Per-Session QoS

First Published: March 20, 2006
Last Updated: March 25, 2009

The Per-Session QoS feature is one of two features bundled with the QoS: Broadband Aggregation Enhancements—Phase 1 feature. The Per-Session QoS feature provides the ability to apply quality of service (QoS) features (such as traffic classification, shaping, queuing, and policing) on a per-session basis. The Per-Session QoS feature can be configured using either a virtual template or a RADIUS server.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Per-Session QoS" section on page 17.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

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

Prerequisites for Per-Session QoS

- Verify that the Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA) sessions are enabled.
- Verify that Layer 2 Tunneling Protocol (L2TP) resequencing is disabled.
- A policy map is configured with the QoS feature (for example, traffic policing) to be applied to the network traffic.

Note The Per-Session QoS feature supports hierarchical policy maps.

RADIUS Server-Specific Prerequisites

The following prerequisites apply if you are using a RADIUS server only:

- Authentication, authorization, and accounting (AAA) must be enabled.
- The RADIUS server must be configured.
- The subscriber's user profile on the RADIUS server must be created.

Restrictions for Per-Session QoS

This feature does not support the following items:

- L2TP sequencing.
- Packet dropping (packet discarding). That is, this feature does not allow you to discard packets using the **drop** command.
- Multilink PPP (MLPPP) protocol. That is, multilink bundles are not supported in either a PPP Termination and Aggregation (PTA) or L2TP configuration.
- ATM interfaces (that is, PPPoA sessions) for Cisco IOS Release 12.2(33)SRC.

Information About Per-Session QoS

To configure the Per-Session QoS feature, you should understand the following concepts:

- Benefits of Per-Session QoS, page 2
- Policy Maps and QoS Features, page 3
- Per-Session Traffic Shaping, page 3
- Per-Session Queuing, page 3
- Two Methods for Configuring Per-Session QoS, page 4

Benefits of Per-Session QoS

The ability to apply QoS features on a per-session basis helps the Internet service provider (ISP) to adhere to the Service Level Agreement (SLA) established for handling traffic. Applying QoS on a per-session basis provides a higher degree of granularity when managing traffic on the network.

Policy Maps and QoS Features

A policy map specifies the QoS feature to be applied to network traffic. Examples of QoS features that can be specified in a policy map include traffic classification, shaping, queuing, and policing, among others. Each QoS feature is configured using the appropriate QoS commands.

A RADIUS server is then used to "push" the information in the policy map between the nodes of the network topology.

Policy maps (including hierarchical policy maps) are created using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Per-Session Traffic Shaping

Traffic shaping allows you to control the traffic going out an interface in order to match its flow to the speed of the remote target interface. Traffic shaping ensures that the traffic conforms to policies contracted for it. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data-rate mismatches.

A traffic shaper typically delays excess traffic using a buffer, or a similar mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected.

The Per-Session QoS feature supports traffic shaping. With this feature, traffic shaping is implemented on a per-session basis.

For more information about traffic shaping, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

Per-Session Queuing

The queuing mechanism, Weighted Fair Queuing (WFQ), offers dynamic, fair queuing that divides bandwidth across queues of traffic based on weights. WFQ ensures that all traffic is treated fairly, given its weight.

Class-Based WFQ (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.

The Per-Session QoS feature supports CBWFQ. With this feature, CBWFQ is implemented on a per-session basis.

For more information on CBWFQ, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

Two Methods for Configuring Per-Session QoS

When you configure the Per-Session QoS feature, you can choose one of the following configuration methods:

- Configure the feature using a virtual template.

  This method is considered a "legacy" method. It is of earlier origin and is still an available option for those familiar with using virtual templates.

- Configure the feature using a RADIUS server.

  This method takes advantage of more recent technology and is the recommended method.

How to Configure Per-Session QoS Using a RADIUS Server

The tasks for configuring the Per-Session QoS feature vary according to the configuration method you are using. You can choose to configure the feature using either a virtual template or a RADIUS server.

To configure the feature using a virtual template, see the "Configuring Per-Session QoS Using a Virtual Template" section on page 4.

To configure the feature using a RADIUS server, see the "Configuring Per-Session QoS Using a RADIUS Server" section on page 9.

Configuring Per-Session QoS Using a Virtual Template

This section contains the following tasks:

Configuring the Policy Map

A policy map specifies the QoS feature to be applied to network traffic. Examples of features that can be specified in a policy map include traffic classification and traffic policing.

To configure the policy map, complete the following steps.

Hierarchical Policy Maps

Policy maps can be configured in a hierarchical structure. That is, policy maps can be configured in levels subordinate to one another. The policy map at the highest level is referred to as the "parent" policy map. A subordinate policy map is referred to as the "child" policy map.

A typical hierarchical policy map structure consists of a parent policy map and one child policy map. Configure the child policy map first; then configure the parent policy map. Both types of policy maps are configured in the same manner.

The parent policy map typically contains one class—the class called class-default. The child policy map can contain multiple classes.

Prerequisites

Before configuring the policy map, create the traffic classes and specify the match criteria used to classify traffic. To create traffic classes and specify match criteria, use the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Restrictions

The following restrictions apply to hierarchical policy maps:

- Specify CBWFQ in the child policy map *only*. CBWFQ cannot be specified in the parent policy map.
- Traffic shaping can be specified in *either* the parent policy map *or* the child policy map.

  However, for this feature, you *must* specify traffic shaping in the parent policy map. Specifying traffic shaping in the child policy map is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]
6. **bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*}
7. **priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**]
8. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
9. **service-policy** {**input** | **output**} *policy-map-name*
10. **exit**

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	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	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 name of the policy map. **Note** In a hierarchical policy map structure, the policy map can be either the child or the parent policy map.

	Command or Action	Purpose
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class-default`	Specifies the name of the class whose policy you want to modify, and enters policy-map class configuration mode. • Enter the class name or enter the **class-default** keyword.
Step 5	**shape** [**average** | **peak**] *mean-rate* [[**burst-size**] [*excess-burst-size*]] **Example:** `Router(config-pmap-c)# shape average 128000`	(Optional) Shapes traffic to the indicated bit rate according to the algorithm specified. • Enter the bit rate in bits per second and any optional values. **Note** In a hierarchical policy map structure, traffic shaping can be enabled in *either* the parent policy map *or* the child policy map. However, for this feature, you *must* specify traffic shaping in the parent policy map. Specifying traffic shaping in the child policy map is optional.
Step 6	**bandwidth** {*bandwidth-kbps* | **remaining percent** *percentage* | **percent** *percentage*} **Example:** `Router(config-pmap-c)# bandwidth percent 30`	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. • Enter the bandwidth allocated for the class. **Note** This command configures CBWFQ. In a hierarchical policy map structure, CBWFQ can be configured in the child policy map *only*. CBWFQ cannot be specified in the parent policy map.
Step 7	**priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**] **Example:** `Router(config-pmap-c)# priority 256`	(Optional) Gives priority to a class of traffic belonging to a policy map. • Enter the amount of bandwidth allocated for the class of traffic as either a number (in kbps) or a percentage.
Step 8	**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop`	(Optional) Configures traffic policing. • Enter the bit rate in bits per second (bps), any optional rates, and the actions to take on traffic conforming, exceeding, or violating (optional) the specified rate.
Step 9	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy output child`	(Optional) Attaches the policy map to an input or output interface to be used as the service policy for that interface. • Enter the name of the child policy map. **Note** This command applies to a hierarchical policy map structure *only*. The **service-policy** command attaches the child policy map to the interface.
Step 10	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Returns from policy-map class configuration mode.

What to Do Next

So far, you have created and configured a policy map. If you want to configure additional policy maps (for example, a parent policy map for use in a hierarchical policy map structure), repeat the steps in "Configuring the Policy Map" section on page 4 to configure any additional policy maps.

Otherwise, advance to the "Associating the Policy Map with a Virtual Template" section on page 7.

Note If you are using a RADIUS server, after configuring a policy map, advance to the "Adding the Cisco QoS AV Pairs to the User Profile on the RADIUS Server" section on page 9.

Associating the Policy Map with a Virtual Template

To associate the policy map (where the QoS features are specified) with the virtual template, complete the following steps.

Virtual Templates and Policy Maps

A virtual template is a logical interface configured with generic configuration information for a specific purpose or configuration common to specific users, plus router-dependent information. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed.

A virtual template is configured (defined) on an interface. When a session is enabled (that is, when a packet arrives at the interface), the virtual template inherits the QoS features specified in the policy map for use during the session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **service-policy** {**input** | **output**} *policy-map-name*
5. **exit**

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.

	Command or Action	Purpose
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template and enters interface configuration mode. • Enter the virtual template number.
Step 4	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy output parent`	Attaches the policy map to an input or output interface to be to used as the service policy for that interface. • Enter the name of the policy map. **Note** If you are using a hierarchical policy map structure, this policy map can be either the parent or the child policy map. **Note** This features does not support the **input** keyword. Enter the **output** keyword *only.*
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Returns from interface configuration mode.

Verifying the Configuration

After configuring the policy maps (as many as needed), and associating the policy map(s) with the virtual template on the interface, you may want to verify the configuration. The verification tasks allow you to see whether the policy maps are configured the way you intended.

To verify the configuration, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map session** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]]
3. **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 session** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]] **Example:** `Router# show policy-map session uid 401 output`	Displays the information about the session identified by the unique ID.
Step 3	**exit** **Example:** `Router# exit`	(Optional) Returns from privileged EXEC mode.

What to Do Next

After verifying the configuration, advance to the "Configuration Examples for Per-Session QoS" section on page 11.

Configuring Per-Session QoS Using a RADIUS Server

This section contains the following procedures:

Configuring the Policy Map

A policy map specifies the QoS feature to be applied to network traffic. Examples of features that can be specified in a policy map include packet classification, shaping, queuing, and policing.

To configure the policy map, complete the procedure in the "Configuring the Policy Map" section on page 4 of this document.

After configuring the policy map, return here and complete the steps in "Adding the Cisco QoS AV Pairs to the User Profile on the RADIUS Server" section on page 9.

Adding the Cisco QoS AV Pairs to the User Profile on the RADIUS Server

To configure per-session QoS on the RADIUS server, you must add two Cisco QoS AV pairs to the subscriber's user profile on the RADIUS server. To add the Cisco QoS AV pairs to the subscriber's user profile, complete the following steps on the RADIUS server.

Cisco AV Pairs and VSAs

Cisco AV pairs are part of vendor-specific attributes (VSAs) that allow a policy map to be applied to the router. Cisco AV pairs are a combination of an attribute and a value. The purpose of Cisco VSA (attribute 26) is to communicate vendor-specific information between the router and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

For this configuration, one of two Cisco AV pairs can be used (formatted as shown below):

- lcp:interface-config=service-policy output/input <policy name>

  This Cisco AV pair is considered a “legacy” AV pair. It is of earlier origin but is still an available choice.

- sub-qos-policy-in/out=<policy name>

  This Cisco AV pair takes advantage of more recent technology and is the recommended choice. This Cisco AV pair is the one shown in the configuration tasks and examples.

The Cisco AV pair is added to the subscriber’s user file on the RADIUS server. A subscriber’s user file contains an entry for each user that the RADIUS server will authenticate. Each entry establishes an attribute the user can access.

When looking at a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data.

The Cisco AV pair identifies the policy map that was used to configure the specific QoS features. When the router requests the policy map name (specified in the Cisco AV pair), the policy map is pulled to the router from the RADIUS server when the session is established. The Cisco AV pair applies the appropriate policy map (and, therefore, the QoS feature) directly to the router from the RADIUS server.

SUMMARY STEPS

1. **sub-qos-policy-in/out=<policy name>**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**sub-qos-policy-in/out=<policy name>**
	
	Example:
	`userid Password ="cisco"`
	`Service-Type = Framed,`
	`Framed-Protocol = PPP,`
	`cisco-avpair = "sub-qos-policy-in/out=p23"`
		Enter the Cisco QoS AV pair for policy maps on the RADIUS server in the subscriber’s user file. When the router requests the policy name, the information in the subscriber’s user file is used.
		• Add the Cisco QoS AV pairs to the subscriber’s user file.
		Note The first three lines of the subscriber’s user profile contain the user password, the service type, and the protocol type. This information is entered into the subscriber’s user profile when the profile is first created.

Verifying the Configuration

After adding the Cisco QoS AV Cisco pair to the subscriber's user profile, you may want to verify the configuration. The verification tasks allow you to see whether the QoS features are configured the way you intended.

To verify the configuration, complete the follows steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map session** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]]
3. **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 session** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]] **Example:** `Router# show policy-map session uid 401 output`	Displays the information about the session identified by the unique ID.
Step 3	**exit** **Example:** `Router# exit`	(Optional) Returns from privileged EXEC mode.

Configuration Examples for Per-Session QoS

This section contains the following examples:

Configuring the Policy Map: Example

This section contains examples of a two policy map configurations.

In the first example, a policy map called policy1 has been created and traffic policing has been configured.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# service-policy output policy1
Router(config-pmap-c)# exit
```

In the second example, a hierarchical policy map structure has been configured, with multiple classes and match criteria specified. The child policy map is called policy-child, and the parent policy map is called policy-parent. Priority queuing has been configured in the child policy map, and traffic shaping has been configured in the parent policy map.

```
Router> enable
Router# configure terminal
Router(config)#class-map c1
Router(config-cmap)#match ip dscp ef
Router(config-cmap)#exit
Router(config)#class-map c2
Router(config-cmap)#match ip dscp cs4
Router(config-cmap)#exit
Router(config)#policy-map policy-child
Router(config-pmap)#class c1
Router(config-pmap-c)#priority 256
Router(config-pmap-c)#exit
Router(config-pmap)#class c2
Router(config-pmap-c)#bandwidth 500
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#policy-map policy-parent
Router(config-pmap)#class class-default
Router(config-pmap-c)#shape average 1000000
Router(config-pmap-c)#service-policy policy-child
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#exit
```

Associating the Policy Map with a Virtual Template: Example

This section contains an example of associating a policy map with a virtual template. In this example, the policy map called “policy1” is associated with virtual template 1.

```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

Adding the Cisco QoS AV Pairs to the User Profile on the RADIUS Server: Example

The following is an example of a subscriber's user profile in which the Cisco QoS AV pairs have been added.

The first three lines contain the user password, the service type, and the protocol type. This information is entered into the subscriber's user profile when the user profile is first created.

The last line is an example of the Cisco QoS AV pair added to the user profile.

```
userid    Password ="cisco"
   Service-Type = Framed,
   Framed-Protocol = PPP,
   cisco-avpair = "sub-qos-policy-in/out=p23"
```

Verifying the Configuration: Example

The following section contains sample output of the **show policy-map session** command used to verify the configuration. The sample output allows you to verify the content of the policy maps to ensure that the QoS features (in this case, traffic classification and traffic policing) are configured the way you intended.

```
Router# show policy-map session

SSS session identifier 401 -

  Service-policy output: p23

    Class-map: customer1234 (match-any)
      4464 packets, 249984 bytes
      5 minute offered rate 17000 bps, drop rate 0 bps
      Match: ip dscp cs1  cs2  cs3  cs4
        4464 packets, 249984 bytes
        5 minute rate 17000 bps

    Class-map: customer56 (match-any)
      2232 packets, 124992 bytes
      5 minute offered rate 8000 bps, drop rate 0 bps
      Match: ip dscp cs5  cs6
        2232 packets, 124992 bytes
        5 minute rate 8000 bps
      police:
          cir 20000 bps, bc 10000 bytes
          pir 40000 bps, be 10000 bytes
        conformed 2232 packets, 124992 bytes; actions:
          set-dscp-transmit af21
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit af22
        violated 0 packets, 0 bytes; actions:
          set-dscp-transmit af23
        conformed 8000 bps, exceed 0 bps, violate 0 bps

    Class-map: customer7 (match-any)
      1116 packets, 62496 bytes
      5 minute offered rate 4000 bps, drop rate 4000 bps
      Match: ip dscp cs7
        1116 packets, 62496 bytes
        5 minute rate 4000 bps
```

```
    Class-map: class-default (match-any)
      1236 packets, 68272 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: any
```

In this output of the **show policy-map session** command, traffic classification and traffic policing are applied to the different traffic classes.

```
Router# show policy-map session

SSS session identifier 613 -

  Service-policy output: policy-parent

    Class-map: class-default (match-any)
      206332 packets, 55709640 bytes
      30 second offered rate 863000 bps, drop rate 0 bps
      Match: any
        206332 packets, 55709640 bytes
        30 second rate 863000 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 206334/58186188
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000

      Service-policy : policy-child

        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 52105/14693610

        Class-map: c1 (match-all)
          52104 packets, 14068080 bytes
          30 second offered rate 215000 bps, drop rate 0 bps
          Match: ip dscp ef (46)
          Priority: 256 kbps, burst bytes 6400, b/w exceed drops: 0

        Class-map: c2 (match-all)
          104273 packets, 28153710 bytes
          30 second offered rate 432000 bps, drop rate 0 bps
          Match: ip dscp cs4 (32)
          Queueing
          queue limit 125 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 104273/29404986
          bandwidth 500 kbps

        Class-map: class-default (match-any)
          49955 packets, 13487850 bytes
          30 second offered rate 215000 bps, drop rate 0 bps
          Match: any
            49955 packets, 13487850 bytes
            30 second rate 215000 bps

          queue limit 61 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 49956/14087592
```

Additional References

The following sections provide references related to the Per-Session QoS feature.

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*
QoS features such as traffic classification and traffic policing	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Class maps, policy maps, hierarchical policy maps, and MQC	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Broadband access	"Broadband Access" section of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.4
Broadband aggregation for the Cisco 1000 series router	*Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide*, Release 12.3XI
RADIUS servers and AAA	*Cisco IOS Security Configuration Guide,* Release 12.3
RADIUS accounting and QoS	*RADIUS Accounting for QoS* feature module, Cisco IOS Release 12.2(28)SB
Classification, policing, and marking on Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC)	*QoS: Classification, Policing, and Marking on LAC* feature module, Cisco IOS Release 12.3(8)T

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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands.

Feature Information for Per-Session QoS

Table 1 lists the release history for this feature.

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 1 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 1 Feature Information for Per-Session QoS

Feature Name	Releases	Feature Information
Per-Session QoS	12.2(28)SB 12.2(33)SRC	The Per-Session QoS feature provides the ability to apply quality of service (QoS) features (such as traffic classification, shaping, queuing, and policing) on a per-session basis. In 12.2(28)SB, this feature was introduced on the Cisco 7200 series router. In 12.2(33)SRC, support was added for the Cisco 7600 series router.

Glossary

L2TP—Layer 2 Tunneling Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing virtual private dialup network (VPDN).

LAC—Layer 2 Tunneling Protocol (L2TP) access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol. The connection from the LAC to the remote system is either local or a PPP link.

LNS—L2TP Network Server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC.

PPP— Point-to-Point Protocol. A protocol that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is designed to work with several network layer protocols, such as IP, Internetwork Packet Exchange (IPX), and AppleTalk Remote Access (ARA).

PPPoA—Point-to-Point Protocol over ATM. A feature that allows a PPP session to be initiated on a simple bridging ATM connected client. PPPoA provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator or aggregation concentrator.

PPPoE—Point-to-Point Protocol over Ethernet. A feature that allows a PPP session to be initiated on a simple bridging Ethernet connected client. PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator or aggregation concentrator.

PTA—PPP Termination and Aggregation. A network architecture indicating that after a PPP session is terminated the network traffic is aggregated. For an ISP, the aggregated traffic either remains in the ISP network or routes to the Internet. For a wholesale provider, the aggregated IP traffic will be forwarded to different destinations or domains depending on the service selected.

QoS—quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

SLA—Service Level Agreement. A contract between wholesale service providers and retail service providers.

SSS—Subscriber Service Switch. A switch that provides flexibility on where and how many subscribers are connected to available services and how those services are defined. The primary focus of SSS is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy will manage tunneling of PPP in a policy-based bridging fashion.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

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