IPv6 QoS: MQC Packet Classification

Last Updated: July 11, 2012

The enhancements to the modular QoS CLI allow you to create matches on precedence, DSCP, and IPv6 access group values in both IPv4 and 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 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.

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

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 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map** {*class-name* | **class-default**} **Example:** `Device(config-pmap-c)# class-map clsl`	Creates the specified class and enters QoS class-map configuration mode.

Command or Action	Purpose

Step 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*]
Example:
`Device(config-pmap-c)# match precedence 5`
Example:
`Device(config-pmap-c)# match ip dscp 15`
	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.

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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **multipoint** | **point-to-point** **Example:** `Device(config)# interface gigabitethernet1/1/0 point-to-point`	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	Specifies the IP address of the interface that you want to test.
Step 5	**pvc** [*name*] *vpi/vci* [**ces** | **ilmi** | **qsaal** | **smds**] **Example:** `Device(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.
Step 6	**tx-ring-limit** *ring-limit* **Example:** `Device(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. • Specify the ring limit as the number of packets for Cisco 2600 and 3600 series routers or as the number of memory particles for Cisco 7200 and 7500 series routers.
Step 7	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Device(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. • The packets-matched counter is a part of the queueing feature and is available only on service policies attached in the 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 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
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
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 1 Feature Information for IPv6 QoS: MQC Packet Classification

Feature Name	Releases	Feature Information
IPv6 QoS: MQC Packet Classification	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.6S	The modular QoS CLI allows you to define traffic classes, create and configure traffic policies, and then attach those traffic policies to interfaces. The following commands were introduced or modified: **match access-group name**, **match dscp**, **match precedence**, **set dscp**, **set precedence**.