

Quality of Service for Virtual Private Networks

This document describes the solution for making Cisco IOS Quality of Service (QoS) features operate with tunneling and encryption features.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 3
- Monitoring and Maintaining QoS for VPNs, page 6
- Configuration Examples, page 6
- Command Reference, page 7
- Glossary, page 9

Feature Overview

When packets are encapsulated by tunnel or encryption headers, Quality of Service (QoS) features are unable to examine the original packet headers and correctly classify the packets. Packets traveling across the same tunnel have the same tunnel headers, so the packets are treated identically if the physical interface is congested.

With the growing popularity of Virtual Private Networks (VPNs), the need to classify traffic within a traffic tunnel is gaining importance. QoS features have historically been unable to classify traffic within a tunnel. With the introduction of the Quality of Service for Virtual Private Networks (QoS for VPNs) feature, packets can now be classified before tunneling and encryption occur. The process of classifying features before tunneling and encryption is called preclassification.

The QoS for VPNs feature is designed for tunnel interfaces. When the new feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be adjusted in congested environments. The end result is more effective packet tunneling.

Benefits

The QoS for VPNs feature provides a solution for making Cisco IOS Quality of Service services operate in conjunction with tunneling and encryption on an interface. Cisco IOS software can classify packets and apply the appropriate QoS service before the data is encrypted and tunneled. In addition, when packets are marked using the IP Type of Service byte or differentiated services code point (DSCP) values, the markings are copied to the new, encrypted packet. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

Restrictions

- Interfaces running cascading QoS features, such as generic traffic shaping or custom queuing, are required to have QoS for VPNs enabled or disabled on all cascading features. If the QoS for VPNs feature is enabled on one cascading feature, the QoS for VPNs feature must be enabled on all cascading features. Similarly, if the QoS for VPNs feature is disabled on one cascading feature, the QoS for VPNs feature must be disabled on all cascading features.

Related Features and Technologies

- Quality of Service (QoS)
- Generic Routing Encapsulation (GRE)
- Layer 2 Tunneling Protocol (L2TP)
- IPSec

Supported Platforms

- Cisco 7100 series VPN routers
- Cisco 7200 series routers

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

- No new or modified MIBs are supported by this feature.

RFCs

- No new or modified RFCs are supported by this feature.

Prerequisites

Quality of Service

The system must possess the ability to configure QoS features.

Configuration Tasks

See the following sections for configuration tasks for the QoS for VPNs feature. Each task in the list indicates whether the task is optional or required.

- Configuring QoS for VPNs (Required)
- Verifying QoS for VPNs (Optional)

Configuring QoS for VPNs

For Generic Routing Encapsulation (GRE) and IP in IP (IPIP) tunnel protocols, the 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 command is applied on the virtual-template interface. L2TP clients belonging to identical VPDN groups inherit the preclassification setting. The command can be configured on a per-VPDN tunnel basis.

For IPSec tunnels, the 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.

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.

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

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

Verifying QoS for VPNs

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

Verifying QoS for VPNs with the show interfaces Command

To verify that the QoS for VPNs feature has been successfully enabled on your router, use the **show interfaces** command. The following line in the output 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 your router, use the **show crypto map** command. The following line in the output 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={ proposall,}
QoS pre-classification
```

Troubleshooting Tips

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.

Monitoring and Maintaining QoS for VPNs

Command	Purpose
Router# show interface [<i>tunnel name</i> <i>virtual-template name</i>]	Displays information regarding the tunnel or the virtual template, including the queuing strategy.
Router# show crypto map [<i>map-name</i>]	Displays information regarding the crypto map. If the QoS for VPNs feature is enabled, a “QOS Preclassification” line will appear in the command output.

Configuration Examples

This section provides the following configuration examples:

- GRE/IPIP
- L2F/L2TP
- IPSec

GRE and IPIP Tunnel Protocols

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
```

L2F and L2TP Tunnel Protocols

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
```

IPSec Tunnel Protocols

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
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **qos pre-classify**

qos pre-classify

To enable QoS preclassification, use the **qos pre-classify** command. Use the **no** form of this command to disable the QoS preclassification feature.

qos pre-classify

no qos pre-classify

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE3	This command was introduced.

Usage Guidelines

This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The **qos pre-classify** command is unavailable on all other interface types.

The **qos pre-classify** command can be enabled for IP packets only.

Examples

The following example enables the QoS for VPNs feature:

```
router(config-if)# qos pre-classify
```

Related Commands

Command	Description
show interfaces	Displays the contents of an interface.
show queue	Displays the contents of a queue.

Glossary

QoS—Quality of Service. QoS refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

