Quality of Service for VPNs

The QoS for VPNs feature provides a solution for making Cisco IOS QoS 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. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

Information About Quality of Service for Virtual Private Networks

QoS for VPNs

The QoS for VPNs feature provides a solution for making Cisco IOS QoS 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. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and

destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

How to Configure QoS for VPNs

Configuring QoS When Using IPsec VPNs

This task uses the **qos pre-classify** command to enable QoS preclassification for the packet. QoS preclassification is not supported for all fragmented packets. If a packet is fragmented, each fragment might received different preclassifications.

Note This task is required only if you are using IPsec Virtual Private Networks (VPNs). Otherwise, this task is not necessary. For information about IPsec VPNs, see the "Configuring Security for VPNs with IPsec" module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num*
4. **exit**
5. **interface** *type number* [**name-tag**]
6. **qos pre-classify**
7. **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	**crypto map** *map-name seq-num* **Example:** `Router(config)# crypto map mymap 10`	Enters crypto map configuration mode and creates or modifies a crypto map entry. • Enter the crypto map name and sequence number.
Step 4	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Router(config-crypto-map)# exit`	
Step 5	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.
Step 6	**qos pre-classify** **Example:** `Router(config-if)# qos pre-classify`	Enables QoS preclassification.
Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for QoS for VPNs

Example Configuring QoS When Using IPsec VPNs

The following is an example of configuring QoS when using IPsec VPNs. In this example, the **crypto map** command specifies the IPsec crypto map (mymap 10) to which the **qos pre-classify** command will be applied.

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10

Router(config-crypto-map)# qos pre-classify
Router(config-crypto-map)# exit
```

Additional References for QoS for VPNs

Related Documents

Related Topic	Document Title
Cisco commands	Cisco IOS Master Command 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*
Classifying network traffic	"Classifying Network Traffic" module

Related Topic	Document Title
MQC	“Applying QoS Features Using the MQC” module
Marking network traffic	“Marking Network Traffic” module

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 for VPNs

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 for VPNs

Feature Name	Releases	Feature Information
Quality of Service for Virtual Private Networks	12.2(2)T Cisco IOS XE Release 3.9S	The QoS for VPNs feature provides a solution for making Cisco IOS QoS 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. The QoS for VPN feature allows users to look inside the packet so that packet classification can be done based on original port numbers and based on source and destination IP addresses. This allows the service provider to treat mission critical or multi-service traffic with higher priority across their network.

Feature Name	Releases	Feature Information
QoS: Traffic Pre-classification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.