



Classifying Network Traffic

First Published: May 02, 2005
Last Updated: May 29, 2009

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many quality of service (QoS) features on your network. This module contains conceptual information and the configuration tasks for classifying network traffic.

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 Classifying Network Traffic”](#) section on page 15.

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

- [Prerequisites for Classifying Network Traffic, page 2](#)
- [Information About Classifying Network Traffic, page 2](#)
- [How to Classify Network Traffic, page 5](#)
- [Configuration Examples for Classifying Network Traffic, page 11](#)
- [Additional References, page 13](#)
- [Feature Information for Classifying Network Traffic, page 15](#)
- [Glossary, page 17](#)



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

© 2005–2009 Cisco Systems, Inc. All rights reserved.

Prerequisites for Classifying Network Traffic

In order to mark network traffic, Cisco Express Forwarding (CEF) must be configured on both the interface receiving the traffic and the interface sending the traffic.

Information About Classifying Network Traffic

To classify network traffic, you should understand the following concepts:

- [Purpose of Classifying Network Traffic, page 2](#)
- [Benefits of Classifying Network Traffic, page 2](#)
- [MQC and Network Traffic Classification, page 3](#)
- [Network Traffic Classification match Commands and Match Criteria, page 3](#)
- [Traffic Classification Compared with Traffic Marking, page 4](#)

Purpose of Classifying Network Traffic

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling other QoS features such as traffic shaping and traffic policing on your network.

The goal of network traffic classification is to group traffic based on user-defined criteria so that the resulting groups of network traffic can then be subjected to specific QoS treatments. The QoS treatments might include faster forwarding by intermediate routers and switches or reduced probability of the traffic being dropped due to lack of buffering resources.

Identifying and categorizing network traffic into traffic classes (that is, classifying packets) enables distinct handling for different types of traffic, effectively separating network traffic into different categories. This classification can be associated with a variety of match criteria such as the IP Precedence value, differentiated services code point (DSCP) value, class of service (CoS) value, source and destination MAC addresses, input interface, or protocol type. You classify network traffic by using class maps and policy maps with the Modular Quality of Service Command-Line Interface (MQC). For example, you can configure class maps and policy maps to classify network traffic on the basis of the QoS group, Frame Relay DLCI number, Layer 2 packet length, or other criteria that you specify.

Benefits of Classifying Network Traffic

Classifying network traffic allows you to see what kinds of traffic you have, organize the various kinds of network traffic into traffic classes, and treat some types of traffic differently than others. Identifying and organizing network traffic is the foundation for applying the appropriate QoS feature to that traffic, enabling you to allocate network resources to deliver optimal performance for different types of traffic. For example, high-priority network traffic or traffic matching specific criteria can be singled out for special handling, and thus, help to achieve peak application performance.

MQC and Network Traffic Classification

To configure network traffic classification, you use the Modular Quality of Service Command-Line Interface (MQC).

The MQC is a CLI structure that allows you to complete the following tasks:

- Specify the matching criteria used to define a traffic class.
- Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.
- Apply the policy actions specified in the policy map to an interface, subinterface, or ATM permanent virtual circuit (PVC) by using the **service-policy** command.

For more information about the MQC, see the [“Applying QoS Features Using the MQC”](#) module.

Network Traffic Classification match Commands and Match Criteria

Network traffic classification allows you to group or categorize traffic on the basis of whether the traffic meets one or more specific criteria. For example, network traffic with a specific IP precedence can be placed into one traffic class, while traffic with a specific DSCP value can be placed into another traffic class. The network traffic within that traffic class can be given the appropriate QoS treatment, which you can configure in a policy map later.

You specify the criteria used to classify traffic with a **match** command. [Table 1](#) lists the available **match** commands and the corresponding match criterion.

Table 1 *match Commands and Corresponding Match Criterion*

match Commands¹	Match Criterion
match access group	Access control list (ACL) number
match any	Any match criteria
match class-map	Traffic class name
match cos	Layer 2 class of service (CoS) value
match destination-address mac	MAC address
match discard-class	Discard class value
match dscp	DSCP value
match field	Fields defined in the protocol header description files (PHDFs)
match fr-de	Frame Relay discard eligibility (DE) bit setting
match fr-dlci	Frame Relay data-link connection identifier (DLCI) number
match input-interface	Input interface name
match ip rtp	Real-Time Transport Protocol (RTP) port
match mpls experimental	Multiprotocol Label Switching (MPLS) experimental (EXP) value
match mpls experimental topmost	MPLS EXP value in the topmost label
match not	Single match criterion value to use as an unsuccessful match criterion
match packet length (class-map)	Layer 3 packet length in the IP header

Table 1 *match Commands and Corresponding Match Criterion (continued)*

match Commands¹	Match Criterion
match port-type	Port type
match precedence	IP precedence values
match protocol	Protocol type
match protocol (NBAR)	Protocol type known to network-based application recognition (NBAR)
match protocol citrix	Citrix protocol
match protocol fasttrack	FastTrack peer-to-peer traffic
match protocol gnutella	Gnutella peer-to-peer traffic
match protocol http	Hypertext Transfer Protocol
match protocol rtp	RTP traffic
match qos-group	QoS group value
match source-address mac	Source Media Access Control (MAC) address
match start	Datagram header (Layer 2) or the network header (Layer 3)
match tag (class-map)	Tag type of class map
match vlan (QoS)	Layer 2 virtual local-area network (VLAN) identification number

1. Cisco IOS **match** commands can vary by release and platform. For instance, as of Cisco IOS Release 12.2(31)SB2, the **match vlan** (QoS) command is supported on Cisco 10000 series routers only. For more information, see the command documentation for the Cisco IOS release and platform that you are using.

Traffic Classification Compared with Traffic Marking

Traffic classification and traffic marking are closely related and can be used together. Traffic marking can be viewed as an additional action, specified in a policy map, to be taken on a traffic class.

Traffic classification allows you to organize into traffic classes on the basis of whether the traffic matches specific criteria. For example, all traffic with a CoS value of 2 is grouped into one class, and traffic with DSCP value of 3 is grouped into another class. The match criterion is user-defined.

After the traffic is organized into traffic classes, traffic marking allows you to mark (that is, set or change) an attribute for the traffic belonging to that specific class. For instance, you may want to change the CoS value from 2 to 1, or you may want to change the DSCP value from 3 to 2.

The match criteria used by traffic classification are specified by configuring a **match** command in a class map. The marking action taken by traffic marking is specified by configuring a **set** command in a policy map. These class maps and policy maps are configured using the MQC.

[Table 2](#) compares the features of traffic classification and traffic marking.

Table 2 Traffic Classification Compared with Traffic Marking

	Traffic Classification	Traffic Marking
Goal	Groups network traffic into specific traffic classes on the basis of whether the traffic matches the user-defined criteria.	After the network traffic is grouped into traffic classes, modifies the attributes for the traffic in a particular traffic class.
Configuration Mechanism	Uses class maps and policy maps in the MQC.	Uses class maps and policy maps in the MQC.
CLI	In a class map, uses match commands (for example, match cos) to define the traffic matching criteria.	Uses the traffic classes and matching criteria specified by traffic classification. In addition, uses set commands (for example, set cos) in a policy map to modify the attributes for the network traffic. If a table map was created, uses the table keyword and <i>table-map-name</i> argument with the set commands (for example, set cos precedence table table-map-name) in the policy map to establish the to-from relationship for mapping attributes.

How to Classify Network Traffic

This section contains the following procedures:

- [Creating a Class Map for Classifying Network Traffic, page 5](#) (required)
- [Creating a Policy Map for Applying a QoS Feature to Network Traffic, page 6](#) (required)
- [Attaching the Policy Map to an Interface, page 8](#) (required)
- [Configuring QoS When Using IPsec VPNs, page 10](#) (optional)

Creating a Class Map for Classifying Network Traffic

In this procedure, you create a class map to define traffic classes. Within the class map, the appropriate **match** command is used to specify the matching criteria for the traffic classes.

To create the class map and specify the matching criteria, complete the following steps.



Note

In the following task, the **match fr-dlci** command is shown in Step 4. The **match fr-dlci** command matches traffic on the basis of the Frame Relay DLCI number. The **match fr-dlci** command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see [Table 1 on page 3](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all** | **match-any**]

4. **match fr-dlci** *dlci-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map <i>class-map-name</i> [match-all match-any] Example: Router(config)# class-map class1	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode. <ul style="list-style-type: none"> Enter the class map name.
Step 4	match fr-dlci <i>dlci-number</i> Example: Router(config-cmap)# match fr-dlci 500	(Optional) Specifies the match criteria in a class map. Note The match fr-dlci command classifies traffic on the basis of the Frame Relay DLCI number. The match fr-dlci command is just an example of one of the match commands that can be used. For a list of other match commands, see Table 1 on page 3 .
Step 5	end Example: Router(config-cmap)# end	(Optional) Returns to privileged EXEC mode.

Creating a Policy Map for Applying a QoS Feature to Network Traffic

In this procedure, you create and configure a policy map to use the class map. The policy map applies the appropriate QoS feature to the network traffic based on the traffic classification.

To create and configure a policy map, complete the following steps.



Note

In the following task, the **bandwidth** command is shown at [Step 5](#). The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature you want to use.



Note

Configuring bandwidth on policies that have the class-default class is supported on physical interfaces such as Gigabit Ethernet (GigE), Serial, Mobile Location Protocol (MLP), and Multilink Frame-Relay (MFR), but it is not supported on logical interfaces such as Virtual Access Interface (VAI), Subinterface, and Frame-Relay on Virtual Circuits (FR-VC).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** { *class-name* | **class-default** }
5. **bandwidth** { *bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage* }
6. **end**
7. **show policy-map**
or
show policy-map *policy-map* **class** *class-name*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map <i>policy-map-name</i> Example: Router(config)# policy-map policy1	Specifies the name of the policy map to be created and enters policy-map configuration mode. <ul style="list-style-type: none"> Enter the policy map name.
Step 4	class { <i>class-name</i> class-default } Example: Router(config-pmap)# class class1	Specifies the name of the class and enters policy-map class configuration mode. This class is associated with the class map created earlier. <ul style="list-style-type: none"> Enter the name of the class or enter the class-default keyword.
Step 5	bandwidth { <i>bandwidth-kbps</i> remaining percent <i>percentage</i> percent <i>percentage</i> } Example: Router(config-pmap-c)# bandwidth percent 50	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. <ul style="list-style-type: none"> Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. <p>Note The bandwidth command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.</p>

	Command or Action	Purpose
Step 6	<code>end</code> Example: <code>Router(config-pmap-c)# end</code>	Returns to privileged EXEC mode.
Step 7	<code>show policy-map</code> or <code>show policy-map policy-map class class-name</code> Example: <code>Router# show policy-map</code> or Example: <code>Router# show policy-map policy1 class class1</code>	(Optional) Displays all configured policy maps. or (Optional) Displays the configuration for the specified class of the specified policy map. <ul style="list-style-type: none">Enter the policy map name and the class name.
Step 8	<code>exit</code> Example: <code>Router# exit</code>	(Optional) Exits privileged EXEC mode.

What to Do Next

Create and configure as many policy maps as you need for your network. To create and configure additional policy maps, repeat the steps in the [“Creating a Policy Map for Applying a QoS Feature to Network Traffic”](#) section on page 6. Then attach the policy maps to the appropriate interface, following the instructions in the [“Attaching the Policy Map to an Interface”](#) section on page 8.

Attaching the Policy Map to an Interface

After you create the policy map, you must attach it to an interface. Policy maps can be attached to either the input or output direction of the interface.



Note

Depending on the needs of your network, policy maps can be attached to an interface, a subinterface, or an ATM PVC.

To attach the policy map, complete the following steps.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number [name-tag]`
4. `pvc [name] vpi/vci [ilmi | qsaal | smds | l2transport]`
5. `exit`

6. `service-policy {input | output} policy-map-name`
7. `end`
8. `show policy-map interface type number`
9. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>interface type number [name-tag]</code></p> <p>Example: Router(config)# interface serial4/0</p>	<p>Configures an interface type and enters interface configuration mode.</p> <ul style="list-style-type: none"> Enter the interface type and number.
Step 4	<p><code>pvc [name] vpi/vci [ilmi qsaal smds l2transport]</code></p> <p>Example: Router(config-if)# pvc cisco 0/16</p>	<p>(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.</p> <ul style="list-style-type: none"> Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. <p>Note This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to Step 6.</p>
Step 5	<p><code>exit</code></p> <p>Example: Router(config-atm-vc)# exit</p>	<p>(Optional) Returns to interface configuration mode.</p> <p>Note This step is required only if you are attaching the policy map to an ATM PVC and you completed Step 4. If you are not attaching the policy map to an ATM PVC, advance to Step 6.</p>
Step 6	<p><code>service-policy {input output} policy-map-name</code></p> <p>Example: Router(config-if)# service-policy input policy1</p>	<p>Attaches a policy map to an input or output interface.</p> <ul style="list-style-type: none"> Enter the policy map name. <p>Note 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. When using the service-policy command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.</p>

	Command or Action	Purpose
Step 7	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 8	show policy-map interface <i>type number</i> Example: Router# show policy-map interface serial4/0	(Optional) Displays the traffic statistics of all traffic classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. <ul style="list-style-type: none"> • Enter the type and number.
Step 9	exit Example: Router# exit	(Optional) Exits privileged EXEC mode.

Configuring QoS When Using IPsec VPNs



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.

To configure QoS when using IPsec VPNs, complete the following steps.

Restrictions

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 receive different preclassifications.

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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num</i> Example: Router(config)# crypto map mymap 10	Enters crypto map configuration mode and creates or modifies a crypto map entry. <ul style="list-style-type: none"> Enter the crypto map name and sequence number.
Step 4	exit Example: Router(config-crypto-map)# exit	Returns to global configuration mode.
Step 5	interface <i>type number [name-tag]</i> Example: Router(config)# interface serial4/0	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> 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) Returns to privileged EXEC mode.

Configuration Examples for Classifying Network Traffic

This section contains the following examples:

- [Creating a Class Map for Classifying Network Traffic: Example, page 12](#)
- [Creating a Policy Map for Applying a QoS Feature to Network Traffic: Example, page 12](#)
- [Attaching the Policy Map to an Interface: Example, page 12](#)
- [Configuring QoS When Using IPsec VPNs: Example, page 13](#)

Creating a Class Map for Classifying Network Traffic: Example

The following is an example of creating a class map to be used for traffic classification. In this example, a traffic class called `class1` has been created. Traffic with a Frame Relay DLCI value of 500 will be put in this traffic class.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
Router(config-cmap)# end
```



Note

This example uses the `match fr-dlci` command. The `match fr-dlci` command is just an example of one of the `match` commands that can be used. For a list of other `match` commands, see [Table 1 on page 3](#).

Creating a Policy Map for Applying a QoS Feature to Network Traffic: Example

The following is an example of creating a policy map to be used for traffic classification. In this example, a policy map called `policy1` has been created, and the `bandwidth` command has been configured for `class1`. The `bandwidth` command configures the QoS feature CBWFQ.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router# show policy-map policy1 class class1
Router# exit
```



Note

This example uses the `bandwidth` command. The `bandwidth` command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.

Attaching the Policy Map to an Interface: Example

The following is an example of attaching the policy map to an interface. In this example, the policy map called `policy1` has been attached in the input direction of serial interface 4/0.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
Router# show policy-map interface serial4/0
Router# exit
```

Configuring QoS When Using IPsec VPNs: Example

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 is applied.

```
Router> enable
Router# configure terminal
Router(config)# crypto map mymap 10
Router(config-crypto-map)# exit
Router(config)# interface serial4/0
Router(config-if)# qos pre-classify
Router(config-if)# end
```

Additional References

The following sections provide references related to classifying network traffic.

Related Documents

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
Marking network traffic	“Marking Network Traffic” module
IPsec and VPNs	“Configuring Security for VPNs with IPsec” module
NBAR	“Classifying Network Traffic Using NBAR” module
CAR	“Configuring Committed Access Rate” module

Standards

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

MIBs

MIB	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

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Classifying Network Traffic

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Classifying Network Traffic

Feature Name	Releases	Feature Information
Packet Classification Based on Layer 3 Packet Length	12.2(13)T	<p>This feature provides the added capability of matching and classifying network traffic on the basis of the Layer3 length in the IP packet header. The Layer 3 length is the IP datagram plus the IP header. This new match criteria is in addition to the other match criteria, such as the IP precedence, differentiated services code point (DSCP) value, class of service (CoS), currently available.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Classifying Network Traffic, page 2 • How to Classify Network Traffic, page 5
Packet Classification Using Frame Relay DLCI Number	12.2(13)T	<p>The Packet Classification Using the Frame Relay DLCI Number feature allows customers to match and classify traffic based on the Frame Relay data-link connection identifier (DLCI) number associated with a packet. This new match criteria is in addition to the other match criteria, such as the IP Precedence, differentiated services code point (DSCP) value, class of service (CoS), currently available.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Classifying Network Traffic, page 2 • How to Classify Network Traffic, page 5

Table 3 Feature Information for Classifying Network Traffic (continued)

Feature Name	Releases	Feature Information
Quality of Service for Virtual Private Networks	12.2(2)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring QoS When Using IPsec VPNs, page 10 • Configuring QoS When Using IPsec VPNs: Example, page 13
<p>QoS: Match VLAN</p> <p>Note As of Cisco IOS Release 12.2(31)SB2, the QoS: Match VLAN feature is supported on Cisco 10000 series routers only.</p>	12.2(31)SB2	<p>The QoS: Match VLAN feature allows you to classify network traffic on the basis of the Layer 2 virtual local-area network (VLAN) identification number.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Classifying Network Traffic, page 2 • How to Classify Network Traffic, page 5 <p>The following commands were introduced or modified by this feature: match vlan (QoS), show policy-map interface.</p>

Glossary

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

CoS—class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. A CoS definition comprises a virtual route number and a transmission priority field.

DLCI—data-link connection identifier. A value that specifies a PVC or a switched virtual circuit (SVC) in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant (connected devices might use different values to specify the same connection). In the Local Management Interface (LMI) extended specification, DLCIs are globally significant (DLCIs specify individual end devices).

IPsec—IP security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses Internet Key Exchange (IKE) to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

MPLS—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

PVC—permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

VLAN—virtual LAN. A group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical connections instead of physical connections, they are extremely flexible.

VPN—Virtual Private Network. A network that enables traffic to travel securely over a public or shared network. An IPsec VPN uses encryption and tunneling, encapsulating private IP packets into IPsec-encrypted packets to protect information at the IP level.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2009 Cisco Systems, Inc. All rights reserved.

