QoS: Per-Session Shaping and Queuing on LNS

First Published: April 28, 2005
Last Updated: December 3, 2007

The Quality of Service (QoS): Per-Session Shaping and Queuing on Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) feature provides the ability to shape (for example, transmit or drop) or queue (for transmission later) the traffic going from an Internet service provider (ISP) to an ISP subscriber over LNS. With this feature, the outgoing traffic is shaped or queued on a per-session basis.

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 QoS: Per-Session Shaping and Queuing on LNS" section on page 23.

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 Shaping and Queuing on LNS

- Verify that the PPPoE (or PPPoA) sessions are enabled.
- Verify that L2TP resequencing is disabled.
- This feature uses policy maps in which queuing mechanisms (such as class-based weighted fair queuing [CBWFQ]) are configured.

  A policy map can be configured for a session and for an outgoing interface. With this feature, a policy map (in which a queuing mechanism is configured) cannot be used for both the session and the outgoing interface simultaneously. If a queuing mechanism is in both policy maps, one of these policy maps must be disabled.

Restrictions for Per-Session Shaping and Queuing on LNS

- This feature does not support L2TP sequencing.

Information About Per-Session Shaping and Queuing on LNS

To use the QoS: Per-Session Shaping and Queuing on LNS feature, you should understand the following concepts:

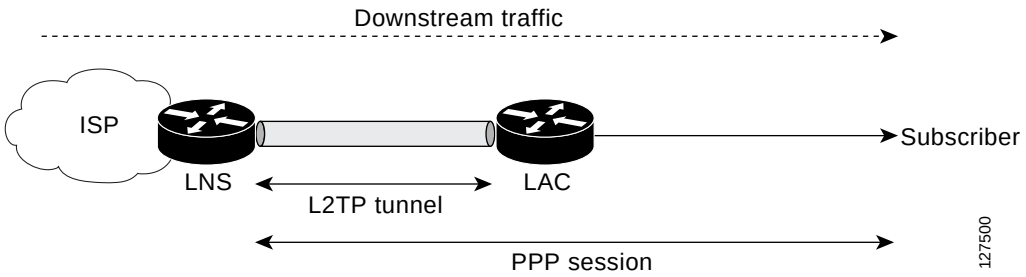
Benefits of Per-Session Shaping and Queuing

The ability to shape or queue traffic on a per-session basis helps to avoid traffic congestion and allows the ISP to adhere to the Service Level Agreement (SLA) established for handling traffic. Shaping or queuing traffic on a per-session basis provides a higher degree of granularity when managing traffic on the network.

Per-Session Shaping and Queuing Sample Topology

Figure 1 is a sample topology for per-session shaping and queuing on LNS.

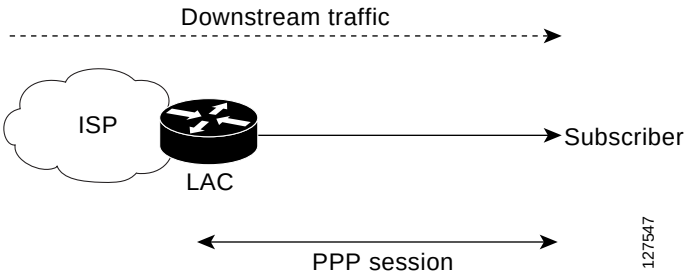
Figure 1 Per-Session Shaping and Queuing Topology (PPP Sessions Forwarded)



In this simplified topology example, downstream traffic is forwarded from the ISP (the source) to an ISP subscriber (the destination) during a PPP session. From an LNS at the ISP, the traffic is transmitted over an L2TP tunnel to an L2TP Access Concentrator (LAC), and then to the subscriber.

Figure 2 illustrates per-session shaping and queuing using a PPP termination and aggregation (PTA) topology.

Figure 2 Per-Session Shaping and Queuing Using a PTA Topology



In this simplified topology example, the downstream traffic is forwarded from the ISP (the source) over a LAC to an ISP subscriber (the destination) during a PPP session.

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 QoS: Per-Session Shaping and Queuing on LNS feature supports traffic shaping. With this feature, traffic shaping is implemented on a per-session basis (that is, when traffic arrives at the interface).

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

Per-Session CBWFQ

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.

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 QoS: Per-Session Shaping and Queuing on LNS feature supports CBWFQ. With this feature, CBWFQ is implemented on a per-session basis (that is, when traffic arrives at the interface).

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

Two Methods for Configuring Per-Session Shaping and Queuing on LNS

When you configure the QoS: Per-Session Shaping and Queuing on LNS 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 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 Shaping and Queuing on LNS

The tasks for configuring the QoS: Per-Session Shaping and Queuing on LNS 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 Queuing and Shaping using a Virtual Template” section on page 4.

To configure the feature using a RADIUS server, see the “Configuring Per-Session Shaping and Queuing using a RADIUS Server” section on page 9.

Configuring Per-Session Queuing and Shaping using a Virtual Template

This section contains the following tasks:

Configuring the Policy Map

A policy map specifies the quality of service (QoS) feature to be applied to network traffic. Examples of features that can be specified in a policy map include class-based weighted fair queuing (CBWFQ) and traffic shaping.

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. **service-policy** *policy-map-name*
8. **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.
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.

	Command or Action	Purpose
Step 7	**service-policy** *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 8	**exit** **Example:** `Router(config-pmap-c)# exit`	(Optional) Exits 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 5 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.
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 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) Exits 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 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) Exits privileged EXEC mode.

What to Do Next?

After verifying the configuration, advance to the "Configuration Examples for Per-Session Shaping and Queuing on LNS" section on page 12.

Configuring Per-Session Shaping and Queuing using a RADIUS Server

This section contains the following tasks:

Configuring the Policy Map

A policy map specifies the quality of service (QoS) feature to be applied to network traffic. Examples of features that can be specified in a policy map include class-based weighted fair queuing (CBWFQ) and traffic shaping.

To configure the policy map, complete the procedure in the "Configuring the Policy Map" section on page 5.

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 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 LNS. 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 LNS 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 LNS requests the policy map name (specified in the Cisco AV pair), the policy map is pulled to the LNS 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 LNS from the RADIUS server.

Prerequisites

- 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.
- The PPP session is established.
- A policy map is configured.

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=parent"`
		Enters the Cisco QoS AV pairs for policy maps on the RADIUS server in the subscriber's user file. When the LNS requests the policy name, the information in the subscriber's user file is used.
		• Add the Cisco QoS AV pair 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 pair to the subscriber's user profile, 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 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) Exits privileged EXEC mode.

Configuration Examples for Per-Session Shaping and Queuing on LNS

This section contains the following examples:

Configuring the Policy Map: Example

This section contains an example of a hierarchical policy map configuration. In this example, two policy maps, one called “parent” (the primary or parent policy map) and one called “child” (the secondary or child policy map) have been configured.

In this example, traffic shaping has been enabled in the parent policy map, and CBWFQ has been enabled in the child policy map. The **service-policy** command has been used to attach the policy map called child to the virtual template interface in the outgoing direction of the interface.

```
Router> enable
Router# configure terminal
Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# exit

Router> enable
Router# configure terminal
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 128000
Router(config-pmap-c)# service-policy child
Router(config-pmap-c)# 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 “parent” is associated with virtual template 1. For a hierarchical policy map structure, the policy map can be either the parent or child policy map.

```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output parent
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=parent"
```

Verifying the Configuration: Example

The following is 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 policy maps are configured the way you intended (that is, that traffic shaping and traffic queuing are enabled and reporting statistics as expected).

```
Router# show policy-map session

 SSS session identifier 1 -

  Service-policy output: parent

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 128 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 512000, bc 12800, be 12800
      target shape rate 512000

      Service-policy : child

        Class-map: prec0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 38 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 30% (153 kbps)

        Class-map: prec2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
```

```
  queue limit 44 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  shape (average) cir 212000, bc 7632, be 7632
  target shape rate 212000

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

  queue limit 44 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```

Additional References

The following sections provide references related to QoS: Per-Session Shaping and Queuing on LNS.

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*, Release 12.4 T
Traffic shaping	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Packet classification	*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
CBWFQ	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Enabling PPPoE and PPPoA sessions	*Cisco IOS Broadband and DSL Configuration Guide*, Release 12.4
Virtual templates	*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4
RADIUS attributes, user files, and dictionary	*Cisco IOS Security Configuration Guide,* Release 12.4
RADIUS servers and AAA	*Cisco IOS Security Configuration Guide,* Release 12.4
Classification, policing, and marking on 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 section documents modified commands only.

- **show policy-map session**

show policy-map session

To display the quality of service (QoS) policy map in effect for the Subscriber Service Switch (SSS) session, use the **show policy-map session** command in user EXEC or privileged EXEC mode.

show policy-map session [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]]

Syntax Description

uid	(Optional) Defines a unique session ID.
uid-number	(Optional) Unique session ID. Ranges from 1 to 65535.
input	(Optional) Displays the upstream traffic of the unique session.
output	(Optional) Displays the downstream traffic of the unique session.
class	(Optional) Identifies the class that is part of the QoS policy-map definition.
class-name	(Optional) Provides a class name that is part of the QoS policy-map definition.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command was also modified to include per-session traffic shaping and traffic queuing statistics, if applicable.
12.2(1st)SRC	This command was integrated into Cisco IOS Release 12.2(1st)SRC and support for the Cisco 7600 series router was added.

Usage Guidelines

Use the **show policy-map session** command with the **uid** keyword to verify the QoS policy map of a unique session ID in the input and output streams in the SSS session.

Use the **show policy-map session** command with the optional **class** *class-name* keyword argument combination to display statistics for a particular class. If you use the **show policy-map session** command without the **class** *class-name* keyword argument combination, statistics for all the classes defined in the QoS policy map display.

Examples

This section contains sample output of the **show policy-map session** command.

Note The output of the **show policy-map session** command varies according to the QoS feature configured in the policy map. For instance, if traffic shaping or traffic queuing are configured in the policy maps, the statistics for those features will be included and the output will vary from what is shown in this section accordingly. Additional self-explanatory fields may appear but the output will be very similar.

The following example from the **show policy-map session** command displays QoS policy-map statistics for traffic in the downstream direction for the QoS policy maps configured:

```
Router# show policy-map session uid 401 output

 SSS session identifier 401 -

  Service-policy output: downstream-policy

    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
      QoS Set
        dscp af11
          Packets marked 4464

    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
      drop

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

Table 1 describes the significant fields shown in the display.

Table 1 show policy-map session Field Descriptions

Field	Description
SSS session identifier	Name of the session identifier.
Service-policy output	Name of the output service policy applied to the specified interface or virtual circuit (VC).

Table 1 show policy-map session Field Descriptions (continued)

Field	Description
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in bps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in bps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria options available, see the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.
QoS Set	Indicates that packet marking is in place.
dscp	Value used in packet marking.
Packets marked	The number of packets marked.
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and peak burst (be) size used for marking packets.
conformed	Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.

Table 1 show policy-map session Field Descriptions (continued)

Field	Description
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.

The following example from the **show policy-map session** command displays QoS policy-map statistics for traffic in the upstream direction for all the QoS policy maps configured:

```
Router# show policy-map session uid 401 input

 SSS session identifier 401 -

  Service-policy input: upstream-policy

    Class-map: class-default (match-any)
      1920 packets, 111264 bytes
      5 minute offered rate 7000 bps, drop rate 5000 bps
      Match: any
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 488 packets, 29452 bytes; actions:
          transmit
        exceeded 1432 packets, 81812 bytes; actions:
          drop
        conformed 7000 bps, exceed 5000 bps
```

Table 2 describes the significant fields shown in the display.

Table 2 show policy-map session Field Descriptions

Field	Description
SSS session identifier	Name of the session identifier.
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Table 2 show policy-map session Field Descriptions (continued)

Field	Description
offered rate	Rate, in bps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in bps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria options available, see the "Modular Quality of Service Command-Line Interface" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and peak burst (be) size used for marking packets.
conformed	Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.

Per-Session Shaping and Queuing show policy-map session Command Output Example

The following is sample output of the **show policy-map session** command when per-session traffic shaping and traffic queuing are enabled. With per-session traffic shaping and queuing configured, traffic shaping and traffic queuing statistics are included in the output.

Note The QoS: Per-Session Shaping and Queuing on LNS feature does not support packet marking. That is, this feature does not support use of the **set** command to mark packets. Therefore, statistics related to packet marking are not included in the output.

```
Router# show policy-map session

 SSS session identifier 1 -

  Service-policy output: parent

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 128 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 512000, bc 12800, be 12800
      target shape rate 512000

      Service-policy : child

        Class-map: prec0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 38 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 30% (153 kbps)

       Class-map: prec2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 44 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 212000, bc 7632, be 7632
          target shape rate 212000

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

```
queue limit 44 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

Table 3 describes the significant fields related to per-session traffic shaping and queuing shown in the display.

Table 3 show policy-map session Field Descriptions - Per-Session Traffic Shaping and Queuing Configured

Field	Description
Queueing	Indicates that traffic queuing is enabled.
queue limit	Displayed the queue limit in packets.
queue depth	Current queue depth of the traffic shaper.
shape (average) cir 212000, bc 7632, be 7632	Indicates that average rate traffic shaping is enabled. Displays the committed information rate (CIR), the committed burst (bc) rate, and the excess burst (be) rate in bytes.
target shape rate 212000	Displays the traffic shaping rate in bytes.

Related Commands

Command	Description
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
show sss session	Displays SSS session status.

Feature Information for QoS: Per-Session Shaping and Queuing on LNS

Table 4 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 4 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 4 Feature Information for QoS: Per-Session Shaping and Queuing on LNS

Feature Name	Releases	Feature Information
QoS: Per-Session Shaping and Queuing on LNS	12.2(27)SBA 12.2(1st)SRC	The Quality of Service (QoS): Per-Session Shaping and Queuing on Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) feature provides the ability to shape (for example, transmit or drop) or queue (for transmission later) the traffic going from an Internet service provider (ISP) to an ISP subscriber over LNS. With this feature, the outgoing traffic is shaped or queued on a per-session basis. In 12.2(27)SBA, this feature was introduced. In 12.2(1st)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.

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.

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).

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

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.