



QoS: Classification, Policing, and Marking on a LAC

First Published: May 27, 2004

Last Updated: April 30, 2007

The QoS: Classification, Policing, and Marking on a LAC feature allows service providers to classify packets based upon the IP type of service (ToS) bits in an embedded IP packet. The classification is used to police the incoming traffic according to the differentiated services code point (DSCP) value. The purpose of classifying the packet by examining its encapsulation is to simplify the implementation and configuration needed for a large number of PPP sessions.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. 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: Classification, Policing, and Marking on a LAC” section on page 13](#).

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

- [Prerequisites for QoS: Classification, Policing, and Marking on a LAC, page 2](#)
- [Restrictions for QoS: Classification, Policing, and Marking on a LAC, page 2](#)
- [Information About QoS: Classification, Policing, and Marking on a LAC, page 2](#)
- [How to Configure QoS: Classification, Policing, and Marking on a LAC, page 4](#)
- [Configuration Examples for QoS: Classification, Policing, and Marking on a LAC, page 5](#)
- [Command Reference, page 10](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 11](#)
- [Feature Information for QoS: Classification, Policing, and Marking on a LAC, page 13](#)
- [Glossary, page 14](#)

Prerequisites for QoS: Classification, Policing, and Marking on a LAC

Configure the Routers

You must configure the client router, the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC), and the L2TP Network Server (LNS) before applying the QoS policy map as described in the [“Configuration Examples for QoS: Classification, Policing, and Marking on a LAC” section on page 5](#).

Verify the State of the Subscriber Service Switch Sessions

You must use the **show sss session** command to verify that the user sessions are enabled on a LAC.

Configure the Interface

You must configure the virtual-template interface before applying the policy map to the session.

Restrictions for QoS: Classification, Policing, and Marking on a LAC

The following restrictions apply to the QoS: Classification, Policing, and Marking on a LAC feature:

- Service-policy on Point-to-Point Protocol over X.25 (PPPoX) interfaces is not supported.
- Class-based queueing and class-based shaping are not supported.
- Layer 2 marking is not supported.
- The QoS MIB is not supported.
- The **clear counters** command does not clear the counters of the QoS policy map.
- Multihop virtual private dial-up networks (VPDNs) are not supported.

Information About QoS: Classification, Policing, and Marking on a LAC

To use the QoS: Classification, Policing, and Marking on a LAC feature, you should understand the following concepts:

- [Benefits of the QoS: Classification, Policing, and Marking on a LAC Feature, page 3](#)
- [QoS Policy Maps and a LAC, page 3](#)
- [Upstream Traffic from the LAC to the LNS, page 3](#)
- [Downstream Traffic from the LNS to the LAC, page 3](#)
- [SSS Sessions on the LAC, page 3](#)

Benefits of the QoS: Classification, Policing, and Marking on a LAC Feature

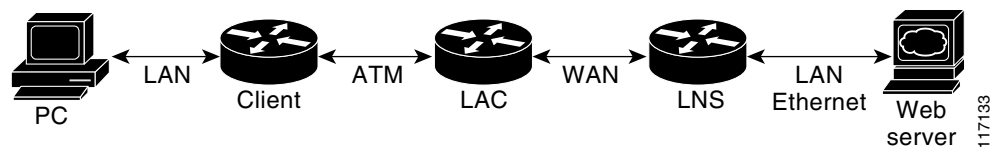
- This feature provides policing and marking on a per-session basis for traffic forwarded into L2TP tunnels to the appropriate LNS and for traffic coming from an L2TP tunnel toward a customer edge router.
- This feature helps recognize the IP ToS value in the Point-to-Point Protocol over Ethernet (PPPoE) encapsulated traffic in order to classify and police the traffic according to the DSCP value.

QoS Policy Maps and a LAC

QoS policing and marking can be achieved by attaching a QoS policy map to the user interface on a LAC in the input and output directions. By using tunnels, input and output service policies can be attached to interfaces. Policy maps get enforced as the packet enters or leaves the tunnel.

Figure 1 shows the deployment of QoS on PPPoE sessions originating at the client and terminating at the LNS.

Figure 1 Sample Topology for QoS on PPoE Sessions



Note

In this sample topology, the LAC is a Cisco 7200 series router.

Upstream Traffic from the LAC to the LNS

Upstream traffic corresponds to packets traversing from the tunnel source to the tunnel destination; in this case, the traffic moves from the LAC to the LNS. The input QoS policy map acts on the upstream traffic before the packet gets encapsulated with the tunnel header.

Downstream Traffic from the LNS to the LAC

Downstream traffic corresponds to packets traversing from the tunnel destination to tunnel source; in this case, the traffic going from the LNS to the LAC. The output QoS policy map acts on the downstream traffic after the tunnel encapsulation is removed from the packet header.

SSS Sessions on the LAC

The Subscriber Service Switch (SSS) session provides you with the infrastructure to apply QoS features on a per-session basis. The SSS session is preconfigured on the virtual template, and you can use this template to provide QoS classification, policing, and marking.

You can verify the statistics of the upstream and downstream traffic from a QoS policy map in an SSS session by using the **show policy-map session** command.

How to Configure QoS: Classification, Policing, and Marking on a LAC

This section contains the following task:

- [Enabling the Service Provider to Verify Traffic Statistics, page 4](#) (optional)

Enabling the Service Provider to Verify Traffic Statistics

To enable a service provider to verify the statistics of the upstream and downstream traffic from a QoS policy map in an SSS session, perform 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 <i>uid-number</i>] [input output [class <i>class-name</i>]] 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 QoS: Classification, Policing, and Marking on a LAC

This section contains the following configuration examples:

- [Configuring the Routers: Example, page 5](#)
- [Verifying the SSS Session: Example, page 8](#)
- [Applying the QoS Policy Map: Example, page 8](#)
- [Configuring the LAC: Example, page 8](#)
- [Verifying the QoS Policy Map for Downstream Traffic: Example, page 8](#)
- [Applying the QoS Policy Map to the Session: Example, page 9](#)
- [Verifying the QoS Policy Map for Upstream Traffic: Example, page 10](#)

**Note**

The following examples show you how to apply QoS policy maps to upstream and downstream user session traffic to achieve the required Service Level Agreements (SLAs) provided by the service provider.

Configuring the Routers: Example

The following example shows the configuration of the routers before the QoS policy map is verified.

Client Configuration

When you log in to the PC, a PPPoE session is established at the client that faces the LAC. This PPPoE session is forwarded through the L2TP tunnel from the LAC to the LNS at which point the PPPoE session terminates.

To apply QoS sessions to the user traffic that originates from the PC to the web server and to the traffic that originates from the web server to the PC, you should apply a QoS policy map to the user session on the LAC in the input and output directions. The classification will be based on the user traffic that originates at the PC and the web traffic that originates at the web server.

This topology supports bidirectional traffic, meaning that traffic can flow from the PC to the web server and from the web server to the PC.

```
username xyz@cisco.com password 0 password1
username qos4-72a password 0 password1
username qos4-72b password 0 password1
```

```
aaa authentication ppp default local
aaa session-id common
```

```
ip cef
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
pppoe-forwarding
```

```
interface ATM5/0
```

```

no ip address
no ip redirects
no ip proxy-arp
no ip mroute-cache
load-interval 30
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
pvc 0/100
 encapsulation aal5snap
 pppoe max-sessions 100
 pppoe-client dial-pool-number 1
!
!interface Dialer1
mtu 1492
ip address negotiated
encapsulation ppp
dialer pool 1
no peer default ip address
no cdp enable
ppp authentication chap callin
ppp chap hostname xyz@cisco.com
ppp chap password 0 cisco
ppp ipcp dns request
!

```

LAC Configuration

The following example shows that the interfaces between the client and the LAC are ATM5/0 interfaces.

```

username xyz@cisco.com password 0 password1
username qos4-72a password 0 password1
username qos4-72b password 0 password1

aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common

ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
vpdn-group 2
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.10.101.2
 local name lac
 no l2tp tunnel authentication
 ip tos reflect
!
pppoe-forwarding

interface Serial3/6
 bandwidth 2015
 ip address 10.10.100.1 255.255.255.0
 no ip redirects
 no ip proxy-arp

```

```

load-interval 30
no keepalive
no cdp enable
!

interface ATM5/0
no ip address
no ip redirects
no ip proxy-arp
load-interval 30
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
pvc 0/100
encapsulation aal5snap
pppoe max-sessions 100
protocol ppp Virtual-Templat1
protocol pppoe
!
!
interface Virtual-Templat1
mtu 1492
no ip address
no peer default ip address
ppp authentication chap
!

```

LNS Configuration

The following example shows that the interface between the LAC and the LNS is a Serial3/6 interface.

```

username xyz@cisco.com password 0 password1
username qos4-72b password 0 password1
username qos4-72a password 0 password1
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common

ip cef
vpdn enable
!
vpdn-group 1
accept-dialin
protocol any
virtual-template 1
terminate-from hostname lac
local name lns
lcp renegotiation always
no l2tp tunnel authentication
ip tos reflect
!

interface Serial3/6
bandwidth 2015
ip address 10.10.100.1 255.255.255.0
no ip redirects
no ip proxy-arp
no ip mroute-cache
load-interval 30
no keepalive
no cdp enable
!

```

Verifying the SSS Session: Example

The following example from the **show sss session** command shows that a user session is enabled on the LAC:

```
Router# show sss session

Current SSS Information: Total sessions 1
Uniq ID Type      State      Service      Identifier      Last Chg
401      PPPoE/PPP  connected  Forwarded      xyz@cisco.com   00:02:06
```

Applying the QoS Policy Map: Example

The following output shows a QoS policy map to be applied to the user session in the output direction, which is the downstream traffic coming into the PC from the web server. The first subclass of traffic within the session is marked with dscp af11, the second subclass is policed, and the third subclass is dropped.

```
class-map match-any customer1234
  match ip dscp cs1 cs2 cs3 cs4
class-map match-any customer56
  match ip dscp cs5 cs6
class-map match-any customer7
  match ip dscp cs7

policy-map downstream-policy
  class customer1234
    set ip dscp af11
  class customer56
    police cir 20000 bc 10000 pir 40000 be 10000
      conform-action set-dscp-transmit af21
      exceed-action set-dscp-transmit af22
      violate-action set-dscp-transmit af23
  class customer7
    drop
```

Configuring the LAC: Example

The following example from the **interface virtual-template** command shows a QoS policy map being applied to the user session on the LAC:

```
Router# configure terminal
Router(config)# interface virtual-template1
Router(config-if)# service-policy output downstream-policy
Router(config-if)# end
```

Verifying the QoS Policy Map for Downstream Traffic: Example

In the following example from the **show policy-map session** command, the QoS policy map is applied for traffic in the downstream direction.

**Note**

The session ID, 401, is obtained from the output of the **show sss session** command in the [“Verifying the SSS Session: Example”](#) section on page 8.

```
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
```

Applying the QoS Policy Map to the Session: Example

In the following example, the service provider applies a QoS policy map to the user session in order to limit the amount of bandwidth that the user session is permitted to consume in the upstream direction from the PC to the web server.

```
Router# configure terminal
Router(config)# policy-map upstream-policy
Router(config-pmap)# class class-default
```

```
Router(config-pmap-c) police cir 8000 bc 1500 be 1500 conform-action transmit
exceed-action drop
Router(config-if)# end
```

This QoS policy map is then applied to the user session as follows:

```
Router# configure terminal
Router(config)# interface virtual-template1
Router(config-if)# service-policy input upstream-policy
Router(config-if)# end
```

Verifying the QoS Policy Map for Upstream Traffic: Example

In the following example from the **show policy-map session** command, the QoS policy map is applied for traffic in the upstream direction.



Note

The session ID, 401, is obtained from the output of the **show sss session** command in the “[Verifying the SSS Session: Example](#)” section on page 8.

```
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
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **show policy-map session**

Additional References

The following sections provide references related to the QoS: Classification, Policing, and Marking on a LAC 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
Information about attaching policy maps to interfaces using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC)	“Applying QoS Features Using the MQC” module
DSCP	“Overview of DiffServ for Quality of Service” 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>	<p>http://www.cisco.com/techsupport</p>

Feature Information for QoS: Classification, Policing, and Marking on a LAC

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 QoS: Classification, Policing, and Marking on a LAC

Feature Name	Releases	Feature Information
QoS: Classification, Policing, and Marking on a LAC	12.3(8)T	<p>The QoS: Classification, Policing, and Marking on the feature allows service providers to classify packets based upon the IP type of service (ToS) bits in an embedded IP packet. The classification is used to police the incoming traffic according to the differentiated services code point (DSCP) value.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About QoS: Classification, Policing, and Marking on a LAC, page 2 How to Configure QoS: Classification, Policing, and Marking on a LAC, page 4 <p>The following command was introduced or modified by this feature: show policy-map session.</p>

Glossary

DSCP—differentiated services code point. A marker in the header of an IP packet that indicates the per-hop behavior given to the packet within the service provider network.

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.

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).

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.

PPoE—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.

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.

ToS—type of service. An 8-bit field carried in an Internet Protocol Version 4 (IPv4) header that can be used to identify packets designated to receive preferential treatment on a class of service (CoS) basis.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.