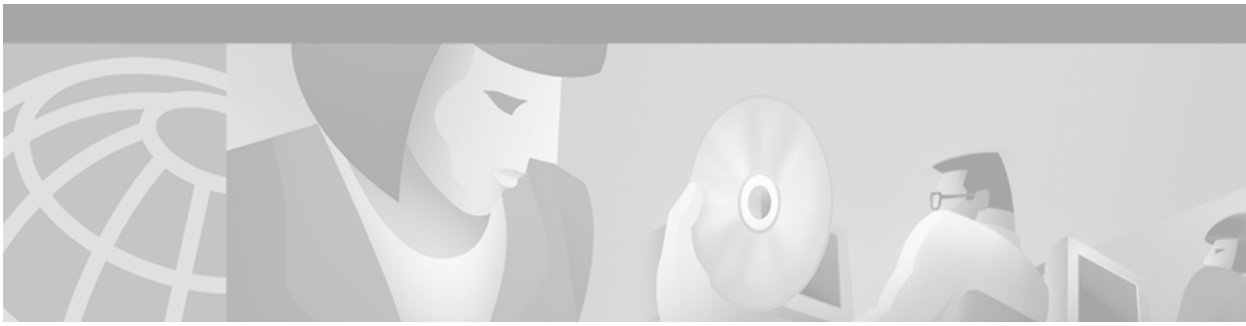

Configuring QoS for Virtual Private Networks

This chapter describes the tasks for configuring the QoS for Virtual Private Networks (VPNs) feature.

For complete conceptual information, see the section "QoS for Virtual Private Networks" in the "Classification Overview" chapter in this book.

For a complete description of the QoS for VPNs commands in this chapter, refer to the *Cisco IOS Quality of Service Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

QoS for VPNs Configuration Task List

To configure the QoS for VPNs feature, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional.

- Configuring QoS for VPNs (Required)
- Verifying QoS for VPNs (Optional)
- Monitoring and Maintaining QoS for VPNs (Optional)

See the end of this chapter for the section "QoS for VPNs Configuration Examples."

Configuring QoS for VPNs

The QoS for VPNs feature, which is enabled by the **qos pre-classify** command, is restricted to tunnel and virtual template interfaces, and crypto map configuration submodes.

For generic routing encapsulation (GRE) and IP in IP (IPIP) tunnel protocols, the **qos pre-classify** command is applied on the tunnel interface, making QoS for VPNs a configuration option on a per-tunnel basis.

For Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) protocols, the **qos pre-classify** command is applied on the virtual template interface. L2TP clients belonging to identical virtual private dial-up network (VPDN) groups inherit the preclassification setting. The **qos pre-classify** command can be configured on a per-VPDN tunnel basis.

For IPSec tunnels, the **qos pre-classify** command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption.

To configure the QoS for VPNs feature on a tunnel or virtual interface basis, use the following commands beginning in global interface mode:

	Command	Purpose
Step 1	`Router(config)# interface [tunnel-name | virtual-template-name]`	Enters interface configuration mode and specifies the tunnel or virtual interface to configure.
Step 2	`Router(config-if)# qos pre-classify`	Enables the QoS for VPNs feature.

To configure the QoS for VPNs feature on the crypto map configuration basis, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto map [map-name]`	Enters crypto map configuration mode and specifies the previously defined crypto map to configure.
Step 2	`Router(config-if)# qos pre-classify`	Enables the QoS for VPNs feature.

Verifying QoS for VPNs

Use the **show interfaces** or **show crypto-map** commands to verify that the QoS for VPNs feature has been successfully enabled on your router.

Note The **show queue** command output displays packet information, including whether the packet is preclassified. In a congested environment, using the **show queue** command might assist in evaluating the environment and reconfiguring your router.

Verifying QoS for VPNs with the show interfaces Command

To verify that the QoS for VPNs feature has been successfully enabled on an interface, use the **show interfaces** command. The following line in the output (which is italicized for emphasis in the example) verifies that the QoS for VPNs feature is successfully enabled.

```
Queuing Strategy: fifo (QOS pre-classification)

Router# show interfaces

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Interface is unnumbered. Using address of Ethernet 3/2 (13.0.0.2)
MTU 1476 bytes, BW 9 Kbit, DLY 500000usec,
reliability 255/255. txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive set (10 sec)
Tunnel source 13.0.0.2 (Ethernet 3/2), destination 13.0.0.1
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Checksumming of packets disabled, fast tunneling enabled
```

```
Last input never, output 00:07:29, output hang never
Last clearing of "show interface" counters 1d05h
Queuing Strategy: fifo (QOS pre-classification)
```

Verifying QoS for VPNs with the show crypto map Command

To verify that the QoS for VPNs feature has been successfully enabled on a crypto map, use the **show crypto map** command. The following line in the output (which is italicized for emphasis in the example) verifies that the QoS for VPNs feature is successfully enabled.

```
QoS pre-classification

Router# show crypto map

Crypto Map "testtag" 10 ipsec-isakmp
Peer = 13.0.0.1
Extended IP access list 102
access-list 102 permit gre host 13.0.0.2 host 13.0.0.1
Current peer:13.0.0.1
Security association lifetime: 4608000 kilobytes/86400 seconds
PFS (Y/N): N
Transform sets={ proposal1,}
QoS pre-classification
```

Monitoring and Maintaining QoS for VPNs

To monitor and maintain the QoS for VPNs feature, use the following commands in user EXEC mode, as needed:

Command	Purpose
Router# **show interfaces** [*tunnel-name* | *virtual-template-name*]	Displays information regarding the tunnel or the virtual template, including the queueing strategy.
Router# **show crypto map** [*map-name*]	Displays information regarding the crypto map. If the QoS for VPNs feature is enabled, a "QoS preclassification" line will appear in the command output.

QoS for VPNs Configuration Examples

The following section provides QoS for VPNs configuration examples:

- Configuring QoS for VPNs for GRE and IPIP Tunnel Protocols Example
- Configuring QoS for VPNs for L2F and L2TP Tunnel Protocols Example
- Configuring QoS for VPNs for IPSec Tunnel Protocols Example

For information on how to configure QoS for VPNs, see the section "QoS for VPNs Configuration Task List" in this chapter.

Configuring QoS for VPNs for GRE and IPIP Tunnel Protocols Example

In the following example, tunnel0 is the tunnel name. The **qos pre-classify** command enables the QoS for VPNs feature on tunnel0.

```
Router(config)# interface tunnel0
Router(config-if)# qos pre-classify
```

Configuring QoS for VPNs for L2F and L2TP Tunnel Protocols Example

In the following example, virtual-template1 is the virtual-template name. The **qos pre-classify** command enables the QoS for VPNs feature on virtual-template1.

```
Router(config)# interface virtual-template1
Router(config-if)# qos pre-classify
```

Configuring QoS for VPNs for IPSec Tunnel Protocols Example

In the following example, secured-partner-X is the crypto map name. The **qos pre-classify** command enables the QoS for VPNs feature on secured-partner-X.

```
Router(config)# crypto map secured-partner-X
Router(config-crypto-map)# qos pre-classify
```