



# IPv6 Quality of Service

---

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.

- [Finding Feature Information, on page 1](#)
- [Information About IPv6 Quality of Service, on page 1](#)
- [How to Configure IPv6 Quality of Service, on page 2](#)
- [Configuration Examples for IPv6 Quality of Service, on page 4](#)
- [Additional References, on page 11](#)
- [Feature Information for IPv6 Quality of Service, on page 12](#)

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

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

## Packet Classification in IPv6

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

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

## How to Configure IPv6 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 (or mark the packets) 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**}

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>policy map</b> <i>policy-map-name</i> <b>Example:</b> 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>
<b>Step 4</b>	<b>class</b> { <i>class-name</i>   <b>class-default</b> } <b>Example:</b> Router(config-pmap)# class class-default	Specifies the treatment for traffic of specified class (or the default class) and enters QoS policy-map class configuration mode.

**Using the Match Criteria to Manage IPv6 Traffic Flows**

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

**SUMMARY STEPS**

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

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>class-map</b> <i>{class-name}</i> <b>class-default</b> <b>Example:</b> <pre>Router(config-pmap-c)# class cls1</pre>	Creates the specified class and enters QoS class-map configuration mode.
<b>Step 4</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <b>match precedence</b> <i>precedence-value</i> [<i>precedence-value precedence-value</i>]</li> <li>• <b>match access-group name</b> <i>ipv6-access-group</i></li> <li>• <b>match [ip] dscp</b> <i>dscp-value</i> [<i>dscp-value dscp-value dscp-value dscp-value dscp-value</i>]</li> </ul> <b>Example:</b> <pre>Router(config-pmap-c)# match precedence 5</pre> <b>Example:</b> <pre>Router(config-pmap-c)# match ip dscp 15</pre>	Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets. or Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class. or 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 GigabitEthernet 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 GigabitEthernet 1/0/0 detail

GigabitEthernet1/0/0 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 GigabitEthernet1/0/0
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

```

## Example: Verifying Packet Marking Criteria

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

```

To verify that packet marking is working as expected, use the **show policy** command. The output of this command shows a 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

```

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.

```
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 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 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.

```
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)
```

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.

Counter	Explanation
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).
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 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.

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 dlc1 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.

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
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 <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.

## Example: Matching DSCP Value

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

```
Router(config)#
  class-map ipdscp15
Router(config-cmap)#
  match ip dscp 15
Router(config)#
  exit
Router(config)#
policy-map priority50
Router(config-pmap)#
  class ipdscp15
Router(config-pmap-c)#
  priority 50
Router(config-pmap-c)#
  exit
Router(config-pmap)#
  exit
Router(config)#
interface gigabitethernet1/0/0
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

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
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
<ul style="list-style-type: none"> <li>• CISCO-CLASS-BASED-QOS-CAPABILITY-MIB</li> <li>• CISCO-CLASS-BASED-QOS-MIB</li> </ul>	<p>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:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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](http://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 12.3 12.2(50)SG 3.2.0SG 15.0(2)SG 12.2(33)SRA 12.2(18)SXE 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.  The following commands were introduced or modified: <b>match dscp</b> , <b>match precedence</b> , <b>set dscp</b> , <b>set precedence</b> .  The following commands were introduced or modified: <b>match access-group name</b> , <b>match dscp</b> , <b>match precedence</b> , <b>set dscp</b> , <b>set precedence</b> .