QoS: Tunnel Marking for L2TPv3 Tunnels

First Published: May 7, 2004
Last Updated: February 28, 2006

The QoS: Tunnel Marking for Layer 2 Tunnel Protocol Version 3 (L2TPv3) Tunnels feature introduces the capability to define and control the quality of service (QoS) for incoming 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 feature information and caveats, see 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 for QoS: Tunnel Marking for L2TPv3 Tunnels" section on page 14.

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

Contents

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

Prerequisites for QoS: Tunnel Marking for L2TPv3 Tunnels

- Cisco Express Forwarding (CEF) must be configured on the interface before L2TPv3 tunnel marking can be used.

  For information on CEF switching, see the "Cisco Express Forwarding Features Roadmap" module.
- Determine the topology and interfaces that need to be configured to mark incoming traffic.

Restrictions for QoS: Tunnel Marking for L2TPv3 Tunnels

- L2TPv3 tunnel marking is supported in input policy-maps only and should not be configured for output policy-maps.
- L2TPv3 tunnel marking is not supported on generic routing encapsulation (GRE) tunnel interfaces.
- It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by **ip tos** commands. The priority of enforcement is as follows when these commands are used simultaneously:
  1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
  2. **ip tos reflect**
  3. **ip tos** *tos-value*

Note This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers configured with the **ip tos** command to use L2TPv3 tunnel marking.

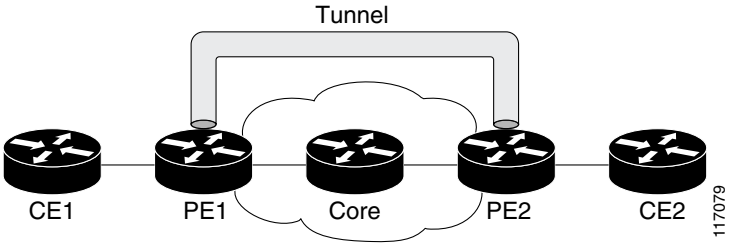
Information About QoS: Tunnel Marking for L2TPv3 Tunnels

L2TPv3 Tunnel Marking Overview

The QoS: Tunnel Marking for L2TPv3 Tunnels feature allows you to define and control QoS for incoming 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) in the header of an L2TPv3 tunneled packet. L2TPv3 tunnel marking can be implemented by using a QoS marking command, such as **set ip** {**dscp** | **precedence**} [**tunnel**], and it can also be implemented in QoS traffic policing. This feature simplifies administrative overhead previously required to control customer bandwidth by allowing you to mark the L2TPv3 tunnel header on the incoming interface on the PE routers.

Figure 1 shows traffic being received from CE1 through PE1's incoming interface on which tunnel marking occurs. The traffic is encapsulated (tunneled) and the tunnel header is marked on PE1. The marked packets travel (tunnel) through the core and are decapsulated automatically on PE2's exit interface. This feature is designed to simplify classifying CE traffic and is configured only in the service provider network. This process is transparent to the customer sites. CE1 and CE2 simply exist as a single network.

Figure 1 Sample Tunnel Marking Topology



Defining Class and Policy Maps for L2TPv3 Tunnel Marking Using the MQC

To configure the tunnel marking for L2TPv3 tunnels, you must define a traffic class, configure 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 the MQC, defining class and policy maps, see the "Applying QoS Features Using the MQC" module.

Configuring L2TPv3 Tunnel Marking

L2TPv3 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. L2TPv3 tunnel marking allows you to mark the header of a L2TPv3 tunnel by setting a DSCP value from 0 to 63 or an IP precedence value from 0 to 7 to control L2TPv3 tunnel traffic bandwidth and priority.

L2TPv3 traffic can also be marked under traffic policing with the **set-dscp-tunnel-transmit** and the **set-prec-tunnel-transmit** commands. The tunnel marking value is from 0 to 63 for the **set-dscp-tunnel-transmit** command and from 0 to 7 for the **set-prec-tunnel-transmit** command. Under traffic policing, tunnel marking can be applied with "conform" and "exceed" 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, L2TPv3 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 L2TPv3 tunnel marking is transparent to customer sites. All internal configuration is preserved.

It is important to distinguish 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 or DSCP values in the header of an IP packet.
- The **set ip precedence tunnel** or **set ip dscp tunnel** commands are used set (mark) the IP precedence or DSCP value in the tunnel header that encapsulates the Layer 2 traffic.

Benefits of L2TPv3 Tunnel Marking

L2TPv3 Tunnel Marking Simplifies Customer Bandwidth Control at the Service Provider Site

L2TPv3 tunnel marking provides a simple mechanism to control the bandwidth of customer L2TPv3 traffic. This feature is configured entirely within the service provider network and only on interfaces that carry incoming traffic on the PE routers.

L2TPv3 Tunnel Marking Requires No Changes to Customer Configurations

The configuration of this feature is transparent to the customer sites and requires no configuration changes and has no impact on customer configurations.

L2TPv3 Definition

L2TPv3 is an Internet Engineering Task Force (IETF) Layer 2 Tunneling Protocol Extensions (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).

L2TPv3 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 L2TPv3 tunnel marking feature with the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** traffic policing commands in policy-map class configuration mode. Under traffic policing, tunnel marking can be applied with “conform” and “exceed” action statements, allowing you to apply a different value automatically for traffic that does not conform to the expected traffic rate.

L2TPv3 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 QoS: Tunnel Marking for L2TPv3 Tunnels

The QoS: Tunnel Marking for L2TPv3 Tunnels feature introduces the capability for a service provider to define and control customer traffic bandwidth and priority on the interfaces of PE routers that carry incoming traffic. This section contains the following procedures.

- Configuring a Class Map, page 5 (required)
- Creating a Policy Map, page 6 (required)
- Attaching the Policy Map to an Interface or a VC, page 8 (required)
- Verifying the Configuration, page 10 (optional)

Configuring a Class Map

To configure a class map, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match** *l2tpv3-match-criteria*
5. **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	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map MATCH_FRDE`	Specifies the name of the class map to be created and enters 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. • Enter class map name. **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.

	Command or Action	Purpose
Step 4	**match** *l2tpv3-match-criteria* **Example:** `Router(config-cmap)# match fr-de`	Enables packet matching based on the specified class. You can enter one of three following **match** commands to define L2TPv3 match criteria tunnel marking: • match atm clp • match cos • match fr-de **Note** This is an example of one match criterion that you can configure with a **match** command. Other criteria include matching on the IP precedence, access-group, or protocol. Enter the **match** command for the criterion you want to specify. For more information about specifying match criteria using the MQC, see the"Applying QoS Features Using the MQC" module.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	(Optional) Exits class-map configuration mode and enters global configuration mode.

Creating a Policy Map

To create a policy map and configure it to set either the precedence or the DSCP value in the header of a L2TPv3 tunneled packet, perform the following tasks.

Restrictions

It is possible to configure L2TPv3 tunnel marking and the **ip tos** command at the same time. However, MQC (L2TPv3) tunnel marking has higher priority over IP ToS commands, meaning that tunnel marking will always rewrite the IP header of the tunnel packet, overwriting the values set by **ip tos** commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

Note This is designed behavior. We recommend that you configure only L2TPv3 tunnel marking and reconfigure any peers, configured with the **ip tos** command, to use L2TPv3 tunnel marking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}

5. **set ip dscp tunnel** *dscp-value*

   or

   set ip precedence tunnel *precedence-value*

   or

   police *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
6. **exit**
7. **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 TUNNEL_MARKING`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class MATCH_FRDE`	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. Also enters policy-map class mode. • Enter the class name or enter the **class-default** keyword.
Step 5	**set ip dscp tunnel** *dscp-value* **Example:** `Router(config-pmap-c)# set ip dscp tunnel 3`	Sets or marks the differentiated services code point (DSCP) value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 63 when configuring DSCP. • Enter the tunnel value.
	or **set ip precedence tunnel** *precedence-value* **Example:** `Router(config-pmap-c)# set ip precedence tunnel 3`	Sets or marks the IP precedence value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 7 when configuring IP precedence. • Enter the tunnel value.

	Command or Action	Purpose
	or **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 8000 conform-action set-dscp-tunnel-transmit 4 exceed-action set-dscp-tunnel-transmit 0` or `Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action set-prec-tunnel-transmit 0`	Configures traffic policing on the basis of the bits per second (bps) specified and the actions specified. If you use traffic policing in your network, you can implement the L2TPv3 tunnel marking feature with the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** traffic policing commands instead of the **set ip dscp tunnel** or the **set ip precedence tunnel** commands shown in Step 5. The tunnel marking value for the traffic policing commands is from 0 to 63 when using **set-dscp-tunnel-transmit** and from 0 to 7 when using **set-prec-tunnel-transmit**. • Enter the bps, any optional burst sizes, and the desired conform and exceed actions. • Enter the **set-dscp-tunnel-transmit** or **set-prec-tunnel-transmit** commands after the **conform-action** keyword. **Note** This is an example of one QoS feature you can configure at this step. Other QoS features include Weighted Random Early Detection (WRED), Weighted Fair Queueing (WFQ), and traffic shaping. Enter the command for the specific QoS feature you want to configure. For more information about QoS features, see the "Quality of Service Overview" module.
Step 6	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits policy-map class configuration mode and enters policy-map configuration mode.
Step 7	**exit** **Example:** `Router(config-pmap)# exit`	(Optional) Exits policy-map configuration mode and enters global configuration mode.

Attaching the Policy Map to an Interface or a VC

To attach the policy map to an interface or a virtual circuit (VC), perform the following task.

Restrictions

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 s to indicate the direction of the interface. This feature is supported only on ingress interfaces with the **input** keyword and should not be configured on egress interfaces with the **output** keyword.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input** | **output**} *policy-map-name*
6. **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 serial 0`	Configures the interface type specified and enters interface configuration mode. • Enter interface type.
Step 4	**pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal** | **smds**] **Example:** `Router(config-if)# pvc cisco 0/16 ilmi`	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode.
Step 5	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	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 varies according your network configuration. • Enter the **input** keyword followed by the policy map name. **Note** For this feature, only the incoming interface configured with the **input** keyword is supported.
Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode.

Verifying the Configuration

To verify that the feature is configured as intended and that either the IP precedence or DSCP value is set as expected, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map interface** *interface-name*

   and/or
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 serial4/0`	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.
and/or		
Step 3	**show policy-map** *policy-map*	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. • Enter a policy map name.
Step 4	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Troubleshooting Tips

The commands in the "Verifying the Configuration" section allow you to verify that you achieved the intended configuration and that the feature is functioning correctly. If, after using the **show** commands listed above, you find that the configuration is not correct or the feature is not functioning as expected, perform these operations.

If the configuration is not the one you intended, complete the following procedures:

- 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 L2TPv3 Tunnels

Example: Configuring Tunnel Marking on L2TPv3 Tunnels

The following is an example of a L2TPv3 tunnel marking configuration. In this sample, a class map called “MATCH_FRDE” has been configured to match traffic based on the Frame Relay DE bit.

```
Router> enable
Router# configure terminal
Router(config)# class-map MATCH_FRDE
Router(config-cmap)# match fr-de
Router(config-cmap)# exit
```

In this 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_FRDE
Router(config-pmap-c)# set ip dscp tunnel 3
Router(config-pmap-c)# end
```

Note This next 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 L2TPv3 tunnel marking. This example shows how L2TPv3 tunnel marking can be enabled under traffic policing.

In this 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** 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 final part of the example configuration, the policy map is attached to serial interface 0 in the inbound (input) direction by specifying the **input** keyword of the **service-policy** command.

```
Router(config)# interface serial 0
Router(config-if)# service-policy input TUNNEL_MARKING
Router(config-if)# end
```

Example: Verifying the Tunnel Marking on L2TPv3 Tunnels Configuration

This section contains sample output from the **show policy-map interface** command and the **show policy-map** command. 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 the tunnel marking on L2TPv3 feature has been configured to set the DSCP in the header of an L2TPv3 tunneled packet.

```
Router# show policy-map interface

 Serial0

  Service-policy input: tunnel

    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0

    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

The following is sample output from the **show policy-map** command. In this sample output, the character string "ip precedence tunnel 4" indicates that the tunnel marking on L2TPv3 feature has been configured to set the IP precedence in the header of an L2TPv3 tunneled packet.

```
Router# show policy-map

Policy Map TUNNEL_MARKING
    Class MATCH_FRDE
      set ip precedence tunnel 4
```

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
DSCP	"Overview of DiffServ for Quality of Service" module

Standards

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

MIBs

MIBs	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 releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support 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 even more content.	http://www.cisco.com/techsupport

Feature Information for QoS: Tunnel Marking for L2TPv3 Tunnels

Table 1 lists the features in this module.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for QoS: Tunnel Marking for L2TPv3 Tunnels

Feature Name	Software Releases	Feature Configuration Information
QoS: Tunnel Marking for L2TPv3 Tunnels	12.0(28)S 12.2(28)SB	The QoS: Tunnel Marking for Layer 2 Tunnel Protocol Version 3 (L2TPv3) Tunnels feature introduces the capability to define and control the quality of service (QoS) for incoming customer traffic on the provider edge (PE) router in a service provider network. In Cisco 12.2(28)SB, this feature was integrated into Cisco IOS Release 12.2(28)SB. The following sections provide information about this feature: • Information About QoS: Tunnel Marking for L2TPv3 Tunnels, page 2 • How to Configure QoS: Tunnel Marking for L2TPv3 Tunnels, page 4