



QoS: Classification Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Read Me First 1

CHAPTER 2

IPv6 Quality of Service 3

- Finding Feature Information 3
- Information About IPv6 Quality of Service 3
 - Implementation Strategy for QoS for IPv6 3
 - Packet Classification in IPv6 4
- How to Configure IPv6 Quality of Service 4
 - Classifying Traffic in IPv6 Networks 4
 - Specifying Marking Criteria for IPv6 Packets 4
 - Using the Match Criteria to Manage IPv6 Traffic Flows 5
- Configuration Examples for IPv6 Quality of Service 6
 - Example: Verifying Cisco Express Forwarding Switching 6
 - Example: Verifying Packet Marking Criteria 7
 - Example: Matching DSCP Value 12
- Additional References 13
- Feature Information for IPv6 Quality of Service 14

CHAPTER 3

IPv6 QoS: MQC Packet Classification 15

- Finding Feature Information 15
- Information About IPv6 QoS: MQC Packet Classification 15
 - Implementation Strategy for QoS for IPv6 15
 - Packet Classification in IPv6 16
- How to Configure IPv6 QoS: MQC Packet Classification 16
 - Classifying Traffic in IPv6 Networks 16
 - Using the Match Criteria to Manage IPv6 Traffic Flows 16

Confirming the Service Policy	17
Configuration Examples for IPv6 QoS: MQC Packet Classification	19
Example: Matching DSCP Value	19
Additional References	20
Feature Information for IPv6 QoS: MQC Packet Classification	21

CHAPTER 4**Packet Classification Based on Layer 3 Packet Length 23**

Finding Feature Information	23
Prerequisites for Packet Classification Based on Layer 3 Packet Length	23
Restrictions for Packet Classification Based on Layer 3 Packet Length	24
Information About Packet Classification Based on Layer 3 Packet Length	24
MQC and Packet Classification Based on Layer 3 Packet Length	24
How to Configure Packet Classification Based on Layer 3 Packet Length	25
Configuring the Class Map to Match on Layer 3 Packet Length	25
Attaching the Policy Map to an Interface	26
Verifying the Layer 3 Packet Length Classification Configuration	27
Troubleshooting Tips	28
Configuration Examples for Packet Classification Based on Layer 3 Packet Length	29
Example Configuring the Layer 3 Packet Length as a Match Criterion	29
Example Verifying the Layer 3 Packet Length Setting	29
Additional References	30
Feature Information for Packet Classification Based on Layer 3 Packet Length	31

CHAPTER 5**IPv6 QoS: MQC Packet Marking/Remarking 33**

Finding Feature Information	33
Information About IPv6 QoS: MQC Packet Marking/Remarking	33
Implementation Strategy for QoS for IPv6	33
Policies and Class-Based Packet Marking in IPv6 Networks	34
Traffic Policing in IPv6 Environments	34
How to Specify IPv6 QoS: MQC Packet Marking/Remarking	34
Specifying Marking Criteria for IPv6 Packets	34
Configuration Examples for IPv6 QoS: MQC Packet Marking/Remarking	35
Example: Verifying Packet Marking Criteria	35
Additional References	40

Feature Information for IPv6 QoS: MQC Packet Marking/Remarking 41

CHAPTER 6

Marking Network Traffic 43

- Finding Feature Information 43
- Prerequisites for Marking Network Traffic 43
- Restrictions for Marking Network Traffic 43
- Information About Marking Network Traffic 44
 - Purpose of Marking Network Traffic 44
 - Benefits of Marking Network Traffic 44
 - How to Mark Traffic Attributes 45
 - Mark Traffic Attributes Using a set Command 45
 - Traffic Marking Procedure Flowchart 46
 - Method for Marking Traffic Attributes 47
 - Using a set Command 47
 - MQC and Network Traffic Marking 47
 - Traffic Classification Compared with Traffic Marking 47
- How to Mark Network Traffic 48
 - Creating a Class Map for Marking Network Traffic 48
 - Creating a Table Map for Marking Network Traffic 49
 - Creating a Policy Map for Applying a QoS Feature to Network Traffic 50
 - What to Do Next 52
 - Attaching the Policy Map to an Interface 52
- Configuration Examples for Marking Network Traffic 53
 - Example: Creating a Class Map for Marking Network Traffic 53
 - Example Creating a Policy Map for Applying a QoS Feature to Network Traffic 54
 - Example: Attaching the Policy Map to an Interface 54
- Additional References for Marking Network Traffic 54
- Feature Information for Marking Network Traffic 55

CHAPTER 7

Classifying Network Traffic 57

- Finding Feature Information 57
- Information About Classifying Network Traffic 57
 - Purpose of Classifying Network Traffic 57
 - Restrictions for Classifying Network Traffic 58

- Benefits of Classifying Network Traffic 58
- MQC and Network Traffic Classification 58
- Network Traffic Classification match Commands and Match Criteria 58
- Traffic Classification Compared with Traffic Marking 60
- How to Classify Network Traffic 61
 - Creating a Class Map for Classifying Network Traffic 61
 - Creating a Policy Map for Applying a QoS Feature to Network Traffic 62
 - What to Do Next 64
 - Attaching the Policy Map to an Interface 64
- Configuration Examples for Classifying Network Traffic 66
 - Example Creating a Class Map for Classifying Network Traffic 66
 - Example Creating a Policy Map for Applying a QoS Feature to Network Traffic 67
 - Example Attaching the Policy Map to an Interface 67
- Additional References 67
- Feature Information for Classifying Network Traffic 68

CHAPTER 8

Class-Based Ethernet CoS Matching and Marking 71

- Finding Feature Information 71
- Prerequisites for Class-Based Ethernet CoS Matching and Marking 71
- Information About Class-Based Ethernet CoS Matching and Marking 72
 - Layer 2 CoS Values 72
- How to Configure Class-Based Ethernet CoS Matching and Marking 72
 - Configuring Class-Based Ethernet CoS Matching 72
 - Configuring Class-Based Ethernet CoS Marking 75
- Configuration Examples for Class-Based Ethernet CoS Matching and Marking 77
 - Example: Configuring Class-Based Ethernet CoS Matching 77
 - Example: Class-Based Ethernet CoS Marking 77
- Additional References for Class-Based Ethernet CoS Matching and Marking 78
- Feature Information for Class-Based Ethernet CoS Matching & Marking 78

CHAPTER 9

QoS Group Match and Set for Classification and Marking 81

- Finding Feature Information 81
- Prerequisites for QoS Group Match and Set for Classification and Marking 81
- Restrictions for QoS Group Match and Set for Classification and Marking 82

Information About QoS Group Match and Set for Classification and Marking	82
QoS Group Values	82
MQC and Traffic Classification and Marking Based on QoS Group Value	82
How to Configure QoS Group Match and Set for Classification and Marking	83
Configuring the Class Map to Match on the QoS Group Value	83
Creating a Policy Map Using the QoS Group Value	84
Attaching the Policy Map to an Interface	85
Configuration Examples for QoS Group Match and Set for Classification and Marking	86
Example: QoS Group Match and Set for Classification and Marking	86
Additional References for QoS Group Match and Set for Classification and Marking	87
Feature Information for QoS Group Match and Set for Classification and Marking	88

CHAPTER 10
Quality of Service for VPNs 89

Finding Feature Information	89
Information About Quality of Service for Virtual Private Networks	89
QoS for VPNs	89
How to Configure QoS for VPNs	90
Configuring QoS When Using IPsec VPNs	90
Configuration Examples for QoS for VPNs	91
Example Configuring QoS When Using IPsec VPNs	91
Additional References for QoS for VPNs	91
Feature Information for QoS for VPNs	92

CHAPTER 11
QoS Match VLAN 95

Finding Feature Information	95
Information About Match VLAN	95
QoS Match VLAN	95
How to Configure Match VLAN	96
Classifying Network Traffic per VLAN	96
Configuration Examples for Match VLAN	98
Example: Classifying Network Traffic per VLAN	98
Additional References for QoS for Match VLAN	99
Feature Information for QoS for Match VLAN	99

CHAPTER 12	Inbound Policy Marking for dVTI	101
	Finding Feature Information	101
	Prerequisites for Inbound Policy Marking for dVTI	101
	Restrictions for Inbound Policy Marking for dVTI	101
	Information About Inbound Policy Marking for dVTI	102
	Inbound Policy Marking	102
	Dynamic Virtual Tunnel Interfaces Overview	102
	Security Associations and dVTI	103
	How to Use Inbound Policy Marking for dVTI	103
	Creating a Policy Map	103
	Attaching a Policy Map to a dVTI	104
	Configuration Example for Inbound Policy Marking for dVTI	105
	Example 1	105
	Example 2 Configuring Inbound Policy Marking	105
	Additional References	106
	Feature Information for Using Inbound Policy Marking for dVTI	108

CHAPTER 13	QoS Tunnel Marking for GRE Tunnels	109
	Finding Feature Information	109
	Prerequisites for QoS Tunnel Marking for GRE Tunnels	109
	Restrictions for QoS Tunnel Marking for GRE Tunnels	109
	Information About QoS Tunnel Marking for GRE Tunnels	110
	GRE Definition	110
	GRE Tunnel Marking Overview	110
	GRE Tunnel Marking and the MQC	111
	GRE Tunnel Marking and DSCP or IP Precedence Values	111
	Benefits of GRE Tunnel Marking	111
	GRE Tunnel Marking and Traffic Policing	111
	GRE Tunnel Marking Values	112
	How to Configure Tunnel Marking for GRE Tunnels	112
	Configuring a Class Map	112
	Creating a Policy Map	113
	Attaching the Policy Map to an Interface or a VC	115

Verifying the Configuration of Tunnel Marking for GRE Tunnels	116
Troubleshooting Tips	117
Configuration Examples for QoS Tunnel Marking for GRE Tunnels	117
Example: Configuring Tunnel Marking for GRE Tunnels	117
Example: Verifying the Tunnel Marking for GRE Tunnels Configuration	118
Additional References	119
Feature Information for QoS Tunnel Marking for GRE Tunnels	120

CHAPTER 14**QoS for dVTI 121**

Finding Feature Information	121
Restrictions for QoS dVTI	121
Information About QoS for dVTI	122
Configuration Examples for QoS for dVTI	122
Example 2 Layer Rate LLQ for dVTI	122
Example 2 Layer Rate LLQ with Bandwidth Guarantees for dVTI	123
Example 3 Layer QoS for dVTI	123
Additional References	124
Feature Information for QoS for dVTI	125

CHAPTER 15**Classifying and Marking MPLS EXP 127**

Finding Feature Information	127
Prerequisites for Classifying and Marking MPLS EXP	127
Restrictions for Classifying and Marking MPLS EXP	127
Information About Classifying and Marking MPLS EXP	128
Classifying and Marking MPLS EXP Overview	128
MPLS Experimental Field	128
Benefits of MPLS EXP Classification and Marking	129
How to Classify and Mark MPLS EXP	129
Classifying MPLS Encapsulated Packets	129
Marking MPLS EXP on All Imposed Labels	130
Marking MPLS EXP on Label Switched Packets	131
Configuring Conditional Marking	132
Configuration Examples for Classifying and Marking MPLS EXP	134
Example: Classifying MPLS Encapsulated Packets	134

Example: Marking MPLS EXP on All Imposed Labels **135**

Example: Marking MPLS EXP on Label Switched Packets **136**

Example: Configuring Conditional Marking **136**

Additional References **137**

Feature Information for Classifying and Marking MPLS EXP **138**



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).



CHAPTER 2

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 3](#)
- [Information About IPv6 Quality of Service, on page 3](#)
- [How to Configure IPv6 Quality of Service, on page 4](#)
- [Configuration Examples for IPv6 Quality of Service, on page 6](#)
- [Additional References, on page 13](#)
- [Feature Information for IPv6 Quality of Service, on page 14](#)

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 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

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy map <i>policy-map-name</i> Example: 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"> • Enter name of policy map you want to create.
Step 4	class <i>{class-name class-default}</i> Example: 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 dscp-value]*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map <i>{class-name}</i> class-default Example: <pre>Router(config-pmap-c)# class cls1</pre>	Creates the specified class and enters QoS class-map configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> • match precedence <i>precedence-value</i> [<i>precedence-value precedence-value</i>] • match access-group name <i>ipv6-access-group</i> • match [ip] dscp <i>dscp-value</i> [<i>dscp-value dscp-value dscp-value dscp-value dscp-value</i>] Example: <pre>Router(config-pmap-c)# match precedence 5</pre> Example: <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 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 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 d1ci 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 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 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	Cisco IOS Master Commands List, All Releases
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"> • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • CISCO-CLASS-BASED-QOS-MIB 	<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>http://www.cisco.com/go/mibs</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.	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 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: match dscp , match precedence , set dscp , set precedence . The following commands were introduced or modified: match access-group name , match dscp , match precedence , set dscp , set precedence .



CHAPTER 3

IPv6 QoS: MQC Packet Classification

- [Finding Feature Information, on page 15](#)
- [Information About IPv6 QoS: MQC Packet Classification, on page 15](#)
- [How to Configure IPv6 QoS: MQC Packet Classification, on page 16](#)
- [Configuration Examples for IPv6 QoS: MQC Packet Classification, on page 19](#)
- [Additional References, on page 20](#)
- [Feature Information for IPv6 QoS: MQC Packet Classification, on page 21](#)

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, queueing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets. These features are available at both the process switching and Cisco Express Forwarding switching paths of IPv6.

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

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

- Know which applications in your network need QoS.

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

Packet Classification in IPv6

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

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

How to Configure IPv6 QoS: MQC Packet Classification

Classifying Traffic in IPv6 Networks

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

Using the Match Criteria to Manage IPv6 Traffic Flows

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables such as privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map <i>{class-name class-default}</i> Example: <pre>Router(config-pmap-c)# class cls1</pre>	Creates the specified class and enters QoS class-map configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> • match precedence <i>precedence-value [precedence-value precedence-value]</i> • match access-group name <i>ipv6-access-group</i> • match [ip] dscp <i>dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]</i> Example: <pre>Router(config-pmap-c)# match precedence 5</pre> Example: <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.

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> multipoint point-to-point Example: Router(config)# interface gigabitethernet1/1/0 point-to-point	Enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [<i>secondary</i>] Example: 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 [<i>name</i>] <i>vpi / vci</i> [<i>ces</i> <i>ilmi</i> <i>qsaal</i> <i>smds</i>] Example: 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	tx-ring-limit <i>ring-limit</i> Example: <pre>Router(config-if-atm-vc)# tx-ring-limit 10</pre>	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"> 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} <i>policy-map-name</i> Example: <pre>Router(config-if-atm-vc)# service-policy output policy9</pre>	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"> 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 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	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	<i>Cisco IOS IPv6 Feature Mapping</i>
Classifying Network Traffic	“Classifying Network Traffic” module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

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 7: Feature Information for IPv6 QoS: MQC Packet Classification

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



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, on page 23](#)
- [Prerequisites for Packet Classification Based on Layer 3 Packet Length, on page 23](#)
- [Restrictions for Packet Classification Based on Layer 3 Packet Length, on page 24](#)
- [Information About Packet Classification Based on Layer 3 Packet Length, on page 24](#)
- [How to Configure Packet Classification Based on Layer 3 Packet Length, on page 25](#)
- [Configuration Examples for Packet Classification Based on Layer 3 Packet Length, on page 29](#)
- [Additional References, on page 30](#)
- [Feature Information for Packet Classification Based on Layer 3 Packet Length, on page 31](#)

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-map cisco** 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** {*maxmaximum-length-value* [*minminimum-length-value*] | *minminimum-length-value* [*maxmaximum-length-value*]}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> Example: Router(config)# class-map class1	Specifies the name of the class map to be created and enters class-map configuration mode. • Enter the class map name.
Step 4	match packet length { <i>maxmaximum-length-value</i> [<i>minminimum-length-value</i>] <i>minminimum-length-value</i> [<i>maxmaximum-length-value</i>]} Example: 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. • Enter the Layer 3 packet length in bytes.

	Command or Action	Purpose
Step 5	end Example: <pre>Router(config-cmap)# end</pre>	(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*] *vpilvci* [*ilmi* | *qsaal* | *smds*]
5. **service-policy** {*input* | *output*} *policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <pre>Device(config)# interface serial4/0/0</pre>	Configures an interface (or subinterface) type and enters interface configuration mode
Step 4	pvc [<i>name</i>] <i>vpilvci</i> [<i>ilmi</i> <i>qsaal</i> <i>smds</i>] Example: <pre>Device(config-if)# pvc cisco 0/16 ilmi</pre>	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode. 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.

	Command or Action	Purpose
Step 5	<p>service-policy {input output} <i>policy-map-name</i></p> <p>Example:</p> <pre>Device(config-if)# service-policy input policy1</pre> <p>Example:</p> <pre>Device(config-if-atm-vc)# service-policy input policy1</pre>	<p>Specifies the name of the policy map to be attached to either the input or output direction of the interface.</p> <p>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.</p>
Step 6	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> <p>Example:</p> <pre>Device(config-if-atm-vc)# end</pre>	<p>(Optional) Exits interface configuration or ATM VC configuration mode and returns to privileged EXEC mode.</p>

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*]] [*dlcid/ci*] [**input| output**]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show class-map [<i>class-map-name</i>]</p> <p>Example:</p> <pre>Router# show class-map class1</pre>	<p>(Optional) Displays all information about a class map, including the match criterion.</p> <ul style="list-style-type: none"> • Enter the class map name.

	Command or Action	Purpose
Step 3	<p>show policy-map interface <i>interface-name</i> [vc [<i>vpi</i>] <i>vci</i>] [<i>dlcid</i>/<i>lci</i>] [input output]</p> <p>Example:</p> <pre>Router# show policy-map interface serial4/0/0</pre>	<p>(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.</p> <ul style="list-style-type: none"> • Enter the interface name.
Step 4	<p>exit</p> <p>Example:</p> <pre>Router# exit</pre>	<p>(Optional) Exits privileged EXEC mode.</p>

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	<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"> • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • 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: 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 8: 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 12.2(18)SXE 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. In Release 12.2(13)T, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(18)SXE. This feature was integrated into Cisco IOS XE Release 2.2. The following commands were introduced or modified: matchpacketlength (class-map), showclass-map , showpolicy-mapinterface .



CHAPTER 5

IPv6 QoS: MQC Packet Marking/Remarking

- [Finding Feature Information, on page 33](#)
- [Information About IPv6 QoS: MQC Packet Marking/Remarking, on page 33](#)
- [How to Specify IPv6 QoS: MQC Packet Marking/Remarking, on page 34](#)
- [Configuration Examples for IPv6 QoS: MQC Packet Marking/Remarking, on page 35](#)
- [Additional References, on page 40](#)
- [Feature Information for IPv6 QoS: MQC Packet Marking/Remarking, on page 41](#)

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 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.

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 (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

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables such as privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy map <i>policy-map-name</i> Example: 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">• Enter name of policy map you want to create.
Step 4	class { <i>class-name</i> class-default } Example: 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.

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:

```
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 9: 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
```

Example: Verifying Packet Marking Criteria

```

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 10: 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).
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 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 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.

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

Table 11: 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

Bandwidth Range	Number of Dynamic Queues
More than 512 kbps	256

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

Table 12: 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 13: 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	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>

Related Topic	Document Title
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: 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 14: Feature Information for IPv6 QoS: MQC Packet Marking/Remarking

Feature Name	Releases	Feature Information
IPv6 QoS: MQC Packet Marking/Remarking	Cisco IOS XE Release 2.1	Class-based marking allows you to set the IPv6 precedence and DSCP values for traffic management.



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, on page 43](#)
- [Prerequisites for Marking Network Traffic, on page 43](#)
- [Restrictions for Marking Network Traffic, on page 43](#)
- [Information About Marking Network Traffic, on page 44](#)
- [How to Mark Network Traffic, on page 48](#)
- [Configuration Examples for Marking Network Traffic, on page 53](#)
- [Additional References for Marking Network Traffic, on page 54](#)
- [Feature Information for Marking Network Traffic, on page 55](#)

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:

- CoS value of an outgoing packet
- Discard-class value
- 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.
- Weighted random early detection (WRED) uses precedence values or DSCP values to determine the probability that the traffic will be dropped. Therefore, the Precedence and DSCP can be used in conjunction with WRED.

How to Mark 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.

This method is further described in the section that follows.

Mark Traffic Attributes 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 15: 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 discard-class	discard-class value	Layer 2	
set dscp	DSCP value in the ToS byte	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



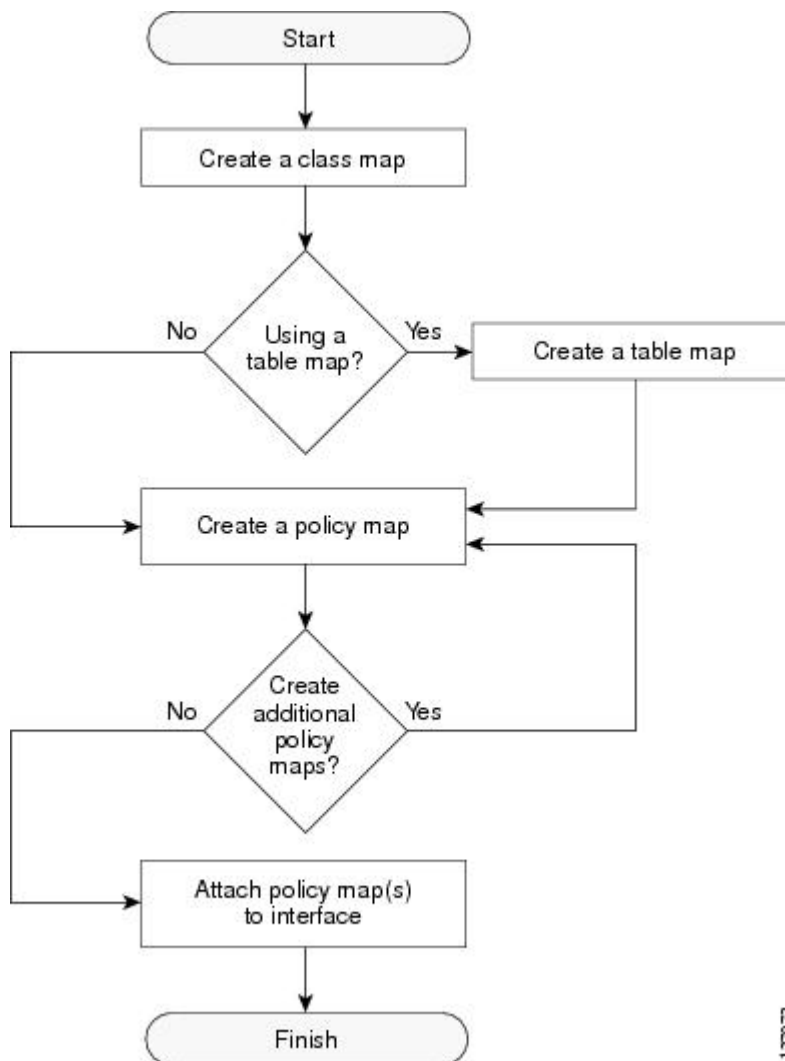
Note The `set qos-group` can be used for L2 traffic on the Cisco ASR 900 RSP3 Module.

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

Traffic Marking Procedure Flowchart

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

Figure 1: Traffic Marking Procedure Flowchart



127073

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

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 16: 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. 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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> [match-all match-any] Example: <pre>Device(config)# class-map class1</pre>	Creates a class map to be used for matching traffic to a specified class and enters class-map configuration mode.
Step 4	match protocol <i>protocol-name</i> Example: <pre>Device(config-cmap)# match protocol ftp</pre>	(Optional) Configures the match criterion for a class map on the basis of the specified protocol. 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.
Step 5	end Example: <pre>Device(config-cmap)# end</pre>	(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 Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	table-map <i>table-map-name</i> map from <i>from-value</i> to <i>to-value</i> [default <i>default-action-or-value</i>] Example: Example: <pre>Device(config)# table-map table-map1 map from 2 to 1</pre>	Creates a table map using the specified name and enters tablemap configuration mode. <ul style="list-style-type: none"> • Enter the name of the table map you want to create. • Enter each value mapping on a separate line. Enter as many separate lines as needed for the values you want to map. • The default keyword and <i>default-action-or-value</i> argument set the default value (or action) to be used if a value is not explicitly designated.
Step 4	end Example: <pre>Device(config-tablemap)# end</pre>	(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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: Device(config)# policy-map policy1	Specifies the name of the policy map and enters policy-map configuration mode.
Step 4	class {<i>class-name</i> class-default} Example: 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 <i>cos-value</i> Example: Device(config-pmap-c)# set cos 2	(Optional) Sets the CoS value in the type of service (ToS) byte. 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 Example: Device(config-pmap-c)# end	Returns to privileged EXEC mode.
Step 7	show policy-map Example: Device# show policy-map	(Optional) Displays all configured policy maps.
Step 8	show policy-map <i>policy-map</i> class <i>class-name</i> Example: 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

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 Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> [name-tag] Example: <pre>Device(config)# interface serial4/0/0</pre>	Configures an interface type and enters interface configuration mode.
Step 4	pvc [<i>name</i>] <i>vpi/vci</i> [ilmi qsaal smds l2transport] Example: <pre>Device(config-if)# pvc cisco 0/16</pre>	(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. 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.

	Command or Action	Purpose
Step 5	exit Example: <pre>Device(config-atm-vc)# exit</pre>	(Optional) Returns to interface configuration mode. 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 Example: <pre>Device(config-if)# service-policy input policy1</pre>	Attaches a policy map to an input or output interface. 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 Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	show policy-map interface type number Example: <pre>Device# show policy-map interface serial4/0/0</pre>	(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. Traffic 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#
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 Ethernet interface 0.

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
MQC	“Applying QoS Features Using the MQC” module
Classifying network traffic	“Classifying Network Traffic” module

Technical Assistance

Description	Link
<p>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.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

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 17: Feature Information for Marking Network Traffic

Feature Name	Software Releases	Feature Configuration Information
<p>Class-Based Marking</p>	<p>Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.2SE</p>	<p>The Class-Based Packet Marking feature provides a user-friendly command-line interface (CLI) for efficient packet marking by which users can differentiate packets.</p> <p>This feature was implemented on Cisco ASR 1000 Series Routers.</p> <p>This feature was integrated into Cisco IOS XE Release 2.2.</p>
<p>Enhanced Packet Marking</p>	<p>Cisco IOS XE Release 3.9S Cisco IOS XE Release 3.14S</p>	<p>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.</p> <p>In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V Series Routers</p> <p>In Cisco IOS XE Release 3.14S, support was added for the Cisco 4000 Series Integrated Services Routers.</p>

Feature Name	Software Releases	Feature Configuration Information
QoS Packet Marking	<p>Cisco IOS XE Release 2.1</p> <p>Cisco IOS XE Release 2.2</p> <p>Cisco IOS XE Release 3.5S</p> <p>Cisco IOS XE Release 3.9S</p> <p>Cisco IOS XE Release 3.14S</p>	<p>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.</p> <p>This feature was implemented on Cisco ASR 1000 Series Routers.</p> <p>This feature was integrated into Cisco IOS XE Software Release 2.2.</p> <p>In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.</p> <p>In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V Series Routers.</p> <p>In Cisco IOS XE Release 3.14S, support was added for the Cisco 4000 Series Integrated Services Routers.</p>
IP DSCP marking for Frame-Relay PVC	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
PXF Based Frame Relay DE Bit Marking	<p>12.2(31)SB2</p> <p>15.0(1)S</p>	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, on page 57](#)
- [Information About Classifying Network Traffic, on page 57](#)
- [How to Classify Network Traffic, on page 61](#)
- [Configuration Examples for Classifying Network Traffic, on page 66](#)
- [Additional References, on page 67](#)
- [Feature Information for Classifying Network Traffic, on page 68](#)

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 see what kinds of traffic you have, organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria, and treat some types of traffic differently than others. 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.

Restrictions for Classifying Network Traffic

- When access lists are used for classification in QoS policies, the following limitations are applicable:
 - The use of wildcards (For example, the any keyword, masks using zeros like 172.0.0.0, subnet masks) in source or destination addresses of permit or deny statements causes a greater consumption of memory on the device. This behavior is particularly important on devices that use software based classification (like Cisco ISR 4000 series devices or CSR1000v) and lower-end platforms with smaller memory capacities and ternary content-addressable memor (TCAMs).
 - The use of deny statements causes greater consumption of TCAM resources on systems that use HW-based classification (ASR1k).

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 18: match Commands and Corresponding Match Criterion

match Commands²	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 protocol citrix	Citrix protocol
match protocol fasttrack	FastTrack peer-to-peer traffic

match Commands ²	Match Criterion
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

² 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 19: 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.

Feature	Traffic Classification	Traffic Marking
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. 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 Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> [match-all match-any] Example: 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. • Enter the class map name.

	Command or Action	Purpose
Step 4	match fr-dlci <i>dlci-number</i> Example: <pre>Router(config-cmap)# match fr-dlci 500</pre>	(Optional) Specifies the match criteria in a class map. 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 Example: <pre>Router(config-cmap)# end</pre>	(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 Step 5. 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.



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 Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: <pre>Router(config)# policy-map policy1</pre>	Specifies the name of the policy map to be created and enters policy-map configuration mode. <ul style="list-style-type: none"> • Enter the policy map name.
Step 4	class {<i>class-name</i> class-default} Example: <pre>Router(config-pmap)# class class1</pre>	Specifies the name of the class and enters policy-map class configuration mode. This class is associated with the class map created earlier. <ul style="list-style-type: none"> • Enter the name of the class or enter the class-default keyword.
Step 5	bandwidth {<i>bandwidth-kbps</i> remaining percent <i>percentage</i> percent <i>percentage</i>} Example: <pre>Router(config-pmap-c)# bandwidth percent 50</pre>	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. <ul style="list-style-type: none"> • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. <p>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.</p>
Step 6	end Example: <pre>Router(config-pmap-c)# end</pre>	Returns to privileged EXEC mode.
Step 7	show policy-map	(Optional) Displays all configured policy maps.
Step 8		or
Step 9	show policy-map <i>policy-map</i> class <i>class-name</i> Example:	(Optional) Displays the configuration for the specified class of the specified policy map. <ul style="list-style-type: none"> • Enter the policy map name and the class name.

	Command or Action	Purpose
Step 10	Router# show policy-map	
Step 11		
Step 12	Router# show policy-map policy1 class class1	
Step 13	exit Example: 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-dlci** 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*] *vpilvci* [**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	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface type number [name-tag] Example: <pre>Router(config)# interface serial4/0/0</pre>	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> Enter the interface type and number.
Step 4	pvc [name] vpi/vci [ilmi qsaal smds l2transport] Example: <pre>Router(config-if)# pvc cisco 0/16</pre>	(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. <ul style="list-style-type: none"> Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. <p>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 .</p>
Step 5	exit Example: <pre>Router(config-atm-vc)# exit</pre>	(Optional) Returns to interface configuration mode. <p>Note This step is required only if you are attaching the policy map to an ATM PVC and you completed Step 4. If you are not attaching the policy map to an ATM PVC, advance to Step 6.</p>
Step 6	service-policy {input output} policy-map-name Example: <pre>Router(config-if)# service-policy input policy1</pre>	Attaches a policy map to an input or output interface. <ul style="list-style-type: none"> Enter the policy map name. <p>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.</p>

	Command or Action	Purpose
Step 7	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 8	show policy-map interface <i>type number</i> Example: 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. • Enter the type and number.
Step 9	exit Example: 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-dlci` 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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
MQC	"Applying QoS Features Using the MQC" module
Marking network traffic	"Marking Network Traffic" module

Related Topic	Document Title
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: 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 20: Feature Information for Classifying Network Traffic

Feature Name	Releases	Feature Information
Packet Classification Using Frame Relay DLCI Number	12.2(13)T Cisco IOS XE Release 2.1 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. 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. 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. The following command was introduced or modified: matchmplsexperimental .



CHAPTER 8

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, on page 71](#)
- [Prerequisites for Class-Based Ethernet CoS Matching and Marking, on page 71](#)
- [Information About Class-Based Ethernet CoS Matching and Marking, on page 72](#)
- [How to Configure Class-Based Ethernet CoS Matching and Marking, on page 72](#)
- [Configuration Examples for Class-Based Ethernet CoS Matching and Marking, on page 77](#)
- [Additional References for Class-Based Ethernet CoS Matching and Marking, on page 78](#)
- [Feature Information for Class-Based Ethernet CoS Matching & Marking , on page 78](#)

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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> Example: Device(config)# class-map voice	Specifies the name of the class map to be created and enters class-map configuration mode.
Step 4	match cos <i>cos-value</i> Example: Device(config-cmap)# match cos 7	Configures the class map to match traffic on the basis of the CoS value.
Step 5	exit Example: Device(config-cmap)# exit	(Optional) Exits class-map configuration mode.
Step 6	class-map <i>class-map-name</i> Example: Device(config)# class-map video-and-data	Specifies the name of the class map to be created and enters class-map configuration mode. <ul style="list-style-type: none"> • Enter the class map name.
Step 7	match cos <i>cos-value</i> Example: Device(config-cmap)# match cos 5	Configures the class map to match traffic on the basis of the CoS value.
Step 8	exit Example: Device(config-cmap)# exit	(Optional) Exits class-map configuration mode.
Step 9	policy-map <i>policy-map-name</i> Example: Device(config)# policy-map cos-based-treatment	Specifies the name of the policy map created earlier and enters policy-map configuration mode.

	Command or Action	Purpose
Step 10	class <i>{class-name class-default}</i> Example: 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 <i>level</i> Example: Device(config-pmap-c)# priority level 1	Specifies the level of the priority service.
Step 12	exit Example: Device(config-pmap-c)# exit	(Optional) Exits policy-map class configuration mode.
Step 13	class <i>{class-name class-default}</i> Example: 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 <i>percentage</i> Example: Device(config-pmap-c)# bandwidth remaining percent 20	Specifies the amount of bandwidth assigned to the class.
Step 15	exit Example: Device(config-pmap-c)# exit	(Optional) Exits policy-map class configuration mode.
Step 16	exit Example: Device(config-pmap)# exit	(Optional) Exits policy-map configuration mode.
Step 17	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 1/0/1	Configures an interface (or subinterface) type and enters interface configuration mode.
Step 18	service-policy <i>{input output} policy-map-name</i> Example:	Specifies the name of the policy map to be attached to either the input or output direction of the interface.

	Command or Action	Purpose
	<pre>Device(config-if)# service-policy output cos-based-treatment</pre>	<p>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.</p>
Step 19	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	(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	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: Device(config)# policy-map cos-set	Specifies the name of the policy map created earlier and enters policy-map configuration mode.
Step 4	class {<i>class-name</i> class-default} Example: 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 <i>cos-value</i> Example: Device(config-pmap-c)# set cos 1	Sets the packet's CoS value.
Step 6	exit Example: Device(config-pmap-c)# exit	Exits policy-map class configuration mode.
Step 7	class {<i>class-name</i> class-default} Example: 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 <i>cos-value</i> Example: Device(config-pmap-c)# set cos 2	Sets the packet's CoS value.
Step 9	end Example: 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
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
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 21: 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 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2SE	This feature allows you to mark and match packets using Class of Service (CoS) values. The following commands were introduced or modified: match cos , set cos .
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 9

QoS Group Match and Set for Classification and Marking

This feature provides the capability of matching and classifying traffic on the basis of the QoS group value.

- [Finding Feature Information, on page 81](#)
- [Prerequisites for QoS Group Match and Set for Classification and Matching, on page 81](#)
- [Restrictions for QoS Group Match and Set for Classification and Marking, on page 82](#)
- [Information About QoS Group Match and Set for Classification and Marking, on page 82](#)
- [How to Configure QoS Group Match and Set for Classification and Marking, on page 83](#)
- [Configuration Examples for QoS Group Match and Set for Classification and Marking, on page 86](#)
- [Additional References for QoS Group Match and Set for Classification and Marking, on page 87](#)
- [Feature Information for QoS Group Match and Set for Classification and Marking, on page 88](#)

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 Group Match and Set for Classification and Matching

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 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 QoS Group Match and Set for Classification and Marking

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.

Information About QoS Group Match and Set for Classification and Marking

QoS Group Values

The QoS group value is a number between 0 and 99 that is set using the **set qos-group** command. The group value can be used to classify packets into QoS groups based on a prefix, autonomous system, and community string. A packet is marked with a QoS group value only while it is being processed within the device. The QoS group value is not included in the packet's header when the packet is transmitted over the output interface. However, the QoS group value can be used to set the value of a Layer 2 or Layer 3 field that is included as part of the packet's headers (such as the MPLS EXP, CoS, and DSCP fields).

MQC and Traffic Classification and Marking Based on QoS Group Value

Use the MQC to enable packet classification and marking based on the QoS group value. The MQC is a CLI that allows you to create traffic classes and 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 that is used to classify traffic (which is then associated with a traffic policy).

The MQC consists of the following three processes:

- Defining a traffic class using 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 using the **service-policy** command.

A traffic class contains three major elements: a name, one or more **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-map cisco** 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.

A policy map also contains three major elements: a name, a traffic class to associate with one or more QoS features, and any individual **set** commands you want to use to mark the network traffic.

How to Configure QoS Group Match and Set for Classification and Marking

Configuring the Class Map to Match on the QoS Group Value

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match qos-group** *qos-group-value*
5. **end**

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 <i>class-map-name</i> Example: Device(config)# class-map class1	Specifies the name of the class map to be created and enters class-map configuration mode.
Step 4	match qos-group <i>qos-group-value</i> Example: Device(config-cmap)# match qos-group 30	Configures the class map to match traffic on the basis of the QoS group value. • Enter the exact value from 0 to 99 used to identify a QoS group value.
Step 5	end Example: Device(config-cmap)# end	(Optional) Exits class-map configuration mode and returns to privileged EXEC mode.

Creating a Policy Map Using the QoS Group Value

The following example shows how to create a policy map (policy1) using a pre-configured class (class1) and how to set the QoS group value based on the packet's original 802.1P CoS value.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set qos-group cos**
6. **end**
7. **show policy-map**
8. **show policy-map** *policy-map* **class** *class-name*
9. **exit**

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	policy-map <i>policy-map-name</i> Example: Device(config)# policy-map policy1	Specifies the name of the policy map created earlier and enters policy-map configuration mode.
Step 4	class { <i>class-name</i> class-default } Example: 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. • Enter the name of the class or enter the class-default keyword.
Step 5	set qos-group cos Example: Device(config-pmap-c)# set qos-group cos	Sets the QoS group value based on the packet's original 802.1P CoS value.
Step 6	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-pmap-c)# end	
Step 7	show policy-map Example: Device# show policy-map	(Optional) Displays all configured policy maps.
Step 8	show policy-map <i>policy-map</i> class <i>class-name</i> Example: Device# show policy-map policy1 class class1	(Optional) Displays the configuration for the specified class of the specified policy map.
Step 9	exit Example: Device# exit	(Optional) Exits 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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: <pre>Device(config)# interface serial4/0/0</pre>	Configures an interface (or subinterface) type and enters interface configuration mode
Step 4	pvc [<i>name</i>] <i>vpi/vci</i> [<i>ilmi</i> <i>qsaal</i> <i>smds</i>] Example: <pre>Device(config-if)# pvc cisco 0/16 ilmi</pre>	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode. 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 { <i>input</i> <i>output</i> } <i>policy-map-name</i> Example: <pre>Device(config-if)# service-policy input policy1</pre> Example: <pre>Device(config-if-atm-vc)# service-policy input policy1</pre>	Specifies the name of the policy map to be attached to either the input or output direction of the interface. 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 Example: <pre>Device(config-if)# end</pre> Example: <pre>Device(config-if-atm-vc)# end</pre>	(Optional) Exits interface configuration or ATM VC configuration mode and returns to privileged EXEC mode.

Configuration Examples for QoS Group Match and Set for Classification and Marking

Example: QoS Group Match and Set for Classification and Marking

The following example shows how to create a class map and policy map for QoS group values, and how to attach the policy to an interface.


```

Device> enable
Device# configure terminal
Device(config)# class-map class1
Device(config-cmap)# match qos-group 30
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set qos-group cos
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface serial4/0/0
Device(config-if)# service-policy input policy1
Device(config-if)# end

```

Additional References for QoS Group Match and Set for Classification and Marking

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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
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 Group Match and Set for Classification and 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 22: Feature Information for QoS Group Match and Set for Classification and Marking

Feature Name	Releases	Feature Information
QoS Group Match and Set for Classification and Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2SE	This feature provides the capability of matching and classifying traffic on the basis of the QoS group value. The following commands were introduced or modified: match qos-group , set qos-group .



CHAPTER 10

Quality of Service for VPNs

The QoS for VPNs feature provides a solution for making Cisco IOS QoS services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before the data is encrypted and tunneled. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

- [Finding Feature Information, on page 89](#)
- [Information About Quality of Service for Virtual Private Networks, on page 89](#)
- [How to Configure QoS for VPNs, on page 90](#)
- [Configuration Examples for QoS for VPNs, on page 91](#)
- [Additional References for QoS for VPNs, on page 91](#)
- [Feature Information for QoS for VPNs, on page 92](#)

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 Quality of Service for Virtual Private Networks

QoS for VPNs

The QoS for VPNs feature provides a solution for making Cisco IOS QoS services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before the data is encrypted and tunneled. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and

destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

How to Configure QoS for VPNs

Configuring QoS When Using IPsec VPNs

This task uses the **qos pre-classify** command to enable QoS preclassification for the packet. QoS preclassification is not supported for all fragmented packets. If a packet is fragmented, each fragment might receive different preclassifications.



Note This task is required only if you are using IPsec Virtual Private Networks (VPNs). Otherwise, this task is not necessary. For information about IPsec VPNs, see the “Configuring Security for VPNs with IPsec” module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num*
4. **exit**
5. **interface** *type number* [**name-tag**]
6. **qos pre-classify**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num</i> Example: Router(config)# crypto map mymap 10	Enters crypto map configuration mode and creates or modifies a crypto map entry. <ul style="list-style-type: none"> • Enter the crypto map name and sequence number.
Step 4	exit Example:	Returns to global configuration mode.

	Command or Action	Purpose
	<code>Router(config-crypto-map)# exit</code>	
Step 5	interface <i>type number</i> [name-tag] Example: <code>Router(config)# interface serial4/0/0</code>	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> • Enter the interface type and number.
Step 6	qos pre-classify Example: <code>Router(config-if)# qos pre-classify</code>	Enables QoS preclassification.
Step 7	end Example: <code>Router(config-if)# end</code>	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for QoS for VPNs

Example Configuring QoS When Using IPsec VPNs

The following is an example of configuring QoS when using IPsec VPNs. In this example, the **crypto map** command specifies the IPsec crypto map (mymap 10) to which the **qos pre-classify** command will be applied.

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10

Router(config-crypto-map)# qos pre-classify
Router(config-crypto-map)# exit
```

Additional References for QoS for VPNs

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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
Classifying network traffic	“Classifying Network Traffic” module

Related Topic	Document Title
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 VPNs

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 23: Feature Information for QoS for VPNs

Feature Name	Releases	Feature Information
Quality of Service for Virtual Private Networks	12.2(2)T Cisco IOS XE Release 3.9S	The QoS for VPNs feature provides a solution for making Cisco IOS QoS services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before the data is encrypted and tunneled. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

Feature Name	Releases	Feature Information
QoS: Traffic Pre-classification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.



CHAPTER 11

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, on page 95](#)
- [Information About Match VLAN, on page 95](#)
- [How to Configure Match VLAN, on page 96](#)
- [Configuration Examples for Match VLAN, on page 98](#)
- [Additional References for QoS for Match VLAN, on page 99](#)
- [Feature Information for QoS for Match VLAN, on page 99](#)

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 Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map { match-any match-all } <i>class-map-name</i> Example: Router(config)# class-map match-any Blue_VRF	Creates a class map and enters class map configuration mode.

	Command or Action	Purpose
Step 4	match vlan <i>vlan-id-number</i> Example: Router(config-cmap)# match vlan 101	Matches traffic on the basis of the range of VLAN identification numbers specified.
Step 5	exit Example: Router(config-cmap)# exit	Returns to global configuration mode.
Step 6	policy-map <i>policy-map-name</i> Example: 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 <i>class-map-name</i> Example: 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 <i>percent</i> Example: Router(config-pmap-c)# bandwidth percent 30	Specifies the bandwidth allocated for a class belonging to a policy map.
Step 9	exit Example: Router(config-pmap-c)# exit	Returns to policy-map configuration mode.
Step 10	exit Example: Router(config-pmap)# exit	Returns to global configuration mode.
Step 11	policy-map <i>policy-map-name</i> Example: 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 <i>class-map-name</i> Example: 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.

	Command or Action	Purpose
Step 13	shape {average peak} <i>cir</i> Example: Router(config-pmap-c)# shape average 9000000000	Specifies the average rate traffic shaping. <ul style="list-style-type: none"> The Committed information rate (CIR), is specified in bits per second (bps).
Step 14	service-policy {input output} <i>policy-map-name</i> Example: 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 Example: Router(config-pmap-c)# exit	Returns to policy-map configuration mode.
Step 16	exit Example: Router(config-pmap)# exit	Returns to global configuration mode.
Step 17	interface <i>type number</i> [name-tag] Example: Router(config)# interface FastEthernet 0/0.1	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> Enter the interface type and number.
Step 18	service-policy {input output} <i>policy-map-name</i> Example: 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.
Step 19	end Example: 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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
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 24: Feature Information for QoS for Match VLAN

Feature Name	Releases	Feature Information
QoS: Match VLAN	12.2(31)SB2 Cisco IOS XE Release 2.1 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 This feature was introduced on Cisco ASR 1000 Series Routers.



CHAPTER 12

Inbound Policy Marking for dVTI

This document provides conceptual information and tasks for using the Inbound Policy Marking for Dynamic Virtual Tunnel Interface feature, which allows you to attach a policy map to a dVTI so that marking instructions are applied to inbound packets.

- [Finding Feature Information, on page 101](#)
- [Prerequisites for Inbound Policy Marking for dVTI, on page 101](#)
- [Restrictions for Inbound Policy Marking for dVTI, on page 101](#)
- [Information About Inbound Policy Marking for dVTI, on page 102](#)
- [How to Use Inbound Policy Marking for dVTI, on page 103](#)
- [Configuration Example for Inbound Policy Marking for dVTI, on page 105](#)
- [Additional References, on page 106](#)
- [Feature Information for Using Inbound Policy Marking for dVTI, on page 108](#)

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 Inbound Policy Marking for dVTI

- Policy map

Restrictions for Inbound Policy Marking for dVTI

The following are not supported:

- Policing
- Network Based Application Recognition (NBAR)-based classification

- Queuing
- Outbound policy marking

Only input QoS policy is supported. Only the marking feature is supported on the input policy. Other QoS configurations may not be blocked but will not be supported.

Information About Inbound Policy Marking for dVTI

Inbound Policy Marking

Marking is the setting of QoS information related to a packet. For the Inbound Policy Marking for dVTI feature, you can attach a policy map to a dVTI so that marking instructions are applied to inbound packets.

Dynamic Virtual Tunnel Interfaces Overview

DVTIs can provide highly secure and scalable connectivity for remote-access VPNs. The dVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels.

DVTIs can be used for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS XE software feature configured on the virtual template interface, such as QoS, NetFlow, or ACLs.

DVTIs function like any other real interface so that you can apply QoS, firewall, other security services as soon as the tunnel is active. QoS features can be used to improve the performance of various applications across the network. Any combination of QoS features offered in Cisco IOS XE software can be used to support voice, video, or data applications.

DVTIs provide efficiency in the use of IP addresses and provide secure connectivity. DVTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using extended authentication (Xauth) User or Unity group, or it can be derived from a certificate. DVTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec dVTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The dVTI simplifies VPN routing and forwarding (VRF)-aware IPsec deployment. The VRF is configured on the interface.

A dVTI requires minimal configuration on the router. A single virtual template can be configured and cloned.

The dVTI creates an interface for IPsec sessions and uses the virtual template infrastructure for dynamic instantiation and management of dynamic IPsec VTIs. The virtual template infrastructure is extended to create dynamic virtual-access tunnel interfaces. DVTIs are used in hub-and-spoke configurations.

In Cisco IOS XE Release 3.4S, support for the following was added:

- Maximum of 2000 dynamic tunnels with QoS applied
- Maximum of 4000 dynamic tunnels (2000 with QoS, 2000 without QoS)
- dVTI QoS LLQ for high-speed access egress shaping with overhead accounting and queuing

Security Associations and dVTI

Security Associations (SAs) are security policy instances and keying material applied to a data flow. IPSec SAs are unidirectional and unique in each security protocol. You need multi SAs for a protected data pipe, one per direction per protocol. The Inbound Policy Marking for dVTI feature uses multi SAs. It enables multiple specific-to-specific SAs to link to one dVTI tunnel.

How to Use Inbound Policy Marking for dVTI

To use the Inbound Policy Marking for dVTI feature, first create a policy map. After creating the policy map, attach it to an interface.

Creating a Policy Map

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class {class-name | class-default}`
5. `set ip dscp ip-dscp-value`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map policy-map-name Example: <pre>Router(config)# policy-map p-map</pre>	Enters QoS policy-map configuration mode and creates a policy map that can be attached to one or more interfaces to specify a service policy,
Step 4	class {class-name class-default} Example: <pre>Router(config-pmap)# class class-default</pre>	Specifies the default class so that you can configure or modify its policy.

	Command or Action	Purpose
Step 5	set ip dscp <i>ip-dscp-value</i> Example: <pre>Router(config-pmap-c)# set ip dscp af21</pre>	Marks a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 6	end Example: <pre>Router(config-pmap-c)# end</pre>	Returns to privileged EXEC mode.

Attaching a Policy Map to a dVTI

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **policy-map** [**type** {**control** | **service**}] *policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface virtual-template <i>number</i> Example: <pre>Router(config)# interface virtual-template 1 type tunnel</pre>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 4	policy-map [type { control service }] <i>policy-map-name</i> Example: <pre>Router(config)# policy-map input policy1</pre>	Enters QoS policy-map configuration mode and attaches this policy map to the interface.

	Command or Action	Purpose
Step 5	end Example: Router(config-pmap-c)# end	Returns to privileged EXEC mode.

Configuration Example for Inbound Policy Marking for dVTI

Example 1

```

class-map match-any RT
  match ip dscp cs5 ef
!
class-map match-any DATA
  match ip dscp cs1 cs2 af21 af22
!
policy-map CHILD
  class RT
    priority
    police 200000
    conform-action transmit exceed-action drop violate-action drop
  class DATA
    bandwidth remaining percent 100
!
policy-map PARENT
  class class-default
    shape average 1000000 account user-defined xx
    service-policy CHILD
!
interface Virtual-Template 1 type tunnel
  ip vrf forwarding Customer1
  service-policy output PARENT

```

Example 2 Configuring Inbound Policy Marking

This shows an example configuration of the hub side of dVTI:

```

aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
policy-map pm1
class class-default
  shape average 1280000
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!

```

```

crypto isakmp key cisco123 address 192.0.2.1
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
  key cisco
  dns 198.51.100.1
  wins 203.0.113.1
  domain cisco.com
  pool dpool
  acl 101
!
crypto isakmp profile vi
  match identity group cisco
  isakmp authorization list default
  client configuration address respond
  virtual-template 1
!
crypto ipsec transform-set trans-set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
  set transform-set trans-set
  set isakmp-profile vi
!
interface FastEthernet0/0
  ip address 203.0.113.254 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 203.0.113.255 255.255.255.0
  duplex auto
  speed 100
!
interface Virtual-Template1 type tunnel
  ip unnumbered FastEthernet0/0
  tunnel source FastEthernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi
  service-policy output pml
!
router eigrp 1
  network 192.168.1.0
  network 1.0.0.0
  no auto-summary
!
ip local pool dpool 192.0.2.1 192.0.2.254
ip route 198.51.100.1 198.51.100.254
!
access-list 101 permit ip 192.168.1.0 255.255.255.0 any

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>

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
Marking Network Traffic	“Marking Network Traffic” module

Standards and RFCs

Standard/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 2697	<i>A Single Rate Three Color Marker</i>
RFC 2698	<i>A Two Rate Three Color Marker</i>
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: 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 Using Inbound Policy Marking for dVTI

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 Inbound Policy Marking for dVTI

Feature Name	Releases	Feature Information
Inbound Policy Marking for dVTI	Cisco IOS XE Release 3.2S	<p>The Inbound Policy Marking for dVTI feature allows you to attach a policy map to a dVTI so that marking instructions are applied to inbound packets.</p> <p>In Cisco IOS XE Release 3.2S, support was added for the Cisco ASR 10000.</p> <p>In Cisco IOS XE Release 3.4S, support for the following was added:</p> <ul style="list-style-type: none"> • Maximum of 2000 dynamic tunnels with QoS applied • Maximum of 4000 dynamic tunnels (2000 with QoS, 2000 without QoS) • dVTI QoS LLQ for high-speed access egress shaping with overhead accounting and queuing <p>The following sections provide information about this feature:</p>



CHAPTER 13

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, on page 109](#)
- [Prerequisites for QoS Tunnel Marking for GRE Tunnels, on page 109](#)
- [Restrictions for QoS Tunnel Marking for GRE Tunnels, on page 109](#)
- [Information About QoS Tunnel Marking for GRE Tunnels, on page 110](#)
- [How to Configure Tunnel Marking for GRE Tunnels, on page 112](#)
- [Configuration Examples for QoS Tunnel Marking for GRE Tunnels, on page 117](#)
- [Additional References, on page 119](#)
- [Feature Information for QoS Tunnel Marking for GRE Tunnels, on page 120](#)

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

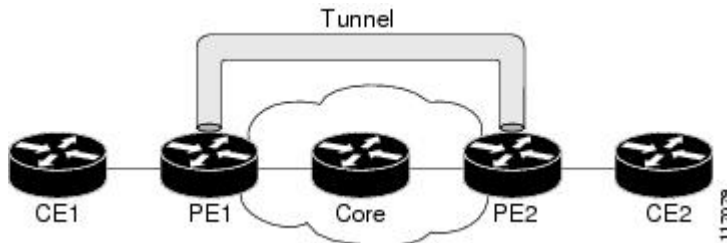
The QoS Tunnel Marking for GRE Tunnels feature allows you to define and control QoS for incoming and outgoing customer traffic on the PE router in a service provider (SP) network. This feature lets you set (mark) either the IP precedence value or the differentiated services code point (DSCP) value in 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 2: 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 difference 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 Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	class-map [match-all match-any] <i>class-map-name</i> Example: <pre>Router(config)# class-map match-any MATCH_PREC</pre>	Specifies the name of the class map to be created and enters QoS class map configuration mode. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		<p>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.</p>
Step 4	<p>match ip precedence <i>precedence-value</i></p> <p>Example:</p> <pre>Router(config-cmap)# match ip precedence 0</pre>	<p>Enables packet matching on the basis of the IP precedence values you specify.</p> <p>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.</p>
Step 5	<p>exit</p> <p>Example:</p> <pre>Router(config-cmap)# exit</pre>	Returns to global configuration mode.
Step 6	<p>class-map [match-all match-any] <i>class-map-name</i></p> <p>Example:</p> <pre>Router(config)# class-map match-any MATCH_DSCP</pre>	Specifies the name of the class map to be created and enters QoS class map configuration mode.
Step 7	<p>match ip dscp <i>dscp-value</i></p> <p>Example:</p> <pre>Router(config-cmap)# match ip dscp 0</pre>	<p>Enables packet matching on the basis of the DSCP values you specify.</p> <ul style="list-style-type: none"> • This command is used by the class map to identify a specific DSCP value marking on a packet. • The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.
Step 8	<p>end</p> <p>Example:</p> <pre>Router(config-cmap)# end</pre>	(Optional) Returns to privileged EXEC mode.

Creating a Policy Map

Perform this task to create a tunnel marking policy map 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 Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: <pre>Router(config)# policy-map TUNNEL_MARKING</pre>	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.
Step 4	class {class-name class-default} Example: <pre>Router(config-pmap)# class MATCH_PREC</pre>	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. <ul style="list-style-type: none"> • Enters policy-map class configuration mode.
Step 5	set ip precedence tunnel <i>precedence-value</i> Example: <pre>Router(config-pmap-c)# set ip precedence tunnel 3</pre>	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 Example: <pre>Router(config-pmap-c)# exit</pre>	Returns to QoS policy-map configuration mode.
Step 7	class {class-name class-default} Example: <pre>Router(config-pmap)# class MATCH_DSCP</pre>	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. <ul style="list-style-type: none"> • Enters policy-map class configuration mode.
Step 8	set ip dscp tunnel <i>dscp-value</i> Example:	Sets the differentiated services code point (DSCP) value in the tunnel header of a GRE-tunneled packet on the ingress

	Command or Action	Purpose
	<code>Router(config-pmap-c)# set ip dscp tunnel 3</code>	interface. The tunnel marking value is a number from 0 to 63 when DSCP is configured.
Step 9	end Example: <code>Router(config-pmap-c)# end</code>	(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 Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <code>Router(config)# interface GigabitEthernet 0/0/1</code>	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	service-policy {input output} <i>policy-map-name</i> Example: <pre>Router(config-if)# service-policy input TUNNEL_MARKING</pre>	Specifies the name of the policy map to be attached to the input or output direction of the interface. <ul style="list-style-type: none"> • 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 Example: <pre>Router(config-if)# end</pre>	(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 Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show policy-map interface <i>interface-name</i> Example: <pre>Router# show policy-map interface GigabitEthernet0/0/1</pre>	(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 <i>policy-map</i> Example: <pre>Router# show policy-map TUNNEL_MARKING</pre>	(Optional) Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

	Command or Action	Purpose
Step 4	exit Example: 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.

```
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.

```
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	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
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: 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 26: 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	<p>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.</p> <p>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.</p>



CHAPTER 14

QoS for dVTI

This module provides conceptual information for using egress QoS on Dynamic Virtual Tunnel Interfaces (dVTI). QoS for dVTI allows you to configure a single dVTI tunnel template. This template is replicated to give connectivity to remote endpoints.

- [Finding Feature Information, on page 121](#)
- [Restrictions for QoS dVTI , on page 121](#)
- [Information About QoS for dVTI , on page 122](#)
- [Configuration Examples for QoS for dVTI , on page 122](#)
- [Additional References, on page 124](#)
- [Feature Information for QoS for dVTI, on page 125](#)

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.

Restrictions for QoS dVTI

- With hierarchical egress policy-maps, the topmost policy may only have class-default
- Priority, bandwidth, fair-queue may only be configured at the lowest level of a policy-map hierarchy containing queuing features
- Only 2000 dVTI tunnels can have QoS configured
- Output QoS may not be configured on both the dVTI tunnel template and the output physical

Information About QoS for dVTI

A single dVTI template can support numerous connections from routers with static VTI (sVTI) configuration. The dVTI template configuration is typically on a hub router. Remote spoke routers have a sVTI configuration that always points to the hub router. QoS for dVTI supports the following:

- Maximum of 4000 dynamic tunnels using QoS from the dVTI tunnel template
- Scalability for an additional 2000 dynamic tunnels with no QoS on the dVTI tunnel template
- Low latency egress queuing on dVTI tunnel templates
- Egress shaping (with and without overhead accounting) on dVTI tunnel templates

Configuration Examples for QoS for dVTI

Example 2 Layer Rate LLQ for dVTI

This example shows how to configure a 2 Layer egress policy-map on the virtual tunnel interface which gives the following:

- ToS-specific rate LLQ for certain traffic
- Overall rate limiting on a per-tunnel basis
- Additional overhead is considered using the account directive on the shape command in the parent shaper

```
class-map match-any real_time
  match ip dscp cs5 ef
!
class-map match-any generic_data
  match ip dscp cs1 cs2 af21 af22
  match ip dscp default
!
policy-map child
class real_time
  police cir 200000
  conform-action transmit
  exceed-action drop
  violate-action drop
  priority
class generic_data
  bandwidth remaining percent 100
!
policy-map parent
  class class-default
  shape average 1000000 account user-defined 30
  service-policy child
!
interface Virtual-Template 1 type tunnel
  service-policy output parent
```

Example 2 Layer Rate LLQ with Bandwidth Guarantees for dVTI

This example shows how to configure a 2 Layer egress policy-map on the virtual tunnel interface which gives the following:

- ToS-specific rate LLQ for certain traffic
- Bandwidth guarantees for other traffic
- Overall rate limiting on a per-tunnel basis

```
class-map match-any real_time
match ip precedence 5
!
class-map match-any higher_data_1
match ip precedence 2
!
class-map match-any higher_data_2
match ip precedence 3
!
policy-map child
  class real_time priority
    police 5000000 conform-action transmit exceed-action drop violate-action drop
  class higher_data_1
    bandwidth remaining percent 50
  class higher_data_2
    bandwidth remaining percent 40
  class class-default
    shape average 10000000
    bandwidth remaining percent 5
!
policy-map parent
  class class-default shape average 15000000
  service-policy child
!
interface Virtual-Template 1 type tunnel
service-policy output parent
```

Example 3 Layer QoS for dVTI

```
policy-map parent
  Class class-default
    Shape average 50000000
    Bandwidth remaining ratio 1
    Service-policy child
!
policy-map child
  Class Red
    Shape average percent 80
    Bandwidth remaining ratio 9
    Service-policy grandchild
  Class Green
    Shape average percent 80
    Bandwidth remaining ratio 2
    Service-policy grandchild
!
policy-map grandchild
  Class voice
    Priority level 1
  Class video
    Priority level 2
```

```

Class data_gold
  Bandwidth remaining ratio 100
Class class-default
  Random-detect dscp-based
!

interface virtual-template101 type tunnel
ip unnumbered loopback101
tunnel source GigabitEthernet0/3/0
service-policy output parent

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards and RFCs

Standard/RFC	Title

MIBs

MB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco software 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 QoS for dVTI

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 dVTI

Feature Name	Releases	Feature Information
QoS for dVTI	Cisco IOS XE Release 2.1	QoS for dVTI configures a single dVTI tunnel template.



CHAPTER 15

Classifying and Marking MPLS EXP

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

- [Finding Feature Information, on page 127](#)
- [Prerequisites for Classifying and Marking MPLS EXP, on page 127](#)
- [Restrictions for Classifying and Marking MPLS EXP, on page 127](#)
- [Information About Classifying and Marking MPLS EXP, on page 128](#)
- [How to Classify and Mark MPLS EXP, on page 129](#)
- [Configuration Examples for Classifying and Marking MPLS EXP, on page 134](#)
- [Additional References, on page 137](#)
- [Feature Information for Classifying and Marking MPLS EXP, on page 138](#)

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 Classifying and Marking MPLS EXP

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

Restrictions for Classifying and Marking MPLS EXP

- MPLS classification and marking can only occur in an operational MPLS Network.

- MPLS EXP classification and marking is supported on the main router interfaces for MPLS packet switching and imposition (simple IP imposition and Ethernet over MPLS (EoMPLS) imposition) and on Ethernet virtual circuits (EVCs) or Ethernet flow points (EFPs) for EoMPLS imposition.
- MPLS EXP classification or marking for bridged MPLS packets on EVCs or EFPs is not supported.
- MPLS EXP marking is supported only in the ingress direction.
- If a packet is classified by IP type of service (ToS) or class of service (CoS) at ingress, it cannot be reclassified by MPLS EXP at egress (imposition case). However, if a packet is classified by MPLS at ingress it can be reclassified by IP ToS, CoS, or Quality of Service (QoS) group at egress (disposition case).
- If a packet is encapsulated in MPLS, the MPLS payload cannot be checked for other protocols such as IP for classification or marking. Only MPLS EXP marking affects packets encapsulated by MPLS.

Information About Classifying and Marking MPLS EXP

Classifying and Marking MPLS EXP Overview

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

- Classify traffic

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

- Police and mark traffic

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

MPLS Experimental Field

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

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

Benefits of MPLS EXP Classification and Marking

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

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

How to Classify and Mark MPLS EXP

Classifying MPLS Encapsulated Packets



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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map [match-all match-any] class-map-name Example: Router(config)# class-map exp3	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode. • Enter the class map name.
Step 4	match mpls experimental topmost mpls-exp-value Example:	Specifies the match criteria.

	Command or Action	Purpose
	Router(config-cmap)# match mpls experimental topmost 3	Note The match mpls experimental topmost command classifies traffic on the basis of the EXP value in the topmost label header.
Step 5	end Example: Router(config-cmap)# end	(Optional) Returns to privileged EXEC mode.

Marking MPLS EXP on All Imposed Labels

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

Before you begin

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

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



Note For IP imposition marking, the IP precedence value is copied to the MPLS EXP value by default.



Note For EVC configuration, a policy map that performs matching based on the CoS and that sets the EXP imposition value should be used to copy CoS values to the EXP value.



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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: <pre>Router(config)# policy-map mark-up-exp-2</pre>	Specifies the name of the policy map to be created and enters policy-map configuration mode. <ul style="list-style-type: none"> • Enter the policy map name.
Step 4	class <i>class-map-name</i> Example: <pre>Router(config-pmap)# class prec012</pre>	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode. <ul style="list-style-type: none"> • Enter the class map name.
Step 5	set mpls experimental imposition <i>mpls-exp-value</i> Example: <pre>Router(config-pmap-c)# set mpls experimental imposition 2</pre>	Sets the value of the MPLS EXP field on all imposed label entries.
Step 6	end Example: <pre>Router(config-pmap-c)# end</pre>	(Optional) Returns to privileged EXEC mode.

Marking MPLS EXP on Label Switched Packets

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

Before you begin



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



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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring Conditional Marking

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

Before you begin



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

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `policy-map policy-map-name`
4. `class class-map-name`
5. `police cir bps bc pir bps be`
6. `conform-action [set-mpls-exp-imposition-transmit mpls-exp-value | set-mpls-exp-topmost-transmit mpls-exp-value]`
7. `exceed-action [set-mpls-exp-imposition-transmit mpls-exp-value | set-mpls-exp-topmost-transmit mpls-exp-value]`
8. `violate-action drop`
9. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map policy-map-name Example: <pre>Router(config)# policy-map ip2tag</pre>	Specifies the name of the policy map to be created and enters policy-map configuration mode. <ul style="list-style-type: none"> • Enter the policy map name.
Step 4	class class-map-name Example: <pre>Router(config-pmap)# class iptcp</pre>	Creates a class map to be used for matching traffic to a specified class, and enters policy-map class configuration mode. <ul style="list-style-type: none"> • Enter the class map name.
Step 5	police cir bps bc pir bps be Example:	Defines a policer for classified traffic and enters policy-map class police configuration mode.

	Command or Action	Purpose
	<pre>Router(config-pmap-c)# police cir 1000000 pir 2000000</pre>	
Step 6	<p>conform-action [set-mpls-exp-imposition-transmit <i>mpls-exp-value</i> set-mpls-exp-topmost-transmit <i>mpls-exp-value</i>]</p> <p>Example:</p> <pre>Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3</pre>	<p>Defines the action to take on packets that conform to the values specified by the policer.</p> <ul style="list-style-type: none"> In this example, if the packet conforms to the committed information rate (cir) or is within the conform burst (bc) size, the MPLS EXP field is set to 3.
Step 7	<p>exceed-action [set-mpls-exp-imposition-transmit <i>mpls-exp-value</i> set-mpls-exp-topmost-transmit <i>mpls-exp-value</i>]</p> <p>Example:</p> <pre>Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2</pre>	<p>Defines the action to take on packets that exceed the values specified by the policer.</p> <ul style="list-style-type: none"> In this example, if the packet exceeds the cir rate and the bc size, but is within the peak burst (be) size, the MPLS EXP field is set to 2.
Step 8	<p>violate-action drop</p> <p>Example:</p> <pre>Router(config-pmap-c-police)# violate-action drop</pre>	<p>Defines the action to take on packets whose rate exceeds the peak information rate (pir) and is outside the bc and be ranges.</p> <ul style="list-style-type: none"> You must specify the exceed action before you specify the violate action. In this example, if the packet rate exceeds the pir rate and is outside the bc and be ranges, the packet is dropped.
Step 9	<p>end</p> <p>Example:</p> <pre>Router(config-pmap-c-police)# end</pre>	(Optional) Returns to privileged EXEC mode.

Configuration Examples for Classifying and Marking MPLS EXP

Example: Classifying MPLS Encapsulated Packets

Defining an MPLS EXP Class Map

The following example defines a class map named exp3 that matches packets that contains MPLS experimental value 3:

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


Defining a Policy Map and Applying the Policy Map to an Ingress Interface

The following example uses the class map created in the example above to define a policy map. This example also applies the policy map to a physical interface for ingress traffic.

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

Defining a Policy Map and Applying the Policy Map to an Egress Interface

The following example uses the class map created in the example above to define a policy map. This example also applies the policy map to a physical interface for egress traffic.

```
Router(config)# policy-map WAN-out
Router(config-pmap)# class exp3
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# service-policy output WAN-out
Router(config-if)# exit
```

Example: Marking MPLS EXP on All Imposed Labels

Defining an MPLS EXP Imposition Policy Map

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

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

Applying the MPLS EXP Imposition Policy Map to a Main Interface

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

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

Applying the MPLS EXP Imposition Policy Map to an EVC

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

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

Example: Marking MPLS EXP on Label Switched Packets

Defining an MPLS EXP Label Switched Packets Policy Map

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

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

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

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

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

Example: Configuring Conditional Marking

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

```
Router(config)# policy-map ip2tag
Router(config-pmap)# class iptcp
Router(config-pmap-c)# police cir 1000000 pir 2000000
Router(config-pmap-c-police)# conform-action set-mpls-exp-imposition-transmit 3
Router(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2
```

```

Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# service-policy input ip2tag

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
Classifying network traffic	“Classifying Network Traffic” module
Marking network traffic	“Marking Network Traffic” module

Standards and RFCs

Standard/RFC	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 software 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 Classifying and Marking MPLS EXP

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

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

Table 28: Feature Information for Classifying and Marking MPLS EXP

Feature Name	Releases	Feature Information
QoS EXP Matching	Cisco IOS XE Release 3.5S	QoS EXP matching allows you to classify and mark packets using the MPLS EXP field. In Cisco IOS XE Release 3.5S, this feature was introduced on the Cisco ASR 903 Router.