap)# class video-and-data` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. |
| **Step 14** | **bandwidth remaining percent** *percentage*<br><br>**Example:**<br>`Device(config-pmap-c)# bandwidth remaining percent 20` | Specifies the amount of bandwidth assigned to the class. |
| **Step 15** | **exit**<br><br>**Example:**<br><br>`Device(config-pmap-c)# exit` | (Optional) Exits policy-map class configuration mode. |
| **Step 16** | **exit**<br><br>**Example:**<br><br>`Device(config-pmap)# exit` | (Optional) Exits policy-map configuration mode. |
| **Step 17** | **interface** *type number*<br><br>**Example:**<br><br>`Device(config)# interface gigabitethernet 1/0/1` | Configures an interface (or subinterface) type and enters interface configuration mode. |
| **Step 18** | **service-policy** {**input**\| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Device(config-if)# service-policy output cos-based-treatment` | Specifies the name of the policy map to be attached to either the input or output direction of the interface.<br><br>**Note** Policy maps can be configured on ingress or egress devices. They can also be attached in the input or output direction of an interface. The direction (input or output) and the device (ingress or egress) to which the policy map should be attached vary according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the device and the interface direction that are appropriate for your network configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **end**<br><br>**Example:**<br><br>`Device(config-if)# end` | (Optional) Exits interface configuration mode and returns to privileged EXEC mode. |

# Configuring Class-Based Ethernet CoS Marking

In the following task, the policy map called cos-set is created to assign different CoS values for different types of traffic.

**Note** This task assumes that the class maps called voice and video-and-data have already been created.

## 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. **exit**
7. **class** {*class-name* | **class-default**}
8. **set cos** *cos-value*
9. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **policy-map** *policy-map-name*<br><br>**Example:**<br>`Device(config)# policy-map cos-set` | Specifies the name of the policy map created earlier and enters policy-map configuration mode. |
| **Step 4** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Device(config-pmap)# class voice` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. |
| **Step 5** | **set cos** *cos-value*<br><br>**Example:**<br>`Device(config-pmap-c)# set cos 1` | Sets the packet's CoS value. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Device(config-pmap-c)# exit` | Exits policy-map class configuration mode. |
| **Step 7** | **class** {*class-name* \| **class-default**}<br><br>**Example:**<br>`Device(config-pmap)# class video-and-data` | Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. This class is associated with the class map created earlier. |
| **Step 8** | **set cos** *cos-value*<br><br>**Example:**<br>`Device(config-pmap-c)# set cos 2` | Sets the packet's CoS value. |
| **Step 9** | **end**<br><br>**Example:**<br>`Device(config-pmap-c)# end` | (Optional) Exits policy-map class configuration mode and returns to privileged EXEC mode. |

# Configuration Examples for Class-Based Ethernet CoS Matching and Marking

## Example: Configuring Class-Based Ethernet CoS Matching

This example creates two classes, voice and video-and-data, to classify traffic based on the CoS values. The CoS-based-treatment policy map is used to set priority and bandwidth values for the classes. The service policy is attached to all packets leaving interface Gigabit Ethernet1/0/1.

**Note** The service policy can be attached to any interface that supports service policies.

```
Device(config)# class-map voice
Device(config-cmap)# match cos 7
Device(config-cmap)# exit
Device(config)# class-map video-and-data
Device(config-cmap)# match cos 5
Device(config-cmap)# exit
Device(config)# policy-map cos-based-treatment
Device(config-pmap)# class voice
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# exit
Device(config-pmap)# class video-and-data
Device(config-pmap-c)# bandwidth remaining percent 20
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)#  interface gigabitethernet1/0/1
Device(config-if)# service-policy output cos-based-treatment
```

## Example: Class-Based Ethernet CoS Marking

```
Device(config)# policy-map cos-set
Device(config-pmap)# class voice
Device(config-pmap-c)# set cos 1
Device(config-pmap-c)# exit
Device(config-pmap)# class video-and-data
Device(config-pmap-c)# set cos 2
Device(config-pmap-c)# end
```

# Additional References for Class-Based Ethernet CoS Matching and Marking

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco commands | Cisco IOS Master Command List, All Releases |

| Related Topic | Document Title |
|---|---|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS Quality of Service Solutions Command Reference* |
| Classifying network traffic | "Classifying Network Traffic" module |
| MQC | "Applying QoS Features Using the MQC" module |
| Marking network traffic | "Marking Network Traffic" module |

### Technical Assistance

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

# Feature Information for Class-Based Ethernet CoS Matching & Marking

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 26: Feature Information for Class-Based Ethernet CoS Matching and Marking***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Class-Based Ethernet CoS Matching and Marking | 12.2(5)T<br>15.0(1)S<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 3.2SE | This feature allows you to mark and match packets using Class of Service (CoS) values.<br>The following commands were introduced or modified: **match cos**, **set cos**. |

| Feature Name | Releases | Feature Information |
| --- | --- | --- |
| User Priority Based QoS Marking for Wireless Deployments | Cisco IOS XE Release 3.2SE | This features allows you to mark and match packets on wireless deployments using the user-priority (CoS) vlaues. |

CHAPTER 10

# QoS Match VLAN

The QoS: Match VLAN feature allows you to classify network traffic on the basis of the Layer 2 virtual local-area network (VLAN) identification number.



## 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 at the end of this module.

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 Match VLAN

### QoS Match VLAN

The QoS: Match VLAN feature allows you to classify network traffic on the basis of the Layer 2 virtual local-area network (VLAN) identification number. To classify network traffic based on the VLAN identification number you create a class-map and specify the match criteria using the **match vlan** command. You then attach the class to a policy-map and use the policy map in a service policy that is attached to an interface.

# How to Configure Match VLAN

## Classifying Network Traffic per VLAN

To classify network traffic on a per VLAN basis, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** {**match-any** | **match-all**} *class-map-name*
4. **match vlan** *vlan-id-number*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** *class-map-name*
8. **bandwidth percent** *percent*
9. **exit**
10. **exit**
11. **policy-map** *policy-map-name*
12. **class** *class-map-name*
13. **shape** {**average** | **peak**} *cir*
14. **service-policy** {**input** | **output**} *policy-map-name*
15. **exit**
16. **exit**
17. **interface** *type number* [**name-tag**]
18. **service-policy** {**input** | **output**} *policy-map-name*
19. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **class-map** {**match-any** \| **match-all**} *class-map-name*<br><br>**Example:**<br>`Router(config)# class-map match-any Blue_VRF` | Creates a class map and enters class map configuration mode. |
| **Step 4** | **match vlan** *vlan-id-number*<br><br>**Example:**<br>`Router(config-cmap)# match vlan 101` | Matches traffic on the basis of the range of VLAN identification numbers specified. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-cmap)# exit` | Returns to global configuration mode. |
| **Step 6** | **policy-map** *policy-map-name*<br><br>**Example:**<br>`Router(config)# policy-map Shared_QoS` | Creates a policy map that can be attached to an interface and enters policy-map configuration mode. |
| **Step 7** | **class** *class-map-name*<br><br>**Example:**<br>`Router(config-pmap)# class Blue_VRF` | Specify the name of the class whose policy you want to create and enters policy-map class configuration mode. |
| **Step 8** | **bandwidth percent** *percent*<br><br>**Example:**<br>`Router(config-pmap-c)# bandwidth percent 30` | Specifies the bandwidth allocated for a class belonging to a policy map. |
| **Step 9** | **exit**<br><br>**Example:**<br>`Router(config-pmap-c)# exit` | Returns to policy-map configuration mode. |
| **Step 10** | **exit**<br><br>**Example:**<br>`Router(config-pmap)# exit` | Returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **policy-map** *policy-map-name*<br><br>**Example:**<br><br>`Router(config)# policy-map COS-OUT-SHAPED` | Creates a policy map that can be attached to an interface and enters policy-map configuration mode. |
| **Step 12** | **class** *class-map-name*<br><br>**Example:**<br><br>`Router(config-pmap)# class FROM_WAN` | Specify the name of the class whose policy you want to create and enters policy-map class configuration mode. |
| **Step 13** | **shape** {**average** \| **peak**} *cir*<br><br>**Example:**<br><br>`Router(config-pmap-c)# shape average 9000000000` | Specifies the average rate traffic shaping.<br><br>• The Committed information rate (CIR), is specified in bits per second (bps). |
| **Step 14** | **service-policy** {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Router(config-pmap-c)# service-policy Shared_QoS` | Specifies the name of the predefined policy map to be used as a QoS policy. |
| **Step 15** | **exit**<br><br>**Example:**<br><br>`Router(config-pmap-c)# exit` | Returns to policy-map configuration mode. |
| **Step 16** | **exit**<br><br>**Example:**<br><br>`Router(config-pmap)# exit` | Returns to global configuration mode. |
| **Step 17** | **interface** *type number* [**name-tag**]<br><br>**Example:**<br><br>`Router(config)# interface FastEthernet 0/0.1` | Configures an interface type and enters interface configuration mode.<br><br>• Enter the interface type and number. |
| **Step 18** | **service-policy** {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br><br>`Router(config-if)# service-policy output COS-OUT-SHAPED` | Attaches a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits interface configuration mode and returns to privileged EXEC mode. |

# Configuration Examples for Match VLAN

## Example: Classifying Network Traffic per VLAN

The following example shows how to classify network traffic on a VLAN basis. The VLAN classified traffic is applied to the FastEthernet 0/0.1 subinterface.

```
interface FastEthernet0/0.1
service-policy output COS-OUT-SHAPED
policy-map COS-OUT-SHAPED
      class ADMIN
      class FROM_WAN
               shape average 900000000
               service-policy Shared_QoS
policy-map Shared_QoS
      ! description -- Bandwidth sharing between VRF --
      class Blue_VRF
               bandwidth percent 3
class-map match-any Blue_VRF
      ! description -- traffic belonging to the VRF Blue --
      match vlan  101
```

# Additional References for QoS for Match VLAN

**Related Documents**

| Related Topic | Document Title |
|---|---|
| Cisco commands | Cisco IOS Master Command 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* |
| Classifying network traffic | “Classifying Network Traffic” module |
| MQC | “Applying QoS Features Using the MQC” module |
| Marking network traffic | “Marking Network Traffic” module |

### Technical Assistance

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

# Feature Information for QoS for Match VLAN

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 27: Feature Information for QoS for Match VLAN***

| Feature Name | Releases | Feature Information |
|---|---|---|
| QoS: Match VLAN | 12.2(31)SB2<br>Cisco IOS XE Release 2.1<br>15.0(1)S | The QoS: Match VLAN feature allows you to classify network traffic on the basis of the Layer 2 virtual local-area network (VLAN) identification number. The following commands were introduced or modified by this feature: **match vlan** (QoS), **show policy-map interface**<br>This feature was introduced on Cisco ASR 1000 Series Routers. |

CHAPTER 11

# Flexible Packet Matching XML Configuration

The Flexible Packet Matching XML Configuration feature allows the use of eXtensible Markup Language (XML) to define traffic classes and actions (policies) to assist in blocking network attacks. The XML file used by Flexible Packet Matching (FPM) is called the traffic classification definition file (TCDF).

The TCDF gives you an alternative to the command-line interface (CLI) as a method to define traffic classification behavior. Traffic classification behavior is identical regardless of the method you use.



## 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 at the end of this module.

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 the Flexible Packet Matching XML Configuration

- A protocol header definition file (PHDF) relevant to the TCDF must be loaded on the router.
- Although access to an XML editor is not required, using one might make the creation of the TCDF easier.
- You must be familiar with XML file syntax.

# Restrictions for the Flexible Packet Matching XML Configuration

### TCDF Image Restriction

TCDF is part of the FPM subsystem. FPM is not included in the Cisco 871 securityk9 image; therefore, TCDF parsing is not present in the Cisco 871 securityk9 image.

The Flexible Packet Matching XML Configuration has the following restrictions:

- The FPM TCDF cannot be used to mitigate an attack that requires stateful classification.
- Because FPM is stateless, it cannot keep track of port numbers being used by protocols that dynamically negotiate ports. Thus, when using the FPM TCDF, port numbers must be explicitly specified.
- FPM cannot perform IP fragmentation or TCP flow reassembly.

# Information About the Flexible Packet Matching XML Configuration

## Traffic Classification Definition Files for the Flexible Packet Matching XML Configuration

FPM uses a TCDF to define policies that can block attacks on the network. FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM users can create their own stateless packet classification criteria and define policies with multiple actions (such as drop, log, or send Internet Control Message Protocol [ICMP] unreachable) to immediately block new viruses, worms, and attacks on the network.

Before the release of the Flexible Packet Matching XML Configuration feature, FPM defined traffic classes (class maps), policies (policy maps), and service policies (attach policy maps to a class maps) through the use of CLI commands. With TCDFs, FPM can use XML as an alternative to the CLI to define classes of traffic and specify actions to apply to the traffic classes. Traffic classification behavior is the same whether you create the behavior using a TCDF or configure it using CLI commands. Once a TCDF is created, it can be loaded on any FPM-enabled device in the network.

# Protocol Header Definition Files for Traffic Classification Definitions

TCDFs require that a relevant PHDF is already loaded on the device. A PHDF defines each field contained in the header of a particular protocol. Each field is described with a name, optional comment, an offset (the location of the protocol header field in relation to the start of the protocol header), and the length of the field. The total length is specified at the end of each PHDF.

The description of a traffic class in a TCDF file can contain header fields defined in a PHDF. If the PHDF is loaded on the router, the class specification to match begins with a list of the protocol headers in the packet. In the TCDF, the traffic class is associated with a policy that binds the match to an action, such as drop, log, or send ICMP unreachable.

FPM provides ready-made definitions for these standard protocols, which can be loaded onto the router with the **load protocol** command: ether.phdf, ip.phdf, tcp.phdf, and udp.phdf. You can also write your own custom PHDFs using XML if one is required for the TCDF.

**Note** Because PHDFs are defined via XML, they are not shown in a running configuration.

# Traffic Classification Description File Format and Use

In the TCDF, you can define one or more classes of traffic and policies that describe specified actions for each class of traffic. The TCDF is an XML file that you create in a text file or with an XML editor. The file that you create must have a filename that has the .tcdf extension.

The TCDF has the following basic format. XML tags are shown in bold text for example purposes only.

```
<tdcf
>
       <class
 ...> ... </class
>
         ...
       <policy
> ... </policy
>
         ...
</tdcf
>
```

For a traffic class, you can identify a match for any field or fields against any part of the packet.

**Note** FPM is stateless and cannot be used to mitigate an attack that requires stateful classification, that is classify across IP fragments, across packets in a TCP stream, or peer-to-peer protocol elements.

Policies can be anything from access control, quality of service (QoS), or even routing decisions. For FPM, the associated actions (policies) might include permit, drop, log, or send ICMP unreachable.

Once loaded, the TCDF-defined classes and policies can be applied to any interface or subinterface and behave in an identical manner as the CLI-defined classes and policies. You can define policies in the TCDF and apply then to any entry point to the network to block new attacks.

# Traffic Class Definitions for a Traffic Classification Definition File

A class can be any traffic stream of interest. You define a traffic stream of interest by matching a particular interface or port, a source address or destination IP address, a protocol or an application. The following sections contain information you should understand before you define the traffic class in the TCDF for FPM configuration:

## Class Element Attributes for a Traffic Classification Definition File

The table below lists and describes the attributes that you can associate with the **class** element in a TCDF for the FPM XML configuration. The **class** element contains attributes you can use to specify the traffic class name, its description and type, where to look in the packet, what kind of match, and when the actions should apply to the traffic.

***Table 28: Attributes for Use with the Class Element in a TCDF for the FPM XMLConfiguration***

| Attribute Name | Use | Type |
|---|---|---|
| name (required) | Specifies the name of the class.<br>**Note** When you use the class element inside policy elements, you need specify the name attribute only. | String |
| type (required) | Specifies the type of class. | Keywords: stack or access-control |
| stack start | Specifies where to look in the packet. By default, the match starts at Layer 3. | Keyword: l2-start |
| match | Specifies the type of match to be performed on the class. | Keywords: all or any<br>• all--All class matches must be met to perform the policy actions.<br>• any--One or more matches within the class must be met to perform the policy actions. |
| undo | Directs the device to remove the class-map when set to true. | Keywords: true or false |

For example, XML syntax for a stack class describing an IP, User Datagram Protocol (UDP), Simple Management Protocol (SNMP) stack might look like this:

```
<class
 name
```

```
="snmp-stack"
type
="stack">
    <match
>
       <eq

field
="ip.protocol" value="x"></eq
>
       <eq

field
="udp.dport"
value
="161"></eq
>
    </match
>
</class
>
```

## Match Element for a Traffic Classification Definition File

The **match** element in the TCDF for FPM XML configuration contains **operator** elements. **Operator** elements are the following: **eq** (equal to), **neq** (not equal to), **lt** (less than), **gt** (greater than), **range** (a value in a specific range, for example, **range** 1 - 25), and **regex** (regular expression string with a maximum length of 32 characters).

In following sections, these various operators are collectively called the operator element.

## Operator Element Attributes for a Traffic Classification Definition File

The table below lists and describes direct matching attributes that you can associate with the **operator**element in a TCDF for the FPM XML configuration.

***Table 29: Direct Matching Attributes to Use with a Match Element in a TCDF for the FPM XML Configuration***

| Attribute Name | Use | Type |
|---|---|---|
| start | Begin the match on a predefined keyword or **Protocol.Field**, if given. | Keyword: l2-start or l3-start<br>Otherwise, a field of a protocol as defined in the PHDF, for example, the source field in the IP protocol. |
| offset | Used with start attribute. Offset from the start point. | Hexadecimal or decimal number, or string constants, **Protocol.Field**, or combination of a constant and **Protocol.Field** with +, -, *, /, &, or \|. |
| size | Used together with start and offset attributes. How much to match. | Specifies the size of the match in bytes. |

| Attribute Name | Use | Type |
|---|---|---|
| mask | Number specifying bits to be matched in protocol or field attributes.<br>Used exclusively with field type of bitset to specify the bits of interest in a bit map. | Decimal or hexadecimal number |
| value | Value on which to match. | String, number, or regular expression |
| field | Specifies the name of the field to be compared. | Name of field as defined in the PHDF |
| next | Identifies the next layer of the protocol. This attribute can be used only in stack type classes. | Keyword that is the name of a protocol defined in the PHDF. |
| undo | Directs the device to remove the particular match operator when set to true. | Keywords: true or false |

# Policy Definitions for a Traffic Classification Definition File

A policy is any action that you apply to a class. You should understand the following information before defining the policy in a TCDF for the FPM XML configuration:

## Policy Element Attributes for a Traffic Classification Definition File

Policies can be anything from access control, QoS, or even routing decisions. For FPM, the associated actions or policies might include drop, log, or send ICMP unreachable. Policies describe the action to take to mitigate attacks on the network.

The table below lists and describes the attributes that you can use with the **policy** element in the TDCF for FPM XML configuration.

***Table 30: Attributes for Use with the Policy Element in a TCDF for the FPM XML Configuration***

| Attribute Name | Use | Type |
|---|---|---|
| name | Name of the policy. | String |
| type | Specifies the type of policy map. | Keyword: access-control |
| undo | Directs the device to remove the policy map when set to true. | Keywords: true or false |

The policy name in this example is sql-slammer, and the action defined for the policy is to drop the packet. This action is to be applied to the class that has the same name as the policy (class name= "sql-slammer").

```
<policy

name
="sql-slammer">
    <class

name
="sql-slammer"></class
>
    <action
>drop</action
>
</policy
>
```

## Action Element for a Traffic Classification Definition File

The **action** element is used to specify actions to associate with a policy. The policy with the **action** element is applied to a defined class. The **action** element can contain any of the following: permit, drop, Log, SendBackIcmp, set, RateLimit, alarm, ResetTcpConnection, and DropFlow. For example:

```
<action
>
   log
</action
>
```

## Traffic Classification Definition File Syntax Guidelines

The following list describes required and optional syntax for the TCDF:

- The TCDF filename must end in the .tcdf extension, for example, sql_slammer.tcdf.
- The TCDF contains descriptions for one or more traffic classes and one or more policy actions.
- The file is encoded in the XML notation.
- The TCDF file should begin with the following version encoding:

**<?xml version="1.0" encoding="UTF-8"?>**

The TCDF is used to define traffic classes and the associated policies with specified actions for the purpose of blocking new viruses, worms, and attacks on the network.

The TCDF is configured in a text or XML editor. The syntax of the TCDF must comply with the XML Version 1.0 syntax and the TCDF schema. For information about Version 1.0 XML syntax, see the document at the following url:

http://www.w3.org/TR/REC-xml/

# How to Create and Load Traffic Classification Definition Files

## Creating a Definition File for the FPM XML Configuration

### SUMMARY STEPS

1. Open a text file or an XML editor and begin the file with the XML version and encoding declaration.
2. Identify the file as a TCDF. For example:
3. Define the traffic class of interest.
4. Identify matching criteria for the defined classes of traffic. For example:
5. Define the action to apply to the defined class. For example:
6. End the traffic classification definition. For example:
7. Save the TCDF file with a filename that has a .tcdf extension, for example: slammer.tcdf.

### DETAILED STEPS

**Step 1** Open a text file or an XML editor and begin the file with the XML version and encoding declaration.

**Example:**

```
<?xml version="1.0" encoding="UTF-8"?>
```

**Step 2** Identify the file as a TCDF. For example:

**Example:**

```
<tcdf
>
```

**Step 3** Define the traffic class of interest.
For example, a stack class describing an IP and UDP stack might be described as follows. In this example, the name of the traffic class is "ip-udp," and the class type is "stack."

**Example:**

```
<class

name
="ip-udp"
type
="stack"></class
>
```

In the following example, the name of the traffic class is slammer, the class type is access control, and the match criteria is all:

**Example:**

```
<class
 name="
slammer
"
type
="access-control"
match
="all"></class
>
```

**Step 4** Identify matching criteria for the defined classes of traffic. For example:

**Example:**

```
    <class

name
="ip-udp"
type
="stack">
       <match
>
          <eq

field
="ip.protocol"
value
="0x11"
next
="udp"></eq
>
       </match
>
    </class
>
    <class
 name="
slammer
"
type
="access-control"
match
="all">
       <match
>
          <eq

field
="udp.dest-port"
value
="0x59A"></eq
>
          <eq

field
="ip.length"
value
="0x194"></eq
>
          <eq

start
="l3-start"
offset
="224"
```

```
size
="4"
value
="0x00401010"></eq
>
       </match
>
    </class
>
```

The traffic of interest in this TCDF matches fields defined in the PHDF files, ip.phdf and udp.phdf. The matching criteria for slammer packets is a UDP destination port number 1434 (0x59A), an IP length not to exceed 404 (0x194) bytes, and a Layer 3 position with a pattern 0x00401010 at 224 bytes from start (offset) of the IP header.

**Step 5** Define the action to apply to the defined class. For example:

**Example:**

```
<policy

name
="fpm-udp-policy">
    <class

name
="slammer"></class
>
    <action
>Drop</action
>
</policy
>
```

The policy name in this example is fpm-udp-policy, and the action defined for the policy is to drop the packet. This action is to be applied to the class that has the name slammer.

**Step 6** End the traffic classification definition. For example:

**Example:**

```
</tcdf
>
```

**Step 7** Save the TCDF file with a filename that has a .tcdf extension, for example: slammer.tcdf.

# Loading a Definition File for the FPM XML Configuration

## SUMMARY STEPS

1. **enable**
2. **show protocol phdf** *protocol-name*
3. **configure terminal**
4. **load protocol** *location:filename*
5. **load classification** *location* **:** *filename*
6. **end**
7. **show class-map** [type {**stack** | **access-control**}] [*class-map-name*]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show protocol phdf** *protocol-name*<br><br>**Example:**<br>`Router# show protocol phdf ip` | Displays protocol information from a specific PHDF.<br>• Use this command to verify that a PHDF file relevant to the TCDF is loaded on the device. |
| **Step 3** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 4** | **load protocol** *location:filename*<br><br>**Example:**<br>`Router(config)# load protocol localdisk1:ip.phdf` | (Optional) Loads a PHDF onto a router.<br>• The specified location must be local to the router.<br>**Note** If the required PHDF is already loaded on the router (see Step 2), skip this step and proceed to Step 5). |
| **Step 5** | **load classification** *location* **:** *filename*<br><br>**Example:**<br>`Router(config)# load classification localdisk1:slammer.tcdf` | Loads a TCDF onto a router.<br>• The specified location must be local to the router. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **end**<br><br>**Example:**<br><br>`Router(config)# end` | Exits to privileged EXEC mode. |
| **Step 7** | **show class-map** [type {**stack** \| **access-control**}] [*class-map-name*]<br><br>**Example:**<br><br>`Router# show class-map sql-slammer` | (Optional) Displays a class map and its matching criteria.<br>• Use this command to verify that a class defined in the TCDF file is available on the device.<br>• The *class-map-name* argument is the name of a class in the TCDF. |

### Examples

The following is sample output from a **show class-map** command that displays the traffic classes defined in the TCDF after it is loaded on the router:

```
Router# show class-map
.
.
.
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
.
.
.
```

## What to Do Next

After you have defined the TCDF, you must apply that policy to an interface as shown in the following task "Associating a Traffic Classification Definition File, on page 128."

# Associating a Traffic Classification Definition File

Perform this task to associate the defination file with an interface or subinterface.

### Before You Begin

The TCDP and FPM must be configured on the device.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **service-policy type access-control** ] {**input** | **output**} *policy-map-name*
5. **end**
6. **show policy-map interface type access-control** ] *interface-name slot/port*[**input** | **output**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot / port*<br><br>**Example:**<br>`Router(config)# interface gigabitEthernet 0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **service-policy type access-control** ] {**input** \| **output**} *policy-map-name*<br><br>**Example:**<br>`Router(config-if)# service-policy type access-control input sql-slammer` | Specifies the type and the name of the traffic policy to be attached to the input or output direction of an interface.<br>• The *policy-map-name* argument is the name of a policy in the TCDF. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Exits to privileged EXEC mode. |
| **Step 6** | **show policy-map interface type access-control** ] *interface-name slot/port*[**input** \| **output**]<br><br>**Example:**<br>`Router# show policy-map interface gigabitEthernet 0/1` | (Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface.<br>• Use this command to verify that policy defined in TCDF is associated with the named interface. |

| | Command or Action | Purpose |
|---|---|---|

# Displaying TCDF-Defined Traffic Classes and Policies

## SUMMARY STEPS

1. **enable**
2. **show class-map [ type { stack | access-control}]** [*class-map-name*]
3. **show class-map type stack** [*class-map name*]
4. **show class-map type access-control** [*class-map-name*]
5. **show policy-map** [*policy-map*]
6. **exit**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show class-map [ type { stack | access-control}]** [*class-map-name*]

Use this command to verify that a class defined in the TCDF file is available on the device. For example:

**Example:**

```
Router# show class-map
.
.
.
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
.
.
.
```

**Step 3** **show class-map type stack** [*class-map name*]

Use this command to display the stack type defined for the class of traffic in the TCDF file. For example:

**Example:**

```
Router# show class-map type stack ip-udp
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
```

**Step 4** **show class-map type access-control** [*class-map-name*]
Use this command to display the access type defined for the class in the TCDF file. For example:

**Example:**

```
Router# show class-map type access-control slammer
class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
```

**Step 5** **show policy-map** [*policy-map*]
Use this command to display the contents of a policy map defined in the TCDF. For example:

**Example:**

```
Router# show policy-map fpm-udp-policy
policy-map type access-control fpm-udp-policy
  class slammer
    drop
```

**Step 6** **exit**
Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

# Configuration Examples for Creating and Loading Traffic Classification Definition Files

**Note** The TCDF files are created in a text file or with an XML editor. In the following examples, XML tags are shown in bold text and field names in italic text. The values for the attributes are entered in quotation marks ("value").

# Example Traffic Classification Definition File for Slammer Packets

The following example shows how to create and load a TCDF for slammer packets (UDP 1434) for the FPM configuration. The match criteria defined within the **class** element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP destination port 1434 (0x59A), and pattern 0x00401010 at 224 bytes from start of IP header. This example also shows how to define the policy "sql-slammer" with the action to drop slammer packets.

```
<?xml version="1.0" encoding="UTF-8"?
>
<tcdf
>
    <class

name
="ip-udp"
type
="stack">
       <match
>
          <eq

field
="ip.protocol"
value
="0x11"
next
="udp"></eq
>
       </match
>
    </class
>
    <class
 name="
slammer
"
type
="access-control"
match
="all">
       <match
>
          <eq

field
="udp.dest-port"
value
="0x59A"></eq
>
          <eq

field
="ip.length"
value
="0x194"></eq
>
          <eq

start
="l3-start"
offset
="224"
size
="4"
value
="0x00401010"></eq
```

```
>
       </match
>
    </class
>
    <policy
 type="access-control"
name
="fpm-udp-policy">
       <class

name
="slammer"></class
>
       <action
>Drop</action
>
    </policy
>
</tcdf
>
```

The following example shows how to load the TCDF file onto the device and apply the policy defined in the file to the interface Gigabit Ethernet 0/1:

```
configure terminal
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-1
class ip-udp
service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input my-policy-1
 end
```

# Example Traffic Classification Definition File for MyDoom Packets

The following example shows how to create and load a TCDF for MyDoom packets in a text file or XML editor for the FPM XML configuration. The match criteria for the MyDoom packets are as follows:

- 90 > IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header

or

- IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header

```
<tcdf
>
    <class

name
="md-stack"
type
="stack">
        <match
>
            <eq

field
="ip.protocol"
value
="6"
```

```
next
="tcp"></eq
>
        </match
>
    </class
>
    <class

type
="access-control"
name
="mydoom1">
        <match
>
            <gt

field
="ip.length"
value
="44"/>
            <lt

field
="ip.length"
value
="90"/>
            <eq

start
="ip.version"
offset
="tcp.headerlength*4+20"
size
="4"

value
="0x47455420"/>
        </match
>
    </class
>
    <class

type
="access-control"
name
="mydoom2">
        <match
>
            <gt
 field="ip.length" value="44"/>
            <eq
 start="ip.version" offset="tcp.headerlength*4+58" size="4"
                value="0x6d3a3830"/>
            <eq
 start="ip.version" offset="tcp.headerlength*4+20" size="4"
                 value="0x47455420"/>
        </match
>
    </class
>
    <policy

name
="fpm-md-stack-policy">
       <class

name
="mydoom1"></class
>
       <action
```

```
>drop</action
>
    </policy
>
    <policy

name
="fpm-md-stack-policy">
       <class

name
="mydoom2"></class
>
       <action
>drop</action
>
    </policy
>
</tcdf
>
```

The following example shows how to load the TCDF file onto the device and apply the policy defined in the file to the interface Ethernet 0/1:

```
configure terminal
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-2
class md-stack
service-policy fpm-md-stack-policy
interface Ethernet 0/1
 service-policy type access-control input my-policy-2
 end
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Additional configuration information for class maps and policy maps | "Applying QoS Features Using the MQC" module |
| Information about and configuration tasks for FPM | "Flexible Packet Matching" module |

### Standards

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

### MIBs

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

### RFCs

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

### 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 Flexible Packet Matching XML Configuration

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 31: Feature Information for Flexible Packet Matching XML Configuration*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Flexible Packet Matching XML Configuration | 12.4(6)T | The Flexible Packet Matching XML Configuration feature provides an Extensible Markup Language (XML)-based configuration file for Flexible Packet Matching (FPM) that can be used to define traffic classes and actions (policies) to assist in the blocking of attacks on a network. The XML file used by FPM is called the traffic classification definition file (TCDF).<br>The TCDF gives you an alternative to the command-line interface (CLI) as a method to define traffic classification behavior. Traffic classification behavior is identical regardless of the method you use.<br>This feature was introduced in Cisco IOS Release 12.4(6)T.<br>The following command was introduced by this feature: **load classification**. |