QoS: Classification Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

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

CONTENTS

IPv6 Quality of Service

QoS features supported for IPv6 environments include packet classification, queueing, traffic shaping, weighted random early detection (WRED), class-based packet marking, and policing of IPv6 packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About IPv6 Quality of Service

Implementation Strategy for QoS for IPv6

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

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

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

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

Packet Classification in IPv6

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

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

How to Configure IPv6 Quality of Service

- Classifying Traffic in IPv6 Networks, page 2
- Specifying Marking Criteria for IPv6 Packets, page 2
- Using Match Criteria to Manage IPv6 Traffic Flows, page 4

Classifying Traffic in IPv6 Networks

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

Specifying Marking Criteria for IPv6 Packets

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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** *policy-map-name* **Example:** `Device(config)# policy map policy1`	Creates a policy map using the specified name and enters QoS policy-map configuration mode. • Enter the name of the policy map that you want to create.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Device(config-pmap)# class class-default`	Specifies the treatment for traffic of a specified class (or the default class) and enters QoS policy-map class configuration mode.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
	• **set** [**ip**] **dscp**{*dscp-value* | *from-field* [**table** *table-map-name*]}
	
	Example:
	`Device(config-pmap-c)#`
	`set precedence cos table table-map1`
	
	Example:
	`Device(config-pmap-c)#`
	`set dscp cos table table-map1`
		Sets the precedence value and the DSCP value based on the CoS value (and action) defined in the specified table map. Both precedence and DSCP cannot be changed in the same packets.

Using Match Criteria to Manage IPv6 Traffic Flows

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map** {*class-name* | **class-default**} **Example:** `Device(config-pmap-c)# class-map clsl`	Creates the specified class and enters QoS class-map configuration mode.

Step 4	Do one of the following:
	• **match precedence** *precedence-value* [*precedence-value precedence-value*]
	• **match access-group name** *ipv6-access-group*
	• **match [ip] dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
	
	Example:
	`Device(config-pmap-c)# match precedence 5`
	
	Example:
	`Device(config-pmap-c)# match ip dscp 15`
		Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.
		or
		Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class.
		or
		Identifies a specific IP DSCP value as a match criterion.

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:

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

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

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

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

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

```
Device# show atm vc 3

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

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

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

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

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

Table 1 Packet Types and the Layer 3 Queue

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

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

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

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

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

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

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

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

The table below defines counters that appear in the example.

Table 2 Packet Counters from show policy-map interface Output

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

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

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

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

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

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

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

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

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

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

Information reported for each class includes the following:

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

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

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

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

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

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

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

Bandwidth Range	Number of Dynamic Queues
Less than or equal to 128 kbps	16
More than 128 kbps and less than or equal to 512 kbps	32
More than 512 kbps and less than or equal to 2000 kbps	64
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
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
Classifying Network Traffic	“Classifying Network Traffic” module
Marking Network Traffic	“Marking Network Traffic” module

Standards and RFCs

Standard/RFC	Title
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 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	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 access-group name**, **match dscp**, **match precedence**, **set dscp**, **set precedence**.

IPv6 QoS: MQC Packet Classification

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About IPv6 QoS: MQC Packet Classification

Implementation Strategy for QoS for IPv6

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

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

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

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

Packet Classification in IPv6

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

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

How to Configure IPv6 QoS: MQC Packet Classification

Classifying Traffic in IPv6 Networks

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

Using Match Criteria to Manage IPv6 Traffic Flows

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map** {*class-name* | **class-default**} **Example:** `Device(config-pmap-c)# class-map clsl`	Creates the specified class and enters QoS class-map configuration mode.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **match precedence** *precedence-value* [*precedence-value precedence-value*]
	• **match access-group name** *ipv6-access-group*
	• **match [ip] dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
	
	Example:
	`Device(config-pmap-c)# match precedence 5`
	
	Example:
	`Device(config-pmap-c)# match ip dscp 15`
		Matches the precedence value. The precedence applies to both IPv4 and IPv6 packets.
		or
		Specifies the name of an IPv6 access list against whose contents packets are checked to determine if they belong to the traffic class.
		or
		Identifies a specific IP DSCP value as a match criterion.

Confirming the Service Policy

Ensure that the traffic flow matches the input or output parameter of the policy. For example, downloading a file from an FTP server generates congestion in the receive direction because the server sends large MTU-sized frames, and the client PC returns small acknowledgments (ACKs).

Before you begin this task, simulate congestion with an extended ping using a large ping size and a large number of pings. Also, try downloading a large file from an FTP server. The file constitutes “disturbing” data and fills the interface bandwidth.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* **multipoint** | **point-to-point**
4. **ip address** *ip-address mask* [**secondary**]
5. **pvc** [*name*] *vpi/vci* [**ces** | **ilmi** | **qsaal** | **smds**]
6. **tx-ring-limit** *ring-limit*
7. **service-policy** {**input** | **output**} *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **multipoint** | **point-to-point** **Example:** `Device(config)# interface gigabitethernet1/1/0 point-to-point`	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	Specifies the IP address of the interface that you want to test.
Step 5	**pvc** [*name*] *vpi/vci* [**ces** | **ilmi** | **qsaal** | **smds**] **Example:** `Device(config-if)# pvc cisco 0/5`	Creates or assigns a name to an ATM PVC, optionally specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode.
Step 6	**tx-ring-limit** *ring-limit* **Example:** `Device(config-if-atm-vc)# tx-ring-limit 10`	Reduces the size of the transmit ring of the interface. Lowering this value accelerates the use of the QoS in the Cisco IOS software. • Specify the ring limit as the number of packets for Cisco 2600 and 3600 series routers or as the number of memory particles for Cisco 7200 and 7500 series routers.
Step 7	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Device(config-if-atm-vc)# service-policy output policy9`	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. • The packets-matched counter is a part of the queueing feature and is available only on service policies attached in the output direction.

Configuration Examples for IPv6 QoS: MQC Packet Classification

- Example: Matching DSCP Value, page 20

Example: Matching DSCP Value

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

```
Router(config)#
 class-map ipdscp15
Router(config-cmap)#
 match ip dscp 15
Router(config)#
 exit
Router(config)#
policy-map priority50
Router(config-pmap)#
 class ipdscp15
Router(config-pmap-c)#
priority 50
Router(config-pmap-c)#
exit
Router(config-pmap)#
 exit
Router(config)#
interface gigabitethernet1/0/0
Router(config-if)#
service-policy input priority55
```

To match on IPv6 packets only, use the **match dscp** command without the **ip** keyword preceded by the **match protocol** command. Ensure that the class map has the **match-all** attribute (which is the default).

```
Router(config)#
 class-map ipdscp15
Router(config-cmap)#
 match protocol ipv6
Router(config-cmap)#
 match dscp 15
Router(config)#
 exit
```

To match packets on both IPv4 and IPv6 protocols, use the **match dscp** command:

```
Router(config)#
 class-map ipdscp15
Router(config-cmap)#
 match dscp 15
```

Additional References

Related Documents

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

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

Feature Information for IPv6 QoS: MQC Packet Classification

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

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

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

Packet Classification Based on Layer 3 Packet Length

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Packet Classification Based on Layer 3 Packet Length

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

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

Restrictions for Packet Classification Based on Layer 3 Packet Length

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

Information About Packet Classification Based on Layer 3 Packet Length

MQC and Packet Classification Based on Layer 3 Packet Length

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

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

The MQC consists of the following three processes:

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

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

The**match** commands are used to specify various criteria for classifying packets. Packets are checked to determine whether they match the criteria specified in the **match** commands. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

How to Configure Packet Classification Based on Layer 3 Packet Length

- Verifying the Layer 3 Packet Length Classification Configuration, page 28

Configuring the Class Map to Match on Layer 3 Packet Length

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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** *class-map-name* **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** {**max***maximum-length-value* [**min***minimum-length-value*] | **min***minimum-length-value* [**max***maximum-length-value*]} **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:** `Router(config-cmap)# end`	(Optional) Exits class-map configuration mode and returns to privileged EXEC mode.

Attaching the Policy Map to an Interface

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. Do one of the following:
   - **service-policy** {**input**| **output**}*policy-map-name*
6. Do one of the following:
   - **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.

	Command or Action	Purpose

Step 3	**interface** *type number*
	
	Example:
	
	Example:
	`Router(config)#`
	`interface serial4/0/0`
		Configures an interface (or subinterface) type and enters interface configuration mode
		• Enter the interface type and number.

Step 4	**pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM VC configuration mode. **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 and proceed with Attaching the Policy Map to an Interface, page 26.

Step 5	Do one of the following:
	• **service-policy** {**input**| **output**}*policy-map-name*
	
	Example:
	`Router(config-if)#`
	`service-policy input policy1`
	
	Example:
	
	Example:
	`Router(config-if-atm-vc)#`
	`service-policy input policy1`
	
	Example:
		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 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.
		• Enter the policy map name.

	Command or Action	Purpose

Step 6	Do one of the following:
	• **end**
	
	Example:
	`Router(config-if)# end`
	
	Example:
	
	Example:
	`Router(config-if-atm-vc)#`
	`end`
		(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Layer 3 Packet Length Classification Configuration

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map** [*class-map-name*] **Example:** `Router# show class-map class1`	(Optional) Displays all information about a class map, including the match criterion. • Enter the class map name.

	Command or Action	Purpose

Step 3	**show policy-map interface** *interface-name* [**vc** [*vpi/*] *vci*] [**dlci***dlci*] [**input**| **output**]
	
	Example:
	
	`Router#`
	`show policy-map interface serial4/0/0`
		(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		
		• Enter the interface name.

Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

• Troubleshooting Tips, page 29

Troubleshooting Tips

The commands in the Verifying the Layer 3 Packet Length Classification Configuration, page 28 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), performs the following operations:

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

Configuration Examples for Packet Classification Based on Layer 3 Packet Length

Example Configuring the Layer 3 Packet Length as a Match Criterion

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

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

Example Verifying the Layer 3 Packet Length Setting

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

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

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

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

```
Router(config)# policy-map mypolicy
Router(config-pmap)# class class1
Router(config-pmap-c)# set qos-group 20
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet4/1/1
Router(config-if)# service-policy input mypolicy
```

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

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC and information about attaching policy maps to interfaces	"Applying QoS Features Using the MQC" module
Additional match criteria that can be used for packet classification	"Classifying Network Traffic" module
Marking network traffic	"Marking Network Traffic" module

Standards

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

MIBs

MIB	MIBs Link
• CISCO-CLASS-BASED-QOS-CAPABILITY-MIB • 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	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. The following commands were introduced or modified: **matchpacketlength** (class-map), **showclass-map**, **showpolicy-mapinterface**.

IPv6 QoS: MQC Packet Marking/Remarking

Class-based marking allows you to set the IPv6 precedence and DSCP values for traffic management.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About IPv6 QoS: MQC Packet Marking/Remarking

Implementation Strategy for QoS for IPv6

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

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

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

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

Policies and Class-Based Packet Marking in IPv6 Networks

You can create a policy to mark each class of traffic with appropriate priority values, using either DSCP or precedence. Class-based marking allows you to set the IPv6 precedence and DSCP values for traffic management. The traffic is marked as it enters the device on the ingress interface. The markings are used to treat the traffic (forward, queue) as it leaves the device 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, page 36

Specifying Marking Criteria for IPv6 Packets

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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** *policy-map-name* **Example:** `Device(config)# policy map policy1`	Creates a policy map using the specified name and enters QoS policy-map configuration mode. • Enter the name of the policy map that you want to create.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Device(config-pmap)# class class-default`	Specifies the treatment for traffic of a specified class (or the default class) and enters QoS policy-map class configuration mode.

	Command or Action	Purpose

Step 5	Do one of the following:
	• **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
	• **set** [**ip**] **dscp**{*dscp-value* | *from-field* [**table** *table-map-name*]}
	
	Example:
	`Device(config-pmap-c)#`
	`set precedence cos table table-map1`
	
	Example:
	`Device(config-pmap-c)#`
	`set dscp cos table table-map1`
		Sets the precedence value and the DSCP value based on the CoS value (and action) defined in the specified table map. Both precedence and DSCP cannot be changed in the same packets.

Configuration Examples for IPv6 QoS: MQC Packet Marking/Remarking

Example: Verifying Packet Marking Criteria

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

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

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

```
Device# show policy p1
  Policy Map p1
    Class c1
      police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface serial 4/1
Device(config-if)# service out p1
Device(config-if)# end
Device# show policy interface s4/1
 Serial4/1
  Service-policy output: p1
```

```
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: precedence 5
      police:
        10000 bps, 1500 limit, 1500 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 4
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps violate 0 bps
    Class-map: class-default (match-any)
      10 packets, 1486 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

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

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

```
Device# show atm vc 3

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

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

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

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

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

Table 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 CEF or fast-switched	Yes	No

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

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

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

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

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

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

The table below defines counters that appear in the example.

Table 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.

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

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

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

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

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

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

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

              Bandwidth 60 (%) Packets Matched 0
              (pkts discards/bytes discards/tail drops) 0/0/0
              mean queue depth: 0
              drops: class  random   tail     min-th   max-th   mark-prob
                     0      0        0        64       128      1/10
                     1      0        0        71       128      1/10
                     2      0        0        78       128      1/10
                     3      0        0        85       128      1/10
```

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

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

Information reported for each class includes the following:

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

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

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

Table 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
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

Bandwidth Range	Number of Dynamic Queues
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	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference

Related Topic	Document Title
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.

Marking Network Traffic

Marking network traffic allows you to set or modify the attributes for traffic (that is, packets) belonging to a specific class or category. When used in conjunction with network traffic classification, marking network traffic is the foundation for enabling many quality of service (QoS) features on your network. This module contains conceptual information and the configuration tasks for marking network traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for Marking Network Traffic

Traffic marking can be configured on an interface, a subinterface, or an ATM permanent virtual circuit (PVC). Marking network traffic is not supported on the following interfaces:

- ATM switched virtual circuit (SVC)
- Fast EtherChannel
- PRI
- Tunnel

Information About Marking Network Traffic

Purpose of Marking Network Traffic

Traffic marking is a method used to identify certain traffic types for unique handling, effectively partitioning network traffic into different categories.

After the network traffic is organized into classes by traffic classification, traffic marking allows you to mark (that is, set or change) a value (attribute) for the traffic belonging to a specific class. For instance, you may want to change the class of service (CoS) value from 2 to 1 in one class, or you may want to change the differentiated services code point (DSCP) value from 3 to 2 in another class. In this module, these values are referred to as attributes.

Attributes that can be set and modified include the following:

- Cell loss priority (CLP) bit
- CoS value of an outgoing packet
- Discard eligible (DE) bit setting in the address field of a Frame Relay frame
- Discard-class value
- DSCP value in the type of service (ToS) byte
- MPLS EXP field value in the topmost label on either an input or an 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 router. The router 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 Precedence, which have 64 and 8, respectively.
- If changing the Precedence or DSCP value is undesirable.

- If a packet (for instance, in a traffic flow) needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router 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.

Method for Marking Traffic Attributes

You 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.

- Using a set Command, page 49

Using a set Command

You specify the traffic attribute 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 below 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	ATM, Frame Relay
set discard-class	discard-class value	Layer 2	ATM, Frame Relay
set dscp	DSCP value in the ToS byte	Layer 3	IP
set fr-de	DE bit setting in the address field of a Frame Relay frame	Layer 2	Frame Relay
set ip tos (route-map)	ToS bits in the header of an IP packet	Layer 3	IP
set mpls experimental imposition	MPLS EXP field on all imposed label entries	Layer 3	MPLS
set mpls experimental topmost	MPLS EXP field value in the topmost label on either an input or an output interface	Layer 3	MPLS
set precedence	precedence value in the packet header	Layer 3	IP

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

set Commands[1]	Traffic Attribute	Network Layer	Protocol
set qos-group	QoS group ID	Layer 3	IP, MPLS

If you are using individual **set** commands, those **set** commands are specified in a policy map. The following is a sample of a 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.

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.

MQC and Network Traffic Marking

To configure network traffic marking, you use the Modular Quality of Service (QoS) Command-Line Interface (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 DSCP value of 3 is grouped into another class. The match criterion is 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.

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

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 criterion.	Uses the traffic classes and matching criterion 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 the Cisco IOS XE release that you are using 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:** `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** *class-map-name* [**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.
Step 4	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol ftp`	(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 IOS XE release. See the command documentation for the Cisco IOS XE release that you are using for a complete list of **match** commands.
Step 5	**end** **Example:** `Router(config-cmap)# end`	(Optional) Returns to privileged EXEC mode.

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

Note The **set cos** command is shown in the steps that follow. The **set cos** command is an example of a **set** command that can be used when marking traffic. Other **set** commands can be used. For a list of other **set** commands, see “Creating a Policy Map for Applying a QoS Feature to Network Traffic”.

The following restrictions apply to creating a QoS policy map:

- Before modifying the encapsulation type from IEEE 802.1 Q to ISL, or vice versa, on a subinterface, detach the policy map from the subinterface. After changing the encapsulation type, reattach the 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 router.
- 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*
9. **exit**

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** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map created earlier and enters policy-map configuration mode. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(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.

	Command or Action	Purpose
Step 5	**set cos** *cos-value* **Example:** `Router(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 “Creating a Policy Map for Applying a QoS Feature to Network Traffic”.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**show policy-map** **Example:** `Router# show policy-map`	(Optional) Displays all configured policy maps.
Step 8	**show policy-map** *policy-map* **class** *class-name* **Example:** `Router# show policy-map policy1 class class1`	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

• What to Do Next, page 54

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 permanent virtual circuit (PVC).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds** | **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**} *policy-map-name*
7. **end**
8. **show policy-map interface** *type number*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.

	Command or Action	Purpose
Step 4	**pvc** [*name*] *vpi/vci* [**ilmi** | **qsaal** | **smds** | **l2transport**] **Example:** `Router(config-if)# pvc cisco 0/16`	(Optional) Creates or assigns a name to an ATM permanent virtual circuit (PVC), specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode. • Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to Step 6 below.
Step 5	**exit** **Example:** `Router(config-atm-vc)# exit`	(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:** `Router(config-if)# service-policy input policy1`	Attaches a policy map to an input or output interface. • Enter the policy map name. **Note** Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 8	**show policy-map interface** *type number* **Example:** `Router# show policy-map interface serial4/0/0`	(Optional) Displays the traffic statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. • Enter the interface type and number.
Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

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 received 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* **Example:** `Router(config)# crypto map mymap 10`	Enters crypto map configuration mode and creates or modifies a crypto map entry. • Enter the crypto map name and sequence number.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config-crypto-map)# exit`	Returns to global configuration mode.
Step 5	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.
Step 6	**qos pre-classify** **Example:** `Router(config-if)# qos pre-classify`	Enables QoS preclassification.
Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

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. The traffic with a protocol type of ftp will be put in this class.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match protocol ftp
Router(config-cmap)# end
```

Example: Creating a Policy Map for Applying a QoS Feature to Network

The following is an example of creating a policy map to be used for traffic marking. In this example, a policy map called policy1 has been created, and the **set dsc** command has been configured for class1.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
```

```
Router(config-pmap-c)# set dscp 2
Router(config-pmap-c)# end
```

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 of the serial interface 4/0/0.

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

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC	“Applying QoS Features Using the MQC” module
Classifying network traffic	“Classifying Network Traffic” module
IPsec and VPNs	“Configuring Security for VPNs with IPsec” module
IPv6 QoS	“IPv6 Quality of Service” module
IPv6 MQC Packet Marking and Remarking	“IPv6 QoS: MQC Packet Marking/Remarking” 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 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
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
Class-Based Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	This feature was implemented on Cisco ASR 1000 Series Routers. This feature was integrated into Cisco IOS XE Software Release 2.2.
Frame Relay DE Bit Marking	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
IP DSCP marking for Frame-Relay PVC	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
QoS Group: Match and Set for Classification and Marking	Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 Series Routers.
QoS Packet Marking	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.5S	This feature was implemented on Cisco ASR 1000 Series Routers. This feature was integrated into Cisco IOS XE Software Release 2.2. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
QoS: Traffic Pre-classification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

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

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, page 65
- Attaching a Policy Map to a dVTI, page 66

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map p-map`	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:** `Router(config-pmap)# class class-default`	Specifies the default class so that you can configure or modify its policy.
Step 5	**set ip dscp** *ip-dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp af21`	Marks a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1 type tunnel`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 4	**policy-map** [**type** {**control** | **service**}] *policy-map-name* **Example:** `Router(config)# policy-map input policy1`	Enters QoS policy-map configuration mode and attaches this policy map to the interface.
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 pm1
!
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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands	*Cisco IOS QoS Command Reference*

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 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 RFCs were created or modified to support 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 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 18 Feature Information for Inbound Policy Marking for dVTI

Feature Name	Releases	Feature Information
Inbound Policy Marking for dVTI	Cisco IOS XE Release 3.2S	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. In Cisco IOS XE Release 3.2S, support was added for the Cisco ASR 10000. 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 The following sections provide information about this feature:

QoS Tunnel Marking for GRE Tunnels

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for QoS Tunnel Marking for GRE Tunnels

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

Restrictions for QoS Tunnel Marking for GRE Tunnels

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

Information About QoS Tunnel Marking for GRE Tunnels

GRE Definition

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

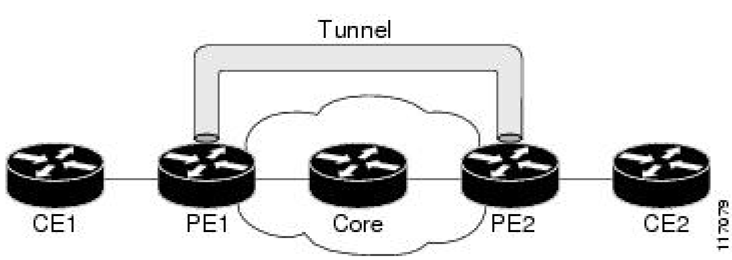
GRE Tunnel Marking Overview

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

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

The figure below shows traffic being received from the CE1 router through the incoming interface on the PE1 router on which tunnel marking occurs. The traffic is encapsulated (tunneled), and the tunnel header is marked on the PE1 router. The marked packets travel (tunnel) through the core and are decapsulated automatically on the exit interface of the PE2 router. This feature is designed to simplify classifying customer edge (CE) traffic and is configured only in the service provider network. This process is transparent to the customer sites. The CE1 and CE2 routers exist as a single network.

Figure 1 Tunnel Marking



GRE Tunnel Marking and the MQC

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

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

GRE Tunnel Marking and DSCP or IP Precedence Values

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

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

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

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

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

Benefits of GRE Tunnel Marking

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

GRE Tunnel Marking and Traffic Policing

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

GRE Tunnel Marking Values

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

How to Configure Tunnel Marking for GRE Tunnels

Configuring a Class Map

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map match-any MATCH_PREC`	Specifies the name of the class map to be created and enters QoS class map configuration mode. • 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. **Note** If the **match-all** or **match-any** keyword is not specified, traffic must match all the match criteria to be classified as part of the traffic class.
Step 4	**match ip precedence** *precedence-value* **Example:** `Router(config-cmap)# match ip precedence 0`	Enables packet matching on the basis of the IP precedence values you specify. **Note** You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Returns to global configuration mode.
Step 6	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map match-any MATCH_DSCP`	Specifies the name of the class map to be created and enters QoS class map configuration mode.
Step 7	**match ip dscp** *dscp-value* **Example:** `Router(config-cmap)# match ip dscp 0`	Enables packet matching on the basis of the DSCP values you specify. • 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	**end** **Example:** `Router(config-cmap)# end`	(Optional) Returns to privileged EXEC mode.

Creating a Policy Map

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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** *policy-map-name* **Example:** `Router(config)# policy-map TUNNEL_MARKING`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters QoS policy-map configuration mode.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class MATCH_PREC`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • Enters policy-map class configuration mode.
Step 5	**set ip precedence tunnel** *precedence-value* **Example:** `Router(config-pmap-c)# set ip precedence tunnel 3`	Sets the IP precedence value in the tunnel header of a GRE-tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 7 when IP precedence is configured.

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

Attaching the Policy Map to an Interface or a VC

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input TUNNEL_MARKING`	Specifies the name of the policy map to be attached to the input or output direction of the interface. • 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:** `Router(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Verifying the Configuration of Tunnel Marking for GRE Tunnels

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

SUMMARY STEPS

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

DETAILED STEPS

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

• Troubleshooting Tips, page 81

Troubleshooting Tips

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

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

Configuration Examples for QoS Tunnel Marking for GRE Tunnels

Example: Configuring Tunnel Marking for GRE Tunnels

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

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

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

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

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

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

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

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

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

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

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

Example: Verifying the Tunnel Marking for GRE Tunnels Configuration

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

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

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

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

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

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

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

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

```
Router# show policy-map

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC	"Applying QoS Features Using the MQC" module
Tunnel marking for Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnels	"QoS: Tunnel Marking for L2TPv3 Tunnels" module

Related Topic	Document Title
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 19 Feature Information for QoS Tunnel Marking for GRE Tunnels

Feature Name	Releases	Feature Information
QoS Tunnel Marking for GRE Tunnels	Cisco IOS XE Release 3.5S	The QoS Tunnel Marking for GRE Tunnels feature introduces the capability to define and control the QoS for incoming customer traffic on the PE router in a service provider network. 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**.

Classifying Network Traffic

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many quality of service (QoS) features on your network. This module contains conceptual information and the configuration tasks for classifying network traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Classifying Network Traffic

Purpose of Classifying Network Traffic

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

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

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

Benefits of Classifying Network Traffic

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

MQC and Network Traffic Classification

To configure network traffic classification, you use the Modular Quality of Service Command-Line Interface (MQC).

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

- Specify the matching criteria used to define a traffic class.
- Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.
- Apply the policy actions specified in the policy map to an interface, subinterface, or ATM permanent virtual circuit (PVC) by using the **service-policy** command.

Network Traffic Classification match Commands and Match Criteria

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

You specify the criteria used to classify traffic with a **match** command. Network Traffic Classification match Commands and Match Criteria, page 88 lists the available **match** commands and the corresponding match criterion.

Table 20 match Commands and Corresponding Match Criterion

match Commands[2]	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 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 protocol gnutella	Gnutella peer-to-peer traffic

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

match Commands[2]	Match Criterion
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

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 DSCP value of 3 is grouped into another class. The match criterion is 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 21 Traffic Classification Compared with Traffic Marking

	Traffic Classification	Traffic Marking
Goal	Groups network traffic into specific traffic classes on the basis of whether the traffic matches the user-defined criteria.	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.

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

	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. If a table map was created, uses the **table** keyword and *table-map-name* argument with the **set** commands (for example, **set cos precedence table** *table-map-name*) in the policy map to establish the to-from relationship for mapping attributes.

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 Creating a Class Map for Classifying Network Traffic, page 91 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 Creating a Class Map for Classifying Network Traffic, page 91.

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** *class-map-name* [**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.
Step 4	**match fr-dlci** *dlci-number* **Example:** `Router(config-cmap)# match fr-dlci 500`	(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 Creating a Class Map for Classifying Network Traffic, page 91.
Step 5	**end** **Example:** `Router(config-cmap)# end`	(Optional) Returns to privileged EXEC mode.

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

Note In the following task, the **bandwidth** command is shown at Creating a Policy Map for Applying a QoS Feature to Network Traffic, page 92. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature you want to use.

Note Configuring bandwidth on policies that have the class-default class is supported on physical interfaces such as Gigabit Ethernet (GigE), Serial, Mobile Location Protocol (MLP), and Multilink Frame-Relay (MFR), but it is not supported on logical interfaces such as Virtual Access Interface (VAI), Subinterface, and Frame-Relay on Virtual Circuits (FR-VC).

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:** `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** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created and enters policy-map configuration mode. • Enter the policy map name.

	Command or Action	Purpose
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class1`	Specifies the name of the class and enters policy-map class configuration mode. This class is associated with the class map created earlier. • Enter the name of the class or enter the **class-default**keyword.
Step 5	**bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*} **Example:** `Router(config-pmap-c)# bandwidth percent 50`	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. **Note** The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**show policy-map**	(Optional) Displays all configured policy maps.
Step 8		or
Step 9	**show policy-map** *policy-map* **class** *class-name* **Example:**	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.
Step 10	Router# show policy-map	
Step 11		
Step 12	Router# show policy-map policy1 class class1	
Step 13	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

• What to Do Next, page 94

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **pvc** [*name*] *vpi/vci* [**ilmi**|**qsaal**|**smds**| **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**}*policy-map-name*
7. **end**
8. **show policy-map interface** *type number*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.

	Command or Action	Purpose
Step 4	**pvc** [*name*] *vpi/vci* [**ilmi**|**qsaal**|**smds**|**l2transport**] **Example:** `Router(config-if)# pvc cisco 0/16`	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode. • Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to Attaching the Policy Map to an Interface, page 95.
Step 5	**exit** **Example:** `Router(config-atm-vc)# exit`	(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 Attaching the Policy Map to an Interface, page 95. If you are not attaching the policy map to an ATM PVC, advance to Attaching the Policy Map to an Interface, page 95.
Step 6	**service-policy** {**input** | **output**}*policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	Attaches a policy map to an input or output interface. • Enter the policy map name. **Note** Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Step 8	**show policy-map interface** *type number*
	
	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.

Configuring QoS When Using IPsec VPNs

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.

Note: This task uses the **qospre-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.

>

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *map-name seq-num* **Example:** `Router(config)# crypto map mymap 10`	Enters crypto map configuration mode and creates or modifies a crypto map entry. • Enter the crypto map name and sequence number.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config-crypto-map)# exit`	Returns to global configuration mode.
Step 5	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.
Step 6	**qos pre-classify** **Example:** `Router(config-if)# qos pre-classify`	Enables QoS preclassification.
Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Returns to 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 Example Creating a Class Map for Classifying Network Traffic, page 98.

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
```

Example Configuring QoS When Using IPsec VPNs

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

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10
Router(config-crypto-map)# exit
Router(config)# interface serial4/0/0
Router(config-if)# qos pre-classify
Router(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC	"Applying QoS Features Using the MQC" module
Marking network traffic	"Marking Network Traffic" module
IPsec and VPNs	"Configuring Security for VPNs with IPsec" module
NBAR	"Classifying Network Traffic Using NBAR" module
IPv6 QoS	“IPv6 Quality of Service” module
IPv6 MQC Packet Classification	“IPv6 QoS: MQC Packet Classification” module

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 22 Feature Information for Classifying Network Traffic

Feature Name	Releases	Feature Information
Class-Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature:
Class-Based Marking	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature:

Feature Name	Releases	Feature Information
Packet Classification Using Frame Relay DLCI Number	Cisco IOS XE Release 2.1	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 sections provide information about this feature:
QoS: Local Traffic Matching Through MQC	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature:
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 sections provide information about this feature: The following command was introduced or modified: **matchatm-clp**.
QoS: Match VLAN	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature:
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 sections provide information about this feature: The following command was introduced or modified: **matchmplsexperimental**.

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. The following sections provide information about this feature:
QoS Group: Match and Set for Classification and Marking	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature:

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

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
- Bandwidth remaining percent may not be configured at the topmost level of a hierarchical policy-map
- 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 2000 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
- QoS pre-classify 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 looback101
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

MIB	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

Property Type	Property Value	Property Description

•