Hierarchical Shaping for MPLS VPNs over IP Tunnels on the Cisco 12000 Series Internet Router

Part Number OL-10921-01 (Rev A0), June 26, 2006

The Hierarchical Shaping for MPLS VPNs over IP Tunnels feature allows you to use a hierarchical Quality of Service (QoS) policy that consists of:

- A parent policy to shape the transmission rate for an entire class of traffic
- A child policy to configure individual queue-based features

Hierarchical shaping is supported only on the output interfaces of IP Services Engine (ISE) and Engine 5 line cards that have are configured for the MPLS VPNs over IP Tunnels feature on a Cisco 12000 series Internet router. The MPLS VPNs over IP Tunnels feature sends Layer 3 Virtual Private Network (VPN) traffic over an IP core network using L2TPv3 multipoint tunneling. Hierarchical shaping supports the interconnection of multiple customers, each with multiple VLANs, over an MPLS VPNs over IP Tunnels-based service-provider network.

History for the Hierarchical Shaping for MPLS VPNs over IP Tunnels Feature

Release	Modification
12.0(31)S1	This feature was introduced on the output interfaces of IP Services Engine (ISE) line cards on the Cisco 12000 series Internet router.
12.0(32)SY	Support was added on the Cisco 12000 series Internet router for output interfaces on Engine 5 line cards.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions.

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

Contents

Prerequisites for Hierarchical Shaping for MPLS VPNs over IP Tunnels

- A Cisco 12000 Series ISE or Engine 5 output interface must be properly configured for MPLS VPN and MPLS VPN over IP Tunnels operation before you configure a hierarchical shaping policy.

  For information about how to configure and use the MPLS VPNs over IP Tunnels feature, refer to *MPLS VPNs over IP Tunnels*.

- To configure a hierarchical shaping policy, you enter configuration commands using the Modular Quality of Service Command-line interface (MQC). The MQC simplifies the configuration of Quality of Service (QoS) features on a router running Cisco IOS Software by providing a common command-line syntax across platforms. The MQC contains the following three steps:

  a. Define a traffic class with the **class-ma**p command

  b. Create a service policy by associating the traffic class with one or more QoS policies (using the **policy-map** command).

  c. Attach the service policy to the interface with the **service-policy** command.

  For more information about using the MQC on a Cisco 12000 series Internet router, refer to:

  – *Part 8: Modular Quality of Service Command-Line Interface* in the *Cisco IOS Quality of Service Solutions Configuration Guide*

  – *Cisco 12000 Series Internet Router: Frequently Asked Questions*

Restrictions for Hierarchical Shaping for MPLS VPNs over IP Tunnels

- In Cisco IOS Release 12.0(31)S1, the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature is supported only on the output interfaces of IP Services Engine (ISE) line cards on a Cisco 12000 series Internet router that is deployed as a provider-edge (PE) router in a VPN service provider network configured for MPLS VPNs over IP Tunnels.

  Starting in Cisco IOS Release 12.0(32)SY, the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature is also supported on output interfaces of Engine 5 line cards.

- The Weighted Random Early Detection (WRED) feature must be configured on VLAN queues for hierarchical shaping to operate correctly in case of queue congestion. See "Configuration Examples of Hierarchical Shaping for MPLS VPNs over IP Tunnels" section on page 6 for more information.

  Without WRED, the buffer manager starts to drop packets when the output buffer is used up. This also causes interfaces not configured for hierarchical shaping to drop some (but not all) packets. The result is a limited output rate for interfaces not configured for hierarchical shaping.

- A hierarchical shaping policy is not supported on a Gigabit Ethernet subinterface. You must configure the parent policy on the main interface in interface configuration mode. The following error message appears if you apply a hierarchical QoS policy using the **service-policy** command on a subinterface:

  ```
  % Hierarchical service policy is necessary on egress interface GigabitEthernet6/0.101.
  ```

- The following restrictions apply when you configure VLAN queues:
  - Only one priority queue is supported for each VLAN.
  - Only two user-defined queues are supported for each VLAN; the default and priority queues are reserved and cannot be configured as user-defined queues. (If you use the **hw-module slot** *number* **qos interface queues 8** command, you can increase the number of VLAN queues to eight: six user-defined queues in addition to the priority and default queue.)
  - You must configure traffic policing on the priority queue to enable the use of the user-defined queues.
  - On the priority queue, only the MQC **police** command is supported; other QoS features such as shaping, Weighted Random Early Detection (WRED), and bandwidth allocation are not supported.

    However, on the user-defined and default queues, the **shape**, **bandwidth**, **random-detect**, and **police** commands are all supported.
  - The shape rate that you configure for a VLAN determines the maximum amount of bandwidth that you can configure on each queue. As a result, the police rate of the priority queue plus the combined bandwidth allocated to the two user-defined queues must be less than the configured shape rate for the entire VLAN. This restriction ensures that the interface provides the committed amount of bandwidth.
  - The total of the shape rates on all VLANs configured on Gigabit Ethernet subinterfaces must be less than the amount of bandwidth used on the main interface.
  - You must configure each shape rate in a multiple of 64000 bps.

Information About Hierarchical Shaping for MPLS VPNs over IP Tunnels

To configure the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature, you should understand the following concepts:

Traffic Shaping

Traffic shaping allows you to manage the traffic going out an interface to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to specific policies contracted for it on the interface. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Traffic shaping limits the rate of transmission of data to one of the following:

- A specific configured rate
- A derived rate based on the level of congestion

As a result, output traffic conforms to the policies established for it, and the flow of traffic does not create congestion caused by sent traffic exceeding the access speed of its remote, target interface.

The rate of transfer depends on the token bucket burst size, mean rate, measurement (time) interval. The mean rate is equal to the burst size divided by the interval.

When traffic shaping is enabled, the bit rate of the interface will not exceed the mean rate over any integral multiple of the interval. In other words, during every interval, a maximum of burst size can be sent. Within the interval, however, the bit rate may be faster than the mean rate at any given time.

For more information about traffic shaping, refer to *Policing and Shaping Overview*.

Hierarchical Shaping

Hierarchical shaping allows you to configure two levels of traffic shaping, using a hierarchical service policy. To configure a hierarchical service policy, use the Modular Quality of Service Command-line interface (MQC) as follows:

1. Configure a child policy using the **policy-map** command to define a service policy that shapes the transmission of a specific class of traffic.
2. Nest the child QoS policy within a parent policy map, which shapes the transmission of a larger class of traffic, with the **service-policy** command.

For example, the following example shows how to create a hierarchical service policy in the service policy called parent:

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 20000000
Router(config-pmap-c)# service-policy child
```

In this example, the child policy is responsible for prioritizing and shaping voice traffic and the parent policy is responsible for shaping all customer traffic. Similarly, in the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature, you can define a child policy to shape customer traffic at the queue level, and a parent policy to shape customer traffic at the interface level.

For detailed information about how to use MQC, refer to *Configuring the Modular Quality of Service Command-Line Interface*.

MPLS VPNs over IP Tunnels

The MPLS VPNs over IP Tunnels feature introduces the capability to deploy Layer 3 Virtual Private Network (VPN) services, as proposed in RFC 2547, *BGP/MPLS VPNs*, over an IP core network using L2TPv3 multipoint tunneling instead of Multiprotocol Label Switching (MPLS). This feature allows L2TPv3 tunnels to be configured as multipoint tunnels to transport IP VPN services across the core IP network. Because multipoint tunnels support multiple endpoints, only one tunnel must be configured on each Provider Edge (PE) router. This feature also introduces a simple packet validation mechanism to enforce VPN integrity.

VPN services are traditionally deployed over IP core networks by configuring MPLS or through L2TPv3 tunnels using point-to-point links. The MPLS VPN over IP Tunnels feature allows you to deploy Layer 3 VPN services by configuring multipoint L2TPv3 tunnels over an existing IP core network. This feature is configured only on PE routers and requires no configuration on the core routers.

The L2TPv3 multipoint tunnel network allows Layer 3 VPN services to be carried through the core without the configuration of MPLS. L2TPv3 multipoint tunnelling supports multiple tunnel endpoints, which creates a full mesh topology that requires only one tunnel to be configured on each PE router. This feature provides the capability for VPN traffic to be carried from enterprise networks across cooperating service provider core networks to remote sites.

Note The configuration of the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature described in this document assumes that the core network has already been configured for the MPLS VPNs over IP Tunnels feature as described in *MPLS VPNs over IP Tunnels*.

Configuration Examples of Hierarchical Shaping for MPLS VPNs over IP Tunnels

On an output Gigabit Ethernet ISE or Engine 5 interface that is already configured for MPLS VPNs over IP Tunnels, hierarchical shaping provides support for customer VLAN traffic. For example, a service provider may have multiple customers, and each customer has multiple VLANs. In this case, you can configure a parent shaping policy for a customer's VLANs and apply a child queuing policy to configure QoS features for the individual queues used by each VLAN:

- A default queue
- A priority queue for low-latency traffic
- Two user-definable queues

The following sections provide sample configurations for the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature:

Configuring Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Gigabit Ethernet VLAN Interface

In the following example, you must apply the complete customer-specific MQC configuration to a Gigabit Ethernet ISE interface. Also, you must enter the appropriate **match vlan** commands in each class map to distinguish the VLAN traffic of different customers.

In this example, two groups of VLAN traffic are defined for two customers: VLANs 129 to133 and VLANs 134 to 138. Each VLAN group is assigned to a separate class in the parent policy. Within each group of VLANs, a QoS policy for four VLAN queues is defined: default, voice (priority queue), gold (user-defined), and silver (user-defined).

All output traffic destined for VLANs 129 to 133 is shaped in aggregate to 100Mb. The 100Mb output is, in turn, handled as defined in the policy map child-129-133. All traffic destined for VLANs 134 to 138 is shaped in aggregate to 200Mb and processed as defined in the policy map child-134-138.

The two child queuing policies configure different QoS settings for the queues in each VLAN group. Also, note how the hierarchical QoS policy is used:

- Parent policy—Defines the shape rate of each group of customer VLANs.
- Child policy—Configures the individual queue-based features.

The parent policy-map is used only to configure the VLAN shape rate. Queue-specific policies are configured in the child policy. In addition, we strongly recommend that you configure Random Early Detection (RED) on all queues using the **random-detect** command to avoid possible buffer starvation in cases of permanent queue congestion.

Note The Cisco implementation of RED, called Weighted Random Early Detection (WRED), combines the capabilities of the RED algorithm with IP Precedence. This combination provides for preferential traffic handling for higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested, and provide differentiated performance characteristics for different classes of service. For more information, refer to Configuring *MDRR and WRED on the Cisco 12000 Series Internet Router Using the Modular QoS Command Line Interface*.

Configuring Gigabit Ethernet VLAN Subinterface

```
interface GigabitEthernet 6/0
  no ip address
  service-policy output parent

interface GigabitEthernet6/0.129
  ip vrf forwarding vpn129
  encapsulation dot1q 129
  ip address 209.165.202.1 255.255.255.0

interface GigabitEthernet6/0.130
  ip vrf forwarding vpn129
  encapsulation dot1q 130
  ip address 209.165.203.1 255.255.255.0

interface GigabitEthernet6/0.131
  ip vrf forwarding vpn129
  encapsulation dot1q 131
  ip address 209.165.204.1 255.255.255.0

interface GigabitEthernet6/0.132
  ip vrf forwarding vpn129
  encapsulation dot1q 132
  ip address 209.165.205.1 255.255.255.0

interface GigabitEthernet6/0.133
  ip vrf forwarding vpn129
  encapsulation dot1q 133
  ip address 209.165.206.1 255.255.255.0

interface GigabitEthernet6/0.134
  ip vrf forwarding vpn134
  encapsulation dot1q 134
  ip address 209.165.207.1 255.255.255.0

interface GigabitEthernet6/0.135
  ip vrf forwarding vpn134
  encapsulation dot1q 135
  ip address 209.165.208.1 255.255.255.0

interface GigabitEthernet6/0.136
  ip vrf forwarding vpn134
  encapsulation dot1q 136
  ip address 209.165.209.1  255.255.255.0

interface GigabitEthernet6/0.137
  ip vrf forwarding vpn134
  encapsulation dot1q 137
  ip address 209.165.210.1  255.255.255.0

interface GigabitEthernet6/0.138
  ip vrf forwarding vpn134
```

```
  encapsulation dot1q 138
  ip address 209.165.211.1 255.255.255.0
```

Configuring Customer VLAN

```
class-map VLAN129-133
  match vlan 129 130 131 132 133

class-map VLAN134-138
  match vlan 134 135 136 137 138
```

Configuring VLAN Queue

```
class-map match-any voice
 match ip precedence 5
class-map match-any gold
 match ip precedence 3
class-map match-any silver
 match ip precedence 1
```

Configuring VLAN Queue Service-policy

```
policy-map child-129-133
 class voice
   priority
   police cir percent 10
 class gold
  bandwidth percent 50
  random-detect
  random-detect precedence [prec] [min] [max]
  shape [shape rate]
 class silver
  bandwidth percent 30
  random-detect
  random-detect precedence [prec] [min] [max]
 class class-default
  bandwidth percent 10
  random-detect
  random-detect precedence [prec] [min] [max]
```

Configuring VLAN Queue Service-policy

```
policy-map child-134-138
 class voice
   priority
   police cir percent 30
 class gold
  bandwidth remaining percent 20
  random-detect
  random-detect precedence [prec] [min] [max]
  shape [shape rate]
 class silver
  bandwidth remaining percent 30
  random-detect
  random-detect precedence [prec] [min] [max]
 class class-default
  bandwidth remaining percent 10
  random-detect
  random-detect precedence [prec] [min] [max]
```

Configuring Customer VLAN Shaping with Nested VLAN Queue Policies

```
policy-map parent
 class VLAN129-133
    shape average 100000000
```

```
   service-policy child-129-133
 class VLAN134-138
   shape average 200000000
   service-policy child-134-138
```

Attaching Customer VLAN Service Policy to Gigabit Ethernet Main Interface

```
interface GigabitEthernet 6/0
   service-policy output parent
```

Verifying Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Gigabit Ethernet VLAN Interface

To display the configuration of hierarchical shaping for customer VLANs on a Gigabit Ethernet ISE interface, use the **show policy-map interface** command. The following example shows the output displayed for the sample configuration in Configuring Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Gigabit Ethernet VLAN Interface, page 6.

In the command output for the Gigabit Ethernet interface, VLANs 129 to 133 are assigned to use queues 32-39; VLANs 134 to 138 are assigned to use queues 40 to 47.

```
Router# show policy-map interface gigabitethernet 6/0
 GigabitEthernet6/0
  Service-policy output: parent (1514)

    Class-map: VLAN129-133 (match-all) (1529/5)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: vlan  129-133 (1530)
      Virtual port: 4
      Shape:
        cir 100000000 bps, Be 20000000 bits

      Service-policy : child-129-133 (1515)

        Class-map: voice (match-any) (1516/1)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 5 (1517)
          Class of service queue: 39
          Queue-limit: 4096 packets (default)
          Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
          Priority
          police:
            cir 10%, burst 250 ms, extended burst 250 ms
            10000000 bps, 312500 limit, 312500 extended limit
            conformed 0 packets, 0 bytes; actions:
              transmit
            exceeded 0 packets, 0 bytes; actions:
              drop
            conformed 0 bps, exceed 0 bps

        Class-map: gold (match-any) (1520/3)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 3  (1521)
          Class of service queue: 33
          Queue-limit: 16384 packets (default)
          Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
          Bandwidth: 50000 kbps, Weight: 76800 bytes
```

```
    Class-map: silver (match-any) (1523/4)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1  (1524)
      Class of service queue: 34
      Queue-limit: 16384 packets (default)
      Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
      Bandwidth: 30000 kbps, Weight: 46080 bytes

    Class-map: class-default (match-any) (1526/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1527)
      Class of service queue: 32
      Queue-limit: 512 packets (default)
      Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
      Bandwidth: 10000 kbps, Weight: 15360 bytes

Class-map: VLAN134-138 (match-all) (1546/6)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: vlan  134-138 (1547)
  Shape:
    cir 200000000 bps, Be 40000000 bits

  Service-policy : child-134-138 (1532)

    Class-map: voice (match-any) (1533/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5  (1534)
      Class of service queue: 47
      Queue-limit: 16384 packets (default)
      Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
      Priority
      police:
        cir 30%, burst 250 ms, extended burst 250 ms
        60000000 bps, 1875000 limit, 1875000 extended limit
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: gold (match-any) (1537/3)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 3  (1538)
      Class of service queue: 41
      Queue-limit: 2048 packets (default)
      Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
      Bandwidth: remaining 20%, 0 kbps, Weight: 30720 bytes

    Class-map: silver (match-any) (1540/4)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1  (1541)
      Class of service queue: 42
      Queue-limit: 2048 packets (default)
      Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
      Bandwidth: remaining 30%, 0 kbps, Weight: 46080 bytes

    Class-map: class-default (match-any) (1543/0)
      0 packets, 0 bytes
```

```
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any  (1544)
    Class of service queue: 40
    Queue-limit: 1024 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Bandwidth: remaining 10%, 0 kbps, Weight: 15360 bytes

  Class-map: class-default (match-any) (1549/0)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any  (1550)
```

Configuring Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Channelized T3 SPA Interface

In the following sample configuration of the Hierarchical Shaping for MPLS VPNs over IP Tunnels feature on a Frame Relay interface, note that:

- **match-all** statements are used in the class-map definitions to match customer traffic using a combined Frame Relay data-link connection identifier (DLCI) number and Type-of-Service (ToS)/IP precedence value.
- The parent policy shapes 100 percent of the total bandwidth on the channelized T3 interface.
- In the child policy, DLCI 101 receives 20 percent of the total link speed, shared among customer traffic with IP precedence values of 0, 3, and 5 (4%, 6%, and 10%, respectively, of the total bandwidth available).
- DLCI 102 receives 50% of the link bandwidth shared equally (25% each) across two queues.
- DLCI 103 receives 30% of the link bandwidth shared equally (10% each) across three queues.

Configuring Customer VLAN (by DLCI) and VLAN Queue (by IP Precedence)

```
class-map match-all DLCI101-prec5
 match ip precedence 5
 match fr-dlci 101

class-map match-all DLCI101-prec3
 match ip precedence 3
 match fr-dlci 101

class-map match-all DLCI101-prec0
 match ip precedence 0
 match fr-dlci 101

class-map match-all DLCI102-prec5
 match ip precedence 3
 match fr-dlci 101

class-map match-all DLCI102-prec3
 match ip precedence 0
 match fr-dlci 101

class-map match-all DLCI103-prec3
 match ip precedence 3
 match fr-dlci 103

class-map match-all DLCI103-prec0
 match ip precedence 0
 match fr-dlci 103
```

Configuring VLAN Queue Service-policy

```
policy-map child
  class DLCI101-prec5
    bandwidth percent 10
 class DLCI101-prec3
    bandwidth percent 6
 class DLCI101-prec0
    bandwidth percent 4
 class DLCI102-prec5
    bandwidth percent 25
 class DLCI102-prec3
    bandwidth percent 25
 class DLCI103-prec5
    bandwidth percent 10
 class DLCI103-prec3
    bandwidth percent 10
 class DLCI103-prec0
    bandwidth percent 10
```

Configuring Customer VLAN Shaping with Nested VLAN Queue Policies

```
policy-map parent
  class class-default
    shape average percent 100
    service-policy child
```

Attaching Customer VLAN Service Policy to Channelized T3 Interface

```
interface Serial1/2/3
  no ip address
  no ip directed-broadcast
  encapsulation frame-relay
  no ip mroute-cache
  crc 32
  frame-relay lmi-type ansi
  frame-relay intf-type dce
  service-policy output parent
```

Verifying Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Channelized T3 SPA Interface

To display the configuration of hierarchical shaping for customer VLANs on a channelized T3 SPA (Engine 5) interface, use the **show policy-map interface** command. The following example shows the output displayed for the sample configuration in Configuring Hierarchical Shaping for MPLS VPNs over IP Tunnels on a Channelized T3 SPA Interface, page 11.

```
Router# show policy-map interface serial1/2/3 output
  Serial1/2/3

   Service-policy output: parent (1746)

     Class-map: class-default (match-any) (5574673/0)
       0 packets, 0 bytes
       5 minute offered rate 0 bps, drop rate 0 bps
       Match: any  (5528770)
       Shape:   cir 100 %, Be 200 ms
         cir 44208 kbps, Be 8841600 bits
```

```
Service-policy : child (320240)

  Class-map: DLCI101-prec5 (match-all) (9047217/75)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 5  (13194642)
    Match: fr-dlci  101 (12915826)
    Class of service queue: 197
    Queue-limit: 1024 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Average queue-depth: 0.000 packets
    Bandwidth: 4424 kbps

  Class-map: DLCI101-prec3 (match-all) (9047185/76)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 3  (13415186)
    Match: fr-dlci  101 (12383346)
    Class of service queue: 198
    Queue-limit: 512 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Average queue-depth: 0.000 packets
    Bandwidth: 2656 kbps

  Class-map: DLCI101-prec0 (match-all) (9047137/77)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 0  (15205122)
    Match: fr-dlci  101 (11998322)
    Class of service queue: 199
    Queue-limit: 256 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Average queue-depth: 0.000 packets
    Bandwidth: 1768 kbps

  Class-map: DLCI102-prec5 (match-all) (3738449/80)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 5  (11669602)
    Match: fr-dlci  102 (15390850)
    Class of service queue: 200
    Queue-limit: 2048 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Average queue-depth: 0.000 packets
    Bandwidth: 11056 kbps

  Class-map: DLCI102-prec3 (match-all) (3738417/79)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 3  (11904754)
    Match: fr-dlci  102 (15202434)
    Class of service queue: 201
    Queue-limit: 2048 packets (default)
    Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
    Average queue-depth: 0.000 packets
    Bandwidth: 11056 kbps
```

```
Class-map: DLCI103-prec5 (match-all) (174721/83)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: fr-dlci  103 (1011426)
  Match: ip precedence 5  (784594)
  Class of service queue: 202
  Queue-limit: 1024 packets (default)
  Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
  Average queue-depth: 0.000 packets
  Bandwidth: 4424 kbps

Class-map: DLCI103-prec3 (match-all) (174689/82)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 3  (11182914)
  Match: fr-dlci  103 (4320994)
  Class of service queue: 203
  Queue-limit: 1024 packets (default)
  Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
  Average queue-depth: 0.000 packets
  Bandwidth: 4424 kbps

Class-map: DLCI103-prec0 (match-all) (174641/81)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: fr-dlci  103 (4026082)
  Match: ip precedence 0  (5901570)
  Class of service queue: 204
  Queue-limit: 1024 packets (default)
  Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
  Average queue-depth: 0.000 packets
  Bandwidth: 4424 kbps

Class-map: class-default (match-any) (264257/0)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any  (15143890)
  Class of service queue: 196
  Queue-limit: 4096 packets (default)
  Current queue-depth: 0 packets, Maximum queue-depth: 0 packets
  Average queue-depth: 0.000 packets
```

Additional References

The following sections provide references related to Hierarchical Shaping for MPLS VPNs over IP Tunnels.

Related Documents

Related Topic	Document Title
MPLS VPNs over IP Tunnels: configuration tasks and commands	*MPLS VPNs over IP Tunnels*
QoS information and configuration tasks, including conceptual information about shaping and how to configure distributed traffic shaping using MQC	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 *Policing and Shaping Overview* *Configuring Distributed Traffic Shaping*
Additional QoS commands	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3
Using the Modular Quality of Service Command-Line Interface (MQC)	*Modular Quality of Service Command-Line Interface* and *Modular Quality of Service Command-Line Interface*

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
• No new or modified MIBs are supported 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	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access more content.	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands.

Glossary

L2TPv3—L2TPv3 is an Internet Engineering Task Force (IETF) l2tpext working group draft that provides several enhancements to L2TP for the capability to tunnel any Layer 2 payload over L2TP. Specifically, L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 virtual private networks (VPNs).

MPLS—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

MQC—Modular Quality of Service (QoS) Command-Line Interface (CLI). A CLI structure that allows users to create traffic polices and attach these polices to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic.

policing—Process used to measure the actual traffic flow across a given connection and compare it to the total admissible traffic flow for that connection. Traffic outside of the agreed upon flow can be tagged (where the CLP bit is set to 1) and can be discarded en route if congestion develops. Traffic policing is used in ATM, Frame Relay, and other types of networks.

QoS—quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

shaping—Use of queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that the traffic fits within the promised traffic envelope for the particular connection. Traffic shaping is used in ATM, Frame Relay, and other types of networks. Also known as metering, shaping, and smoothing.

traffic policy—Configuration of QoS features that should be associated with the traffic that has been classified in a user-specified traffic class or classes. A traffic policy contains three elements: a name, a traffic class (specified with the **class** command), and the QoS features.

VLAN—virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses *tunneling* to encrypt all information at the IP level.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.