QoS Tunnel Marking for GRE Tunnels

Last Updated: August 11, 2011

The QoS Tunnel Marking for GRE 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.

Note For Cisco IOS Release 12.4(15)T2, the QoS Tunnel Marking for GRE Tunnels feature is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF).

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 Table at the end of this document.

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 configure Cisco Express Forwarding (CEF) on the interface before GRE tunnel marking can be used.
- You must determine the topology and interfaces that need to be configured to mark incoming traffic.

Restrictions for QoS Tunnel Marking for GRE Tunnels

- GRE tunnel marking is supported in input policy maps only and should not be configured for output policy maps.
- It is possible to configure GRE tunnel marking and the **ip tos** command at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) GRE 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:
- **set ip dscp tunnel** or **set ip precedence tunnel** (GRE tunnel marking)
- **ip tos reflect**
- **ip tos** *tos-value*

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

Information About QoS Tunnel Marking for GRE Tunnels

GRE Definition

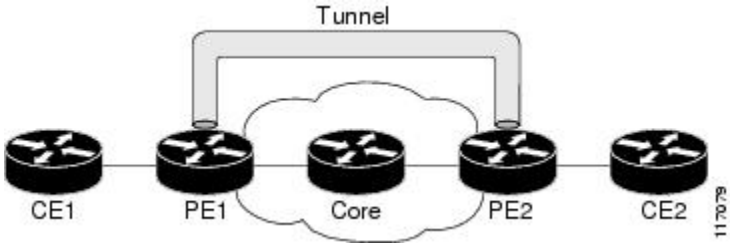
Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

GRE Tunnel Marking Overview

The QoS Tunnel Marking for GRE Tunnels feature allows you to define and control QoS for incoming 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 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 GRE tunnel header on the incoming interface on the PE routers.

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 simply exist as a single network.



GRE Tunnel Marking and the MQC

To configure the tunnel marking for GRE tunnels, you must 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" 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, 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.

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 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.

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 only on interfaces that carry incoming 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** actions (or keywords) of the **police** command 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.

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 fr-de**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map 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.
Step 4	**match fr-de** **Example:** `Router(config-cmap)# match fr-de`	Enables packet matching on the basis of the specified class. You can enter one of the following three **match** commands to define the match criteria for GRE tunnel marking: • match atm clp • match cos • match fr-de **Note** This is only 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 that 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	**end** **Example:** `Router(config-cmap)# end`	(Optional) Returns to privileged EXEC mode.

Creating a Policy Map

Note It is possible to configure GRE tunnel marking and the **ip tos** command at the same time. However, MQC (GRE) 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** (GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos** tos-value

Note This is the designed behavior. We recommend that you configure only GRE tunnel marking and reconfigure any peers, configured with the **ip tos** command, to use GRE 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*
6.
7. **set ip precedence tunnel** *precedence-value*
8.
9. Do one of the following:
   - **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
10. **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	**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 configuration 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 GRE-tunneled packet on the ingress interface. The tunnel marking value is a number from 0 to 63 when configuring DSCP. • Enter the tunnel value.
Step 6		
Step 7	**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 GRE-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.
Step 8		

	Command or Action	Purpose

Step 9	Do one of the following:
	• **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`
	Example:
	`exceed-action set-dscp-tunnel-transmit 0`
	Example:
	Example:
	Example:
	`Router(config-pmap-c)# police 8000 conform-action set-prec-tunnel-transmit 4 exceed-action set-prec-tunnel-transmit 0`
	Example:
		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 GRE tunnel marking feature with the **set-dscp-tunnel-transmit**or **set-prec-tunnel-transmit** keywords of the police command instead of the **set ip dscp tunnel** or the **set ip precedence tunnel** commands.
		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 that 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 that you want to configure. For more information about QoS features, see the "Quality of Service Overview" module.

Step 10	**end** **Example:** `Router(config-pmap-c)# end`	(Optional) Returns to privileged EXEC mode.

Attaching the Policy Map to an Interface or a VC

Note 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. 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. 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.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface serial 0`	Configures the specified interface type and enters interface configuration mode. • Enter the interface type.

Command or Action	Purpose
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 virtual circuit configuration mode.

Step 5 Do one of the following:
• **service-policy** {**input**| **output**} *policy-map-name*
 	
Example:
`Router(config-if)#`
`service-policy input policy1`
 	
Example:
 	
Example:
 	
Example:
`Router(config-if-atm-vc)#`
`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 vary 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 Do one of the following:
• **end**
 	
Example:
`Router(config-if)# end`
 	
Example:
 	
Example:
`Router(config-if-atm-vc)#`
`end`
	(Optional) Returns to privileged EXEC mode.

Verifying the Configuration of Tunnel Marking for GRE Tunnels

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 serial4/0`
		(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 3	**show policy-map** *policy-map*
	
	Example:
	`Router#`
	`show policy-map policy1`
		(Optional) 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) Returns to user EXEC mode.

• Troubleshooting Tips, page 11

Troubleshooting Tips

The commands in the Verifying the Configuration of Tunnel Marking for GRE Tunnels, page 11 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 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_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)# end
```

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 GRE tunnel marking. This example shows how GRE 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** 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 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 for GRE 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 GRE tunnel marking has been configured to set the DSCP value in the header of a GRE-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 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_FRDE
      set ip precedence tunnel 4
```

Additional References

Related Documents

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

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

Feature Name	Releases	Feature Information
QoS Tunnel Marking for GRE Tunnels	12.4(15)T2 12.2(33)SRC 12.2(33)SB	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. **Note** For Cisco IOS Release 12.4(15)T2, the QoS Tunnel Marking for GRE Tunnels feature is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). 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**.