



# Implementing QoS for IPv6

---

**First Published: November 25, 2002**

**Last Updated: October 5, 2008**

This module provides information about and tasks for implementing quality of service (QoS) features in IPv6 environments, specifically the application of the Differentiated Services (DiffServ) QoS features to IPv6 packets.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Implementing QoS for IPv6”](#) section on page 18.

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

## Contents

- [Prerequisites for Implementing QoS for IPv6, page 2](#)
- [Restrictions for Implementing QoS for IPv6, page 2](#)
- [Information About Implementing QoS for IPv6, page 2](#)
- [How to Implement QoS for IPv6, page 4](#)
- [Configuration Examples for Implementing QoS for IPv6, page 15](#)
- [Additional References, page 16](#)
- [Feature Information for Implementing QoS for IPv6, page 18](#)



---

**Americas Headquarters:**

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

# Prerequisites for Implementing QoS for IPv6

This document assumes that you are familiar with IPv4. Refer to the publications referenced in the [“Additional References”](#) section for IPv4 configuration and command reference information.

## Restrictions for Implementing QoS for IPv6

The following QoS features are not supported for managing IPv6 traffic:

- Compressed Real-Time Protocol (CRTTP)
- Network-based application recognition (NBAR)
- Committed access rate (CAR)
- Priority queueing (PQ)
- Custom queueing (CQ)

### Platform-Specific Information and Restrictions

IPv6 QoS is supported on Cisco 12000 series Internet routers in Cisco IOS Release 12.0(28)S. Certain features of IPv6 QoS are not supported in Release 12.0(28)S. These features include packet classification.

## Information About Implementing QoS for IPv6

The following sections provide information about the QoS features available for managing IPv6 traffic:

- [Implementation Strategy for QoS for IPv6, page 2](#)
- [Packet Classification in IPv6, page 3](#)
- [Policies and Class-Based Packet Marking in IPv6 Networks, page 3](#)
- [Congestion Management in IPv6 Networks, page 3](#)
- [Congestion Avoidance for IPv6 Traffic, page 4](#)
- [Traffic Policing in IPv6 Environments, page 4](#)

## Implementation Strategy for QoS for IPv6

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

All of the QoS features available for IPv6 environments are managed from the modular QoS command-line interface (CLI). The modular QoS CLI allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.

To implement QoS in networks running IPv6, follow the same steps that you would follow to implement QoS in networks running only IPv4. At a very high level, the basic steps for implementing QoS are as follows:

1. Know which applications in your network need QoS.

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

## Packet Classification in IPv6

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

The enhancements to the modular QoS CLI (MQC) allow you to create matches on precedence, DSCP, and IPv6 access group values in both IPv4 and IPv6 packets. The **match** command allows matches to be made on DSCP values and precedence for both IPv4 and IPv6 packets. See [“Using the Match Criteria to Manage IPv6 Traffic Flows” section on page 6](#) for configuration guidelines and to see the **match dscp** and **match precedence** command descriptions.

## 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.

Use the **set dscp** and **set precedence** commands for packet marking. These commands have been modified to handle both IPv4 and IPv6 traffic. See the [“Specifying Marking Criteria for IPv6 Packets” section on page 5](#) for configuration guidelines for using these commands.

## Congestion Management in IPv6 Networks

Once you have marked the traffic, you can use the markings to build a policy and classify traffic on the rest of the network segments. If you keep the policy simple (no more than about four classes), it will be easier to manage. Class-based and flow-based queuing are supported for IPv6. The processes and tasks

use the same commands and arguments to configure various queueing options for both IP and IPv6. Refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* for configuration and usage instructions of queueing features.

## Congestion Avoidance for IPv6 Traffic

WRED implements the RED-based drop policy on the packets that are likely to overflow the limits of Class-based Weighted Fair Queueing (CBWFQ). WRED supports class-based and flow-based (using DSCP or precedence values) queueing. The WRED commands apply to both IPv4 and IPv6 with no changes.

## Traffic Policing in IPv6 Environments

Congestion management for IPv6 is similar to its implementation for IP packets, and the commands used to configure queueing and traffic shaping features for IPv6 environments are the same commands as those used for IP. 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.

Although no changes to existing configuration or command usage for policing are required for use in IPv6 environments, the **police** command has been enhanced to mark both IPv4 and IPv6 packets when the following keyword options are used in confirm action, exceed action, and violate action:

- **set-dscp-transmit**
- **set-precedence-transmit**

## How to Implement QoS for IPv6

These configuration tasks describe how to classify traffic with match criteria and use the match criteria to manage traffic flows. The following sections are included:

- [Restrictions for Classifying Traffic in IPv6 Networks, page 4](#) (required)
- [Specifying Marking Criteria for IPv6 Packets, page 5](#) (required)
- [Using the Match Criteria to Manage IPv6 Traffic Flows, page 6](#) (required)
- [Verifying Packet Marking Criteria, page 8](#) (optional)
- [Confirming the Service Policy, page 13](#) (optional)

## Restrictions for Classifying Traffic in IPv6 Networks

Except for the modifications to the **match dscp** and **match precedence** commands and the addition of the IPv6-specific **match access-group name** command, the functionality of all of the **match** commands is the same for both IPv4 and IPv6.

The **set cos** and **match cos** commands for 802.1Q (dot1Q) interfaces are supported only for Cisco Express Forwarding-switched packets. Process-switched packets, such as router-generated packets, are not marked when these options are used.

## Specifying Marking Criteria for IPv6 Packets

The following task establishes the match criteria (or marks the packets) that will be used later 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. **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
- or
- set [ip] dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

### DETAILED STEPS

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable  | Enables such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                        | Enters global configuration mode.  |
| Step 3 | <b>policy map</b> <i>policy-map-name</i><br><br><b>Example:</b><br>Router(config)# policy map policy1 | Creates a policy map using the specified name and enters QoS policy-map configuration mode. <ul style="list-style-type: none"> <li>• Enter name of policy map you want to create.</li> </ul> |

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 4 | <pre><b>class</b> {<i>class-name</i>   <b>class-default</b>}</pre> <p><b>Example:</b><br/>Router(config-pmap)# class class-default</p>   | Specifies the treatment for traffic of specified class (or the default class) and enters QoS policy-map class configuration mode. |
| Step 5 | <pre><b>set precedence</b> {<i>precedence-value</i>   <i>from-field</i> [<b>table</b> <i>table-map-name</i>]}</pre> <p>or</p> <pre><b>set [ip] dscp</b> {<i>dscp-value</i>   <i>from-field</i> [<b>table</b> <i>table-map-name</i>]}</pre> <p><b>Example:</b><br/>Router(config-pmap-c)# set dscp cos table table-map1</p> <p>or</p> <pre>Router(config-pmap-c)# set precedence cos table table-map1</pre> |   |

## Troubleshooting Tips

### Confirm That Cisco Express Forwarding Is Enabled

Use the **show cef interface**, **show ipv6 cef**, **show ipv6 interface neighbors**, and **show interface statistics** commands to confirm that Cisco Express Forwarding is enabled and that packets are being Cisco Express Forwarding-switched.

### Confirm That Packets Are Cisco Express Forwarding-Switched

Use the **show policy-map interface** command to display per-interface, per-policy Cisco Express Forwarding-switching statistics.

## Using the Match Criteria to Manage IPv6 Traffic Flows

The following task describes how to use the **match** commands to match the traffic to the policies that you establish. 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. **match precedence** *precedence-value* [*precedence-value* *precedence-value*]
- or
- match access-group name** *ipv6-access-group*

or

**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 | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>   | <p>Enables such as privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>   |
| Step 2 | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>  | <p>Enters global configuration mode.</p>  |
| Step 3 | <p><b>class-map</b> {<i>class-name</i>   <b>class-default</b>}</p> <p><b>Example:</b><br/>Router(config-pmap-c)# class cls1</p>   | <p>Creates the specified class and enters QoS class-map configuration mode.</p>   |
| Step 4 | <p><b>match precedence</b> <i>precedence-value</i> [<i>precedence-value precedence-value</i>]</p> <p>or</p> <p><b>match access-group name</b> <i>ipv6-access-group</i></p> <p>or</p> <p><b>match [ip] dscp</b> <i>dscp-value</i> [<i>dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value</i>]</p> <p><b>Example:</b><br/>Router(config-pmap-c)# match precedence 5</p> <p>or</p> <p>Router(config-pmap-c)# match access-group name ipv6acl</p> <p>or</p> <p>Router(config-pmap-c)# match ip dscp 15</p> | <p>Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.</p> <p>or</p> <p>Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class.</p> <p>or</p> <p>Identifies a specific IP DSCP value as a match criterion.</p> |

### Examples

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

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# class-m c1
Router(config-cmap)# match precedence 5
```

```

Router(config-cmap)# end
Router#
Router(config)# policy p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police 10000 conform set-prec-trans 4

```

## Verifying Packet Marking Criteria

To verify that packet marking is working as expected, use the `show policy` command. The interesting information from the output of this command is the difference in the number of total packets versus the number of packets marked.

```

Router# show policy p1

Policy Map p1
  Class c1
    police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface serial 4/1
Router(config-if)# service out p1
Router(config-if)# end

Router# 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

```

## Interpreting Packet Counters in show policy-map interface Command Output

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 modular QoS CLI.

Congestion typically occurs when a fast ingress interface feeds a relatively slow egress interface. A common congestion point is a branch-office router with an Ethernet port facing the LAN and a serial port facing the WAN. Users on the LAN segment are generating 10 Mbps of traffic, which is being fed into a T1 with 1.5 Mbps of bandwidth.

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.

```
Router# 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 IOS 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.

### Number of Packets and Packets Matched

Service policies apply only to packets stored in the Layer 3 queues. [Table 1](#) 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 Cisco Express Forwarding-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           |
| Packets that are Cisco Express Forwarding- or fast-switched   | Yes        | No            |

The following example shows these guidelines applied to the **show policy-map interface** command output. The four key counters are shown in boldface type.

```
Router# 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)
```

[Table 2](#) defines the counters that appear in the example in boldfaced type.

**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 Management Information Base (MIB). They no longer appear in the <b>show policy-map</b> command output in current releases of Cisco IOS.  |
| 5 minute offered rate 0 bps, drop rate 0 bps | Use the <b>load-interval</b> command to change this value and make it a more instantaneous value. The lowest value is 30 seconds; however, statistics displayed in the <b>show policy-map interface</b> 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 Cisco Express Forwarding- 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 queuing 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.

## Conversation Number Allocation

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

```
Router# 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, routers 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.

[Table 3](#) 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                       |

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

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

Table 4 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                       |
| 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 IOS software assigns a conversation or queue number as shown in Table 5.

**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 (formerly known as CDP) 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 <b>show policy-map</b> 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.  |

## Confirming the Service Policy

This task tests the packets matched counter and your 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 atm slot/0. subinterface-number** {multipoint | point-to-point}
4. **ip address ip-address mask** [secondary]
5. **pvc** [name] vpi/vci [ces | ilmi | qsaal | smps]
6. **tx-ring-limit** ring-limit
7. **service-policy** {input | output} policy-map-name

## DETAILED STEPS

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal   | Enters global configuration mode.   |
| Step 3 | <b>interface atm slot/0. subinterface-number</b><br>{multipoint   point-to-point}<br><br><b>Example:</b><br>Router(config)# interface atm 1/0.1<br>point-to-point} | Enters interface configuration mode.  |
| Step 4 | <b>ip address ip-address mask</b> [secondary]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.1.1.1<br>255.255.255.0                                    | Specifies the IP address of the interface you want to test.   |
| Step 5 | <b>pvc</b> [name] vpi/vci [ces   ilmi   qsaal   smps]<br><br><b>Example:</b><br>Router(config-if)# 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. |

|        | Command or Action   | Purpose  |
|--------|---|--|
| Step 6 | <b>tx-ring-limit</b> <i>ring-limit</i><br><br><b>Example:</b><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. <ul style="list-style-type: none"> <li>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.</li> </ul> |
| Step 7 | <b>service-policy</b> { <b>input</b>   <b>output</b> } <i>policy-map-name</i><br><br><b>Example:</b><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. <ul style="list-style-type: none"> <li>Note that the packets matched counter is a part of queueing feature and is available only on service policies attached in output direction.</li> </ul>        |

## Configuration Examples for Implementing QoS for IPv6

This section provides the following configuration examples:

- [Verification of Cisco Express Forwarding Switching: Example, page 15](#)
- [Matching DSCP Value: Example, page 16](#)

### Verification of Cisco Express Forwarding Switching: Example

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0. 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 1/0/0 detail

Ethernet1/0/0 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 Ethernet1/0/0
  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
```

## Matching DSCP Value: Example

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 1/0/0. 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 fa1/0/0
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
Router(config)# exit
```

## Additional References

The following sections provide references related to the Implementing QoS for IPv6 feature.

### Related Documents

| Related Topic  | Document Title   |
|--|--|
| IPv6 supported feature list  | <a href="#">“Start Here: Cisco IOS Software Release Specifics for IPv6 Features,” Cisco IOS IPv6 Configuration Guide</a> |
| IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <a href="#">Cisco IOS IPv6 Command Reference</a>   |

### 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, 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><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title  |
|----------|--|
| RFC 2474 | <i>Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</i> |
| RFC 2475 | <i>An Architecture for Differentiated Services Framework</i>                                   |
| RFC 2597 | <i>Assured Forwarding PHB</i>  |
| RFC 2598 | <i>An Expedited Forwarding PHB</i>   |
| RFC 2640 | <i>Internet Protocol, Version 6 Specification</i>  |
| RFC 2697 | <i>A Single Rate Three Color Marker</i>  |
| RFC 2698 | <i>A Two Rate Three Color Marker</i>   |

## Technical Assistance

| Description   | Link  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Implementing QoS for IPv6

Table 6 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(2)T or a later release appear in the table.

For information about a feature in this technology that is not documented here, see the [Start Here: Cisco IOS Software Release Specifics for IPv6 Features](#) roadmap.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 6 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 6** Feature Information for Implementing QoS for IPv6

| Feature Name                        | Releases   | Feature Information   |
|-------------------------------------|--|---|
| IPv6 quality of service (QoS)       | 12.0(28)S <sup>1</sup><br>12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | QoS features supported for IPv6 environments include packet classification, queuing, traffic shaping, WRED, class-based packet marking, and policing of IPv6 packets.   |
| IPv6 QoS: MQC packet classification | 12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T                           | <p>The modular QoS CLI allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Packet Classification in IPv6, page 3</a></li> <li>• <a href="#">Specifying Marking Criteria for IPv6 Packets, page 5</a></li> </ul> |

**Table 6** Feature Information for Implementing QoS for IPv6 (continued)

| Feature Name                            | Releases   | Feature Information   |
|---|--|---|
| IPv6 QoS: MQC traffic shaping           | 12.0(28)S <sup>1</sup><br>12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | 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.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Traffic Policing in IPv6 Environments, page 4</a></li> <li>• <a href="#">Interpreting Packet Counters in show policy-map interface Command Output, page 8</a></li> </ul> |
| IPv6 QoS: MQC traffic policing          | 12.0(28)S <sup>1</sup><br>12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | Configuration or command usage for policing are the same in IPv6 environments as for IPv4 environments.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Traffic Policing in IPv6 Environments, page 4</a></li> </ul>   |
| IPv6 QoS: MQC packet marking/re-marking | 12.0(28)S <sup>1</sup><br>12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><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.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Policies and Class-Based Packet Marking in IPv6 Networks, page 3</a></li> <li>• <a href="#">Traffic Policing in IPv6 Environments, page 4</a></li> </ul>   |
| IPv6 QoS: queueing                      | 12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T                           | Class-based and flow-based queueing are supported for IPv6.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Congestion Management in IPv6 Networks, page 3</a></li> <li>• <a href="#">Traffic Policing in IPv6 Environments, page 4</a></li> <li>• <a href="#">Interpreting Packet Counters in show policy-map interface Command Output, page 8</a></li> </ul>   |
| IPv6 QoS: MQC WRED-based drop           | 12.0(28)S <sup>1</sup><br>12.2(33)SRA<br>12.2(18)SXE <sup>2</sup><br>12.2(13)T<br>12.3<br>12.3(2)T<br>12.4<br>12.4(2)T | WRED implements the RED-based drop policy on the packets that are likely to overflow the limits of CBWFQ.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Implementation Strategy for QoS for IPv6, page 2</a></li> <li>• <a href="#">Congestion Avoidance for IPv6 Traffic, page 4</a></li> </ul>   |

1. Feature is supported on Cisco 12000 series Internet routers in Cisco IOS Release 12.0(28)S.
2. Cisco IOS Release 12.2(18)SXE provides support for this feature. Cisco IOS Release 12.2(18)SXE is specific to Cisco Catalyst 6500 and Cisco 7600 series routers.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002–2009 Cisco Systems, Inc. All rights reserved.