MobileNext Broadband Gateway

Quality of Service (QoS) for GGSN/PDN Gateway

Published: 2012-04-12

Copyright © 2012, Juniper Networks, Inc.

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

MobileNext Broadband Gateway Quality of Service (QoS) for GGSN/PDN Gateway
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation . . . xi
Documentation and Release Notes . . . xi
Supported Platforms . . . xi
Documentation Conventions . . . xi
Documentation Feedback . . . xiii
Requesting Technical Support . . . xiii
Self-Help Online Tools and Resources . . . xiv
Opening a Case with JTAC . . . xiv

Part 1 Overview

Chapter 1 QoS Overview . . . 3

Quality of Service Overview . . . 3
Initial QoS . . . 4
Differentiated Services . . . 4
QoS Parameters in 3G Networks . . . 4
Default Conversion of (3G) Traffic Classes to (4G) QoS Class Identifiers on the Broadband Gateway . . . 6
QoS Parameters in 4G Networks . . . 7
Aggregate Maximum Bit Rate . . . 8
Allocation and Retention Priority . . . 8
Preemption . . . 9
Call Admission Control Overview . . . 10
Enforcing Call Admission Control . . . 10
Managing Bandwidth . . . 10
Managing the Number of Bearers . . . 11
Managing Resource Thresholds . . . 11
Default Resource Threshold Settings . . . 11
Class of Service (CoS) Policy Profile Overview . . . 12
Policing Subscriber Traffic on the Broadband Gateway Overview . . . 13
Applying Rewrite Rules on Mobile Interfaces Overview . . . 14
Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets . . . 15
Processing of ToS Values for Upstream Subscriber Packets . . . 15
Processing of ToS Values for Downstream Subscriber Packets . . . 16
Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior . . . 17
Configuring QoS on the Broadband Gateway Overview . . . 18

Part 2 Configuration

Chapter 2 Configuration Tasks 23

Configuring the Maximum Number of Bearers 23
Configuring Bandwidth Pools 24
Configuring Preemption for Call Admission Control 25
Configuring Resource Thresholds for 3G and 4G Networks 26
Configuring a Classifier Profile for 3G and 4G Networks 27
Configuring a CoS Policy Profile for 4G Networks 29
Configuring a CoS Policy Profile for 3G Networks 32
Configuring a CoS Policy Profile for 3G and 4G Networks 37
Configuring a Local Policy 43
Applying a Local Policy 44
Configuring Ingress Rewrite Rules for a Mobile Interface 45
Configuring Egress Rewrite Rules for a Mobile Interface 45
Applying Ingress Rewrite Rules to a Mobile Interface 46
Applying Egress Rewrite Rules to Mobile Interfaces 47

Chapter 3 Configuration Examples 49

Example: Configuring Quality of Service on GGSN/P-GW 49

Chapter 4 Configuration Statements 87

[edit unified-edge gateways] Hierarchy Level 87
[edit unified-edge cos-cac] Hierarchy Level 87
[edit unified-edge local-policies] Hierarchy Level 89
aggregated-qos-control (CoS Policy Profiles) 91
allocation-retention-priority (CoS Policy Profiles) 92
bearers-load (Resource Threshold Profiles) 93
classifier-profile (Local Policies) 94
classifier-profiles 95
class-of-service (MobileNext Broadband Gateway) 96
cos-cac 98
cos-policy-profile (Local Policies) 101
cos-policy-profiles 102
cpu (Resource Threshold Profiles) 104
default-bearer-qci (CoS Policy Profiles) 105
description (Class of Service) 106
downgrade-gtp-v1-gbr-bearers (Guaranteed Bit Rate Bandwidth Pools) 107
dl-bandwidth-pool (Local Policies) 108
dscp-ipv6 (Egress Rewrite Rules) 109
dscp-ipv6 (Ingress Rewrite Rules) 110
dscp (Egress Rewrite Rules) 111
dscp (Ingress Rewrite Rules) 112
exceed-action (QoS Policer Action) 113
forwarding-class (QoS Class Identifier) 114
gbr-bandwidth-pools (Class of Service) 115
gbr-bearer (QoS Policer Action) 116
guaranteed-bit-rate-downlink (PDP QoS Control) 117
guaranteed-bit-rate-uplink (PDP QoS Control) 119
high (Resource Threshold Profiles) 121

Copyright © 2012, Juniper Networks, Inc.

inet-precedence (Egress Rewrite Rules) . . . 122
inet-precedence (Ingress Rewrite Rules) . . . 123
ingress-rewrite-rules . . . 124
interfaces (Class of Service) . . . 125
local-policies (QoS) . . . 126
local-policy-profile (Broadband Gateway) . . . 127
loss-priority (QoS Class Identifier) . . . 128
low (Resource Threshold Profiles) . . . 129
maximum-bandwidth (Guaranteed Bit Rate Bandwidth Pools) . . . 130
maximum-bearers (Broadband Gateway) . . . 131
maximum-bit-rate-downlink (Aggregated QoS Control) . . . 132
maximum-bit-rate-downlink (PDP QoS Control) . . . 134
maximum-bit-rate-uplink (Aggregated QoS Control) . . . 136
maximum-bit-rate-uplink (PDP QoS Control) . . . 138
memory (Resource Threshold Profiles) . . . 139
mif (Class of Service) . . . 140
non-gbr-bearer (QoS Policer Action) . . . 141
pdp-qos-control (CoS Policy Profiles) . . . 142
policer-action (CoS Policy Profiles) . . . 143
preemption (GGSN or P-GW) . . . 144
protocol (Egress Rewrite Rules) . . . 145
qci (PDP QoS Control) . . . 146
qos-class-identifier (Classifier Profiles) . . . 147
resource-threshold-profiles (QoS) . . . 148
resource-threshold-profile (Local Policies) . . . 149
rewrite-rules (Egress) . . . 150
roamer-classifier-profile (Local Policies) . . . 151
roamer-cos-policy-profile (Local Policies) . . . 152
ul-bandwidth-pool (Local Policies) . . . 153
unit (Mobile Interface for Class of Service) . . . 154
violate-action (QoS Policer Action) . . . 155
visitor-classifier-profile (Local Policies) . . . 156
visitor-cos-policy-profile (Local Policies) . . . 157

Part 3 Administration

Chapter 5 **Monitoring . . . 161**

Verifying Quality of Service . . . 161

Chapter 6 **Operational Commands . . . 163**

show unified-edge ggsn-pgw statistics traffic-class . . . 164
show unified-edge ggsn-pgw status . . . 166
show unified-edge ggsn-pgw status preemption-list . . . 171
show unified-edge ggsn-pgw subscribers . . . 174
show unified-edge ggsn-pgw subscribers traffic-class . . . 186

Part 4 Index

Index . . . 191

Copyright © 2012, Juniper Networks, Inc.

Copyright © 2012, Juniper Networks, Inc.

List of Figures

Part 1 Overview

Chapter 1 QoS Overview 3

Figure 1: Key QoS Parameters for PDP Context Requests 5
Figure 2: Key QoS Parameters for 4G Default Bearer Requests 8
Figure 3: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags 17

Copyright © 2012, Juniper Networks, Inc.

List of Tables

About the Documentation xi

Table 1: Notice Icons xii
Table 2: Text and Syntax Conventions xii

Part 1 Overview

Chapter 1 QoS Overview 3

Table 3: Traffic Classes for 3G Networks 5
Table 4: Mapping of Traffic Classes to Qos Class Identifiers 6
Table 5: QoS Class Identifiers for 4G Networks 7
Table 6: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values 8
Table 7: Mapping of Release 9 ARP Values to Pre-Release 9 ARP Values 9

Part 2 Configuration

Chapter 2 Configuration Tasks 23

Table 8: Mapping of EPS Bearer ARP to Release 99 Bearer Parameter ARP 26

Chapter 4 Configuration Statements 87

Table 9: default-bearer-qci Configuration Scenarios 105
Table 10: guaranteed-bit-rate-downlink Configuration Scenarios 117
Table 11: guaranteed-bit-rate-downlink Configuration Scenarios 119
Table 12: maximum-bit-rate-downlink Configuration Scenarios 132
Table 13: maximum-bit-rate-downlink Configuration Scenarios 134
Table 14: maximum-bit-rate-uplink Configuration Scenarios 136
Table 15: maximum-bit-rate-uplink Configuration Scenarios 138

Part 3 Administration

Chapter 6 Operational Commands 163

Table 16: show unified-edge ggsn-pgw status Output Fields 167
Table 17: show unified-edge ggsn-pgw status preemption-list Output Fields . . . 172
Table 18: show unified-edge ggsn-pgw subscribers Output Fields 176

Copyright © 2012, Juniper Networks, Inc.

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books .

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX240 Routers
- MX960 Routers
- MX480 Routers

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**

Copyright © 2012, Juniper Networks, Inc.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

Copyright © 2012, Juniper Networks, Inc.

PART 1

Overview

- QoS Overview on page 3

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 1

QoS Overview

- Quality of Service Overview on page 3
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 15
- Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior on page 17
- Configuring QoS on the Broadband Gateway Overview on page 18

Quality of Service Overview

Quality of service (QoS) allows both subscribers and services to be differentiated. Premium subscribers can be prioritized over basic subscribers, while real-time services can be prioritized over non-real-time services. The importance of QoS increases during periods of congestion. An unloaded network can meet the needs of all subscribers and services. However, as the network load increases, the prioritization of traffic determines whether performance for subscribers and services can be maintained or will be degraded.

In a mobile network, network resources are shared among multiple services (including Internet, voice, video, e-mail, and file sharing), each of which has different QoS requirements in terms of required bit rates, acceptable packet loss rates, and packet delay. On the MobileNext Broadband Gateway, you configure QoS profiles and policies to define the QoS treatment for mobile subscribers in 3G and 4G networks.

This topic covers:

- Initial QoS on page 4
- Differentiated Services on page 4
- QoS Parameters in 3G Networks on page 4
- Default Conversion of (3G) Traffic Classes to (4G) QoS Class Identifiers on the Broadband Gateway on page 6
- QoS Parameters in 4G Networks on page 7

Copyright © 2012, Juniper Networks, Inc.

- Aggregate Maximum Bit Rate on page 8
- Allocation and Retention Priority on page 8
- Preemption on page 9

Initial QoS

When a bearer is first established on the broadband gateway, an initial level of QoS is assigned to the bearer based on QoS attributes in the QoS information element (IE) that specify the traffic characteristics for a bearer. Traffic characteristics include delay class, reliability class, precedence class, and traffic class or traffic handling priority (3G subscribers) or QoS Class Identifier (QCI) (4G subscribers).

NOTE: For 3G subscribers, the broadband gateway converts the traffic class to a QCI based on the 3GPP specification 23.401 ANNEX E. For more information, see "QoS Parameters in 3G Networks" on page 4.

Differentiated Services

The broadband gateway supports QoS using the Differentiated Services (DiffServ) model. The DiffServ model is a multiple-service model that addresses different QoS requirements. With DiffServ, the network tries to deliver a particular kind of service based on the QoS specified by each packet, for example, using the 6-bit DiffServ code point (DSCP) setting in IP packets.

Standards for Differentiated Services are described in the following documents:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*

QoS Parameters in 3G Networks

In a 3G network, subscriber traffic is classified based on traffic classes. Each traffic class is associated with a maximum bit rate and (for GBR bearers) a guaranteed bit rate, which can be configured independently for uplink and downlink subscriber traffic. To define the packet-forwarding treatment for bearer requests received on the broadband gateway, you configure a QoS classifier profile to map each traffic class (and for the Interactive class, traffic class, and traffic handling priority) to a forwarding class and packet loss priority (PLP).

NOTE: If no classifier profile is configured on the broadband gateway to map the traffic classes to a forwarding class and packet loss priority, the classification specified in the bearer request, coming from either the Gn or Gi interface, is carried over.

Table 3 on page 5 shows the supported traffic classes, as defined in the 3GPP standards.

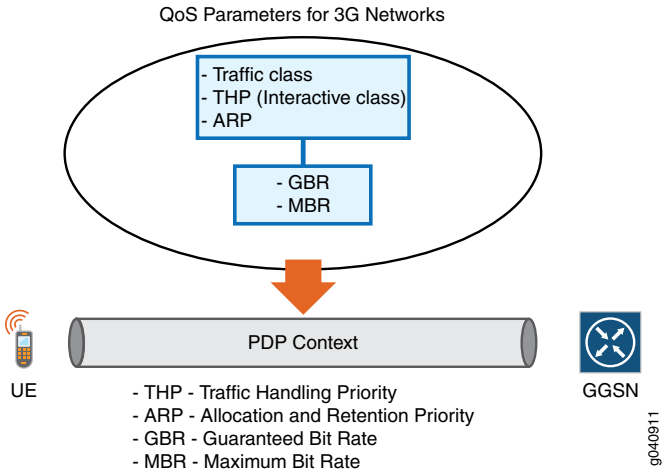
Copyright © 2012, Juniper Networks, Inc.

Table 3: Traffic Classes for 3G Networks

Traffic Class	Description	Example Services
Conversational	Conversational pattern with very low delay and jitter. This is the most delay-sensitive traffic class.	Voice and real-time multimedia messaging such as VoIP and video conferencing.
Streaming	Delay and jitter requirements are not as strict as with conversational traffic class.	Streaming type applications such as video on demand.
Interactive	Interactive class enables prioritization between packet data protocol (PDP) contexts, which allows end-user or service prioritization. Interactive class is associated with a traffic handling priority (THP). THP values can be 1 through 3.	Streaming type applications such as video on demand, Web browsing, and Telnet.
Background	Best effort is acceptable for data delivery. This is the least delay-sensitive traffic class.	Background type applications such as e-mail and FTP.

A policy profile defines the QoS treatment to apply for each traffic class or traffic handling priority. Figure 1 on page 5 shows the QoS parameters that the broadband gateway evaluates to determine whether to limit, upgrade, or reject an incoming PDP context request.

Figure 1: Key QoS Parameters for PDP Context Requests



The guaranteed bit rate (GBR), shown in Figure 1 on page 5, defines the minimum bit rate that is expected to be available to the PDP context when required. The GBR signifies that a certain amount of bandwidth is reserved for the PDP context, regardless of whether or not the GBR is used. Consequently, a PDP context with a GBR always takes up resources even when no traffic is forwarded. Under normal operating conditions, the PDP context should not experience any packet loss due to congestion on the network. This is ensured because the PDP context is subject to admission control during initial setup, and a network allows the PDP context with a GBR only if sufficient resources are available. You can specify the GBR independently for uplink and downlink traffic.

The maximum bit rate (MBR), shown in Figure 1 on page 5, defines the maximum bit rate that is expected to be available to the PDP context when required. An MBR limits

Copyright © 2012, Juniper Networks, Inc.

the bit rate that will be provided to a PDP context. Any traffic that exceeds the MBR can be dropped. You can specify the MBR independently for uplink and downlink traffic.

Default Conversion of (3G) Traffic Classes to (4G) QoS Class Identifiers on the Broadband Gateway

For 3G subscribers, the broadband gateway converts the traffic class to a QCI, based on the 3GPP specification 23.401 ANNEX E. Table 4 on page 6 shows the mapping between standardized QCI values and the Release 99 (GTPv1) QoS parameters.

Table 4: Mapping of Traffic Classes to Qos Class Identifiers

QCI	Traffic Class	Traffic Handling Priority	Signaling Indication	Source Statistics Descriptor
1	Conversational	N/A	N/A	Speech.
2	Conversational	N/A	N/A	Unknown. NOTE: When QCI 2 is mapped to pre-Release 8 QoS parameter values, the Transfer Delay parameter is set to 150 ms. When pre-Rel-8 QoS parameter values are mapped to a QCI, QCI 2 is used for conversational/unknown if the Transfer Delay parameter is greater or equal to 150 ms.
3	Conversational	N/A	N/A	Unknown. NOTE: When QCI 3 is mapped to pre-Release 8 QoS parameter values, the Transfer Delay parameter is set to 80 ms as the lowest possible value, according to TS 23.107 [54]. When pre-Release 8 QoS parameter values are mapped to a QCI, QCI 3 is used for conversational/unknown if the Transfer Delay parameter is lower than 150 ms.
4	Streaming	N/A	N/A	Unknown. NOTE: When QCI 4 is mapped to pre-Release 8 QoS parameter values, it is mapped to Streaming/Unknown. When pre-Release 8 QoS parameter values are mapped to a QCI, Streaming/Unknown and Streaming/Speech are both mapped to QCI 4.
5	Interactive	1	Yes	N/A
6	Interactive	1	No	N/A
7	Interactive	2	No	N/A
8	Interactive	3	No	N/A
9	Background	N/A	N/A	N/A

Copyright © 2012, Juniper Networks, Inc.

QoS Parameters in 4G Networks

In a 4G network, subscriber traffic is classified based on the QoS Class Identifier (QCI), which is associated with priority, specify delay, and packet loss values, and determines the user plane treatment for IP packets transported on a bearer. The QCI determines which bearers are categorized as GBR (dedicated) and which are categorized as non-GBR (default). The broadband gateway supports only default bearers, which correspond to QCI values 5 through 9. The broadband gateway does not support dedicated bearers, which correspond to QCI values 1 through 4. Table 5 on page 7 shows the supported QoS Class Identifiers and the associated set of QoS characteristics, as defined in the 3GPP standards.

Table 5: QoS Class Identifiers for 4G Networks

Qos Class Identifier	Priority	Packet Delay (in milliseconds)	Packet Error Loss Rate	Example Services
5	1	100 ms	10^{-6}	IP Multimedia Subsystem (IMS) signaling
6	7	10 ms	10^{-3}	Voice, video (live streaming), Interactive gaming
7	6	300 ms	10^{-6}	Video (buffered streaming), TCP-based (e-mail, chat, FTP, P2P file sharing)
8	8			
9	9			

The priority associated with each QCI is applied when packets are forwarded across the network. Higher-priority packets are transferred before lower-priority packets.

The packet delay budget associated with each QCI defines an upper boundary for the packet delay between the user equipment and the policy and charging enforcement function (PCEF) within the broadband gateway.

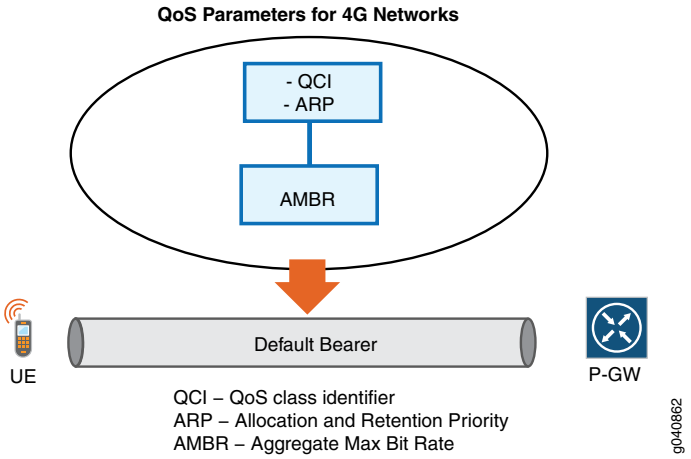
The packet error loss rate defines the percentage of higher layer packets—for example, IP packets—that are lost during periods when the network is not congested.

NOTE: **To define the packet-forwarding treatment for bearer requests received on the broadband gateway, each QCI must be mapped to a forwarding class and packet loss priority (PLP) in the QoS classifier profile. If a QCI is not mapped to a forwarding class and PLP, the classification specified in the bearer request, coming from either the S5 or SGi interface, is carried over.**

A policy profile defines the QoS treatment to be applied to default bearer requests based on the configured QoS parameters. Figure 2 on page 8 shows the QoS parameters that the broadband gateway processes to determine whether to limit, upgrade, or reject bearer requests.

Copyright © 2012, Juniper Networks, Inc.

Figure 2: Key QoS Parameters for 4G Default Bearer Requests



Each default bearer is associated with a QCI value, aggregate maximum bit rate (AMBR), and allocation and retention priority (ARP) value.

Aggregate Maximum Bit Rate

The aggregate maximum bit rate (AMBR) defines the maximum allowed throughput for user equipment (UE) based on the sum of all total bit rates that all non-GBR bearers associated with an access point name (APN) are allowed to use. Thus the AMBR limits the total non-GBR traffic for an APN. You can configure the AMBR independently for uplink and downlink traffic.

Allocation and Retention Priority

The allocation and retention priority (ARP) indicates a priority level for the allocation and retention of bearers. The mobile network uses ARP to decide whether to accept a request to establish a bearer, or reject the request when resources are limited. When performing admission control and network resources are limited, the network uses the ARP to prioritize establishing or modifying bearers with a higher ARP (lower numerically) over bearers with a lower ARP. The more sensitive the QoS application, the lower the corresponding PL or ARP value.

In a 4G network, ARP priority level (PL) values range from 1 through 15, where 1 corresponds to the highest priority and 15 corresponds to the lowest priority. In a 3G network, GTPv1 (pre-Release 9) ARP values range from 1 through 3, where 1 corresponds to the highest priority and 3 corresponds to the lowest priority. By default, the broadband gateway converts GTPv1 pre-Release 9 ARP values to Release 9 ARP values, based on the 3GPP specification 23.401 ANNEX E. Table 6 on page 8 shows how the broadband gateway maps GTPv1 pre-Release 9 bearer parameter ARP values to Release 9 GTPv2 ARP values.

Table 6: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values

GTPv1 Pre-release 9 ARP	GTPv1/v2 Release 9 ARP
1	1
2	6

Copyright © 2012, Juniper Networks, Inc.

Table 6: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values *(continued)*

3	11

Conversely, when subscriber calls come in with a pre-Release 9 ARP value, the broadband gateway performs the required ARP conversion to ensure that the call goes back out with the appropriate ARP value. Table 7 on page 9 shows how the broadband gateway converts GTPv2 Release 9 bearer parameter ARP values to GTPv1 pre-Release 9 ARP values.

Table 7: Mapping of Release 9 ARP Values to Pre-Release 9 ARP Values

GTPv2 Release 9 ARP	GTPv1 Pre-Release 9 ARP
1-5	1
6-10	2
11-15	3

Preemption

The broadband gateway uses ARP values to manage the allocation and retention of resources for bearers. When preemption is enabled, the broadband gateway evaluates the priority level (PL) and the preemption vulnerability (PVI) and preemption capability (PCI) flags in the GTPv2 information element (IE) to determine whether a bearer is a candidate for deletion:

- PCI—Preemption capability information determines whether a bearer with a lower PL priority level should be dropped to free up the required resources.
- PVI—Preemption vulnerability information determines whether a bearer is a candidate for dropping by another preemption capable bearer with a higher PL value.
- PL—Priority level information defines the allocation and retention priority of the bearer.

NOTE: For GTPv1 pre-Release9 PDP contexts, the broadband gateway uses ARP values to determine the preemption capability and preemption vulnerability. By default, preemption capability and preemption vulnerability are enabled. Optionally, you can configure the **gtpv1-pci-disable** and **gtpv1-pvi-disable** options to disable preemption capability and/or preemption vulnerability.

Related Documentation

- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters

Copyright © 2012, Juniper Networks, Inc.

- Example: Configuring QoS and CAC on a S-GW

Call Admission Control Overview

Call admission control (CAC) on the MobileNext Broadband Gateway ensures that required network resources are available for real-time data traffic such as voice and video. CAC maintains information about all resources available on the broadband gateway and resources that have been allocated to bearers. Call admission is based on resource availability and the priority of the bearer, and allows the broadband gateway to reject or downgrade (Create or Modify) bearer requests when the CPU, memory, or bearer load for upstream or downstream traffic exceeds configured CAC thresholds.

This topic covers:

- Enforcing Call Admission Control on page 10
- Managing Bandwidth on page 10
- Managing the Number of Bearers on page 11
- Managing Resource Thresholds on page 11
- Default Resource Threshold Settings on page 11

Enforcing Call Admission Control

Call admission control is enforced only when a local policy profile is configured at the system level or access point name (APN) level on the broadband gateway.

Managing Bandwidth

A bandwidth pool limits the number of guaranteed bit rate (GBR) bearers that can be supported on the broadband gateway (at the APN level or system level) per traffic class. Because a broadband gateway provides a limited amount of bandwidth, it must keep track of the amount of allocated bandwidth when receiving create/update PDP context requests with GBR requirements.

NOTE: **You configure bandwidth pools to provide GBR requirements for 3G networks.**

When admitting bearers, and especially bearers with GBR requirements, the broadband gateway must reject requests when the bandwidth requirements cannot be guaranteed. However, the bandwidth guarantees are only soft guarantees in that the broadband gateway can only restrict the total bandwidth guaranteed to the bearers; no hardware resources are allocated in the system for a bearer with a GBR.

Bandwidth is reserved at the system level or access point name (APN) level based on where the local policy is configured. A local policy configured at the system level specifies a bandwidth pool for all APNs that do not have an explicitly configured bandwidth pool. A bandwidth pool associated with multiple APNs is shared among all bearers of those

Copyright © 2012, Juniper Networks, Inc.

APNs. A local policy configured at the APN level specifies a bandwidth pool reserved for bearers associated with the specific APN.

Managing the Number of Bearers

A broadband gateway provides resource control for the number of bearers. In the control plane and data plane, a set of resources is allocated to each bearer regardless of the bandwidth requirements for the bearer, and the broadband gateway should always specify the maximum number of bearers allowed at the system level, or APN level, or both. When the number of bearers at the system level or APN level reaches the maximum limit, no bearer requests other than delete bearer requests are allowed.

Managing Resource Thresholds

You configure the following parameters for resource thresholds to control traffic flow at either the system level or APN level:

- Bearer load—Specifies a more precise level of admission control when bearer load reaches a configured lower or upper threshold.
- Memory load—Specifies a more precise level of admission control when memory utilization reaches a configured lower or upper threshold.
- CPU load—Specifies a more precise level of admission control when CPU load reaches a configured lower or upper threshold.

Each threshold parameter includes a low and high threshold setting that is associated with an allocation and retention priority (ARP).

NOTE: **When subscriber traffic on the broadband gateway exceeds the configured low or high resource threshold settings, only Create Session requests with a higher-priority ARP (GTPv1) or PL (GTPv2) are allowed. When the limits for bearer, CPU, or memory load exceed the configured threshold limits, the broadband gateway can preempt bearers with a lower priority.**

Default Resource Threshold Settings

If you do not explicitly configure resource threshold settings on the broadband gateway, the following resource threshold default values apply:

- CPU and bearer load default values:
  - High threshold—85 percent
  - High threshold priority level—5
  - Low threshold—70 percent
  - Low threshold priority level—10

Copyright © 2012, Juniper Networks, Inc.

- Memory load default values:
  - High threshold—90 percent
  - High threshold priority level—5
  - Low threshold—80 percent
  - Low threshold priority level—10

Related Documentation

- Quality of Service Overview on page 3
- Class of Service (CoS) Policy Profile Overview on page 12
- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Class of Service (CoS) Policy Profile Overview

You configure a CoS policy profile to define additional call admission control characteristics that the MobileNext Broadband Gateway uses during call setup to decide whether to admit a bearer.

A CoS policy profile manages the following resources and settings:

- Maximum QoS Class Identifier (QCI)—Any default bearer set up with a QCI value that is of a higher priority (numerically lower) than the configured maximum QCI value is downgraded by default. A Modify bearer request that specifies a higher-priority QCI than the configured maximum QCI will be downgraded to a maximum QCI value. Optionally, you can configure the broadband gateway to allow bearers with a lower-priority QCI than the configured value to be upgraded or rejected.
- Maximum (non-GBR) traffic class—Any bearer set up with a traffic class or traffic handling priority that is of a higher traffic class than the configured maximum traffic class (mapped to a QCI value 5 through 9) is downgraded by default. A modify bearer request that is of a higher traffic class than the configured maximum traffic class is downgraded to the maximum traffic class. Optionally, you can configure the broadband gateway to allow bearer requests of a lower traffic class to be upgraded or rejected.
- Aggregate maximum bit rate (AMBR)—In a 4G network, the AMBR specifies the total maximum bit rate for all default bearers associated with a specific gateway or access point name (APN). A bearer request that specifies a higher AMBR than the configured value is downgraded by default. Optionally, you can configure the broadband gateway to allow bearers with a higher AMBR than the configured value to be upgraded or rejected. You can configure different AMBR values for uplink and downlink traffic.
- Maximum bit rate (MBR)—In a 3G network, each traffic class specifies the maximum bit rate allowed. A bearer request that specifies a higher MBR than the configured maximum value is downgraded by default. Optionally, you can configure the broadband

 Copyright © 2012, Juniper Networks, Inc.

gateway to allow bearers with a lower MBR than the configured value to be upgraded or rejected. You can configure different maximum bit rates for uplink and downlink traffic.

- Guaranteed bit rate (GBR)— In a 3G network, the conversational and streaming traffic classes specify the maximum guaranteed bit rate allowed. A bearer request that specifies a higher GBR than the configured maximum value is downgraded by default. Optionally, you can configure the broadband gateway to allow bearers with a lower GBR than the configured value to be upgraded or rejected. You can configure different guaranteed bit rates for uplink and downlink traffic.

Related Documentation

- Quality of Service Overview on page 3
- Call Admission Control Overview on page 10
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Policing Subscriber Traffic on the Broadband Gateway Overview

To enforce bandwidth limits for subscriber traffic on the MobileNext Broadband Gateway, you configure the policer action to apply to traffic that exceeds the maximum or guaranteed bit rates. The policer actions control packet behavior by transmitting or changing the packet loss priority (PLP) of packets when the subscriber traffic exceeds configured limits.

The broadband gateway uses a two-rate policer to enforce bandwidth rates.

For non-GBR bearers, you configure the **violate-action** option to specify how bearer data is treated when it exceeds the maximum bit rate (MBR) value with which a PDP context was established or the aggregate maximum bit rate (AMBR) value with which a default bearer was established. For GBR bearers, you configure the **violate-action** option to specify how bearer data is treated traffic exceeds the configured MBR and the **exceed-action** option to define how guaranteed bit rate (GBR) bearer data is treated when the GBR exceeds the GBR value with which the PDP context was established.

For non-GBR bearers, **violate-action** option allows either of the following actions for bearers that exceed the AMBR (4G) or MBR (3G):

- Transmit the packet without changing the PLP
- Set the PLP to “high.”

NOTE: **The default behavior of violate-action is drop. Data that exceeds the MBR is dropped by default. Data within the MBR is transmitted with PLP set to “high.”**

For GBR bearers (3G subscribers), the broadband gateway supports the following options:

- **exceed-action**—Specifies one of the following actions for bearers that exceed the GBR:
  - Set the PLP to “high” (the default).
  - Transmit the packet without changing the PLP.
- **violate-action**—Specifies one of the following actions for bearers that exceed the MBR:
  - Set the PLP to “high.”
  - Transmit the packet without changing PLP.

NOTE: **The default behavior of exceed-action is to set the PLP to “high” and violate-action is to drop. Data that exceeds the GBR but is within the MBR is transmitted with PLP set to “high”. Data that exceeds the MBR is dropped.**

Related Documentation

- Quality of Service Overview on page 3
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Applying Rewrite Rules on Mobile Interfaces Overview

For each mobile interface on the MobileNext Broadband Gateway (one mobile interface per access point name [APN]), you must configure ingress and egress rewrite rules and apply them to the interfaces. This provides the required DSCP marking for subscriber packets. The rewrite rules that you configure and apply to a mobile interface provides the required DSCP marking for all subscriber packets associated with the APN to which the mobile interface maps.

An ingress rewrite rule (**ingress-rewrite-rules**) sets the type-of-service (ToS) bits based on the forwarding class and loss priority of the upstream subscriber packet received on the mobile interface. For upstream traffic, the rewrite rule is applied to packets exiting the anchor Packet Forwarding Engine towards the Gn or S5 interface. The ingress rewrite rule writes into the outer IP header only.

An egress rewrite rule (**rewrite-rules**) sets the ToS bits based on the forwarding class and loss priority of a downstream subscriber packet received on the mobile interface. For downstream subscriber traffic, the rewrite rule is applied to packets exiting the (egress) anchor Packet Forwarding Engine towards the Gi or SGi interface. An egress rewrite rule writes into the outer IP header, and optionally, inner IP header for the GPRS tunneling protocol (GTP) packet.

Copyright © 2012, Juniper Networks, Inc.

NOTE: Egress rewrite rules must not be applied to the Ethernet interfaces on MX Series routers that receive downstream subscriber traffic from the broadband gateway. If configured, egress rewrite rules on the Ethernet interface will overwrite the QoS treatment configured on the broadband gateway for subscriber packets.

Related Documentation

- Quality of Service Overview on page 3
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 15
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets

To provide the required QoS treatment for upstream and downstream subscriber traffic, GTP-U packets are processed at multiple points in the data path.

This topic describes the upstream and downstream operations performed on GTP-U packets on the MobileNext Broadband Gateway.

- Processing of ToS Values for Upstream Subscriber Packets on page 15
- Processing of ToS Values for Downstream Subscriber Packets on page 16

Processing of ToS Values for Upstream Subscriber Packets

The broadband gateway processes upstream GTP-U packets from a Gn/S5 interface to a Gi/SGi interface.

The following steps describe the processing of type-of-service (ToS) values for upstream GTP-U packets:

1. A GTP-U packet arrives on the mobile (Ethernet) interface, and a behavior aggregate (BA) classifier evaluates the ToS value of the subscriber packet to derive an appropriate Junos OS forwarding class and packet loss priority (PLP).
2. The GTP-U packet is sent to the appropriate queue on the Packet Forwarding Engine. (The forwarding class determines the queue.)
3. The packet is sent to the anchor Packet Forwarding Engine where the GTP packet header is decapsulated.

Copyright © 2012, Juniper Networks, Inc.

NOTE: A classifier profile must be configured on the broadband gateway to provide a mapping from a traffic class/QCI to a forwarding class and PLP.

4. Subscriber tunnel endpoint identifier (TEID) lookup identifies the traffic class or QCI for the packet. The traffic class or QCI is mapped to a forwarding class and PLP, based on the classifier profile configured on the broadband gateway.
5. The packet is sent out on the anchor Packet Forwarding Engine where the egress rewrite rule applied on the mobile interface takes the forwarding class and PLP (Step 4) as input values to derive the appropriate DSCP marking before sending the packet to the SGi/Gi interface.

NOTE: An egress rewrite rule must be configured and applied to each mobile interface to provide the required DSCP marking for subscriber traffic.

6. The packet is sent out on the correct Gi or SGi interface.

Processing of ToS Values for Downstream Subscriber Packets

The broadband gateway processes downstream GTP-U packets from a Gi or SGi to a Gn or S5 interface.

The following steps describe the processing of ToS values for downstream GTP-U packets:

1. The GTP-U packet arrives from the Gi or SGi interface, and is sent to the anchor Packet Forwarding Engine associated with the virtual routing and forwarding (VRF) route.
2. On the anchor Packet Forwarding Engine, an IP address lookup identifies the TEID for the GTP header and, before encapsulation, the traffic class/QCI maps to a forwarding class and PLP, based on the classifier profile configured on the broadband gateway.
3. The packet is sent out from the anchor Packet Forwarding Engine where the ingress rewrite rule applied on the mobile interface takes the forwarding class and PLP (Step 2) as input values to derive the appropriate DSCP marking.
4. The packet is encapsulated with TEID and outer IP address in the GTP header, which is used for route table lookup for the SGSN/S-GN and sent to the egress Packet Forwarding Engine interface.
5. The packet is sent out on the correct Gn or S5 interface.

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior

GTPv1 subscriber packets that contain NQN and Upgrade flags in Create/Update PDP context requests can affect the QoS treatment during processing on the MobileNext Broadband Gateway. Consequently, incoming requests might not be upgraded even though the local policy configured on the broadband gateway warrants an upgrade of the traffic class, maximum bit rate, or ARP for subscriber packets.

Figure 3 on page 17 shows how negotiated QoS values are affected based on the presence of NQN or Upgrade flags in Create/Update PDP context requests.

Figure 3: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags

Case	GTP Message	Upgrade Flag	NQN	Local Policy	Requested QoS	Response	Local Policy	Requested QoS	Response	Local Policy	Requested QoS	Response
		0- False, 1- True										
1	Create	0	0	1024-Upgrade	512	512	TC-Upgrade	interactive	interactive	ARP-Upgrade	2	2
2	Create	0	0	1024-Upgrade	1500	1024	TC-Upgrade	conv	streaming	ARP-Upgrade	1	2
3	Create	1	0	1024-Upgrade	512	1024	TC-Upgrade	interactive	streaming	ARP-Upgrade	3	2
4	Create	1	0	1024-Upgrade	1500	1024	TC-Upgrade	conv	streaming	ARP-Upgrade	1	2
5	Create	0	0	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
6	Create	0	0	1024-Downgrade	1500	1024	TC-Downgrade	conv	streaming	ARP-Downgrade	1	2
7	Create	1	0	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
8	Create	1	0	1024-Downgrade	1500	1024	TC-Downgrade	conv	streaming	ARP-Downgrade	1	2
9	Update	0	0	1024-Upgrade	512	512	TC-Upgrade	interactive	interactive	ARP-Upgrade	3	3
10	Update	0	0	1024-Upgrade	1500	1024	TC-Upgrade	conversational	streaming	ARP-Upgrade	1	2
11	Update	1	0	1024-Upgrade	512	512	TC-Upgrade	interactive	interactive	ARP-Upgrade	3	3
12	Update	1	0	1024-Upgrade	1500	1024	TC-Upgrade	conversational	streaming	ARP-Upgrade	1	2
13	Update	0	1	1024-Upgrade	512	512	TC-Upgrade	interactive	interactive	ARP-Upgrade	3	3
14	Update	0	1	1024-Upgrade	1500	REJECT	TC-Upgrade	conversational	reject	ARP-Upgrade	1	reject
15	Update	1	1	1024-Upgrade	512	512	TC-Upgrade	interactive	interactive	ARP-Upgrade	3	3
16	Update	1	1	1024-Upgrade	1500	REJECT	TC-Upgrade	conversational	reject	ARP-Upgrade	1	reject
17	Update	0	0	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
18	Update	0	0	1024-Downgrade	1500	1024	TC-Downgrade	conversational	streaming	ARP-Downgrade	1	2
19	Update	1	0	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
20	Update	1	0	1024-Downgrade	1500	1024	TC-Downgrade	conversational	streaming	ARP-Downgrade	1	2
21	Update	0	1	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
22	Update	0	1	1024-Downgrade	1500	REJECT	TC-Downgrade	conversational	reject	ARP-Downgrade	1	reject
23	Update	1	1	1024-Downgrade	512	512	TC-Downgrade	interactive	interactive	ARP-Downgrade	3	3
24	Update	1	1	1024-Downgrade	1500	REJECT	TC-Downgrade	conversational	reject	ARP-Downgrade	1	reject

For Create PDP context requests arriving on the broadband gateway, the NQN and Upgrade flags can affect QoS negotiation as follows:

The Upgrade flag in a Create PDP context affects the upgrade behavior configured in the local policy for MBR, GBR, traffic class, and ARP value.

- For Cases 1 and 3 in Figure 3 on page 17, the QoS response results are different because the Upgrade Flag is set for Case 3. For example, MBR 512 versus 1024, traffic class interactive versus streaming, and ARP upgrade occurs for Case 3 only.
- For Cases 9 and 11 in Figure 3 on page 17, the combination of NQN and Upgrade flags in the Update PDP context prevent the expected upgrade of requested QoS values for MBR, traffic class, and ARP behavior, as configured in the local policy.

NOTE: **The Upgrade flag in a Create PDP context does not affect the downgrade behavior configured in the local policy.**

For Update PDP context requests arriving on the broadband gateway, the NQN and Upgrade flags can also affect QoS negotiation. For example, for Cases 14 and 16 in Figure 3 on page 17, the request is rejected because the NQN flag is set.

NOTE: **The Upgrade flag in a Update PDP context does not affect the downgrade behavior configured in the local policy.**

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring QoS on the Broadband Gateway Overview

Configuring quality of service (QoS) on the MobileNext BroadBand Gateway for a 3G or 4G network is a multistep process in which you configure the resource threshold profiles, classifier profiles, and CoS policy profiles that are then specified in local policies to provide call admission control (CAC) and prioritization of subscriber traffic when the network load increases.

The following steps describe the high-level process for configuring QoS for 3G and 4G networks:

1. Configure the number of bearers at the system level or access point name (APN) level.
2. Configure bandwidth pools to ensure that sufficient bandwidth is available when guaranteed bit rate (GBR) packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses bandwidth pools to either accept or reject the GBR PDP contexts based on availability of bandwidth, or to negotiate and reserve the bandwidth.
3. Configure preemption at the gateway level to enable preemption for GTPv2 bearers. For GTPv1 pre-Release 9 PDP contexts, you can enable preemption capability and preemption vulnerability independently. The broadband gateway uses ARP values to manage the allocation and retention of resources for bearers. When preemption is enabled, the broadband gateway evaluates the priority level (PL) and the preemption vulnerability (PVI) and preemption capability (PCI) flags in the GTPv2 information element (IE) to determine whether a bearer is a candidate for deletion.

   NOTE: **Preemption is disabled by default.**

4. Configure a resource threshold profile to define call admission control to manage load thresholds for the number of bearers, memory load, and CPU load.
5. Configure a classifier profile—Each traffic class or traffic handling priority (3G) and QoS Class Identifier (QCI) (4G) is mapped to a forwarding class and packet loss priority (PLP).

Copyright © 2012, Juniper Networks, Inc.

NOTE: For 3G bearers, the broadband gateway converts the traffic class to a QCI based on the 3GPP specification 23.401 ANNEX E. Thus, to configure packet forwarding for 3G traffic classes, you map the forwarding class and PLP for the QCI that maps to a traffic class. For more information about how 3G traffic classes are mapped to QCI values, see "Quality of Service Overview" on page 3.

NOTE: You can configure separate classifier profiles for home, roaming, and visitor subscriber traffic.

6. Configure a class-of-service (CoS) policy profile to define how traffic is divided into classes and specify whether to upgrade or limit bearer requests based on availability of system resources.

   NOTE: You can configure separate CoS policy profiles for home, roaming, and visitor subscriber traffic.

7. Configure a local policy to define overall QoS treatment for subscriber traffic in 3G networks or 4G networks. A local policy includes the configuration of bandwidth pools (for uplink and downlink), classifier profiles, a resource threshold profile, and CoS policy profiles. You can configure separate CoS policy profiles for home, roaming, and visitor subscriber traffic.

   NOTE: You can configure multiple classifier profiles and CoS policy profiles to address QoS configuration requirements for home, roaming, and visitor subscriber traffic.

8. Apply a local policy at the gateway level or APN level.
9. Configure ingress and egress rewrite rules for upstream and downstream subscriber traffic.
10. Apply ingress and egress rewrite rules on mobile interfaces to provide Differentiated Services code point (DSCP) marking for upstream and downstream subscriber traffic.

Related Documentation

- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Copyright © 2012, Juniper Networks, Inc.

PART 2

Configuration

- Configuration Tasks on page 23
- Configuration Examples on page 49
- Configuration Statements on page 87

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 2

Configuration Tasks

- Configuring the Maximum Number of Bearers on page 23
- Configuring Bandwidth Pools on page 24
- Configuring Preemption for Call Admission Control on page 25
- Configuring Resource Thresholds for 3G and 4G Networks on page 26
- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring a CoS Policy Profile for 4G Networks on page 29
- Configuring a CoS Policy Profile for 3G Networks on page 32
- Configuring a CoS Policy Profile for 3G and 4G Networks on page 37
- Configuring a Local Policy on page 43
- Applying a Local Policy on page 44
- Configuring Ingress Rewrite Rules for a Mobile Interface on page 45
- Configuring Egress Rewrite Rules for a Mobile Interface on page 45
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Applying Egress Rewrite Rules to Mobile Interfaces on page 47

Configuring the Maximum Number of Bearers

You configure the maximum bearers to specify an upper limit on the number of bearers allowed at the system level or access point name (APN) level.

When the total number of active bearers at the gateway level or APN level reaches the maximum configured limit, the MobileNext Broadband Gateway rejects new bearer requests.

- Configure the maximum number of active bearers allowed at the gateway level.

  [edit unified-edge gateways ggsn-pgw *MBG1*]
  user@host# **set maximum-bearers** ***5000000***

- For each APN, configure the maximum number of active bearers allowed at the APN level.

  [edit unified-edge gateways ggsn-pgw *MBG1* apn-services apns *apn-1*]
  user@host# **set maximum-bearers** ***10000***

Copyright © 2012, Juniper Networks, Inc.

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring Bandwidth Pools

You configure a bandwidth pool to ensure that sufficient bandwidth is available when guaranteed bit rate (GBR) packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses bandwidth pools to either accept or reject the GBR PDP contexts based on availability of bandwidth, or to negotiate and reserve the bandwidth.

To configure a bandwidth pool:

1. Specify a name for the bandwidth pool.

   [edit unified-edge cos-cac]
   user@host# **edit gbr-bandwidth-pools** ***bw-pool-1***

2. Configure the total bandwidth of the pool, in megabits per second (Mbps).

   [edit unified-edge cos-cac gbr-bandwidth-pools *bw-pool-1*]
   user@host# **set maximum-bandwidth** ***500000***

3. (Optional) Specify that when the bearer load on the broadband gateway reaches the configured bandwidth threshold, then create or modify PDP context requests can be downgraded, starting with lower priority requests.

   [edit unified-edge cos-cac gbr-bandwidth-pools *bw-pool-1*]
   user@host# **set downgrade-gtp-v1-gbr-bearers**

   NOTE: If the **downgrade-gtp-v1-gbr-bearers** option is configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are downgraded to the Background traffic class. If the **downgrade-gtp-v1-gbr-bearers** option is not configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are rejected.

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18

Copyright © 2012, Juniper Networks, Inc.

Configuring Preemption for Call Admission Control

You can enable preemption at the gateway level to enable the preemption capability indicator (PCI) and preemption vulnerability indicator (PVI) flags. Preemption is disabled by default. In a 4G network, the PVI and PCI bit values are included with the allocation and retention priority (ARP). In a 3G network, PDP context requests do not support the PVI and PCI flags, and the MobileNext Broadband Gateway uses ARP values to determine preemption capability and preemption vulnerability. GTPv1 subscribers. Preemption takes effect when the high threshold for bearer or memory load (configured in a **resource-threshold-profile**) is reached on the MobileNext Broadband Gateway.

To enable preemption on the broadband gateway:

- To enable preemption for both GTPv1 and GTPv2 subscribers:

  [edit unified-edge gateways ggsn-pgw *MBG1* preemption]
  user@host# set *enable*

- To enable only PVI for GTPv1 subscribers:

  [edit unified-edge gateways ggsn-pgw *MBG1* preemption]
  user@host# set *enable*
  user@host# set *gtpv1-pci-disable*

- To enable only PCI for GTPv1 subscribers:

  [edit unified-edge gateways ggsn-pgw *MBG1* preemption]
  user@host# set *enable*
  user@host# set *gtpv1-pvi-disable*

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring Resource Thresholds for 3G and 4G Networks

You configure a resource threshold profile to ensure that when the bearer load, CPU load, or memory load at the access point name (APN) or gateway level on the MobileNext Broadband Gateway reaches a specified threshold, only create session requests that meet or exceed a designated allocation and retention priority (ARP) level are admitted.

Table 8 on page 26 shows the mapping of EPS bearer ARP to Release 99 bearer parameter ARP.

Table 8: Mapping of EPS Bearer ARP to Release 99 Bearer Parameter ARP

EPS Bearer Priority Level	Release 99 Bearer Parameter ARP
1	1
6	2
11	3

To configure a resource threshold profile:

1. Specify a name for the resource threshold.

   [edit unified-edge cos-cac]
   user@host# **edit resource-threshold-profiles** *resource-threshold-1*

2. Configure the bearer priority level and threshold limits for the number of bearers:

   a. Configure the bearer priority when the number of bearers reaches the lower threshold. The following configuration specifies that when the number of bearers exceeds 70 percent of the allowed limit, only Create Session requests with a priority level equal to or higher than the specified ARP value are accepted:

      [edit unified-edge cos-cac resource-threshold-profiles *resource-threshold-1* bearers-load low]
      user@host# **set percentage** *70*
      user@host# **priority-level** *10*

   b. Configure the bearer priority when the number of bearers reaches the upper threshold. The following configuration specifies that when the number of bearers exceeds 85 percent, only Create Session requests with a priority level equal to or higher than the specified ARP values are accepted:

      [edit unified-edge cos-cac resource-threshold-profiles *resource-threshold-1* bearers-load high]
      user@host# **set percentage** *85*
      user@host# **set priority-level** *4*

3. Configure the bearer priority and threshold limits for the CPU load:

   a. Configure a lower limit for the CPU load.

      [edit unified-edge cos-cac resource-threshold-profiles *resource-threshold-1* cpu low]

Copyright © 2012, Juniper Networks, Inc.

```
user@host# set percentage 70
user@host# set priority-level 10
```

b. Configure an upper limit for the CPU load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
  high]
user@host# set percentage 85
user@host# set priority-level 4
```

4. Configure the bearer priority and threshold limits for the memory load:

a. Configure a lower limit for the memory load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
  low]
user@host# set percentage 70
user@host# set priority-level 10
```

b. Configure an upper limit for the memory load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
  high]
user@host# set percentage 85
user@host# set priority-level 10
```

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- Call Admission Control Overview on page 10
- Example: Configuring Quality of Service on GGSN/P-GW on page 49
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring a Classifier Profile for 3G and 4G Networks

A classifier profile defines the quality of service (QoS) classification for a MobileNext Broadband Gateway configured as a Gateway GPRS Support Node/Packet Data Network Gateway (GGSN/P-GW). You can configure a QoS class identifier (QCI) value and associated forwarding class and loss priority to define the packet-forwarding treatment for both 3G and 4G bearers. Each QCI is associated with priority, delay, and packet loss values.

NOTE: **The broadband gateway maps Release 99 QoS parameter values to standardized QCI values as defined in GTTP Specification 23.401 ANNEX E.**

To configure a classifier profile to map each QCI value to a forwarding class and packet loss priority:

1. Specify a name for the classifier profile.

```
[edit unified-edge cos-cac]
```

user@host# **edit classifier-profiles** ***classifier-profile-1***

2. Configure a packet-forwarding treatment that maps to the conversational traffic class.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***2*** **forwarding-class** ***af3*** **loss-priority** ***low***

3. Configure a packet-forwarding treatment that maps to the streaming traffic class.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***4*** **forwarding-class** ***af2*** **loss-priority** ***low***

4. Configure a packet-forwarding treatment for IP Multimedia Subsystem (IMS) signaling traffic that also maps to the Interactive traffic class with Traffic Handling Priority (THP) 1.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***5*** **forwarding-class** ***af2*** **loss-priority** ***low***

5. Configure a packet forwarding treatment for video (buffered streaming) traffic that also maps to the Interactive traffic class with THP 2.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***6*** **forwarding-class** ***af2*** **loss-priority** ***low***

6. Configure a packet forwarding treatment for voice, video (live streaming), and interactive gaming traffic that also maps to the Interactive traffic class with THP 2.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***7*** **forwarding-class** ***af3*** **loss-priority** ***low***

7. Configure a packet forwarding treatment for background traffic that also maps to the Interactive traffic class with THP 3.

   [edit unified-edge cos-cac classifier-profiles *classifier-profile-1*]
   user@host# **set qos-class-identifier** ***8*** **forwarding-class** ***be*** **loss-priority** ***low***

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- Example: Configuring Quality of Service on GGSN/P-GW on page 49
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Configuring a CoS Policy Profile for 4G Networks

In a 4G network, a class-of-service (CoS) policy profile defines the highest QoS Class Identifier (QCI) value that can be accepted at the access point name (APN) level or gateway level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority (ARP). By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the AMBR value of the bearer request is downgraded. A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the policer rates.

Before you begin, complete the following tasks:

- Configure a CoS classifier profile.
- Configure a CoS resource threshold profile.

To configure a CoS policy profile for a 4G network:

1. Specify a name for the CoS policy profile.

   [edit unified-edge cos-cac]
   user@host# **edit cos-policy-profiles** ***policy-profile-2***

2. Negotiate the QCI value for 4G subscribers by doing one of the following:

   - Downgrade the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6*

     NOTE: When the default (downgrade) behavior is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.

   - Upgrade the QCI value of create session requests that come in with a lower QCI value (numerically higher) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6* **upgrade**

     NOTE: When the **upgrade** option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is upgraded to the configured value.

   - Reject the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6* **reject**

     NOTE: When the **reject** option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the create session request is rejected. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.

   NOTE: If the QCI value is not specified, the broadband gateway uses the UE/SGW requested or negotiated QCI value.

3. Negotiate the ARP value for 4G subscribers when a bearer is established or modified:

Copyright © 2012, Juniper Networks, Inc.

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior):

  [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
  user@host# **set allocation-retention-priority** *7*

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are rejected:

  [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
  user@host# **set allocation-retention-priority** *7* **reject**

NOTE: **If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.**

4. Negotiate uplink and downlink AMBR for 4G subscribers by doing one of the following:

   - Specify that bearer requests with an AMBR value higher than the configured value are downgraded to the configured AMBR value, and bearer requests with a lower value than the configured AMBR value are accepted (the default behavior):

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* aggregate-qos-control]
     user@host# **set maximum-bit-rate-uplink** *15000*
     user@host# **set maximum-bit-rate-downlink** *25000*

   - Specify that bearer requests with a lower AMBR value than the configured value are upgraded to the configured AMBR value, and bearer requests with a higher AMBR value than the configured value are downgraded:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* aggregate-qos-control]
     user@host# **set maximum-bit-rate-uplink** *15000* **upgrade**
     user@host# **set maximum-bit-rate-downlink** *25000* **upgrade**

   - Specify that bearer requests with a higher AMBR value than the configured value are rejected, and bearer requests with a lower AMBR value than the configured value are accepted:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* aggregate-qos-control]
     user@host# **set maximum-bit-rate-uplink** *15000* **reject**
     user@host# **set maximum-bit-rate-downlink** *25000* **reject**

5. Configure the policer action to define how default bearer data is treated when it exceeds the AMBR value with which the default bearer was established.

   [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* policer-action non-gbr-bearer]
   user@host# **set violate-action** ***set-loss-priority-high***

   When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the AMBR is transmitted with PLP high.

NOTE: By default, bearers that exceed the AMBR are dropped.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring a CoS Policy Profile for a 3G Network on page 32
- Configuring a CoS Policy Profile for 3G and 4G Networks on page 37
- Example: Configuring Quality of Service on GGSN/P-GW on page 49
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring a CoS Policy Profile for 3G Networks

In a 3G network, the class-of-service (CoS) policy profile defines the highest non-GBR traffic class mapped to a QoS class identifier (QCI) that can be accepted at an access point name (APN) or gateway level, the maximum bit rate (MBR), the guaranteed bit rate (GBR) for each traffic class, and the allocation and retention priority (ARP). A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the configured GBR, MBR, or both. By default, when a PDP context request has a higher MBR or GBR value than the value configured in the CoS policy profile, the packet data protocol (PDP) context request is downgraded.

Before you begin, complete the following tasks:

- Configure a CoS resource threshold profile.
- Configure CoS bandwidth pools.
- Configure a CoS classifier profile.

To configure a CoS policy profile for a 3G network:

1. Specify a name for the CoS policy profile.

```
[edit unified-edge cos-cac]
user@host# edit cos-policy-profiles policy-profile-2
```


Copyright © 2012, Juniper Networks, Inc.

2. Negotiate the non-GBR traffic class for 3G subscribers by doing one of the following:

   - Downgrade the traffic class of create PDP context requests that come in with a higher traffic class than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci *6***

     NOTE: When default (downgrade) behavior is configured, if a create PDP context request comes in with higher traffic class (mapped to QCI) than the value configured on the broadband gateway, the traffic class is downgraded to the configured value. If a create PDP context request comes in with a lower traffic class (numerically higher QCI) than the configured traffic class, then the traffic class is accepted.

   - Upgrade the traffic class of create PDP context requests that come in with a lower traffic class (numerically higher QCI) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci *6* upgrade**

     NOTE: when upgrade option is configured, if a create PDP context request comes in with higher traffic class (numerically lower QCI) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, then the QCI value is upgraded to the configured value.

   - Reject the traffic class of create PDP context requests that come in with a higher traffic class (numerically lower QCI) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci *6* reject**

     NOTE: When reject option is configured, if a create PDP context comes in with higher traffic class (numerically lower QCI) than the value configured on the broadband gateway, the create PDP context is rejected. If a create PDP context comes in with a lower traffic class (numerically higher QCI) than the configured QCI, then the traffic class is accepted as is.

   NOTE: If the QCI/traffic class value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated traffic class value.

3. Negotiate the ARP value for 3G a when a PDP context is established or modified:

- Specify that PDP contexts that come in with a lower ARP (numerically higher) than the configured value are accepted, and PDP contexts with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior):

  [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
  user@host# **set allocation-retention-priority *7***

- Specify that PDP contexts that come in with a lower ARP (numerically higher) than the configured value are accepted, and that PDP contexts with a higher ARP (numerically lower) are rejected:

  [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
  user@host# **set allocation-retention-priority *7* reject**

NOTE: **For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.**

NOTE: **If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.**

4. Negotiate uplink and downlink MBR for 3G non-GBR PDP contexts by doing one of the following:

   - Specify that PDP context requests that come in with an MBR value higher than the configured value are downgraded to the configured MBR value, and PDP context requests that come in with a lower value than the configured MBR value are accepted (the default behavior):

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink *15000***
     user@host# **set maximum-bit-rate-downlink *25000***

   - Specify that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink *15000* upgrade**
     user@host# **set maximum-bit-rate-downlink *25000* upgrade**

   - Specify that PDP context requests that come in with a higher MBR value than the configured value are rejected, and PDP context requests that come in with a lower MBR value than the configured value are accepted:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink *15000* reject**

 Copyright © 2012, Juniper Networks, Inc.

```
user@host# set maximum-bit-rate-downlink 25000 reject
```

5. Negotiate the uplink and downlink GBR for 3G GBR bearers by doing one of the following:

   - Specify that PDP context requests that come in with a GBR value higher than the configured value are downgraded to the configured GBR value, and PDP context requests that come in with a lower value than the configured GBR value are accepted (the default behavior):

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000
     user@host# set guaranteed-bit-rate-downlink 25000
     ```

   - Specify that PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded:

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000 upgrade
     user@host# set guaranteed-bit-rate-downlink 25000 upgrade
     ```

   - Specify that PDP context requests that come in with a higher GBR value than the configured values are rejected, and PDP context requests that come in with a lower GBR value than the configured value are accepted:

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000 reject
     user@host# set guaranteed-bit-rate-downlink 25000 reject
     ```

6. Negotiate the uplink and downlink MBR for non-GBR PDP contexts by configuring each traffic class using the default, upgrade, or reject option.

   NOTE: The following traffic classes are configured using the default (downgrade) behavior, which specifies that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded.

   a. Configure an MBR for the Interactive traffic class with Traffic Handling Priority (THP) 1 and signaling indication enabled:

      ```
      [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
      user@host# set qci 5 maximum-bit-rate-uplink 10000
      user@host# set qci 5 maximum-bit-rate-downlink 20000
      ```

   b. Configure an MBR for the Interactive traffic class with THP 1:

      ```
      [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
      user@host# set qci 6 maximum-bit-rate-uplink 10000
      user@host# set qci 6 maximum-bit-rate-downlink 20000
      ```

   c. Configure an MBR for Interactive traffic class with THP 2:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 7 maximum-bit-rate-uplink 10000
user@host# set qci 7 maximum-bit-rate-downlink 20000
```

d. Configure an MBR for Interactive traffic class with THP 3:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 8 maximum-bit-rate-uplink 10000
user@host# set qci 8 maximum-bit-rate-downlink 20000
```

e. Configure an MBR for the Background traffic class:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 9 maximum-bit-rate-uplink 10000
user@host# set qci 9 maximum-bit-rate-downlink 10000
```

7. Configure the policer action to define how non-GBR bearer data should be treated when it exceeds the MBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
  non-gbr-bearer]
user@host# set violate-action set-loss-priority-high
```

When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the MBR is transmitted with PLP high.

NOTE: By default, GTPv1 subscribers that exceed the MBR are dropped.

8. Configure the action to take when the GBR exceeds the GBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action gbr-bearer]
user@host# set exceed-action transmit
```

NOTE: By default, PDP contexts that exceed the GBR are set to PLP HIGH. When **exceed action** is configured with **transmit**, PDP contexts exceeding that GBR are transmitted with same PLP as PDP contexts within the GBR.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring a CoS Policy Profile for a 4G Network on page 29
- Configuring a CoS Policy Profile for 3G and 4G Networks on page 37
- Example: Configuring Quality of Service on GGSN/P-GW on page 49
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Configuring a CoS Policy Profile for 3G and 4G Networks

In a 3G network, the class-of-service (CoS) policy profile defines the highest traffic class (mapped to QoS Class Identifier (QCI)) that can be accepted at an access point name (APN) or gateway level, the maximum bit rate (MBR) and guaranteed bit rate (GBR) for packet data protocol (PDP) contexts, and the allocation and retention priority (ARP). The CoS policy also specifies the policer actions when subscriber traffic exceeds the configured MBR and GBR values. By default, when a PDP context request has a higher MBR or GBR value than the value configured in the CoS policy profile, the MBR or GBR value of the PDP context request is downgraded.

NOTE: For GTPv1 subscribers, the MobileNext Broadband Gateway converts the traffic class to a QCI (as defined in the 3GPP specification 23.401 ANNEX E) and applies the COS policy based on the configured QCI values.

In a 4G network, a CoS policy profile defines the highest QCI value that can be accepted at the APN level or gateway level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority. By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the AMBR value of bearer request is downgraded.

Before you begin, complete the following tasks:

- Configure a CoS classifier profile for 3G and 4G networks.
- Configure CoS bandwidth pools (for 3G networks only).
- Configure a CoS resource threshold profile for 3G and 4G networks.

To configure a CoS policy profile for 3G and 4G networks:

1. Specify a name for the CoS policy profile.

   [edit unified-edge cos-cac]
   user@host# edit cos-policy-profiles *policy-profile-2*

2. Negotiate the QCI value for 4G subscribers and the traffic class for 3G subscribers by doing one of the following:

   - Downgrade the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6*

     NOTE: When the default (downgrade) behavior is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted.

   - Upgrade the QCI value of create session requests that come in with a lower QCI value (numerically higher) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6* **upgrade**

     NOTE: When the upgrade option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is upgraded to the configured value.

   - Reject the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]
     user@host# **set default-bearer-qci** *6* **reject**

     NOTE: When the reject option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is rejected. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.

3. Negotiate the ARP value for 3G and 4G subscribers when a PDP context or bearer is established or modified:

   - Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior):

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2*]

Copyright © 2012, Juniper Networks, Inc.

```
user@host# set allocation-retention-priority 7
```

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are rejected:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set allocation-retention-priority 7 reject
```

NOTE: For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.

NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

4. Negotiate uplink and downlink AMBR for 4G subscribers by doing one of the following:

- Specify that bearer requests with an AMBR value higher than the configured value are downgraded to the configured AMBR value, and bearer requests with a lower value than the configured AMBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000
user@host# set maximum-bit-rate-downlink 25000
```

- Specify that bearer requests with a lower AMBR value than the configured value are upgraded to the configured AMBR value, and bearer requests with a higher AMBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 upgrade
user@host# set maximum-bit-rate-downlink 25000 upgrade
```

- Specify that bearer requests with a higher AMBR value than the configured value are rejected, and bearer requests with a lower AMBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 reject
user@host# set maximum-bit-rate-downlink 25000 reject
```

Copyright © 2012, Juniper Networks, Inc.

NOTE: **If the AMBR value is not specified, the broadband gateway uses the UE/MME requested or negotiated AMBR value.**

5. Negotiate uplink and downlink MBR for 3G non-GBR PDP contexts by doing one of the following:

   - Specify that PDP context requests that come in with an MBR value higher than the configured value are downgraded to the configured MBR value, and PDP context requests that come in with a lower value than the configured MBR value are accepted (the default behavior):

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink** ***15000***
     user@host# **set maximum-bit-rate-downlink** ***25000***

   - Specify that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink** ***15000*** **upgrade**
     user@host# **set maximum-bit-rate-downlink** ***25000*** **upgrade**

   - Specify that PDP context requests that come in with a higher MBR value than the configured value are rejected, and PDP context requests that come in with a lower MBR value than the configured value are accepted:

     [edit unified-edge cos-cac cos-policy-profiles *policy-profile-2* pdp-qos-control]
     user@host# **set maximum-bit-rate-uplink** ***15000*** **reject**

Copyright © 2012, Juniper Networks, Inc.

```
user@host# set maximum-bit-rate-downlink 25000 reject
```

6. Negotiate the uplink and downlink GBR for 3G GBR bearers by doing one of the following:

   - Specify that PDP context requests that come in with a GBR value higher than the configured value are downgraded to the configured GBR value, and PDP context requests that come in with a lower value than the configured GBR value are accepted (the default behavior):

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000
     user@host# set guaranteed-bit-rate-downlink 25000
     ```

   - Specify that PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded:

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000 upgrade
     user@host# set guaranteed-bit-rate-downlink 25000 upgrade
     ```

   - Specify that PDP context requests that come in with a higher GBR value than the configured values are rejected, and PDP context requests that come in with a lower GBR value than the configured value are accepted:

     ```
     [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
     user@host# set guaranteed-bit-rate-uplink 15000 reject
     user@host# set guaranteed-bit-rate-downlink 25000 reject
     ```

7. Negotiate the uplink and downlink MBR for non-GBR PDP contexts, you configure each traffic class using either the default, upgrade, or reject behavior.

   NOTE: The following traffic classes are configured using the default (downgrade) behavior. PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded.

   a. Configure an MBR for the Interactive traffic class with Traffic Handling Priority (THP) 1 and signaling indication enabled:

      ```
      [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
      user@host# set qci 5 maximum-bit-rate-uplink 10000
      user@host# set qci 5 maximum-bit-rate-downlink 20000
      ```

   b. Configure an MBR for the Interactive traffic class with THP 1:

      ```
      [edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
      user@host# set qci 6 maximum-bit-rate-uplink 10000
      user@host# set qci 6 maximum-bit-rate-downlink 20000
      ```

   c. Configure an MBR for Interactive traffic class with THP 2:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 7 maximum-bit-rate-uplink 10000
user@host# set qci 7 maximum-bit-rate-downlink 20000
```

d. Configure an MBR for Interactive traffic class with THP 3:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 8 maximum-bit-rate-uplink 10000
user@host# set qci 8 maximum-bit-rate-downlink 20000
```

e. Configure an MBR for the Background traffic class:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 9 maximum-bit-rate-uplink 10000
user@host# set qci 9 maximum-bit-rate-downlink 10000
```

8. Configure the policer action to define how non-GBR bearer data is treated when it exceeds the MBR value with which the PDP context was established or the AMBR value with which the default bearer was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
  non-gbr-bearer]
user@host# set violate-action set-loss-priority-high
```

When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the MBR is transmitted with PLP high.

NOTE: By default, GTPv1 subscribers that exceed the MBR and GTPv2 subscribers that exceed the AMBR are dropped.

9. Configure the policer actions to take to define how GBR bearer data is treated:

a. Configure the policer action to define how GBR bearer data is treated when the MBR exceeds the MBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
  non-gbr-bearer]
user@host# set violate-action set-loss-priority-high
```

b. Configure the policer actions to take to define how GBR bearer data is treated when the GBR exceeds the GBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
  gbr-bearer]
user@host# set exceed-action transmit
```

NOTE: By default, PDP contexts that exceed the GBR are set to PLP HIGH. When **exceed action** is configured with **transmit**, PDP contexts exceeding the GBR are transmitted with the same PLP as PDP contexts within the GBR.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12

Copyright © 2012, Juniper Networks, Inc.

- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring a Local Policy

A local policy defines the quality-of-service (QoS) treatment to be applied at the system level or access point name (APN) level for the MobileNext Broadband Gateway. A local policy applied at the APN level takes priority over a local policy applied at the system level. A local policy defines traffic by classes and specifies the different levels of throughput and packet loss when congestion occurs.

Before you begin, configure each of the following QoS features:

- Bandwidth pool—Limits the GBR bandwidth usage at the system level or APN level. The broadband gateway's call admission control (CAC) uses bandwidth pools to negotiate and reserve bandwidth.
- Resource threshold profiles—Limit CPU and memory load. When the number of bearers or system load (memory, CPU, and queue depth) reaches a configured low or high threshold, only higher-priority bearer requests are allowed.
- Classifier profiles—Define the mapping of traffic classes (a traffic class or QoS Class Identifier [QCI]) to a forwarding class and packet loss priority (PLP). You configure separate classifier profiles for home, roaming, and visitor subscriber traffic.
- CoS policy profiles—Configure separate class-of-service (CoS) profiles for home, roaming, and visitor subscriber traffic.

To configure a local policy:

1. Specify a name for the local policy.

   [edit unified-edge]
   user@host# **edit local-policies** ***local-policy-2***

2. Specify the classifier profiles to include in the local policy to define the mapping of each traffic class to a forwarding class and PLP.

   [edit unified-edge local-policies *local-policy-2*]
   user@host# **set classifier-profile** ***home-classifier-profile-1***
   user@host# **set roamer-classifier-profile** ***roaming-classifier-profile-1***
   user@host# **set visitor-classifier-profile** ***visiting-classifier-profile-1***

3. Specify the CoS policy profiles to include in the local policy to define the QoS parameters for bearer setup and teardown.

   [edit unified-edge local-policies *local-policy-2*]
   user@host# **set policy-profile** ***home-policy-profile-1***
   user@host# **set roamer-policy-profile** ***roaming-policy-profile-1***
   user@host# **set visitor-policy-profile** ***visiting-policy-profile-1***

4. Specify the resource threshold profile to include in the local policy to define admission control for managing system overload conditions.

Copyright © 2012, Juniper Networks, Inc.

[edit unified-edge local-policies *local-policy-2*]
user@host# **set resource-threshold-profiles** ***resource-threshold--profile-1***

5. Specify a bandwidth pool for downlink traffic.

   [edit unified-edge local-policies *local-policy-2*]
   user@host# **set dl-bandwidth-pool** ***bw-pool-downlink-1***

6. Specify a bandwidth pool for uplink traffic.

   [edit unified-edge local-policies *local-policy-2*]
   user@host# **set ul-bandwidth-pool** ***bw-pool-uplink-1***

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring the Maximum Number of Bearers on page 23
- Configuring Bandwidth Pools on page 24
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Applying a Local Policy

A local policy defines the QoS treatment to be applied at the system level or access point name (APN) level for a MobileNext Broadband Gateway. A local policy applied at the APN level takes priority over a local policy applied at the system level.

Before you begin, you must configure a local policy to define the QoS treatment to be applied at the system level or APN level for a broadband gateway.

- To apply a local policy at the system level:

  [edit gateways ggsn-pgw *MBG1*]
  user@host# **edit local-policy-profile** ***local-policy1***

- To apply a local policy at the access point name (APN) level:

  [edit gateways ggsn-pgw *MBG1* apn-services apns *apn1*]
  user@host# **edit local-policy-profile** ***local-policy2***

Related Documentation

- Configuring a Local Policy on page 43
- Configuring the Maximum Number of Bearers on page 23
- Configuring Bandwidth Pools on page 24
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Configuring Ingress Rewrite Rules for a Mobile Interface

You configure egress rewrite rules and then apply those rules to change DiffServ code point (DSCP) bits or IP precedence bits for subscriber packets received on a mobile interface.

To create an ingress rewrite rule for a mobile interface:

1. Specify a name for the ingress rewrite rules.

   [edit class-of-service rewrite-rules]
   user@host# edit dscp *dscp_v4_ingress_rw*

2. Configure a rewrite rules mapping on DSCP, DSCP IPv6, or IP precedence values; for example:

   [edit class-of-service rewrite-rules dscp *dscp_v4_ingress_rw*]
   user@host# set forwarding class *af1* loss-priority *high* code-point *001110*
   user@host# set forwarding class *af1* loss-priority *low* code-point *001010*
   user@host# set forwarding class *af2* loss-priority *high* code-point *010110*
   user@host# set forwarding class *af2* loss-priority *low* code-point *010010*
   user@host# set forwarding class *af3* loss-priority *high* code-point *011110*
   user@host# set forwarding class *af3* loss-priority *low* code-point *011010*
   user@host# set forwarding class *af4* loss-priority *high* code-point *100110*
   user@host# set forwarding class *af4* loss-priority *low* code-point *100010*
   user@host# set forwarding class *be* loss-priority *low* code-point *000000*

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring Egress Rewrite Rules for a Mobile Interface on page 45
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Configuring Egress Rewrite Rules for a Mobile Interface

You configure egress rewrite rules and then apply those rules to change DiffServ code point (DSCP) bits or IP precedence bits for subscriber packets received on a mobile interface.

To create an egress rewrite rule for a mobile interface:

1. Specify a name for the egress rewrite rules.

   [edit class-of-service rewrite-rules]
   user@host# edit dscp *dscp_v4_egress_rw*

2. Configure a rewrite rules mapping on DSCP, DSCP IPv6, or IP precedence values; for example:

   [edit class-of-service rewrite-rules dscp *dscp_v4_egress_rw*]
   user@host# set forwarding class *af1* loss-priority *high* code-point *001110*

Copyright © 2012, Juniper Networks, Inc.

```
user@host# set forwarding class af1 loss-priority low code-point 001010
user@host# set forwarding class af2 loss-priority high code-point 010110
user@host# set forwarding class af2 loss-priority low code-point 010010
user@host# set forwarding class af3 loss-priority high code-point 011110
user@host# set forwarding class af3 loss-priority low code-point 011010
user@host# set forwarding class af4 loss-priority high code-point 100110
user@host# set forwarding class af4 loss-priority low code-point 100010
user@host# set forwarding class be loss-priority low code-point 000000
```

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring Ingress Rewrite Rules for a Mobile Interface on page 45
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Applying Ingress Rewrite Rules to a Mobile Interface

You apply ingress rewrite rules to change the DiffServ code point (DSCP), DSCPv6, or IP precedence value in the IP header of the upstream subscriber packets. You can specify rewrite rules for DSCPv4, DSCPv6, or IP precedence values.

The rewrite rule is applied for Gn-to-Gi traffic at the mobile interface and rewrites into the outer IP header of the subscriber packet only.

NOTE: **DSCP marking on the subscriber packet is required for mobile traffic. If ingress rewrite rules are not configured and applied to the mif interface, the default mcos-dscp-default or mcos-dscpv6-default rewrite rules apply.**

Before you begin, complete the following tasks:

- Configure an ingress rewrite rule.
- Configure the mobile interfaces.

To apply a rewrite rule to the outer IP header, specify the name of the rewrite rule that you want to apply to the mobile interface; for example:

```
[edit class-of-service interfaces mif unit 0 ingress-rewrite-rules]
user@host# set dscp uplink_rewrite_v4_dscp
```

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring QoS on the Broadband Gateway Overview on page 18
- Applying Egress Rewrite Rules to Mobile Interfaces on page 47
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

Applying Egress Rewrite Rules to Mobile Interfaces

You apply egress rewrite rules to change the DiffServ code point (DSCP), DSCPv6, or IP precedence value in the IP header of downstream subscriber packets. You can specify rewrite rules for DSCPv4, DSCPv6, or IP precedence values.

An egress rewrite rule for downstream (Gi-to-Gn or SGi-to-S5) traffic is applied at the mobile interface and rewrites into the inner IP header, and optionally, outer IP header, or both inner and outer IP headers.

NOTE: **DSCP marking on the subscriber packet is required for mobile traffic. If egress rewrite rules are not configured and applied to the mobile interfaces, the default mcos-dscp-default or mcos-dscpv6-default rewrite rules apply.**

Before you begin, complete the following tasks:

- Configure the mobile interfaces.
- Configure an egress rewrite rule.

To apply an egress rewrite rule to change DSCP, DSCPv6, or IP precedence values in the IP header of downstream subscriber packets:

- To apply a DSCP (IPv4) rewrite rule to the inner IP header, specify the name of the rewrite rule you want to apply to the mobile interface.

  [edit class-of-service interfaces mif unit 0 rewrite-rules]
  user@host# **set dscp** ***downlink_rewrite_v4_dscp_inner***

- To apply a rewrite rule on the outer IP header, specify the name of the rewrite rule you want to apply to the mobile interface and include the **gtp-inet-outer** option.

  [edit class-of-service interfaces mif unit 0 rewrite-rules]
  user@host# **set dscp** ***downlink_rewrite_v4_dscp_outer*** **protocol gtp-inet-outer**

- To apply a DSCP rewrite rule to both the inner and outer IP headers, specify the name of the rewrite rule you want to apply to the mobile interface and include the **gtp-inet-both** option.

  [edit class-of-service interfaces mif unit 0 rewrite-rules]
  user@host# **set dscp** ***downlink_rewrite_v4_dscp*** **protocol gtp-inet-both**

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Configuring QoS on the Broadband Gateway Overview on page 18
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 3

Configuration Examples

- Example: Configuring Quality of Service on GGSN/P-GW on page 49

Example: Configuring Quality of Service on GGSN/P-GW

This example describes how to configure quality of service (QoS) on the MobileNext Broadband Gateway, and consists of the following sections:

- Requirements on page 49
- Overview on page 50
- Configuration on page 51
- Verification on page 82

Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway software package

Before you begin:

- Configure mobile interfaces for access point names (APNs)
- Configure APNs on the broadband gateway
- Configure Junos OS class-of-service (CoS) forwarding classes

Overview

In a mobile network, the availability of network resources is shared among multiple services (including Internet, voice, video, e-mail, and file sharing), each of which has different QoS requirements in terms of required bit rates, acceptable packet loss rates, and packet delay. You configure QoS on the broadband gateway to prioritize subscriber traffic and provide better service to certain services or subscribers to the detriment of other services and subscribers.

To configure QoS on the broadband gateway, you create a set of QoS profiles that are then referenced in a local policy, which defines the QoS treatment for 3G 4G subscriber traffic on the broadband gateway. You configure the following profiles and policies:

- Classifier profiles—Define the mapping of each traffic class and QoS Class Identifier (QCI) to a forwarding class and packet loss priority. You configure a separate classifier profiles for home, visiting, and roaming subscribers on 3G and 4G networks. Each classifier profile uses a GTPv2 QCI to define forwarding treatment for 3G and 4G subscribers. For 3G subscribers, the broadband gateway maps the GTPv1 traffic class or traffic handling priorities to the equivalent GTPv2 QCI and applies the classification. For example, a GTPv1 subscriber that arrives on the gateway with Interactive traffic class and THP 1 and signaling indication enabled maps to QCI 5, and data for this subscriber is classified based on the QCI 5 forwarding treatment you configure in the classifier profile. For information about mapping of QCI values to Release 99 QoS parameter values, see the "Quality of Service Overview" on page 3.
- Resource threshold profiles—Define the thresholds for number of bearers, memory, and CPU load. Call admission control (CAC) is based on the configured resource thresholds and allows only higher priority traffic when low or high resource thresholds are exceeded. You can configure a single resource threshold profile at the gateway level for 3G and 4G subscribers.
- CoS policy profiles—Define the negotiation of QoS parameters to determine when bearer requests can be upgraded, downgraded, or rejected. You define CoS policy profiles to provide separate QoS configurations for home, visiting, and roaming subscribers on 3G and 4G networks.
- Bandwidth pools—Define bandwidth pools to limit guaranteed bit rate (GBR) utilization (3G networks).
- Local policies—Define the overall CoS and call admission control behavior for 3G and 4G subscriber traffic. A local policy is applied at either the gateway or access point name (APN) level. A local policy applied at the APN level takes priority over a local policy applied at the gateway. Each local policy includes the classifier profiles, resource threshold profiles, and CoS policy profiles that define the overall QoS treatment for 3G subscriber traffic, 4G subscriber traffic, or both. A local policy can include multiple classifier profiles, resource threshold profiles, and CoS policy profiles to provide QoS treatment specific to the home, visiting, and roaming subscribers on 3G and 4G networks.
- Rewrite rules—Provide the required DiffServ code point (DSCP) marking of subscriber packets for uplink and downlink traffic.

 Copyright © 2012, Juniper Networks, Inc.

Configuration

To configure QoS on the broadband gateway, perform the following tasks:

- Configuring Classifier Profiles for Home Subscribers on 3G and 4G Networks on page 51
- Configuring Classifier Profiles for Roaming Subscribers on 3G and 4G Networks on page 52
- Configuring Classifier Profiles for Visitor Subscribers on 3G and 4G Networks on page 53
- Configuring a System-Wide Classifier Profile on page 54
- Configuring a System-Wide Resource Threshold Profile on page 55
- Configuring a CoS Policy Profile for Home Subscribers on a 3G Network on page 56
- Configuring a CoS Policy Profile for Home Subscribers on a 4G Network on page 59
- Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network on page 60
- Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network on page 63
- Configuring a CoS Policy Profile for Visiting Subscribers on a 3G Network on page 64
- Configuring a CoS Policy Profile for Visiting Subscribers on a 4G Network on page 67
- Configuring a System-Wide CoS Policy Profile on page 68
- Configuring Bandwidth Pools on page 71
- Configuring a Local Policy for 3G Networks on page 72
- Configuring a Local Policy for 4G Networks on page 73
- Configuring a System-Wide Local Policy on page 74
- Applying the Local Policies on page 75
- Configuring DSCP Ingress Rewrite Rules for IPv4 Packets on page 76
- Configuring DSCP Ingress Rewrite Rules for IPv6 Packets on page 77
- Configuring DSCP Egress Rewrite Rules for IPv4 Packets on page 78
- Configuring DSCP Egress Rewrite Rules for IPv6 Packets on page 79
- Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 80
- Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 80
- Configuring the Maximum Number of Bearers on page 81
- Enabling Preemption on page 81

Configuring Classifier Profiles for Home Subscribers on 3G and 4G Networks

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 2
   forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 4
   forwarding-class af2 loss-priority low
```

```
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 5
   forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 6
   forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 7
   forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 8
   forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 9
   forwarding-class af4 loss-priority low
```

Step-by-Step Procedure

To configure a classifier profile for home subscribers on 3G and 4G Networks:

1. Specify a name for the home classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 2 forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 4 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 5 forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 6 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 7 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 8 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
   qos-class-identifier 9 forwarding-class af4 loss-priority low
```

Results

From configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Classifier Profiles for Roaming Subscribers on 3G and 4G Networks

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 2
   forwarding-class af1 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 4
   forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 5
   forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 6
   forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 7
   forwarding-class af4 loss-priority low
```


Copyright © 2012, Juniper Networks, Inc.

```
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 8
  forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 9
  forwarding-class be loss-priority high
```

Step-by-Step Procedure

To configure classifier profiles for roaming subscribers on 3G and 4G networks:

1. Specify a name for the roamer classifier profile and map each 3G traffic class and 4G Qos Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 2 forwarding-class af1 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 4 forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 5 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 6 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 7 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 8 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
  qos-class-identifier 9 forwarding-class be loss-priority high
```

Configuring Classifier Profiles for Visitor Subscribers on 3G and 4G Networks

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 2
  forwarding-class af1 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 4
  forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 5
  forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 6
  forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 7
  forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 8
  forwarding-class be loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 9
  forwarding-class nc loss-priority high
```

Step-by-Step Procedure

To configure classifier profiles for visitor subscribers on 3G and 4G networks:

1. Specify a name for the visitor classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 2 forwarding-class af1 loss-priority high
```

```
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 4 forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 5 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 6 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 7 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 8 forwarding-class be loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
  qos-class-identifier 9 forwarding-class nc loss-priority high
```

Configuring a System-Wide Classifier Profile

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 2
  forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 4
  forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 5
  forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 6
  forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 7
  forwarding-class nc loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 8
  forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 9
  forwarding-class be loss-priority high
```

Step-by-Step Procedure

To configure the system-wide classifier profile for 3G and 4G networks:

1. Specify a name (**system_wide**) for the classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 2 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 4 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 5 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 6 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 7 forwarding-class nc loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 8 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
  qos-class-identifier 9 forwarding-class be loss-priority high
```


Copyright © 2012, Juniper Networks, Inc.

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a System-Wide Resource Threshold Profile

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load low
  percentage 60
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load low
  priority-level 7
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load high
  percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load high
  priority-level 4
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu low percentage
  70
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu low priority-level
  7
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu high percentage
  80
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu high priority-level
  4
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory low percentage
  85
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory low
  priority-level 10
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory high percentage
  90
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory high
  priority-level 5
```

Step-by-Step Procedure To configure resource threshold profiles for subscribers on 3G and 4G networks:

1. Configure the low and high thresholds for bearer load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  bearers-load low percentage 60
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  bearers-load low priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  bearers-load high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  bearers-load high priority-level 4
```

2. Configure the low and high thresholds for the CPU load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  cpu low percentage 70
```

```
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  cpu low priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  cpu high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  cpu high priority-level 4
```

3. Configure the low and high thresholds for the memory load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  memory low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  memory low priority-level 10
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  memory high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
  memory high priority-level 5
```

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Home Subscribers on a 3G Network

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles home_v1 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
  maximum-bit-rate-uplink 3072 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
  maximum-bit-rate-downlink 3072 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
  guaranteed-bit-rate-uplink 3008 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
  guaranteed-bit-rate-downlink 3008 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 6
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 6
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 7
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 7
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 8
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 8
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 9
  maximum-bit-rate-uplink 896
```

 Copyright © 2012, Juniper Networks, Inc.

```
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 9
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action non-gbr-bearer
  violate-action transmit
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action gbr-bearer
  exceed-action transmit
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for home subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the **upgrade** option to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value):

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
     default-bearer-qci 6 upgrade
   ```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
     allocation-retention-priority 5
   ```

   NOTE: For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.

   NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
     pdp-qos-control maximum-bit-rate-uplink 3072 upgrade
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
     pdp-qos-control maximum-bit-rate-downlink 3072 upgrade
   ```

4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control guaranteed-bit-rate-uplink 3008 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control guaranteed-bit-rate-downlink 3008 upgrade
```

5. Configure the uplink and downlink maximum bit rates for the non-GBR traffic classes:

   a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication):

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

   b. Configure an MBR for the Interactive traffic class with THP 2:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

   c. Configure an MBR for the Interactive traffic class with THP 3:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

   d. Configure an MBR for the Background traffic class:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
  pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
  non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
  gbr-bearer exceed-action transmit
```


Copyright © 2012, Juniper Networks, Inc.

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
  gbr-bearer violate-action transmit
```

Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Home Subscribers on a 4G Network

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles home_v2 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 allocation-retention-priority 5 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 aggregate-qos-control
  maximum-bit-rate-uplink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 aggregate-qos-control
  maximum-bit-rate-downlink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 policer-action non-gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for home subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and specify the **upgrade** option to upgrade the QCI value of bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests with a higher QCI.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  default-bearer-qci 6 upgrade
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  allocation-retention-priority 5
```

NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

3. Specify that bearers that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregate-qos-control maximum-bit-rate-uplink 2048
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregate-qos-control maximum-bit-rate-downlink 2048
```

4. Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  policer-action non-gbr-bearer violate-action transmit
```

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles roamer_v1 default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles roamer_v1 allocation-retention-priority 6
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  maximum-bit-rate-uplink 2500
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  maximum-bit-rate-downlink 2500
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  guaranteed-bit-rate-uplink 2372
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  guaranteed-bit-rate-downlink 2372
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 6
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 6
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 7
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 7
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 8
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 8
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 9
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 9
  maximum-bit-rate-downlink 896
```

 Copyright © 2012, Juniper Networks, Inc.

```
set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action non-gbr-bearer
  violate-action transmit
set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action gbr-bearer
  exceed-action transmit
set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for roaming subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the default to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
     default-bearer-qci 6
   ```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
     allocation-retention-priority 5
   ```

   NOTE: For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.

   NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are accepted, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
     pdp-qos-control maximum-bit-rate-uplink 2500
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
     pdp-qos-control maximum-bit-rate-downlink 2500
   ```

4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are accepted, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control guaranteed-bit-rate-uplink 2372
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control guaranteed-bit-rate-downlink 2372
```

5. Configure the uplink and downlink maximum bit rates for traffic classes for non-GBR PDP contexts:

   a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

   b. Configure an MBR for the Interactive traffic class with THP 2.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

   c. Configure an MBR for the Interactive traffic class with THP 3.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

   d. Configure an MBR for the Background traffic class.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  policer-action non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  policer-action gbr-bearer exceed-action transmit
```


Copyright © 2012, Juniper Networks, Inc.

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  policer-action gbr-bearer violate-action transmit
```

Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles roamer_v2 default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles roamer_v2 allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregate-qos-control
  maximum-bit-rate-uplink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregate-qos-control
  maximum-bit-rate-downlink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 policer-action non-gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for roaming subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and accept bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests that come in with a higher QCI.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  default-bearer-qci 6
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  allocation-retention-priority 5
```

NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

3. Specify that bearers that come in with a lower MBR value than the configured value accepted, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregate-qos-control maximum-bit-rate-uplink 1600
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregate-qos-control maximum-bit-rate-downlink 1600
```

4. Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  policer-action non-gbr-bearer violate-action transmit
```

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Visiting Subscribers on a 3G Network

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles visitor_v1 default-bearer-qci 7
set unified-edge cos-cac cos-policy-profiles visitor_v1 allocation-retention-priority 9
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  maximum-bit-rate-uplink 2048 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  maximum-bit-rate-downlink 2048 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  guaranteed-bit-rate-uplink 1984 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  guaranteed-bit-rate-downlink 1984 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 6
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 6
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 7
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 7
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 8
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 8
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 9
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 9
  maximum-bit-rate-downlink 896
```

 Copyright © 2012, Juniper Networks, Inc.

```
set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action non-gbr-bearer
  violate-action transmit
set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action gbr-bearer
  exceed-action transmit
set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for visitor subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the default to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
     default-bearer-qci 7
   ```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted, and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
     allocation-retention-priority 9
   ```

   NOTE: For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.

   NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
     pdp-qos-control maximum-bit-rate-uplink 2048 upgrade
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
     pdp-qos-control maximum-bit-rate-downlink 2048 upgrade
   ```

4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control guaranteed-bit-rate-uplink 1984 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control guaranteed-bit-rate-downlink 1984 upgrade
```

5. Configure the uplink and downlink maximum bit rates for traffic classes for non-GBR PDP contexts:

   a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

   b. Configure an MBR for the Interactive traffic class with THP 2.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

   c. Configure an MBR for the Interactive traffic class with THP 3.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

   d. Configure an MBR for the Background traffic class.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  policer-action non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  policer-action gbr-bearer exceed-action transmit
```


Copyright © 2012, Juniper Networks, Inc.

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
  policer-action gbr-bearer violate-action transmit
```

Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a CoS Policy Profile for Visiting Subscribers on a 4G Network

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles visitor_v2 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v2 allocation-retention-priority 5
  upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregate-qos-control
  maximum-bit-rate-uplink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregate-qos-control
  maximum-bit-rate-downlink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 policer-action non-gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for visitor subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and specify the **upgrade** option to upgrade the QCI value of bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests with a higher QCI.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
  default-bearer-qci 6 upgrade
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
  allocation-retention-priority 5
```

NOTE: If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

3. Specify that bearers that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
  aggregate-qos-control maximum-bit-rate-uplink 1600
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
  aggregate-qos-control maximum-bit-rate-downlink 1600
```

4. Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
  policer-action non-gbr-bearer violate-action transmit
```

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a System-Wide CoS Policy Profile

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles system_wide default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles system_wide allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
  maximum-bit-rate-uplink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
  maximum-bit-rate-downlink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
  guaranteed-bit-rate-uplink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
  guaranteed-bit-rate-downlink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 6
  maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 6
  maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 7
  maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 7
  maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 8
  maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 8
  maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 9
  maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 9
  maximum-bit-rate-downlink 256
```

 Copyright © 2012, Juniper Networks, Inc.

```
set unified-edge cos-cac cos-policy-profiles system_wide aggregate-qos-control
  maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide aggregate-qos-control
  maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide policer-action gbr-bearer
  exceed-action transmit
set unified-edge cos-cac cos-policy-profiles system_wide policer-action gbr-bearer
  violate-action transmit
set unified-edge cos-cac cos-policy-profiles system_wide policer-action non-gbr-bearer
  violate-action transmit
```

Step-by-Step Procedure

To configure a CoS policy profile for subscribers in 3G and 4G networks:

1. Specify a name for the CoS policy profile, negotiate the QCI for 3G/4G subscribers, and accept bearer requests that come in with a lower traffic class/QCI than the configured value and downgrade requests with a higher traffic class/QCI.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     default-bearer-qci 6
   ```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior).

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     allocation-retention-priority 5
   ```

3. Specify that PDP context requests that come in with a lower MBR value than the configured value are accepted and PDP context requests that come in with a higher MBR value than the configured value are downgraded to the configured MBR value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     pdp-qos-control maximum-bit-rate-uplink 512
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     pdp-qos-control maximum-bit-rate-downlink 512
   ```

4. Specify that PDP context requests that come in with a lower GBR value than the configured value are accepted, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

   ```
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     pdp-qos-control guaranteed-bit-rate-uplink 512
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     pdp-qos-control guaranteed-bit-rate-downlink 512
   ```

5. Configure the uplink and downlink maximum bit rates for the non-GBR traffic classes:

   a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

      ```
      [edit]
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 6 maximum-bit-rate-uplink 256
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 6 maximum-bit-rate-downlink 256
      ```

   b. Configure an MBR for the Interactive traffic class with THP 2.

      ```
      [edit]
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 7 maximum-bit-rate-uplink 256
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 7 maximum-bit-rate-downlink 256
      ```

   c. Configure an MBR for the Interactive traffic class with THP 3.

      ```
      [edit]
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 8 maximum-bit-rate-uplink 256
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 8 maximum-bit-rate-downlink 256
      ```

   d. Configure an MBR for the Background traffic class.

      ```
      [edit]
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 9 maximum-bit-rate-uplink 256
      user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
        pdp-qos-control qci 9 maximum-bit-rate-downlink 256
      ```

6. Configure the action to take for non-GBR bearer requests when the AMBR or MBR exceeds the configured value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     policer-action non-gbr-bearer violate-action transmit
   ```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     policer-action gbr-bearer exceed-action transmit
   ```

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
     policer-action gbr-bearer violate-action transmit
   ```


Copyright © 2012, Juniper Networks, Inc.

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring Bandwidth Pools

Step-by-Step Procedure You configure a bandwidth pools for uplink and downlink subscriber traffic to ensure that sufficient bandwidth is available when packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses the bandwidth pools to negotiate and reserve bandwidth for PDP contexts with a guaranteed bit rate (GBR).

1. Specify a name for the uplink bandwidth pool.

   [edit]
   user@host# **edit unified-edge cos-cac gbr-bandwidth-pools bw_pool_uplink**

2. Specify a name for the downlink bandwidth pool.

   [edit]
   user@host# **edit unified-edge cos-cac gbr-bandwidth-pools bw_pool_downlink**

3. Configure the total bandwidth for each bandwidth pool, in megabits per second (Mbps).

   [edit]
   user@host# **set unified-edge cos-cac bandwidth-pools bw_pool_uplink bandwidth *125000***
   user@host# **set unified-edge cos-cac bandwidth-pools bw_pool_downlink bandwidth *500000***

4. (Optional) Specify that when bearer load reaches the configured bandwidth threshold for uplink or downlink, the create/modify PDP context requests can be downgraded, starting with lower priority requests.

   [edit]
   user@host# **set unified-edge cos-cac bandwidth-pools bw_pool_uplink downgrade-gtp-v1-gbr-bearers**
   user@host# **set unified-edge cos-cac bandwidth-pools bw_pool_downlink downgrade-gtp-v1-gbr-bearers**

NOTE: If the **downgrade-gtp-v1-gbr-bearers** option is configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are downgraded to the Background traffic class. If the **downgrade-gtp-v1-gbr-bearers** option is not configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are rejected.

Configuring a Local Policy for 3G Networks

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit unified-edge local-policies local_v1
set unified-edge local-policies local_v1 resource-threshold-profile resource_pgw
set unified-edge local-policies local_v1 classifier-profile home_pgw
set unified-edge local-policies local_v1 cos-policy-profile home_v1
set unified-edge local-policies local_v1 roamer-classifier-profile roamer_pgw
set unified-edge local-policies local_v1 roamer-cos-policy-profile roamer_v1
set unified-edge local-policies local_v1 visitor-classifier-profile visitor_pgw
set unified-edge local-policies local_v1 visitor-cos-policy-profile visitor_v1
set unified-edge local-policies local_v1 dl-bandwidth-pool bw_pool_downlink
set unified-edge local-policies local_v1 ul-bandwidth-pool bw_pool_uplink
```

Step-by-Step Procedure

A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a local policy:

1. Specify a name for the local policy.

   ```
   [edit]
   user@ggsn-pgw# edit unified-edge local-policies local_v1
   ```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge local-policies local_v1 resource-threshold-profile
     resource_pgw
   ```

3. Specify the classifier profiles for the local policy to define the mapping of traffic classes and QCIs to a forwarding class and loss priority.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge local-policies local_v1 classifier-profile home_pgw
   user@ggsn-pgw# set unified-edge local-policies local_v1 roamer-classifier-profile
     roamer_pgw
   user@ggsn-pgw# set unified-edge local-policies local_v1 visitor-classifier-profile
     visitor_pgw
   ```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

   ```
   [edit]
   user@ggsn-pgw# set unified-edge local-policies local_v1 cos-policy-profile home_v1
   user@ggsn-pgw# set unified-edge local-policies local_v1 roamer-cos-policy-profile
     roamer_v1
   user@ggsn-pgw# set unified-edge local-policies local_v1 visitor-cos-policy-profile
     visitor_v1
   ```

5. Specify a bandwidth pool for downlink traffic.

   ```
   [edit]
   ```


Copyright © 2012, Juniper Networks, Inc.

```
user@host# set unified-edge local-policies local_v1 dl-bandwidth-pool
  bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit]
user@host# set unified-edge local-policies local_v1 ul-bandwidth-pool
  bw_pool_uplink
```

Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Local Policy for 4G Networks

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit unified-edge local-policies local_v2
set unified-edge local-policies local_v2 resource-threshold-profile resource_pgw
set unified-edge local-policies local_v2 classifier-profile home_pgw
set unified-edge local-policies local_v2 cos-policy-profile home_v2
set unified-edge local-policies local_v2 roamer-classifier-profile roamer_pgw
set unified-edge local-policies local_v2 roamer-cos-policy-profile roamer_v2
set unified-edge local-policies local_v2 visitor-classifier-profile visitor_pgw
set unified-edge local-policies local_v2 visitor-cos-policy-profile visitor_v2
set unified-edge local-policies local_v2 dl-bandwidth-pool bw_pool_downlink
set unified-edge local-policies local_v2 ul-bandwidth-pool bw_pool_uplink
```

Step-by-Step Procedure

A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a local policy:

1. Specify a name for the local policy.

```
[edit]
user@ggsn-pgw# edit unified-edge local-policies local_v2
```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v2 resource-threshold-profile
  resource_pgw
```

3. Specify the classifier profiles for the local policy to define the mapping of QCIs to a forwarding class and loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v2 classifier-profile home_pgw
user@ggsn-pgw# set unified-edge local-policies local_v2 roamer-classifier-profile
  roamer_pgw
```

```
user@ggsn-pgw# set unified-edge local-policies local_v2 visitor-classifier-profile
  visitor_pgw
```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v2 cos-policy-profile home_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 roamer-cos-policy-profile
  roamer_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 visitor-cos-policy-profile
  visitor_v2
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_v2 dl-bandwidth-pool
  bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_v2 ul-bandwidth-pool
  bw_pool_uplink
```

Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a System-Wide Local Policy

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit unified-edge local-policies local_system_wide
set unified-edge local-policies local_system_wide resource-threshold-profile resource_pgw
set unified-edge local-policies local_system_wide classifier-profile system_wide
set unified-edge local-policies local_system_wide cos-policy-profile system_wide
set unified-edge local-policies local_system_wide dl-bandwidth-pool bw_pool_downlink
set unified-edge local-policies local_system_wide ul-bandwidth-pool bw_pool_uplink
```

Step-by-Step Procedure

A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a system-wide local policy:

1. Specify a name for the local policy.

```
[edit]
user@ggsn-pgw# edit unified-edge local-policies local_system_wide
```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

Copyright © 2012, Juniper Networks, Inc.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide
  resource-threshold-profile resource_pgw
```

3. Specify the classifier profile for the local policy to define the mapping of traffic classes and QCIs to a forwarding class and loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide classifier-profile
  system_wide
```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide
  cos-policy-profile system_wide
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_system_wide dl-bandwidth-pool
  bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_system_wide ul-bandwidth-pool
  bw_pool_uplink
```

Results From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

Applying the Local Policies

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set gateways ggsn-pgw MBG1 local-policy-profile local_system_wide
set gateways ggsn-pgw MBG1 apn-services apns qosv1.com local-policy-profile local_v1
set gateways ggsn-pgw MBG1 apn-services apns qosv2.com local-policy-profile local_v2
```

Step-by-Step Procedure You apply a local policy at the system level or APN level. A local policy applied at the APN level overrides a local policy at the system level.

1. At the gateway level, apply the system-wide local policy.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 local-policy-profile local_system_wide
```

2. At the APN level, apply the local policy for 3G subscriber traffic.

```
[edit]
```

```
user@host# set gateways ggsn-pgw MBG1 apn-services apns qosv1.com
  local-policy-profile local_v1
```

3. At the APN level, apply the local policy for 4G subscriber traffic.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 apn-services apns qosv2.com
  local-policy-profile local_v2
```

Configuring DSCP Ingress Rewrite Rules for IPv4 Packets

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscpv4_ingress_rw]
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
  high code-point 001110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
  low code-point 001010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
  high code-point 010110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
  low code-point 010010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
  high code-point 011110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
  low code-point 011010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
  high code-point 100110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
  low code-point 100010
```

Step-by-Step Procedure

To configure the ingress rewrite rules for IPv4 packets:

1. Specify a name for the ingress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp dscpv4_ingress_rw
```

2. Configure the ingress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af4 loss-priority high code-point 100110
```


Copyright © 2012, Juniper Networks, Inc.

```
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
  class af4 loss-priority low code-point 100010
```

Configuring DSCP Ingress Rewrite Rules for IPv6 Packets

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscpv6_ingress_rw
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af1 loss-priority
  high code-point 001110
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af1 loss-priority
  low code-point 001010
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af2 loss-priority
  high code-point 010110
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af2 loss-priority
  low code-point 010010
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af3 loss-priority
  high code-point 011110
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af3 loss-priority
  low code-point 011010
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af4 loss-priority
  high code-point 100110
set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding class af4 loss-priority
  low code-point 100010
```

Step-by-Step Procedure

To configure the ingress rewrite rules for IPv6 packets:

1. Specify a name for the ingress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscpv6_ingress_rw
```

2. Configure the ingress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp dscpv6_ingress_rw forwarding
  class af4 loss-priority low code-point 100010
```

Copyright © 2012, Juniper Networks, Inc.

Configuring DSCP Egress Rewrite Rules for IPv4 Packets

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscpv4_egress_rw
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af1 loss-priority
  high code-point 001110
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af1 loss-priority
  low code-point 001010
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af2 loss-priority
  high code-point 010110
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af2 loss-priority
  low code-point 010010
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af3 loss-priority
  high code-point 011110
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af3 loss-priority
  low code-point 011010
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af4 loss-priority
  high code-point 100110
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af4 loss-priority
  low code-point 100010
set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class be loss-priority
  low code-point 000000
```

Step-by-Step Procedure

To configure the egress rewrite rules for IPv4 packets:

1. Specify a name for the egress rewrite rules.

   ```
   [edit ]
   user@host# edit class-of-service rewrite-rules dscp dscp_v4_egress_rw
   ```

2. Configure the egress rewrite rules mappings for traffic on the mobile interface.

   ```
   [edit]
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af1 loss-priority high code-point 001110
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af1 loss-priority low code-point 001010
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af2 loss-priority high code-point 010110
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af2 loss-priority low code-point 010010
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af3 loss-priority high code-point 011110
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af3 loss-priority low code-point 011010
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af4 loss-priority high code-point 100110
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class af4 loss-priority low code-point 100010
   user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
     class be loss-priority low code-point 000000
   ```


Copyright © 2012, Juniper Networks, Inc.

Configuring DSCP Egress Rewrite Rules for IPv6 Packets

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af1
   loss-priority high code-point 001110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af1
   loss-priority low code-point 001010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af2
   loss-priority high code-point 010110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af2
   loss-priority low code-point 010010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af3
   loss-priority high code-point 011110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af3
   loss-priority low code-point 011010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af4
   loss-priority high code-point 100110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af4
   loss-priority low code-point 100010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class be
   loss-priority low code-point 000000
```

Step-by-Step Procedure

To configure the ingress rewrite rules for IPv6 packets:

1. Specify a name for the egress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
```

2. Configure the egress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class af4 loss-priority low code-point 100010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
   forwarding class be loss-priority low code-point 000000
```

Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp dscpv4_ingress_rw
set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp-ipv6 dscpv6_ingress_rw
set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp dscpv4_ingress_rw
set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp-ipv6 dscpv6_ingress_rw
```

Step-by-Step Procedure

To specify the ingress rewrite rules to apply to rewrite DSCPv4 and DSCPv6 values for incoming subscriber packets on the mif.0 and mif.1 mobile interfaces, which correspond to the **qosv1.com** and **qosv2.com** APNs for 3G subscriber traffic and 4G subscriber traffic, respectively:

1. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 3G subscriber packets arriving on the **qosv1.com** APN (mif.0), specify the names of the rewrite rules that you want to apply to the mobile interface.

   ```
   [edit]
   user@host# set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp
     dscpv4_ingress_rw
   user@host# set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp-ipv6
     dscpv6_ingress_rw
   ```

2. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 4G subscriber packets arriving on the **qosv2.com** APN (mif.1), specify the names of the rewrite rules that you want to apply to the mobile interface.

   ```
   [edit]
   user@host# set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp
     dscpv4_ingress_rw
   user@host# set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp-ipv6
     dscpv6_ingress_rw
   ```

Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set class-of-service interfaces mif unit 0 rewrite-rules dscp dscpv4_egress_rw protocol
  gtp-inet-both
set class-of-service interfaces mif unit 0 rewrite-rules dscp dscpv6_egress_rw protocol
  gtp-inet-both
set class-of-service interfaces mif unit 1 rewrite-rules dscp dscpv4_egress_rw protocol
  gtp-inet-both
set class-of-service interfaces mif unit 1rewrite-rules dscp dscpv6_egress_rw protocol
  gtp-inet-both
```


Copyright © 2012, Juniper Networks, Inc.

Step-by-Step Procedure

To apply an egress rewrite rule to rewrite DSCPv4 and DSCPv6 values to both the inner and outer IP headers of downstream subscriber packets, specify the name of the rewrite rules you want to apply to the mobile interfaces and include the **gtp-inet-both** option:

1. To apply egress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 3G subscriber packets arriving on the **qosv1.com** APN (mif.0), specify the names of the rewrite rules that you want to apply to the mobile interface.

```
[edit]
user@host# set class-of-service interfaces mif unit 0 rewrite-rules dscp
  dscpv4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 0 rewrite-rules dscp
  dscpv6_egress_rw protocol gtp-inet-both
```

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
  dscpv4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
  dscpv6_egress_rw protocol gtp-inet-both
```

2. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 4G subscriber packets arriving on the **qosv2.com** APN (mif.1), specify the names of the rewrite rules that you want to apply to the mobile interface.

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
  dscpv4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
  dscpv6_egress_rw protocol gtp-inet-both
```

Configuring the Maximum Number of Bearers

Step-by-Step Procedure

You configure the maximum bearers to specify an upper limit on the number of bearers allowed at the system level and, optionally, the APN level. When the total number of active bearers at the system level or APN level reaches the maximum configured limit, the broadband gateway rejects new bearer requests.

To configure the maximum number of active bearers:

1. Configure the number of maximum bearers allowed at the system level.

```
[edit]
user@host# set unified-edge gateways ggsn-pgw MBG1 maximum-bearers 5000000
```

Enabling Preemption

Step-by-Step Procedure

You can enable preemption at the system level to enable the preemption capability indicator (PCI) and preemption vulnerability indicator (PVI) flags. Preemption is disabled by default.

To enable preemption or both 3G (GTPv1) and 4G (GTPv2) subscriber traffic:

1. Configure preemption at the system level.

```
[edit]
```

```
user@host# set unified-edge gateways ggsn-pgw MBG1 preemption enable
```

Verification

To display QoS statistics for 3G and 4G subscriber packets to verify that the QoS configuration on the broadband gateway is working properly, you can perform the following tasks:

- Display QoS Statistics for 4G Subscriber Packets with a Specified Allocation Retention Priority: on page 82
- Display 4G Subscriber Information for Traffic Marked with a Specified QCI on page 83
- Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class on page 83
- Display the Requested and Negotiated QoS Parameters for Mobile Subscribers on page 84

Display QoS Statistics for 4G Subscriber Packets with a Specified Allocation Retention Priority:

Purpose Verify that the QoS configuration is working properly by displaying statistics such as session establishment attempts, peer initiated sessions, and gateway initiated session deactivations.

Action

```
user@host> show unified-edge ggsn-pgw statistics arp 10
Control plane statistics:
    Gn/S5 signaling msgs rcvd:                  0
    Gn/S5 signaling msgs sent:                  50001
    Gn/S5 signaling msgs dropped:               0
    Gn/S5 signaling bytes rcvd:                 0
    Gn/S5 signaling bytes sent:                 0
    Total GTP tunnels created:                  0
    Session establishment attempts:             50221
    Successful session establishments:          4476
    MS/peer initiated session deactivations:    0
    Successful MS/peer initiated deactivations: 0
    Gateway initiated session deactivations:    0
    Successful gateway initiated deactivations: 0
    Session Establishments Failed (by GTP cause):
        Others               0
        Service unavailable: 0
        System failure:      0
        No resources:        47762
        No address:          0
        Service denied:      0
        Authentication Fail: 0
        APN access denied:   0
Data plane GTP statistics (Gn/S5/S8):
    Input     packets:          0
    Input     bytes:            0
    Output    packets:          0
    Output    bytes:            0
    Discarded packets:          0
Data plane GTP statistics (Gi):
    Input     packets:          0
    Input     bytes:            0
```

 Copyright © 2012, Juniper Networks, Inc.

```
    Output    packets:          0
    Output    bytes:            0
    Discarded packets:          0
```

Meaning This output shows the attempted session requests and the requests that were successfully established for 4G subscriber traffic with the specified ARP value.

Display 4G Subscriber Information for Traffic Marked with a Specified QCI

Purpose Verify that the QoS configuration is working properly for 4G subscribers by showing statistics for subscriber packets with a specified QCI.

Action

```
user@host> show unified-edge ggsn-pgw statistics qci 5
 regress@brainstorm> show unified-edge ggsn-pgw qos statistics qci 5
Control plane statistics:
    Gn/S5 signaling msgs rcvd:                  0
    Gn/S5 signaling msgs sent:                  10
    Gn/S5 signaling msgs dropped:               0
    Gn/S5 signaling bytes rcvd:                 0
    Gn/S5 signaling bytes sent:                 0
    Total GTP tunnels created:                  0
    Session establishment attempts:             10
    Successful session establishments:          10
    MS/peer initiated session deactivations:    0
    Successful MS/peer initiated deactivations: 0
    Gateway initiated session deactivations:    0
    Successful gateway initiated deactivations: 0
    Session Establishments Failed (by GTP cause):
        Others               0
        Service unavailable: 0
        System failure:      0
        No resources:        0
        No address:          0
        Service denied:      0
        Authentication Fail: 0
        APN access denied:   0
```

Meaning This output shows the Create Session requests that were successfully established for 4G mobile subscriber packets with the specified QCI value.

Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class

Purpose Verify that the QoS configuration is working properly for 3G subscribers by showing statistics for subscriber packets of the specified traffic class.

Action

```
user@host> show unified-edge ggsn-pgw statistics traffic-class conversational
 Control plane statistics:
    Gn/S5 signaling msgs rcvd:                  0
    Gn/S5 signaling msgs sent:                  15
    Gn/S5 signaling msgs dropped:               0
    Gn/S5 signaling bytes rcvd:                 0
    Gn/S5 signaling bytes sent:                 0
    Total GTP tunnels created:                  0
    Session establishment attempts:             15
```

```
    Successful session establishments:          15
    MS/peer initiated session deactivations:    0
    Successful MS/peer initiated deactivations: 0
    Gateway initiated session deactivations:    0
    Successful gateway initiated deactivations: 0
    Session Establishments Failed (by GTP cause):
        Others               0
        Service unavailable: 0
        System failure:      0
        No resources:        0
        No address:          0
        Service denied:      0
        Authentication Fail: 0
        APN access denied:   0
Data plane GTP statistics (Gn/S5/S8):
    Input     packets:          0
    Input     bytes:            0
    Output    packets:          0
    Output    bytes:            0
    Discarded packets:          0
Data plane GTP statistics (Gi):
    Input     packets:          0
    Input     bytes:            0
    Output    packets:          0
    Output    bytes:            0
    Discarded packets:          0
```

Meaning This output shows the Create Session requests that were successfully established for 3G subscriber traffic of the conversational class.

Display the Requested and Negotiated QoS Parameters for Mobile Subscribers

Purpose Verify the negotiated QoS parameters for a mobile subscriber.

Action

```
user@host> show unified-edge ggsn-pgw subscribers extensive
Subscriber Information:
    IMSI: 332215553443196    IMEI: 1122334455667795
    MSISDN: 3326555562       Time Zone: None    (DST): None
    Status: Visitor
User Location Info:
      MCC:  None  MNC:  None
      LAC: 0x0  CI: 0x0     SAC: 0x0  RAC: 0x0  TAC: 0x0  ECI: 0x0
    RAT Type: E-UTRAN
  PDN Session:
    APN name: juniper.com
    IPv4 Address: 20.0.4.8          IPv6 Address: None
    Direct Tunnel: Disabled         Session Duration: 3d 20:38:38
    Local Control address: 10.1.1.1 Remote Control address: 30.1.1.2
    TEID Control Local: 0x9001800   TEID Control Remote: 0x10d
    Peer CSID: 0                    Remote CSID: 0
    Addressing scheme: Local        Selection mode: from-ms
    Session PIC: 0 /0  (FPC/PIC)    Anchor PFE: 2 /0  (FPC/PIC)
    Session State: Established      GTP Version: 2
    Serving network: MCC: 231  MNC :215
    Negotiated APN AMBR: Downlink: 1000 kbps    Uplink: 1000 kbps
    Requested APN AMBR: Downlink: 1000 kbps     Uplink: 1000 kbps
  Bearer:
    NSAPI/EBI: 5                     Charging ID: 0x9001800
    Local Data address: 10.1.1.1     Remote Data address: 30.1.1.2
```

 Copyright © 2012, Juniper Networks, Inc.

```
Local TEID: 0x111000             Remote TEID: 0x10e
Bearer State: Established        Substate: -
Idle Timeout: 0   min(0 -0,0)   AAA Interim Interval: 0   min(0 -0,0)
Negotiated QoS Parameters:
 QCI: 5    ARP: 11/0 /0   (PL/PVI/PCI)
 Forwarding Class:  -              Loss Priority:  -
Requested QoS Parameters:
 QCI :5   ARP : 11/0 /0   (PL/PVI/PCI)
Charging information:
 Profile ID: 0
 State: Init         Previous State: Init
```

Meaning This output shows the negotiated and requested QoS parameters for mobile subscribers.

Related Documentation

- Quality of Service Overview on page 3
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- Configuring QoS on the Broadband Gateway Overview on page 18
- Configuring S-GW-Specific CAC Parameters
- Example: Configuring QoS and CAC on a S-GW

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 4

Configuration Statements

- [edit unified-edge gateways] Hierarchy Level on page 87
- [edit unified-edge cos-cac] Hierarchy Level on page 87
- [edit unified-edge local-policies] Hierarchy Level on page 89

[edit unified-edge gateways] Hierarchy Level

Each of the following topics lists the statements at a sub-hierarchy of the **[edit unified-edge gateways]** hierarchy.

- [edit unified-edge gateways ggsn-pgw <gateway-name>] Hierarchy Level
- [edit unified-edge gateways sgw <gateway-name>] Hierarchy Level

Related Documentation

- [edit unified-edge] Hierarchy Level
- Notational Conventions Used in Junos OS Configuration Hierarchies

[edit unified-edge cos-cac] Hierarchy Level

```
unified-edge {
  cos-cac {
    classifier-profiles {
      name {
        description description;
        qos-class-identifier qci-value {
          forwarding-class class-name;
          loss-priority (high | low);
        }
      }
    }
    cos-policy-profiles {
      name {
        aggregated-qos-control {
          maximum-bit-rate-downlink {
            mbr-downlink;
            reject;
            upgrade;
          }
          maximum-bit-rate-uplink {
```

```
        mbr-uplink;
        reject;
        upgrade;
      }
    }
    allocation-retention-priority {
      priority-value;
      reject;
    }
    default-bearer-qci {
      qci-value;
      reject;
      upgrade;
    }
    description description;
    pdp-qos-control {
      guaranteed-bit-rate-downlink {
        gbr-downlink;
        reject;
        upgrade;
      }
      guaranteed-bit-rate-uplink {
        gbr-uplink;
        reject;
        upgrade;
      }
      maximum-bit-rate-downlink {
        mbr-downlink;
        reject;
        upgrade;
      }
      maximum-bit-rate-uplink {
        mbr-uplink;
        reject;
        upgrade;
      }
      qci qci-value {
        maximum-bit-rate-downlink {
          mbr-downlink;
          reject;
          upgrade;
        }
        maximum-bit-rate-uplink {
          mbr-uplink;
          reject;
          upgrade;
        }
      }
    }
    policer-action {
      gbr-bearer {
        exceed-action (drop | transmit);
        violate-action (set-loss-priority-high | transmit);
      }
      non-gbr-bearer {
        violate-action (set-loss-priority-high | transmit);
```


Copyright © 2012, Juniper Networks, Inc.

```
                }
            }
        }
    }
    gbr-bandwidth-pools {
        name {
            downgrade-gtp-v1-gbr-bearers;
            maximum-bandwidth maximum-bandwidth;
        }
    }
    resource-threshold-profiles {
        name {
            bearers-load {
                high {
                    percentage percentage;
                    priority-level priority-level;
                }
                low {
                    percentage percentage;
                    priority-level priority-level;
                }
            }
            cpu {
                high {
                    percentage percentage;
                    priority-level priority-level;
                }
                low {
                    percentage percentage;
                    priority-level priority-level;
                }
            }
            description description;
            memory {
                high {
                    percentage percentage;
                    priority-level priority-level;
                }
                low {
                    percentage percentage;
                    priority-level priority-level;
                }
            }
        }
    }
}
```

Related Documentation

- Notational Conventions Used in Junos OS Configuration Hierarchies

[edit unified-edge local-policies] Hierarchy Level

```
unified-edge {
    local-policies {
        policy-name {
```

```
            cos-policy-profile name;
            classifier-profile name;
            description description;
            dl-bandwidth-pool name;
            resource-threshold-profile name;
            roamer-classifier-profile name;
            roamer-cos-policy-profile name;
            ul-bandwidth-pool name;
            visitor-classifier-profile  name;
            visitor-cos-policy-profile name;
        }
    }
}
```

Related Documentation

- [edit unified-edge] Hierarchy Level
- Notational Conventions Used in Junos OS Configuration Hierarchies

Copyright © 2012, Juniper Networks, Inc.

aggregated-qos-control (CoS Policy Profiles)

Syntax

```
aggregated-qos-control {
  maximum-bit-rate-downlink {
    mbr-downlink;
    reject;
    upgrade;
  }
  maximum-bit-rate-uplink {
    mbr-uplink;
    reject;
    upgrade;
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name*]

Description

Configure the aggregate maximum bit rate (AMBR) for uplink and downlink traffic.

The AMBR specifies the total maximum bit rate for all non-GBR bearers (4G) associated with an IP Connectivity Access Network (IP-CAN) session. A bearer request that specifies a higher AMBR than the configured value is downgraded by default.

The remaining statements are explained separately.

Default

If you do not configure this statement, then the requested AMBR is accepted by the gateway.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- cos-policy-profiles on page 102

allocation-retention-priority (CoS Policy Profiles)

Syntax

```
allocation-retention-priority {
  priority-value;
  reject;
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W. **reject** statement added in Junos OS Mobility Release 11.4W.

Description

Configure the allocation and retention priority (ARP) for the class of service (CoS) policy profile. This configuration is primarily used to determine whether the establishment or modification of PDP contexts (3G) or bearers (4G) are accepted or rejected.

Create PDP Context requests and Create Session requests with priority value numerically greater than the configured priority value are accepted, and requests with numerically lower value are downgraded to the configured value.

Default

If this statement is not included, then the broadband gateway uses the ARP value sent in the Create PDP Context Request or Create Session Request message.

Options

priority-value—Specify the priority level for the PDP context or bearer.

Range: 1 through 15

reject—Specify that PDP contexts or bearers with priority level numerically lower than configured value are rejected.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- **cos-policy-profiles on page 102**
- Quality of Service Overview on page 3

Copyright © 2012, Juniper Networks, Inc.

bearers-load (Resource Threshold Profiles)

Syntax

```
bearers-load {
  high {
    percentage percentage;
    priority-level priority-level;
  }
  low {
    percentage percentage;
    priority-level priority-level;
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac resource-threshold-profiles *name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the lower and upper limits for the bearer load in the resource threshold profile. The bearer load specifies a precise level of admission control when the bearer load reaches a configured lower or upper threshold.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Resource Thresholds for 3G and 4G Networks on page 26
- **resource-threshold-profiles (QoS) on page 148**

classifier-profile (Local Policies)

Syntax classifier-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the classifier profile for home subscribers. A classifier profile defines the packet forwarding treatment for each bearer depending on its QoS Class Identifiers (QCIs).

Options ***profile-name***—Name of the classifier profile.

NOTE: **The classifier policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac classifier-profiles] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **classifier-profiles on page 95**
- **local-policies (QoS) on page 126**

Copyright © 2012, Juniper Networks, Inc.

classifier-profiles

Syntax

```
classifier-profiles {
  name {
    description description;
    qos-class-identifier qci-value {
      forwarding-class class-name;
      loss-priority (high | low);
    }
  }
}
```

Hierarchy Level [edit unified-edge cos-cac]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure a QoS classifier profile, which defines the packet forwarding treatment for each bearer (for the broadband gateway) depending on its QoS Class Identifiers (QCIs). The QCI is associated with priority, delay, and packet loss values.

Default If you do not configure the classifier profile, then no classification is done based on the mobile CoS parameters.

Options *name*—Name of the classifier profile.

The remaining statements are explained separately.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring QoS on the Broadband Gateway Overview on page 18
- **cos-cac on page 98**
- Quality of Service Overview on page 3

class-of-service (MobileNext Broadband Gateway)

Syntax

```
class-of-service {
  interfaces {
    mif. number {
      unit logical-unit-number {
        ingress-rewrite-rules {
          [dscp (rewrite-rule-name | default)];
          [dscp-ipv6 (rewrite-rule-name | default)];
          [inet-precedence (rewrite-rule-name | default)];
          }
        }
        rewrite-rules {
          [dscp (rewrite-rule-name | default)] {
            protocol [(gtp-inet-both | gtp-inet-outer)];
          }
          [dscp-ipv6 (rewrite-rule-name | default)] {
            protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
          }
          [inet-precedence (rewrite-rule-name | default)] {
            protocol [(gtp-inet-both | gtp-inet-outer)];
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the class of service (CoS) for the 3GPP support for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW). At the first instance, you must configure the ingress and egress rewrite rules to set the value of the CoS bits within the IP header of upstream and downstream subscriber packets received on the mobile interface. Later, you must apply the ingress and egress rewrite rules to the mobile interface to set CoS values for upstream and downstream packets. Within ingress and egress, you can specify rewrite rules for DSCP v4, DSCP v6, or IP precedence values.

NOTE: **For the S-GW, the configuration at the mobile interface level does not apply. Instead, class of service is configured on Junos OS interfaces.**

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Copyright © 2012, Juniper Networks, Inc.

Related Documentation

- [edit class-of-service] Hierarchy Level
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Configuring QoS on the Broadband Gateway Overview on page 18

Copyright © 2012, Juniper Networks, Inc.

cos-cac

Syntax

```
cos-cac {
  classifier-profiles {
    name {
      description description;
      qos-class-identifier qci-value {
        forwarding-class class-name;
        loss-priority (high | low);
      }
    }
  }
  cos-policy-profiles {
    name {
      aggregated-qos-control {
        maximum-bit-rate-downlink {
          mbr-downlink;
          reject;
          upgrade;
        }
        maximum-bit-rate-uplink {
          mbr-uplink;
          reject;
          upgrade;
        }
      }
      allocation-retention-priority {
        priority-value;
        reject;
      }
      default-bearer-qci {
        qci-value;
        reject;
        upgrade;
      }
      description description;
      pdp-qos-control {
        guaranteed-bit-rate-downlink {
          gbr-downlink;
          reject;
          upgrade;
        }
        guaranteed-bit-rate-uplink {
          gbr-uplink;
          reject;
          upgrade;
        }
        maximum-bit-rate-downlink {
          mbr-downlink;
          reject;
          upgrade;
        }
        maximum-bit-rate-uplink {
          mbr-uplink;
```


Copyright © 2012, Juniper Networks, Inc.

```
            reject;
            upgrade;
          }
          qci qci-value {
            maximum-bit-rate-downlink {
              mbr-downlink;
              reject;
              upgrade;
            }
            maximum-bit-rate-uplink {
              mbr-uplink;
              reject;
              upgrade;
            }
          }
        }
        policer-action {
          gbr-bearer {
            exceed-action (drop | transmit);
            violate-action (set-loss-priority-high | transmit);
          }
          non-gbr-bearer {
            violate-action (set-loss-priority-high | transmit);
          }
        }
      }
    }
    gbr-bandwidth-pools {
      name {
        downgrade-gtp-v1-gbr-bearers;
        maximum-bandwidth maximum-bandwidth;
      }
    }
    resource-threshold-profiles {
      name {
        bearers-load {
          high {
            percentage percentage;
            priority-level priority-level;
          }
          low {
            percentage percentage;
            priority-level priority-level;
          }
        }
        cpu {
          high {
            percentage percentage;
            priority-level priority-level;
          }
          low {
            percentage percentage;
            priority-level priority-level;
          }
        }
        description description;
```

```
            memory {
              high {
                percentage percentage;
                priority-level priority-level;
              }
              low {
                percentage percentage;
                priority-level priority-level;
              }
            }
          }
        }
      }
```

Hierarchy Level [edit unified-edge]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the set of parameters for the class of service (CoS) call admission control (CAC).

Call admission control on the broadband gateway ensures that the required network resources are available for real-time data traffic such as voice and video. Call admission control maintains information about all resources available on the broadband gateway and resources that have been allocated to bearers.

The remaining statements are explained separately.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- [edit unified-edge cos-cac] Hierarchy Level on page 87
- Configuring QoS on the Broadband Gateway Overview on page 18
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- Quality of Service Overview on page 3

 Copyright © 2012, Juniper Networks, Inc.

cos-policy-profile (Local Policies)

Syntax cos-policy-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the class-of-service (CoS) policy profile for home subscribers. You configure a CoS policy profile to define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters.

Options ***profile-name***—Name of the CoS policy profile name.

NOTE: **The CoS policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac cos-policy-profiles] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **cos-policy-profiles on page 102**
- **local-policies (QoS) on page 126**

cos-policy-profiles

Syntax

```
cos-policy-profiles {
  name {
    aggregated-qos-control {
      maximum-bit-rate-downlink {
        mbr-downlink;
        reject;
        upgrade;
      }
      maximum-bit-rate-uplink {
        mbr-uplink;
        reject;
        upgrade;
      }
    }
    allocation-retention-priority {
      priority-value;
      reject;
    }
    default-bearer-qci {
      qci-value;
      reject;
      upgrade;
    }
    description description;
    pdp-qos-control {
      guaranteed-bit-rate-downlink {
        gbr-downlink;
        reject;
        upgrade;
      }
      guaranteed-bit-rate-uplink {
        gbr-uplink;
        reject;
        upgrade;
      }
      maximum-bit-rate-downlink {
        mbr-downlink;
        reject;
        upgrade;
      }
      maximum-bit-rate-uplink {
        mbr-uplink;
        reject;
        upgrade;
      }
      qci qci-value {
        maximum-bit-rate-downlink {
          mbr-downlink;
          reject;
          upgrade;
        }
        maximum-bit-rate-uplink {
```


Copyright © 2012, Juniper Networks, Inc.

```
                mbr-uplink;
                reject;
                upgrade;
            }
        }
    }
    policer-action {
        gbr-bearer {
            exceed-action (drop | transmit);
            violate-action (set-loss-priority-high | transmit);
        }
        non-gbr-bearer {
            violate-action (set-loss-priority-high | transmit);
        }
    }
  }
}
```

Hierarchy Level [edit unified-edge cos-cac]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Define the policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters. For a 3G network, the CoS policy profile defines the highest traffic class that can be accepted at an APN or gateway level, the maximum bit rate and guaranteed bit rate for bearers, and the allocation and retention priority. For a 4G network, the CoS policy profile defines the highest QoS Class Identifier (QCI) value that can be accepted at the APN level or gateway level, the aggregated maximum bit rate (AMBR) for default bearers, and the priority level.

Options *name*—Name of the CoS policy profile.

Range: Up to 64 characters

The remaining statements are explained separately.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- [edit unified-edge cos-cac] Hierarchy Level on page 87
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- Configuring QoS on the Broadband Gateway Overview on page 18

cpu (Resource Threshold Profiles)

Syntax

```
cpu {
  high {
    percentage percentage;
    priority-level priority-level;
  }
  low {
    percentage percentage;
    priority-level priority-level;
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac resource-threshold-profiles *name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the lower and upper limits for the CPU load (at the session PIC level) in the resource threshold profile. The CPU load specifies a precise level of admission control when the CPU load for a session PIC reaches a configured lower or upper threshold.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Resource Thresholds for 3G and 4G Networks on page 26
- **resource-threshold-profiles (QoS) on page 148**

Copyright © 2012, Juniper Networks, Inc.

default-bearer-qci (CoS Policy Profiles)

Syntax

```
default-bearer-qci {
   qci-value;
   reject;
   upgrade;
}
```

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name*]

Description Configure the QoS Class Identifier (QCI) for default bearers. Table 9 on page 105 explains the different configuration scenarios for this statement.

Table 9: default-bearer-qci Configuration Scenarios

Scenario	Behavior
Only ***qci-value*** configured	Create PDP Context Requests and Create Session Requests with QCI values numerically greater than or equal to the configured QCI value are accepted, and requests numerically lower than the configured QCI are downgraded to the configured QCI.
qci-value and **reject** configured	Create PDP Context Requests and Create Session Requests with QCI values numerically greater than or equal to the configured QCI value are accepted, and requests numerically lower than the configured QCI are rejected.
qci-value and **upgrade** configured	Create PDP Context Requests and Create Session Requests with QCI values numerically greater than the configured QCI value are upgraded to the configured QCI, and requests numerically lower than configured QCI are downgraded to the configured QCI.
qci-value, **reject** and **upgrade** configured	Create PDP Context Requests and Create Session Requests with QCI values numerically greater than the configured QCI value are upgraded to the configured QCI, and requests numerically lower than configured QCI are rejected.

Default If this statement is not included, then the broadband gateway accepts the QCI value in the Create PDP Context Request or Create Session Request message.

Options ***qci-value***—Specify the QCI value for the default bearer.

NOTE: **If you configure the default-bearer-qci statement, then you must specify the QCI value.**

Range: 5 through 9

reject—Specify that default bearers with QCI value numerically lower than the specified QCI are rejected.

upgrade—Specify that the configured QCI value is enforced for the default bearers.

Required Privilege Level
unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation
- Call Admission Control Overview on page 10
- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring QoS on the Broadband Gateway Overview on page 18
- **cos-policy-profiles on page 102**
- Quality of Service Overview on page 3

description (Class of Service)

Syntax
description *description*;

Hierarchy Level
[edit unified-edge cos-cac classifier-profiles *name*],
[edit unified-edge cos-cac cos-policy-profiles *name*],
[edit unified-edge cos-cac resource-threshold-profiles *name*],
[edit unified-edge local-policies *name*],

Description
Enter a description for the classifier profile, QoS policy profile, resource threshold profile, or the local policy.

Options
description—Description.

Required Privilege Level
unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation
- **classifier-profiles on page 95**
- **cos-policy-profiles on page 102**
- **local-policies (QoS) on page 126**
- **resource-threshold-profiles (QoS) on page 148**

Copyright © 2012, Juniper Networks, Inc.

downgrade-gtp-v1-gbr-bearers (Guaranteed Bit Rate Bandwidth Pools)

Syntax downgrade-gtp-v1-gbr-bearers;

Hierarchy Level [edit unified-edge cos-cac bandwidth-pools *name* gbr-bandwidth-pools *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Specify that the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) should downgrade the traffic class of GTPv1 guaranteed bit rate (GBR) bearers to background traffic class. When the bandwidth requested by the bearers is greater than available maximum bandwidth in the pool, then the gateway downgrades the traffic class of GTPv1 GBR bearers.

Default If you do not include this statement, then Create or Modify Bearer Requests are rejected when the bandwidth requested by the bearers is greater than the available maximum bandwidth in the pool.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Bandwidth Pools on page 24
- Configuring QoS on the Broadband Gateway Overview on page 18
- **gbr-bandwidth-pools (Class of Service) on page 115**

dl-bandwidth-pool (Local Policies)

Syntax dl-bandwidth-pool *pool-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the bandwidth pool for limiting the downlink bandwidth usage at the gateway or at the APN level.

Options ***pool-name***—Name of the downlink bandwidth pool.

NOTE: **The bandwidth pool must be previously configured on the broadband gateway at the [edit unified-edge cos-cac gbr-bandwidth-pools] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **gbr-bandwidth-pools (Class of Service) on page 115**
- **local-policies (QoS) on page 126**

 Copyright © 2012, Juniper Networks, Inc.

dscp-ipv6 (Egress Rewrite Rules)

Syntax

```
[dscp-ipv6 (rewrite-rule-name | default)] {
  protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
}
```

Hierarchy Level

[edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the DiffServ code point (DSCP) IPv6 egress rewrite rule for the mobile interface. The rewrite rule changes the DSCP IPv6 value in the IP header of downstream (Gi to Gn or SGi to S5 traffic) subscriber packets. The rewrite rule can be applied to the inner IP header, the outer IP header, or both inner and outer IP header.

Options

rewrite-rule-name—Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules dscp-ipv6] hierarchy level.**

default—Apply the default rewrite rule.

The remaining statement is explained separately

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Egress Rewrite Rules to Mobile Interfaces on page 47
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **rewrite-rules (Egress) on page 150**

dscp-ipv6 (Ingress Rewrite Rules)

Syntax [dscp-ipv6 (*rewrite-rule-name* | default)];

Hierarchy Level [edit class-of-service interfaces mif unit *interface-unit-number* ingress-rewrite-rules]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the DiffServ code point (DSCP) IPv6 ingress rewrite rule for the mobile interface. The rewrite rule changes the DSCP IPv6 value only in the outer IP header of upstream (Gn to Gi or S5 to SGi traffic) subscriber packets.

Options ***rewrite-rule-name***——Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules dscp-ipv6] hierarchy level.**

default—Apply the default rewrite rule.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **ingress-rewrite-rules on page 124**

 Copyright © 2012, Juniper Networks, Inc.

dscp (Egress Rewrite Rules)

Syntax

```
[dscp (rewrite-rule-name | default)] {
  protocol [(gtp-inet-both | gtp-inet-outer)];
}
```

Hierarchy Level

[edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the DiffServ code point (DSCP) egress rewrite rule for the mobile interface. The rewrite rule changes the DSCP value in the IP header of downstream (Gi to Gn or SGi to S5 traffic) subscriber packets. The rewrite rule can be applied to the inner IP header, the outer IP header, or both the inner and outer IP headers.

Options

rewrite-rule-name—Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules dscp] hierarchy level.**

default—Apply the default rewrite rule.

The remaining statement is explained separately

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Egress Rewrite Rules to Mobile Interfaces on page 47
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **rewrite-rules (Egress) on page 150**

dscp (Ingress Rewrite Rules)

Syntax [dscp (*rewrite-rule-name* | default)];

Hierarchy Level [edit class-of-service interfaces mif unit *interface-unit-number* ingress-rewrite-rules]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the DiffServ code point (DSCP) ingress rewrite rule for the mobile interface. The rewrite rule changes the DSCP value only in the outer IP header of upstream (Gn to Gi or S5 to SGi traffic) subscriber packets.

Options ***rewrite-rule-name***—Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules dscp] hierarchy level.**

default—Apply the default rewrite rule.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **ingress-rewrite-rules on page 124**

 Copyright © 2012, Juniper Networks, Inc.

exceed-action (QoS Policer Action)

Syntax exceed-action (drop | transmit);

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* policer-action gbr-bearer]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the policer action that is applied when the subscriber traffic exceeds the configured guaranteed bit rate (GBR) for GBR PDP contexts. The policer action controls packet behavior by setting the packet loss priority (PLP) to high, transmitting the packet without changing the PLP, or by dropping the packet.

Default If you do not include this statement, then the default action is to set the PLP to high.

Options **drop**—Drop the packet.

transmit—Transmit the packet without changing the PLP.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- gbr-bearer (QoS Policer Action) on page 116

forwarding-class (QoS Class Identifier)

Syntax forwarding-class *class-name*;

Hierarchy Level [edit unified-edge cos-cac classifier-profiles *name* qos-class-identifier]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the forwarding class associated with the QoS Class Identifier (QCI) for the QoS classifier profile.

NOTE: **If you specify a QCI value, you must specify the forwarding class.**

Options ***class-name***—Specify the forwarding class name; for example, assured-forwarding or best-effort.

Range: Up to 64 characters

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring QoS on the Broadband Gateway Overview on page 18
- **qos-class-identifier (Classifier Profiles) on page 147**
- Quality of Service Overview on page 3

 Copyright © 2012, Juniper Networks, Inc.

gbr-bandwidth-pools (Class of Service)

Syntax

```
gbr-bandwidth-pools {
  name {
    downgrade-gtp-v1-gbr-bearers;
    maximum-bandwidth maximum-bandwidth;
  }
}
```

Hierarchy Level [edit unified-edge cos-cac]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the bandwidth pools for guaranteed bit rate (GBR) PDP contexts class-of-service call admission control (CoS-CAC) on the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).

A GBR bandwidth pool limits the number of GBR packet data protocol (PDP) contexts that can be supported on the GGSN or P-GW, at the gateway level or the access point name (APN) level. Configuring a GBR bandwidth pool provides sufficient bandwidth for PDP contexts to be created or modified. Call admission control (CAC) uses the GBR bandwidth pools to negotiate and reserve bandwidth for PDP contexts with a guaranteed bit rate.

Options *name*—Name of the GBR bandwidth pool that can be attached, via the local policy, to the APN or gateway.

Range: Up to 64 characters

The remaining statements are explained separately.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Bandwidth Pools on page 24
- Configuring QoS on the Broadband Gateway Overview on page 18
- **cos-cac on page 98**

gbr-bearer (QoS Policer Action)

Syntax

```
gbr-bearer {
  exceed-action (drop | transmit);
  violate-action (set-loss-priority-high | transmit);
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name* policer-action]

Release Information

Statement introduced in Junos OS Mobility Release 11.4W.

Description

Specify the policer action that is applied when the subscriber traffic exceeds the GBR or MBR for GBR PDP contexts. You can specify the policer action for the following:

- When traffic exceeds the configured GBR for PDP contexts.
- When the traffic exceeds the configured maximum bit rate (MBR) in a 3G network.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- policer-action (CoS Policy Profiles) on page 143

Copyright © 2012, Juniper Networks, Inc.

guaranteed-bit-rate-downlink (PDP QoS Control)

Syntax

```
guaranteed-bit-rate-downlink {
  gbr-downlink;
  reject;
  upgrade;
}
```

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]

Description Configure the guaranteed bit rate (GBR) for downlink traffic for Packet Data Protocol (PDP) contexts (3G).

The GBR defines the minimum bit rate that is expected to be available to the PDP context when required. This means that a certain amount of bandwidth is always reserved for the PDP context, regardless of whether the GBR is used or not. Therefore, a PDP context with a GBR always takes up resources even when there is no traffic.

Table 10 on page 117 explains the different configuration scenarios for this statement.

Table 10: guaranteed-bit-rate-downlink Configuration Scenarios

Scenario	Behavior
Only ***gbr-downlink*** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are accepted, and requests greater than the configured GBR are downgraded to the configured GBR and accepted.
gbr-downlink and **reject** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are accepted, and requests greater than the configured GBR are rejected.
gbr-downlink and **upgrade** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are upgraded to the configured GBR, and requests greater than the configured GBR are downgraded to the configured GBR and accepted.
gbr-downlink, **reject** and **upgrade** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are upgraded to the configured GBR, and requests greater than the configured GBR are rejected.

Options ***gbr-downlink***—Specify the GBR in the downlink direction.

NOTE: **If you configure the guaranteed-bit-rate-downlink statement, then you must specify the GBR value in the downlink direction.**

Range: 1 through 256,000 kbps

reject—Specify that PDP contexts higher than the specified downlink GBR are rejected.

upgrade—Specify that the configured GBR value is applied to the PDP context.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **pdp-qos-control (CoS Policy Profiles) on page 142**

Copyright © 2012, Juniper Networks, Inc.

guaranteed-bit-rate-uplink (PDP QoS Control)

Syntax

```
guaranteed-bit-rate-uplink {
  gbr-uplink;
  reject;
  upgrade;
}
```

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]

Description Configure the guaranteed bit rate (GBR) for uplink traffic for Packet Data Protocol (PDP) contexts (3G).

The GBR defines the minimum bit rate that is expected to be available to the PDP context when required. This means that a certain amount of bandwidth is always reserved for the PDP context, regardless of whether the GBR is used or not. Therefore, a PDP context with a GBR always takes up resources even when there is no traffic.

Table 11 on page 119 explains the different configuration scenarios for this statement.

Table 11: guaranteed-bit-rate-downlink Configuration Scenarios

Scenario	Behavior
Only ***gbr-uplink*** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are accepted, and requests greater than the configured GBR are downgraded to the configured GBR and accepted.
gbr-uplink and **reject** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are accepted, and requests greater than the configured GBR are rejected.
gbr-uplink and **upgrade** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are upgraded to the configured GBR, and requests greater than the configured GBR are downgraded to the configured GBR and accepted.
gbr-uplink, **reject** and **upgrade** configured	Create PDP Context Requests with GBR lesser than or equal to the configured GBR value are upgraded to the configured GBR, and requests greater than the configured GBR are rejected.

Options ***gbr-uplink***—Specify the GBR in the uplink direction.

NOTE: **If you configure the guaranteed-bit-rate-uplink statement, then you must specify the GBR value in the uplink direction.**

Range: 1 through 256,000 kbps

reject—Specify that PDP contexts higher than the specified uplink GBR are rejected.

upgrade—Specify that PDP contexts higher than the specified uplink GBR are upgraded.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **pdp-qos-control (CoS Policy Profiles) on page 142**

Copyright © 2012, Juniper Networks, Inc.

high (Resource Threshold Profiles)

Syntax

```
high {
   percentage percentage;
   priority-level priority-level;
}
```

Hierarchy Level

[edit unified-edge cos-cac resource-threshold-profiles *name* bearers-load],
[edit unified-edge cos-cac resource-threshold-profiles *name* cpu],
[edit unified-edge cos-cac resource-threshold-profiles *name* memory]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the upper threshold limit for the bearer load, CPU load, or memory load. You can specify the upper threshold limit as a percentage of the maximum threshold.

When the bearer load, CPU load, or memory load exceeds the corresponding specified threshold percentage, then only Create Session requests or Create Bearer (Serving Gateway only) requests equal to or higher than the specified priority level are accepted.

Default

If you do not include this statement, then the following defaults apply:

- Upper limit of 85 percent and priority level of 5 for bearer load or CPU load
- Upper limit of 90 percent and priority level of 5 for memory load

Options

percentage *percentage*—Upper limit (in percent) of the maximum resource threshold.

NOTE: **If you include the high statement, then the upper limit must be specified.**

Range: 1 through 100

priority-level *priority-level*—Upper limit bearer priority level.

Range: 1 through 15

Default: 5

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- bearers-load (Resource Threshold Profiles) on page 93
- cpu (Resource Threshold Profiles) on page 104
- memory (Resource Threshold Profiles) on page 139

Copyright © 2012, Juniper Networks, Inc.

inet-precedence (Egress Rewrite Rules)

Syntax

```
[inet-precedence (rewrite-rule-name | default)] {
  protocol [(gtp-inet-both | gtp-inet-outer)];
}
```

Hierarchy Level

[edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the IP precedence egress rewrite rule for the mobile interface. The rewrite rule changes the IP precedence value in the IP header of downstream (Gi to Gn or SGi to S5 traffic) subscriber packets. The rewrite rule can be applied to the inner IP header, the outer IP header, or both inner and outer IP header.

Options

rewrite-rule-name—Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules inet-precedence] hierarchy level.**

default—Apply the default rewrite rule.

The remaining statement is explained separately

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Egress Rewrite Rules to Mobile Interfaces on page 47
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **rewrite-rules (Egress) on page 150**

Copyright © 2012, Juniper Networks, Inc.

inet-precedence (Ingress Rewrite Rules)

Syntax [inet-precedence (*rewrite-rule-name* | default)];

Hierarchy Level [edit class-of-service interfaces mif unit *interface-unit-number* ingress-rewrite-rules]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the IP precedence ingress rewrite rule for the mobile interface. The rewrite rule changes the IP precedence value only in the outer IP header of upstream (Gn to Gi or S5 to SGi traffic) subscriber packets .

Options ***rewrite-rule-name***—Name of the rewrite rule.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules inet-precedence] hierarchy level.**

default—Apply the default rewrite rule.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **ingress-rewrite-rules on page 124**

ingress-rewrite-rules

Syntax

```
ingress-rewrite-rules {
   [dscp (rewrite-rule-name | default)];
   [dscp-ipv6 (rewrite-rule-name | default)];
   [inet-precedence (rewrite-rule-name | default)];
   }
}
```

Hierarchy Level

[edit class-of-service interfaces mif unit *logical-unit-number*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Apply a previously configured ingress rewrite rule to the mobile interface. The rewrite rule is applied to upstream (Gn to Gi or S5 to SGi traffic) subscriber packets at the mobile interface and rewrites only into the outer IP header of the subscriber packet.

NOTE: **The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules] hierarchy level.**

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- **unit (Mobile Interface for Class of Service) on page 154**

Copyright © 2012, Juniper Networks, Inc.

interfaces (Class of Service)

Syntax

```
interfaces {
  mif. number {
    unit logical-unit-number {
      ingress-rewrite-rules {
        [dscp (rewrite-rule-name | default)];
        [dscp-ipv6 (rewrite-rule-name | default)];
        [inet-precedence (rewrite-rule-name | default)];
        }
      }
      rewrite-rules {
        [dscp (rewrite-rule-name | default)] {
          protocol [(gtp-inet-both | gtp-inet-outer)];
        }
        [dscp-ipv6 (rewrite-rule-name | default)] {
          protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
        }
        [inet-precedence (rewrite-rule-name | default)] {
          protocol [(gtp-inet-both | gtp-inet-outer)];
        }
      }
    }
  }
}
```

Hierarchy Level

[edit class-of-service]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the mobile interfaces to set the CoS values for upstream and downstream subscriber packets.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- **class-of-service (MobileNext Broadband Gateway) on page 96**

local-policies (QoS)

Syntax

```
local-policies {
  policy-name {
    cos-policy-profile name;
    classifier-profile name;
    description description;
    dl-bandwidth-pool name;
    resource-threshold-profile name;
    roamer-classifier-profile name;
    roamer-cos-policy-profile name;
    ul-bandwidth-pool name;
    visitor-classifier-profile  name;
    visitor-cos-policy-profile name;
  }
}
```

Hierarchy Level

[edit unified-edge]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Configure the local policy, which defines the quality of service (QoS) to be applied at the gateway level or at the access point name (APN) level for the broadband gateway. A local policy applied at the APN level takes priority over a local policy applied at the gateway level. A local policy defines traffic by classes and specifies the different levels of throughput and packet loss when congestion occurs.

The remaining statements are explained separately.

Options

policy-name—Name of the local policy.

Range: Up to 64 characters

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- [edit unified-edge local-policies] Hierarchy Level on page 89
- Configuring QoS on the Broadband Gateway Overview on page 18

Copyright © 2012, Juniper Networks, Inc.

local-policy-profile (Broadband Gateway)

Syntax local-policy-profile *local-policy-profile*;

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name*],
[edit unified-edge gateways sgw *gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the **[edit unified-edge gateways sgw *name*]** hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Specify a local policy profile for the broadband gateway.

- For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), the local policy profile is a combination of the quality-of-service (QoS) policy (**cos-policy-profile**), the classifier policy (**classifier-profile**), and the resource threshold policy (**resource-threshold-policy**).
- For the broadband gateway configured as a Serving Gateway (S-GW), the local policy profile is a combination of the classifier policy (**classifier-profile**) and the resource threshold policy (**resource-threshold-policy**).

NOTE: **The local policy profile must already be configured at the [edit unified-edge] hierarchy level.**

Options ***local-policy-profile***—Name of the local policy profile.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation
- local-policy-profile (APN) (P-GW only)

loss-priority (QoS Class Identifier)

Syntax loss-priority (high | low);

Hierarchy Level [edit unified-edge cos-cac classifier-profiles *name* qos-class-identifier]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the packet loss priority associated with the QoS Class Identifier (QCI) for the QoS classifier profile.

NOTE: **If you specify a QCI value, you must specify the packet loss priority.**

Options

high—Set the packet loss priority to high, which means that means that packets are more susceptible to being dropped.

low—Set the packet loss priority to low, which means that means that packets are less susceptible to being dropped.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring QoS on the Broadband Gateway Overview on page 18
- **qos-class-identifier (Classifier Profiles) on page 147**
- Quality of Service Overview on page 3

 Copyright © 2012, Juniper Networks, Inc.

low (Resource Threshold Profiles)

Syntax

```
low {
   percentage percentage;
   priority-level priority-level;
}
```

Hierarchy Level

[edit unified-edge cos-cac resource-threshold-profiles *name* bearers-load],
[edit unified-edge cos-cac resource-threshold-profiles *name* cpu],
[edit unified-edge cos-cac resource-threshold-profiles *name* memory]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the lower threshold limit for the bearer load, CPU load, or memory load. You can specify the lower threshold limit as a the percentage of the maximum threshold.

When the bearer load, CPU load, or memory load exceeds the corresponding specified threshold percentage, then only Create Session requests or Create Bearer (Serving Gateway only) requests equal to or higher than the specified priority level are accepted.

Default

If you do not include this statement, then the following defaults apply:

- Lower limit of 70 percent and priority level of 10 for bearer load or CPU load
- Lower limit of 80 percent and priority level of 10 for memory load

Options

percentage *percentage*—Lower limit (in percent) of the maximum resource threshold.

NOTE: **If you include the low statement, then the lower limit must be specified.**

Range: 1 through 100

priority-level *priority-level*—Lower limit bearer priority level.

Range: 1 through 15

Default: 10

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- bearers-load (Resource Threshold Profiles) on page 93
- cpu (Resource Threshold Profiles) on page 104
- memory (Resource Threshold Profiles) on page 139

Copyright © 2012, Juniper Networks, Inc.

maximum-bandwidth (Guaranteed Bit Rate Bandwidth Pools)

Syntax maximum-bandwidth *maximum-bandwidth*;

Hierarchy Level [edit unified-edge cos-cac bandwidth-pools *name* gbr-bandwidth-pools *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Specify the total maximum bandwidth for the guaranteed bit rate (GBR) bandwidth pool on the broadband gateway.

NOTE: **If you configure a GBR bandwidth pool, then you must configure the total maximum bandwidth.**

Options ***maximum-bandwidth***—Total maximum bandwidth, in megabits per second (Mbps), of the maximum bandwidth pool.

Range: 50,000 through 500,000 Mbps

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Bandwidth Pools on page 24
- Configuring QoS on the Broadband Gateway Overview on page 18
- **gbr-bandwidth-pools (Class of Service) on page 115**

 Copyright © 2012, Juniper Networks, Inc.

maximum-bearers (Broadband Gateway)

Syntax maximum-bearers *maximum-bearers*;

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name*],
[edit unified-edge gateways sgw *gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the **[edit unified-edge gateways sgw *name*]** hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), configure the maximum number of Evolved Packet System (EPS) bearers or packet data protocol (PDP) contexts allowed.

For the broadband gateway configured as a Serving Gateway (S-GW), configure the maximum number of EPS bearers allowed.

Options ***maximum-bearers***—Maximum number of bearers for the broadband gateway.

Range: 100,000 through 12,000,000 bearers

Default: 12,000,000 bearers

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring the Maximum Number of Bearers on page 23
- maximum-bearers (APN) (P-GW only)

maximum-bit-rate-downlink (Aggregated QoS Control)

Syntax

```
maximum-bit-rate-downlink {
  mbr-downlink;
  reject;
  upgrade;
}
```

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* aggregated-qos-control]

Description Configure the aggregate maximum bit rate (AMBR) for downlink traffic.

The AMBR specifies the total maximum bit rate (MBR) for all non-GBR bearers (4G) associated with a specific gateway or access point name (APN). Table 12 on page 132 explains the different configuration scenarios for this statement.

Table 12: maximum-bit-rate-downlink Configuration Scenarios

Scenario	Behavior
Only ***mbr-downlink*** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are accepted, and requests greater than the configured AMBR are downgraded to the configured AMBR and accepted.
mbr-downlink and **reject** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are accepted, and requests greater than the configured AMBR are rejected.
mbr-downlink and **upgrade** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are upgraded to the configured AMBR, and requests greater than the configured AMBR are downgraded to the configured AMBR and accepted.
mbr-downlink, **reject** and **upgrade** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are upgraded to the configured AMBR, and requests greater than the configured AMBR are rejected.

Options ***mbr-downlink***—Specify the MBR in the downlink direction.

NOTE: **If you configure the maximum-bit-rate-downlink statement, then you must specify the MBR value in the downlink direction.**

Range: 1 through 256,000 kbps

reject—Specify that bearers higher than the specified downlink MBR are rejected.

upgrade—Specify that the configured MBR value is applied to the bearer.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

 Copyright © 2012, Juniper Networks, Inc.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **aggregated-qos-control (CoS Policy Profiles) on page 91**

maximum-bit-rate-downlink (PDP QoS Control)

Syntax

```
maximum-bit-rate-downlink {
  mbr-downlink;
  reject;
  upgrade;
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control],
[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control qci *qci-value*]

Description

Configure the maximum bit rate (MBR) for downlink traffic for Packet Data Protocol (PDP) contexts (3G).

The MBR defines the maximum bit rate that is expected to be available to the PDP context when required. The MBR limits the bit rate that is provided to a PDP context.

Table 13 on page 134 explains the different configuration scenarios for this statement.

Table 13: maximum-bit-rate-downlink Configuration Scenarios

Scenario	Behavior
Only ***mbr-downlink*** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are accepted, and requests greater than the configured MBR are downgraded to the configured MBR and accepted.
mbr-downlink and **reject** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are accepted, and requests greater than the configured MBR are rejected.
mbr-downlink and **upgrade** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are upgraded to the configured MBR, and requests greater than the configured MBR are downgraded to the configured MBR and accepted.
mbr-downlink, **reject** and **upgrade** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are upgraded to the configured MBR, and requests greater than the configured MBR are rejected.

NOTE: The configuration at the **[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control qci *qci-value*]** hierarchy level takes precedence over the configuration at the **[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]** hierarchy level.

Options

mbr-downlink—Specify the MBR in the downlink direction.

NOTE: If you configure the **maximum-bit-rate-downlink** statement, then you must specify the MBR value in the downlink direction.

Copyright © 2012, Juniper Networks, Inc.

Range: 1 through 256,000 kbps

reject—Specify that PDP contexts higher than the specified downlink MBR are rejected.

upgrade—Specify that the configured MBR value is applied to PDP contexts.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **pdp-qos-control (CoS Policy Profiles) on page 142**
- **qci (PDP QoS Control) on page 146**

maximum-bit-rate-uplink (Aggregated QoS Control)

Syntax

```
maximum-bit-rate-uplink {
  mbr-uplink;
  reject;
  upgrade;
}
```

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* aggregated-qos-control]

Description Configure the aggregate maximum bit rate (AMBR) for uplink traffic.

The AMBR specifies the total maximum bit rate (MBR) for all non-GBR bearers (4G) associated with a specific gateway or access point name (APN). Table 14 on page 136 explains the different configuration scenarios for this statement.

Table 14: maximum-bit-rate-uplink Configuration Scenarios

Scenario	Behavior
Only ***mbr-uplink*** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are accepted, and requests greater than the configured AMBR are downgraded to the configured AMBR and accepted.
mbr-uplink and **reject** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are accepted, and requests greater than the configured AMBR are rejected.
mbr-uplink and **upgrade** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are upgraded to the configured AMBR, and requests greater than the configured AMBR are downgraded to the configured AMBR and accepted.
mbr-uplink, **reject** and **upgrade** configured	Create Session Requests with AMBR lesser than or equal to the configured AMBR value are upgraded to the configured AMBR, and requests greater than the configured AMBR are rejected.

Options ***mbr-uplink***—Specify the MBR in the uplink direction.

NOTE: **If you configure the maximum-bit-rate-uplink statement, then you must specify the MBR value in the uplink direction.**

Range: 1 through 256,000 kbps

reject—Specify that bearers higher than the specified uplink MBR are rejected.

upgrade—Specify that the configured MBR value is applied to the bearer.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

 Copyright © 2012, Juniper Networks, Inc.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **aggregated-qos-control (CoS Policy Profiles) on page 91**

maximum-bit-rate-uplink (PDP QoS Control)

Syntax

```
maximum-bit-rate-uplink {
  mbr-uplink;
  reject;
  upgrade;
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control],
[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control qci *qci-value*]

Description

Configure the maximum bit rate (MBR) for uplink traffic for Packet Data Protocol (PDP) contexts.

The MBR defines the maximum bit rate that is expected to be available to the PDP context when required. The MBR limits the bit rate that is provided to a PDP context.

Table 15 on page 138 explains the different configuration scenarios for this statement.

Table 15: maximum-bit-rate-uplink Configuration Scenarios

Scenario	Behavior
Only ***mbr-uplink*** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are accepted, and requests greater than the configured MBR are downgraded to the configured MBR and accepted.
mbr-uplink and **reject** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are accepted, and requests greater than the configured MBR are rejected.
mbr-uplink and **upgrade** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are upgraded to the configured MBR, and requests greater than the configured MBR are downgraded to the configured MBR and accepted.
mbr-uplink, **reject** and **upgrade** configured	Create PDP Context Requests with MBR lesser than or equal to the configured MBR value are upgraded to the configured MBR, and requests greater than the configured MBR are rejected.

NOTE: The configuration at the **[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control qci *qci-value*]** hierarchy level takes precedence over the configuration at the **[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]** hierarchy level.

Options

mbr-uplink—Specify the MBR in the uplink direction.

NOTE: If you configure the **maximum-bit-rate-uplink** statement, then you must specify the MBR value in the uplink direction.

Copyright © 2012, Juniper Networks, Inc.

Range: 1 through 256,000 kbps

reject—Specify that PDP contexts higher than the specified uplink MBR are rejected.

upgrade—Specify that the configured MBR value is applied to PDP contexts.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **pdp-qos-control (CoS Policy Profiles) on page 142**
- **qci (PDP QoS Control) on page 146**

memory (Resource Threshold Profiles)

Syntax

```
memory {
  high {
    percentage percentage;
    priority-level priority-level;
  }
  low {
    percentage percentage;
    priority-level priority-level;
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac resource-threshold-profiles *name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Specify the lower and upper limits for the memory load or utilization (at the session PIC level) in the resource threshold profile. The memory load specifies a precise level of admission control when the memory load or utilization for a session PIC reaches a configured lower or upper threshold.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Resource Thresholds for 3G and 4G Networks on page 26
- **resource-threshold-profiles (QoS) on page 148**

mif (Class of Service)

Syntax

```
mif {
  unit logical-unit-number {
    ingress-rewrite-rules {
      [dscp (rewrite-rule-name | default)];
      [dscp-ipv6 (rewrite-rule-name | default)];
      [inet-precedence (rewrite-rule-name | default)];
      }
    }
    rewrite-rules {
      [dscp (rewrite-rule-name | default)] {
        protocol [(gtp-inet-both | gtp-inet-outer)];
      }
      [dscp-ipv6 (rewrite-rule-name | default)] {
        protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
      }
      [inet-precedence (rewrite-rule-name | default)] {
        protocol [(gtp-inet-both | gtp-inet-outer)];
      }
    }
  }
}
```

Hierarchy Level

[edit class-of-service interfaces]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Configure the mobile interface for applying ingress and egress rewrite rules to upstream and downstream subscriber packets.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- interfaces (Class of Service) on page 125

Copyright © 2012, Juniper Networks, Inc.

non-gbr-bearer (QoS Policer Action)

Syntax

```
non-gbr-bearer {
  violate-action (set-loss-priority-high | transmit);
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name* policer-action]

Release Information

Statement introduced in Junos OS Mobility Release 11.4W.

Description

Specify the policer action that is applied when the subscriber traffic exceeds the MBR rate for non-GBR PDP contexts (3G) or AMBR for non-GBR bearers (4G). You can specify the policer action to take when the traffic exceeds the configured maximum bit rate (MBR) in a 3G network, or when the traffic the exceeds the configured aggregate maximum bit rate (AMBR) in a 4G network.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- policer-action (CoS Policy Profiles) on page 143

pdp-qos-control (CoS Policy Profiles)

Syntax

```
pdp-qos-control {
  guaranteed-bit-rate-downlink {
    gbr-downlink;
    reject;
    upgrade;
  }
  guaranteed-bit-rate-uplink {
    gbr-uplink;
    reject;
    upgrade;
  }
  maximum-bit-rate-downlink {
    mbr-downlink;
    reject;
    upgrade;
  }
  maximum-bit-rate-uplink {
    mbr-uplink;
    reject;
    upgrade;
  }
  qci qci-value {
    maximum-bit-rate-downlink {
      mbr-downlink;
      reject;
      upgrade;
    }
    maximum-bit-rate-uplink {
      mbr-uplink;
      reject;
      upgrade;
    }
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name*]

Description

Configure the QoS parameters for Packet Data Protocol (PDP) contexts (3G). You can configure the guaranteed bit rate (GBR) and maximum bit rate (MBR) for both uplink and downlink traffic applicable to all QCI values. You can also configure the MBR for a specific QCI value, which takes precedence over the configuration at the higher (**[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]**) hierarchy level.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Configuring a CoS Policy Profile for 3G and 4G Networks on page 37

Copyright © 2012, Juniper Networks, Inc.

- Configuring a CoS Policy Profile for a 3G Network on page 32
- Configuring a CoS Policy Profile for a 4G Network on page 29
- Quality of Service Overview on page 3
- **cos-policy-profiles on page 102**

policer-action (CoS Policy Profiles)

Syntax

```
policer-action {
  gbr-bearer {
    exceed-action (drop | transmit);
    violate-action (set-loss-priority-high | transmit);
  }
  non-gbr-bearer {
    violate-action (set-loss-priority-high | transmit);
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name*]

Description

Configure the policer actions that are applied when the subscriber traffic exceeds the maximum or guaranteed bit rates. The broadband gateway uses a two-rate policer to enforce bandwidth rates for subscriber traffic.

NOTE: **This configuration is applicable only for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).**

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Policing Subscriber Traffic on the Broadband Gateway Overview on page 13
- **cos-policy-profiles on page 102**

preemption (GGSN or P-GW)

Syntax

```
preemption {
   enable;
   gtpv1-pci-disable;
   gtpv1-pvi-disable;
}
```

Hierarchy Level

[edit unified-edge gateways ggsn-pgw *gateway-name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Configure whether preemption should be enabled or disabled on the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW). Preemption aids in call admission control and enables the gateway to accommodate higher priority bearers over the lower priority ones, based on the Preemption Capability Indicator (PCI) and Preemption Vulnerability Indicator (PVI).

The PCI value defines whether a bearer with a lower priority level (PL) should be dropped to free the resources required. The PVI value defines whether a bearer is liable to be dropped in favor of a preemption-capable bearer with a higher priority level value.

Preemption can be applied based on bearer load or memory load, both of which can be configured at the **[edit unified-edge cos-cac resource-threshold-profiles]** hierarchy level.

NOTE: **The gtpv1-pci and gtpv1-pvi values are valid only for General Packet Radio Service (GPRS) tunneling protocol version 1 (GTPv1) subscribers.**

Options

enable—Enable preemption on the GGSN or P-GW.

If you do not specify a value, preemption is disabled by default.

gtpv1-pci-disable—Disable the preemption capability indicator for GTPv1 subscribers.

If you do not specify a value, the preemption capability indicator is enabled by default.

gtpv1-pvi-disable—Disable the preemption vulnerability indicator for GTPv1 subscribers.

If you do not specify a value, the preemption vulnerability indicator is enabled by default.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Preemption for Call Admission Control on page 25

Copyright © 2012, Juniper Networks, Inc.

protocol (Egress Rewrite Rules)

Syntax protocol [*protocol-type*];

Hierarchy Level [edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules dscp],
[edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules dscp-ipv6],
[edit class-of-service interfaces mif unit *interface-unit-number* rewrite-rules inet-precedence]

Description Specify where the egress rewrite rule should be applied to downstream (Gi to Gn or S5 to SGi traffic) subscriber packets.

Default If this statement is not configured, then the egress rewrite rules are applied to the inner IP header only.

Options ***protocol-type***—Apply the rewrite rule to one or more of the following:

- **mpls**—(DSCP IPv6 only) IPv6 packets entering the MPLS tunnel.
- **gtp-inet-outer**—Outer IP header only.
- **gtp-inet-both**—Both inner and outer IP header.

To specify multiple attributes at one time, include the attributes in square brackets ([]).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- **dscp (Egress Rewrite Rules) on page 111**
- **dscp-ipv6 (Egress Rewrite Rules) on page 109**
- **inet-precedence (Egress Rewrite Rules) on page 122**

qci (PDP QoS Control)

Syntax

```
qci qci-value {
  maximum-bit-rate-downlink {
    mbr-downlink;
    reject;
    upgrade;
  }
  maximum-bit-rate-uplink {
    mbr-uplink;
    reject;
    upgrade;
  }
}
```

Hierarchy Level

[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]

Description

Configure the maximum bit rate (MBR) for both uplink and downlink for QoS Class Identifier (QCI) values for non-guaranteed bit rate (GBR) Packet Data Protocol (PDP) contexts (3G).

The uplink and downlink MBR specified for the QCI value overrides the corresponding uplink and downlink MBR at the **[edit unified-edge cos-cac cos-policy-profiles *name* pdp-qos-control]** hierarchy level.

Options

qci-value—QCI value.

Range: 5 through 9

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Class of Service (CoS) Policy Profile Overview on page 12
- Quality of Service Overview on page 3
- **pdp-qos-control (CoS Policy Profiles) on page 142**

Copyright © 2012, Juniper Networks, Inc.

qos-class-identifier (Classifier Profiles)

Syntax

```
qos-class-identifier qci-value {
  forwarding-class class-name;
  loss-priority (high | low);
}
```

Hierarchy Level

[edit unified-edge cos-cac classifier-profiles *name*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Configure the QoS Class Identifier (QCI) mapping for the classifier profile. You can configure the QCI value and the associated forwarding class and packet loss priority based on traffic requirements. You can configure the packet-forwarding treatment by assigning a forwarding class and packet loss priority for each QCI.

NOTE: **If you specify a QCI value, you must specify the forwarding class and the packet loss priority.**

Options

qci-value—QCI value.

Range: 1 through 9

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring QoS on the Broadband Gateway Overview on page 18
- **classifier-profiles on page 95**
- Quality of Service Overview on page 3

resource-threshold-profiles (QoS)

Syntax

```
resource-threshold-profiles {
  name {
    bearers-load {
      high {
        percentage percentage;
        priority-level priority-level;
      }
      low {
        percentage percentage;
        priority-level priority-level;
      }
    }
    cpu {
      high {
        percentage percentage;
        priority-level priority-level;
      }
      low {
        percentage percentage;
        priority-level priority-level;
      }
    }
    description description;
    memory {
      high {
        percentage percentage;
        priority-level priority-level;
      }
      low {
        percentage percentage;
        priority-level priority-level;
      }
    }
  }
}
```

Hierarchy Level [edit unified-edge cos-cac]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the resource threshold profile. The resource threshold profile ensures that when the bearer load, CPU load, or memory load at the access point name (APN) or the gateway level on the broadband gateway reaches a specified threshold, then only Create Session requests or Create Bearer (Serving Gateway only) requests with a priority higher than what is configured are allowed.

NOTE: Even though the configuration of resource threshold profiles is not mandatory, the default values for the upper and lower threshold limits for various loads are applied at the gateway level. There are no defaults at the APN level.

Copyright © 2012, Juniper Networks, Inc.

Options *name*—Name of the resource threshold profile.

Range: Up to 64 characters

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Call Admission Control Overview on page 10
- Configuring Resource Thresholds for 3G and 4G Networks on page 26
- **cos-cac on page 98**

resource-threshold-profile (Local Policies)

Syntax resource-threshold-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the resource threshold profile for the local policy. The resource threshold profile specifies the limit for the bearer load, CPU load, or memory load.

Options *profile-name*—Name of the resource threshold profile.

NOTE: **The resource threshold profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac resource-threshold-profiles] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **resource-threshold-profiles (QoS) on page 148**
- **local-policies (QoS) on page 126**

rewrite-rules (Egress)

Syntax

```
rewrite-rules {
  [dscp (rewrite-rule-name | default)] {
    protocol [(gtp-inet-both | gtp-inet-outer)];
  }
  [dscp-ipv6 (rewrite-rule-name | default)] {
    protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
  }
  [inet-precedence (rewrite-rule-name | default)] {
    protocol [(gtp-inet-both | gtp-inet-outer)];
  }
}
```

Hierarchy Level

[edit class-of-service interfaces mif unit *logical-unit-number*]

Release Information

Statement introduced in Junos OS Mobility Release 11.2W.

Description

Apply a previously configured egress rewrite rule to the mobile interface. The rewrite rule is applied to the downstream (Gi to Gn or SGi to S5 traffic) subscriber packets. The rewrite rule can be applied to the inner IP header, the outer IP header, or both inner and outer IP header.

NOTE: The rewrite rule must be previously defined at the [edit class-of-service rewrite-rules] hierarchy level.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Egress Rewrite Rules to Mobile Interfaces on page 47
- unit (Mobile Interface for Class of Service) on page 154

Copyright © 2012, Juniper Networks, Inc.

roamer-classifier-profile (Local Policies)

Syntax roamer-classifier-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the classifier profile for roaming subscribers. A classifier profile defines the packet forwarding treatment for each bearer depending on its QoS Class Identifiers (QCIs).

Options ***profile-name***—Name of the roamer classifier profile.

NOTE: **The classifier policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac classifier-profiles] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **classifier-profiles on page 95**
- **local-policies (QoS) on page 126**

roamer-cos-policy-profile (Local Policies)

Syntax roamer-cos-policy-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the CoS policy profile for roaming subscribers. You configure a CoS policy profile to define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters.

Options ***profile-name***—Name of the roamer CoS policy profile.

NOTE: The CoS policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac cos-policy-profiles] hierarchy level.

Required Privilege Level interface, unified-edge—To view this statement in the configuration.
interface-control, unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- cos-policy-profiles on page 102
- local-policies (QoS) on page 126

 Copyright © 2012, Juniper Networks, Inc.

ul-bandwidth-pool (Local Policies)

Syntax ul-bandwidth-pool *pool-name* ;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the bandwidth pool for limiting the downlink bandwidth usage at the gateway or at the APN level.

Options ***pool-name***—Name of the uplink bandwidth pool.

NOTE: **The bandwidth pool must be previously configured on the broadband gateway at the [edit unified-edge cos-cac gbr-bandwidth-pools] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **gbr-bandwidth-pools (Class of Service) on page 115**
- **local-policies (QoS) on page 126**

unit (Mobile Interface for Class of Service)

Syntax

```
unit logical-unit-number {
  ingress-rewrite-rules {
    [dscp (rewrite-rule-name | default)];
    [dscp-ipv6 (rewrite-rule-name | default)];
    [inet-precedence (rewrite-rule-name | default)];
    }
  }
  rewrite-rules {
    [dscp (rewrite-rule-name | default)] {
      protocol [(gtp-inet-both | gtp-inet-outer)];
    }
    [dscp-ipv6 (rewrite-rule-name | default)] {
      protocol [(mpls | gtp-inet-both | gtp-inet-outer)];
    }
    [inet-precedence (rewrite-rule-name | default)] {
      protocol [(gtp-inet-both | gtp-inet-outer)];
    }
  }
}
```

Hierarchy Level

[edit class-of-service interfaces mif]

Description

Specify a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options

logical-unit-number—Number of the logical unit

Range: 0 through 16,384

The remaining statements are explained separately.

Required Privilege Level

Related Documentation

- Applying Rewrite Rules on Mobile Interfaces Overview on page 14
- Applying Ingress Rewrite Rules to a Mobile Interface on page 46
- mif (Class of Service) on page 140

Copyright © 2012, Juniper Networks, Inc.

violate-action (QoS Policer Action)

Syntax violate-action (set-loss-priority-high | transmit);

Hierarchy Level [edit unified-edge cos-cac cos-policy-profiles *name* policer-action gbr-bearer],
[edit unified-edge cos-cac cos-policy-profiles *name* policer-action non-gbr-bearer]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the policer action that is applied when the subscriber traffic exceeds the configured maximum bit rate (MBR) in a 3G network, or when the traffic the exceeds the configured aggregate maximum bit rate (AMBR) in a 4G network. The policer action controls packet behavior by dropping the packet, setting the packet loss priority (PLP) to high, or transmitting the packet without changing the PLP.

You can configure this policer action for both guaranteed bit rate (GBR) PDP contexts, and non-GBR bearers or PDP contexts.

Default If you do not include this statement, then the default action is to drop the packet.

Options **set-loss-priority-high**—Set the PLP to high.

transmit—Transmit the packet without changing the PLP.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring QoS on the Broadband Gateway Overview on page 18
- gbr-bearer (QoS Policer Action) on page 116
- non-gbr-bearer (QoS Policer Action) on page 141

visitor-classifier-profile (Local Policies)

Syntax visitor-classifier-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the classifier profile for visiting subscribers. A classifier profile defines the packet forwarding treatment for each bearer depending on its QoS Class Identifiers (QCIs).

Options ***profile-name***—Name of the visitor classifier profile.

NOTE: **The classifier policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac classifier-profiles] hierarchy level.**

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- **classifier-profiles on page 95**
- **local-policies (QoS) on page 126**

 Copyright © 2012, Juniper Networks, Inc.

visitor-cos-policy-profile (Local Policies)

Syntax visitor-cos-policy-profile *profile-name*;

Hierarchy Level [edit unified-edge local-policies *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the CoS policy profile for visiting subscribers. You configure a CoS policy profile to define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters.

Options ***profile-name***—Name of the visitor CoS policy profile.

NOTE: The CoS policy profile must be previously configured on the broadband gateway at the [edit unified-edge cos-cac cos-policy-profiles] hierarchy level.

Required Privilege Level unified-edge—To view this statement in the configuration.
unified-edge-control—To add this statement to the configuration.

Related Documentation

- Configuring a Local Policy on page 43
- Configuring QoS on the Broadband Gateway Overview on page 18
- cos-policy-profiles on page 102
- local-policies (QoS) on page 126

Copyright © 2012, Juniper Networks, Inc.

PART 3

Administration

- Monitoring on page 161
- Operational Commands on page 163

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 5

Monitoring

- Verifying Quality of Service on page 161

Verifying Quality of Service

Purpose Display QoS statistics for subscriber packets.

Action

- To display QoS statistics information for the specified gateway:

  user@host> **show unified-edge ggsn-pgw statistics** ***gateway***

- To display subscriber information for traffic marked with the specified GTPv1 allocation retention priority:

  user@host> **show unified-edge ggsn-pgw statistics gtpv1-arp** ***arp-value***

  NOTE: You can specify an ARP value of 1 through 3.

- To display subscriber information for traffic marked with the specified GTPv2 allocation retention priority:

  user@host> **show unified-edge ggsn-pgw statistics gtpv2-priority-level** ***arp-value***

  NOTE: You can specify an ARP value of 1 through 15.

- To display subscriber information for traffic marked with the specified GTPv1 allocation retention priority:

  user@host> **show unified-edge ggsn-pgw statistics** ***gtpv1-arp***

- To display subscriber information for traffic marked with the specified QoS Class Identifier:

  user@host> **show unified-edge ggsn-pgw statistics qci** ***qci-value***

  NOTE: You can specify a QCI value of 1 through 9.

Copyright © 2012, Juniper Networks, Inc.

- To display subscriber information for traffic marked with the specified traffic class:

  user@host> **show unified-edge ggsn-pgw statistics traffic-class (background | conversational | interactive | streaming)**

- To display the status information for the interactive traffic class with a specified traffic handling priority:

  show unified-edge ggsn-pgw statistics traffic-class interactive traffic-handling-priority*traffic-handling-priority*

NOTE: You can specify a traffic-handling priority value of 1 through 3.

Related Documentation

- Configuring a Classifier Profile for 3G and 4G Networks on page 27
- Configuring a CoS Policy Profile for 3G and 4G Networks on page 37
- Configuring QoS on the Broadband Gateway Overview on page 18

Copyright © 2012, Juniper Networks, Inc.

CHAPTER 6

Operational Commands

show unified-edge ggsn-pgw statistics traffic-class

Syntax

show unified-edge ggsn-pgw statistics traffic-class (background | conversational | interactive | streaming)
<traffic-handling-priority *traffic-handling-priority*>

Release Information

Command introduced in Junos OS Mobility Release 11.4W.

Description

Display the statistics for the specified traffic class one or more Gateway GPRS Support Nodes (GGSNs) or Packet Data Network Gateways (P-GWs).

Options

traffic-class (background | conversational | interactive | streaming)—Display the status information for the specified traffic class.

traffic-handling-priority *traffic-handling-priority*—(Optional) Display the status information for the specified traffic handling priority. You can specify a traffic handling priority value of 1 through 3.

NOTE: **This field is applicable only if the traffic class is specified as interactive.**

Required Privilege Level

view

Related Documentation

- clear unified-edge ggsn-pgw statistics
- show unified-edge ggsn-pgw statistics

List of Sample Output

show unified-edge ggsn-pgw statistics traffic-class interactive on page 164
show unified-edge ggsn-pgw statistics traffic-class interactive traffic–handling-priority 1 on page 165

Output Fields

The output fields for the **show unified-edge ggsn-pgw statistics traffic-class** command are a subset of the output fields for the **show unified-edge ggsn-pgw statistics** command. Please refer to the explanation of the output fields for the **show unified-edge ggsn-pgw statistics** command.

Sample Output

show unified-edge ggsn-pgw statistics traffic-class interactive

```
user@host> show unified-edge ggsn-pgw statistics traffic-class interactive
Gateway: gw1
Control plane statistics:
    Session establishment attempts:             22
    Successful session establishments:          22
    MS/peer initiated session deactivations:    20
    Successful MS/peer initiated deactivations: 20
    Gateway initiated session deactivations:    0
    Successful gateway initiated deactivations: 0
Data plane GTP statistics (Gn/S5/S8):
```


Copyright © 2012, Juniper Networks, Inc.

```
    Input     packets:          10
    Input     bytes:            1000
    Output    packets:          10
    Output    bytes:            1168
    Discarded packets:          0
Data plane GTP statistics (Gi):
    Input     packets:          10
    Input     bytes:            1168
    Output    packets:          10
    Output    bytes:            1000
    Discarded packets:          0
```

show unified-edge ggsn-pgw statistics traffic-class interactive traffic–handling-priority 1

```
user@host> show unified-edge ggsn-pgw statistics traffic-class interactive
traffic–handling-priority 1
Gateway: gw1
Control plane statistics:
    Session establishment attempts:             22
    Successful session establishments:          22
    MS/peer initiated session deactivations:    20
    Successful MS/peer initiated deactivations: 20
    Gateway initiated session deactivations:    0
    Successful gateway initiated deactivations: 0
Data plane GTP statistics (Gn/S5/S8):
    Input     packets:          10
    Input     bytes:            1000
    Output    packets:          10
    Output    bytes:            1168
    Discarded packets:          0
Data plane GTP statistics (Gi):
    Input     packets:          10
    Input     bytes:            1168
    Output    packets:          10
    Output    bytes:            1000
    Discarded packets:          0
```

show unified-edge ggsn-pgw status

Syntax

show unified-edge ggsn-pgw status
<apn-name *apn-name*>
<brief | detail>
<fpc-slot *fpc-slot*>
<gateway *gateway*>
<gtpv1-arp *gtpv1-arp*>
<gtpv2-priority-level *gtpv2-priority-level*>
<pic-slot *pic-slot*>
<pdn-type>
<qci *qci*>
<rat-type (eutran | gan | geran | hspa | others | utran | wlan)>
<traffic-class (background | conversational | interactive | streaming)>

Release Information

Command introduced in Junos OS Mobility Release 11.2W. **extensive** and **pdn-type** options introduced in Junos OS Mobility Release 11.4W.

Description

Display the status information, such as the number of subscribers, active sessions, and so on, for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then status information for all GGSNs and P-GWs is displayed.

Options

none—(Same as brief) Display the status information in brief.

apn-name *apn-name*—(Optional) Display the status information for the specified access point name (APN).

brief | detail | extensive—(Optional) Display the specified level of output.

fpc-slot *fpc-slot*—(Optional) Display the status information for the specified FPC slot number.

gateway *gateway*—(Optional) Display the status information for the specified GGSN or P-GW.

gtpv1-arp *gtpv1-arp*—(Optional) Display the status information for the GTPv1 Allocation and Retention Priority (ARP) value specified. You can specify a GTPv1 ARP value of 1 through 3.

gtpv2-priority-level *gtpv2-priority-level*—(Optional) Display the status information for the GTPv2 priority specified. You can specify a priority of 1 through 15.

pdn-type—(Optional) Display the number of active sessions according to the type of Packet Data Network (PDN): IPv4, IPv6, and both IPv4 and IPv6.

pic-slot *pic-slot*—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

qci *qci*—(Optional) Display the status information for the specified QoS Class Identifier (QCI). You can specify a QCI of 1 through 9.

Copyright © 2012, Juniper Networks, Inc.

rat-type (eutran | gan | geran | hspa | others | utran | wlan)—(Optional) Display the status information for the specified Radio Access Technology (RAT).

traffic-class (background | conversational | interactive | streaming)—(Optional) Display the status information for the specified traffic class.

Required Privilege Level view

Related Documentation

- show unified-edge ggsn-pgw status gtp-peer
- show unified-edge ggsn-pgw status preemption-list on page 171
- show unified-edge ggsn-pgw status session-state

List of Sample Output

show unified-edge ggsn-pgw status on page 168
show unified-edge ggsn-pgw status detail on page 168
show unified-edge ggsn-pgw status detail on page 169
show unified-edge ggsn-pgw status extensive on page 169
show unified-edge ggsn-pgw status pdn-type detail on page 169

Output Fields Table 16 on page 167 lists the output fields for the **show unified-edge ggsn-pgw status** command. Output fields are listed in the approximate order in which they appear.

Table 16: show unified-edge ggsn-pgw status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
FPC SLOT	FPC slot number of the interface for which the status information is displayed.	**detail**
PIC SLOT	PIC slot number of the FPC for which the status information is displayed.	**detail**
State	State of the services or session PIC on the GGSN or P-GW: • **Standalone** • **Active**—PIC is an active member. • **Backup**—PIC is a backup.	**detail**
Type	Indicates whether the PIC is a session PIC or a services PIC.	**detail**
Active Subscribers	Number of active subscribers.	All levels none
Active Subscribers (with services)	Number of active subscribers who are using subscriber-aware services and who are anchored on a services PIC.	
Active Sessions	Number of active sessions.	All levels none

Copyright © 2012, Juniper Networks, Inc.

Table 16: show unified-edge ggsn-pgw status Output Fields *(continued)*

Field Name	Field Description	Level of Output
Active Bearers	Number of active bearers or Packet Data Protocol (PDP) contexts.	All levels none
CPU Load (%)	Percentage of the CPU load.	All levels none
Memory Load (%)	Percentage of the memory load.	All levels none
Connections to Session PICs	Connections between the services PIC and the session PICs. This field is displayed only when the services PIC has a connection to one or more session PICs.	extensive
IPv4 Active Sessions	Number of active IPv4 sessions.	**pdn-type**
IPv6 Active Sessions	Number of active IPv6 sessions.	**pdn-type**
IPv4-v6 Active Sessions	Number of active IPv4-IPv6 sessions.	**pdn-type**

Sample Output

show unified-edge ggsn-pgw status

```
user@host> show unified-edge ggsn-pgw status
Gateway: PGW
    Active Subscribers                  :               3
    Active Subscribers (with services)  :               0
    Active Sessions                     :               3
    Active Bearers                      :               3
    CPU Load (%)                        :               0
    Memory Load (%)                     :               55
```

show unified-edge ggsn-pgw status detail

```
user@host> show unified-edge ggsn-pgw status detail
Gateway: PGW
    FPC SLOT: 4    PIC SLOT: 0
    State                               :               Standalone
    Type                                :               Session-PIC
    Active Subscribers                  :               3
    Active Sessions                     :               3
    Active Bearers                      :               3
    CPU Load (%)                        :               0
    Memory Load (%)                     :               55
    FPC SLOT: 4    PIC SLOT: 1
    State                               :               Standalone
    Type                                :               Session-PIC
    Active Subscribers                  :               0
    Active Sessions                     :               0
    Active Bearers                      :               0
```


Copyright © 2012, Juniper Networks, Inc.

```
    CPU Load (%)                        :               0
    Memory Load (%)                     :               55
```

show unified-edge ggsn-pgw status detail

```
user@host> show unified-edge ggsn-pgw status detail
Gateway: PGW
    FPC SLOT: 4    PIC SLOT: 0
    State                               :               Standalone
    Type                                :               Session-PIC
    Active Subscribers                  :               3
    Active Sessions                     :               3
    Active Bearers                      :               3
    CPU Load (%)                        :               0
    Memory Load (%)                     :               55
    FPC SLOT: 4    PIC SLOT: 1
    State                               :               Standalone
    Type                                :               Session-PIC
    Active Subscribers                  :               0
    Active Sessions                     :               0
    Active Bearers                      :               0
    CPU Load (%)                        :               0
    Memory Load (%)                     :               55
```

show unified-edge ggsn-pgw status extensive

```
user@host> show unified-edge ggsn-pgw status extensive
Gateway: PGW

    FPC SLOT: 1   PIC SLOT: 0
    State                               :             Active
    Type                                :             Service-PIC
    Active Subscribers                  :             0
    Active Sessions                     :             0
    CPU Load (%)                        :             0
    Memory Load (%)                     :             22
    Connections to Session PICs         :
                                                      ms-2/0

    FPC SLOT: 2   PIC SLOT: 0
    State                               :             Active
    Type                                :             Session-PIC
    Active Subscribers                  :             0
    Active Sessions                     :             0
    Active Bearers                      :             0
    CPU Load (%)                        :             0
    Memory Load (%)                     :             29
```

show unified-edge ggsn-pgw status pdn-type detail

```
user@host> show unified-edge ggsn-pgw status pdn-type detail
Gateway: PGW
    FPC SLOT: 4    PIC SLOT: 0
    State                               :               Standalone
    Type                                :               Session-PIC
    IPv4 Active Sessions                :            3
    IPv6 Active Sessions                :            0
    IPv4-v6 Active Sessions             :            0
    FPC SLOT: 4    PIC SLOT: 1
    State                               :               Standalone
    Type                                :               Session-PIC
```

```
IPv4 Active Sessions                :            0
IPv6 Active Sessions                :            0
IPv4-v6 Active Sessions             :            0
```


Copyright © 2012, Juniper Networks, Inc.

show unified-edge ggsn-pgw status preemption-list

Syntax

show unified-edge ggsn-pgw status preemption-list
<brief | detail>
<fpc-slot *fpc-slot*>
<gateway *gateway*>
<pic-slot *pic-slot*>

Release Information

Command introduced in Junos OS Mobility Release 11.2W.
gateway option introduced in Junos OS Mobility Release 11.4W.

Description

Display the preemption list for guaranteed bit rate (GBR) and non-GBR bearers for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.

NOTE:

- In load conditions, to accommodate higher-priority bearers, lower-priority bearers are preempted. This list displays the number of bearers in each candidate priority level for preemption.
- This command displays a preemption list only if preemption is enabled on the GGSN or P-GW.

Options

none—(Same as brief) Display the preemption list information in brief.

brief | detail —(Optional) Display the specified level of output.

fpc-slot *fpc-slot*—(Optional) Display the preemption list information for the specified Flexible PIC Concentrator (FPC) slot number. You must specify a PIC slot number along with an FPC slot number.

gateway—(Optional) Display the preemption list information for the specified GGSN or P-GW.

pic-slot *pic-slot*—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Related Documentation

- show unified-edge ggsn-pgw status on page 166

List of Sample Output

show unified-edge ggsn-pgw status preemption-list brief on page 172
show unified-edge ggsn-pgw status preemption-list detail on page 172

Output Fields Table 17 on page 172 lists the output fields for the **show unified-edge ggsn-pgw status preemption-list** command. Output fields are listed in the approximate order in which they appear.

Table 17: show unified-edge ggsn-pgw status preemption-list Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of GGSN or P-GW.	All levels
FPC Slot	FPC slot number of the interface for which the preemption list information is displayed.	**detail**
PIC Slot	PIC slot number of the FPC for which the preemption list information is displayed.	**detail**
Priority Level	Priority of the call that was set up: 1 is the highest and 15 is the lowest. For each priority level, the following information is displayed: • **GBR**—Number of GBR bearers for the corresponding priority level. • **NON-GBR**—Number of GBR bearers for the corresponding priority level.	All levels

Sample Output

show unified-edge ggsn-pgw status preemption-list brief

```
user@host> show unified-edge ggsn-pgw status preemption-list brief
Gateway: PGW

                                    GBR          NON-GBR

    Priority Level 1     :        0             1
    Priority Level 2     :        0              11
    Priority Level 3     :        0              0
    Priority Level 4     :        0              0
    Priority Level 5     :        0              0
    Priority Level 6     :        0              0
    Priority Level 7     :        0              0
    Priority Level 8     :        0              0
    Priority Level 9     :        0              0
    Priority Level 10    :        0              0
    Priority Level 11    :        0              0
    Priority Level 12    :        0              0
    Priority Level 13    :        0              0
    Priority Level 14    :        0              0
    Priority Level 15    :        0              0
```

show unified-edge ggsn-pgw status preemption-list detail

```
user@host> show unified-edge ggsn-pgw status preemption-list detail
Gateway: PGW

    Preemption List status:

    FPC SLOT: 0   PIC SLOT: 0

                                    GBR          NON-GBR

    Priority Level 1     :        0             0
    Priority Level 2     :        0              6
```


Copyright © 2012, Juniper Networks, Inc.

```
    Priority Level 3     :       0             0
    Priority Level 4     :       0             0
    Priority Level 5     :       0             0
    Priority Level 6     :       0             0
    Priority Level 7     :       0             0
    Priority Level 8     :       0             0
    Priority Level 9     :       0             0
    Priority Level 10    :       0             0
    Priority Level 11    :       0             0
    Priority Level 12    :       0             0
    Priority Level 13    :       0             0
    Priority Level 14    :       0             0
    Priority Level 15    :       0             0


    Preemption List status:

    FPC SLOT: 0   PIC SLOT: 1

                                GBR         NON-GBR

    Priority Level 1     :       0            0
    Priority Level 2     :       0             0
    Priority Level 3     :       0             0
    Priority Level 4     :       0             0
    Priority Level 5     :       0             0
    Priority Level 6     :       0             0
    Priority Level 7     :       0             0
    Priority Level 8     :       0             0
    Priority Level 9     :       0             0
    Priority Level 10    :       0             0
    Priority Level 11    :       0             0
    Priority Level 12    :       0             0
    Priority Level 13    :       0             0
    Priority Level 14    :       0             0
    Priority Level 15    :       0             0

[...output truncated...]
```

show unified-edge ggsn-pgw subscribers

Syntax

show unified-edge ggsn-pgw subscribers
<apn *apn-name*>
<brief | detail | extensive>
<fpc-slot *fpc-slot*>
<gateway *gateway*>
<gtp-version *gtp-version*>
<gtpv1-arp *gtpv1-arp*>
<gtpv2-priority-level *gtpv2-priority-level*>
<imsi *imsi*>
<msisdn *msisdn*>
<pdn-type (ipv4 | ipv4-v6 | ipv6)>
<peer *peer*>
<pic-slot *pic-slot*>
<qci *qci*>
<roaming-status (home | roamer | visitor)>
<routing-instance *routing-instance*>
<services *service-name*>
<session-state (acquire-address | authorizing | bearer-update | deleting | established)>
<v4-addr *v4-addr*>
<v6-addr *v6–addr*>

Release Information

Command introduced in Junos OS Mobility Release 11.2W.
Support for the **services** and **pdn-type** attributes introduced in Junos OS Mobility Release 11.4W.

Description

Display the subscriber information one or more Gateway GPRS Support Nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then subscriber information for all GGSNs and P-GWs is displayed.

Options

none—(Same as brief) Display the subscriber information in brief.

apn ***apn-name***—(Optional) Display the subscriber information for the specified access point name (APN).

brief | detail | extensive —(Optional) Display the specified level of output.

fpc-slot ***fpc-slot***—(Optional) Display the subscriber information for the specified FPC slot number.

gateway ***gateway***—(Optional) Display the subscriber information for the specified gateway.

gtp-version ***gtp-version***—(Optional) Display the subscriber information for the GTP version number (0 through 2) specified.

gtpv1-arp ***gtpv1-arp***—(Optional) Display the subscriber information for the GTPv1 Allocation and Retention Priority (ARP) value specified. You can specify a GTPv1 ARP value of 1 through 3.

gtpv2-priority-level ***gtpv2-priority-level***—(Optional) Display the subscriber information for the GTPv2 priority specified. You can specify a priority of 1 through 15.

Copyright © 2012, Juniper Networks, Inc.

imsi *imsi*—(Optional) Display the subscriber information for the specified International Mobile Subscriber Identity (IMSI).

msisdn *msisdn*—(Optional) Display the subscriber information for the specified mobile station ISDN (MSISDN) number.

pdn-type (ipv4 | ipv4-v6 | ipv6)—(Optional) Display the subscriber information for the specified Packet Data Network (PDN) type or session type. You can specify the following PDN or session types:

- **ipv4**—Subscribers with only IPv4 sessions.
- **ipv4-v6**—Subscribers with both IPv4 and IPv6 sessions.
- **ipv6**—Subscribers with only IPv6 sessions.

peer *peer*—(Optional) Display the subscriber information for the specified peer IP address.

pic-slot *pic-slot*—(Optional) Display the subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

qci *qci*—(Optional) Display the subscriber information for the specified QoS Class Identifier (QCI).

roaming-status (home | roamer | visitor)—(Optional) Display the subscriber information for the specified roaming status.

routing-instance *routing-instance*—(Optional) Display the subscriber information for the specified routing instance.

services *service-name*—(Optional) Display the information for subscribers who are using the specified subscriber-aware service and who are anchored on a services PIC. Currently, HTTP Content Management **hcm** is the only service supported.

session-state (acquire-address | authorizing | bearer-update | deleting | established)—(Optional) Display the subscriber information for the specified session state. You can specify the following session states:

- **acquire-address**—Sessions for which the IP address is being acquired.
- **authorizing**—Sessions waiting for initial authorization.
- **bearer-update**—Sessions which are being updated.
- **deleting**—Sessions being deleted.
- **established**—Sessions already established.

v4-addr *v4-addr*—(Optional) Display the subscriber information for the specified IPv4 address of the subscriber's user equipment (UE).

v6-addr *v6-addr*—(Optional) Display the subscriber information for the specified IPv6 address of the subscriber's user equipment.

Copyright © 2012, Juniper Networks, Inc.

Required Privilege Level view

Related Documentation
- clear unified-edge ggsn-pgw subscribers
- show unified-edge ggsn-pgw subscribers charging
- show unified-edge ggsn-pgw subscribers traffic-class on page 186

List of Sample Output
show unified-edge ggsn-pgw subscribers on page 182
show unified-edge ggsn-pgw subscribers detail on page 182
show unified-edge ggsn-pgw subscribers extensive (GTP Version 1 Subscribers) on page 183
show unified-edge ggsn-pgw subscribers extensive (GTP Version 2 Subscribers) on page 184

Output Fields Table 18 on page 176 lists the output fields for the **show unified-edge ggsn-pgw subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
IMSI	IMSI of the subscriber's user equipment.	**brief** none
MSISDN	MSISDN number of the subscriber's user equipment.	**brief** none
Subscriber Address	IP address of the subscriber's user equipment.	**brief** none
Peer Address	IP address of the GTP peer through which the subscriber is connected to the broadband gateway.	**brief** none
APN	Access point name (APN), on the broadband gateway, to which the subscriber is attached.	**brief** none
Subscriber Information:		
UE		
IMSI	IMSI of the subscriber's user equipment.	**detail** **extensive**

 Copyright © 2012, Juniper Networks, Inc.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output
IMEI	International Mobile Station Equipment Identity (IMEI) of the subscriber's user equipment.	**detail** **extensive**
MSISDN	MSISDN number of the subscriber's user equipment.	**extensive**
Time Zone	Time zone to which the subscriber belongs.	**extensive**
DST	Daylight saving time applicable within the time zone.	**extensive**
RAT Type	Type of Radio Access Technology (RAT) used.	**detail** **extensive**
User Location Info:		
MCC	Mobile country code (MCC) of the subscriber.	**extensive**
MNC	Mobile network code (MNC) of the subscriber.	**extensive**
LAC	Location area code (LAC) of the subscriber.	**extensive**
CI	Cell Identity (CI) of the subscriber.	**extensive**
SAC	Service area code (SAC) of the subscriber.	**extensive**
RAC	Routing area code (RAC) of the subscriber.	**extensive**
TAC	Tracking area code (TAC) of the subscriber.	**extensive**
ECI	E-UTRAN Cell identifier (ECI) of the subscriber.	**extensive**
PDN Session:		
APN name	Access point name for the Packet Data Network (PDN) session.	**detail** **extensive**
IPv4 Address	IPV4 address of the subscriber.	**detail** **extensive**
IPv6 Address	IPV6 address of the subscriber.	**detail** **extensive**
GTP Version	GTP version used for the control plane.	**detail** **extensive**

Copyright © 2012, Juniper Networks, Inc.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Address Assignment	Indicates the method used to allocate the subscriber's address: • **AAA**—Address was allocated by the authentication, authorization, and accounting (AAA) server. • **DCHP**—Address was allocated by the gateway using the IP addresses returned by the Dynamic Host Configuration Protocol (DHCP) server. • **Local**—Address was allocated by the gateway based on the local mobile pool or mobile pool group configured on the APN. • **Static**—Address was pre-allocated to the user equipment.	
Local Control IP	Local IPV4 address of the broadband gateway to which the peer (Serving GPRS Support Node [SGSN] or S-GW [Serving Gateway]) will send the control messages for the subscriber.	**detail** **extensive**
Remote Control IP	IP address of the peer (SGSN or S-GW) to which the broadband gateway will send control messages for the subscriber.	**detail** **extensive**
Local Control TEID	Tunnel endpoint identifier (TEID) allocated locally by the broadband gateway for the control plane or signaling messages. The control peers (SGSN or S-GW) send this TEID in all control messages to the broadband gateway.	**detail** **extensive**
Remote Control TEID	Control TEID for the session, which is allocated by the remote control peer (SGSN or S-GW). The broadband gateway sends this TEID in the GTP header in all control messages to the peer.	**detail** **extensive**
Peer CSID	Connection Set Identifier (CSID) allocated by the GTP peer (S-GW).	**extensive**
Remote CSID	CSID allocated by the Mobility Management Entity (MME). It identifies the connection set on the MME to which the session belongs.	**extensive**
Selection mode	APN selection mode provided by the SGSN or S-GW in the Create Request message.	**extensive**
Session PIC	FPC and PIC slots for the session PIC on which the subscriber control session is present.	**detail** **extensive**
PFE	FPC and PIC slots for the Packet Forwarding Engine for the PDP session.	**detail** **extensive**
Service PIC	FPC and PIC slot numbers of the services PIC on which the subscriber services are anchored.	**detail** **extensive**
Session State	State of the subscriber session on the signaling plane.	**detail** **extensive**

Copyright © 2012, Juniper Networks, Inc.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Session Duration	Duration of the PDP session.	**detail** **extensive**
Roaming Status	Roaming status of the subscriber; that is, whether the subscriber is a visitor, home subscriber, or a roamer.	**detail** **extensive**
Serving network	The following information about the network that is serving the subscriber (that the subscriber is attached to) is displayed: • **MCC**—Mobile country code of the network. • **MNC**—Mobile network code of the network.	**detail** **extensive**
Direct Tunnel	Status of the GTPv1 direct tunnel: enabled or disabled.	**detail** **extensive**
Negotiated APN AMBR	The aggregate maximum bit rate (AMBR) negotiated for the PDP session is displayed for the following: • **Downlink**—Negotiated AMBR in the downlink direction. • **Uplink**—Negotiated AMBR in the uplink direction.	**detail** **extensive**
Requested APN AMBR	The AMBR requested by the user equipment for the session is displayed for the following: • **Downlink**—Requested AMBR in the downlink direction. • **Uplink**—Requested AMBR in the uplink direction.	**extensive**
Bearer:		
NSAPI/EBI	Network Service Access Point Identifier (NSAPI) or the Evolved Packed System Bearer ID (EBI) for the session.	**detail** **extensive**
Local Data IP	IP address of the broadband gateway to which the peer sends the data packets for the PDP context or bearer.	**detail** **extensive**
Remote Data IP	IP address of the peer to which the broadband gateway sends the data packets for the PDP context or bearer.	**detail** **extensive**
Local Data TEID	Data TEID allocated by the broadband gateway which identifies the data tunneling endpoint for all data packets coming in from the data peer. This is sent in the GTP header for all data packets coming from the peer GTP nodes (SGSN or S-GW).	**detail** **extensive**
Remote Data TEID	Data TEID allocated by the data plane peer for the session which identifies the data tunneling endpoint for all data packets sent from the broadband gateway to the remote peer.	**detail** **extensive**

Copyright © 2012, Juniper Networks, Inc.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bearer State	Represents the state of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway.	**detail** **extensive**
Substate	Represents the substate of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway.	**extensive**
Idle Timeout	Idle timeout for the session, in minutes.	**detail** **extensive**
AAA Interim Interval	Authentication, authorization, and accounting (AAA) interim account timer, in minutes.	**detail** **extensive**

Negotiated QoS Parameters	The following QoS parameters negotiated by the user equipment are displayed:
	• For GTP version 1 subscribers:
	  • **Traffic Class**—Conversational, streaming, interactive, or background.
	  • **ARP**—Allocation and retention priority (ARP).
	  • **Traffic Handling Priority**
	  • **Transfer Delay**—Transfer delay in milliseconds.
	  • **MBR Uplink**—Maximum bit rate (MBR) in the uplink direction, in kbps.
	  • **MBR Downlink**—MBR in the downlink direction, in kbps.
	  • **Signaling Indicator**—Signaling indication sent by the user equipment in the QoS Information Element (IE);1 indicates Yes and 0 indicates No. This field is valid only for the interactive traffic class.
	  • **Forwarding Class**
	  • **Loss Priority**—Packet loss priority
	• For GTP version 2 subscribers:
	  • **QCI**—QoS Class Identifier.
	  • **ARP: (PL/PVI/PCI)**—The following parameters related to ARP are displayed:
	  • Priority level (PL)
	  • Preemption Vulnerability Indicator (PVI)
	  • Preemption Capability Indicator (PCI)
	  • **Forwarding Class**
	  • **Loss Priority**—Packet loss priority
		detail
		extensive

Copyright © 2012, Juniper Networks, Inc.

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output

Requested QoS Parameters	The following QoS parameters negotiated by the user equipment are displayed:
	• For GTP version 1 subscribers:
	  • **Traffic Class**—Conversational, streaming, interactive, or background.
	  • **ARP**
	  • **Traffic Handling Priority**
	  • **Transfer Delay**
	  • **MBR Uplink**—MBR in the uplink direction, in kbps.
	  • **MBR Downlink**—MBR in the downlink direction, in kbps.
	  • **Signaling Indicator**—Signaling indication sent by the user equipment in the QoS Information Element (IE);1 indicates Yes and 0 indicates No. This field is valid only for the interactive traffic class.
	  • **Forwarding Class**
	  • **Loss Priority**—Packet loss priority
	• For GTP version 2 subscribers:
	  • **QCI**—QoS Class Identifier
	  • **ARP: (PL/PVI/PCI)**—The following parameters related to ARP are displayed:
	  • Priority Level
	  • Preemption Vulnerability Indicator (PVI)
	  • Preemption Capability Indicator (PCI)
		extensive

Charging information	The following information related to charging is displayed:
	• **Charging ID**—Charging ID for the session. The charging ID is the unique bearer identity sent in accounting messages and in Charging Data Records (CDRs).
	• **Profile ID**—ID of the charging profile associated with the bearer.
	• **State**—(extensive only) Current charging state for the bearer.
	• **Previous State**—(extensive only) Previous charging state for the bearer.
	• **Profile selection criteria**—(extensive only) Selection source (home, visitor, roamer, and default) for the charging profile for the bearer.
	• **Offline charging information**—(extensive only) The following details of offline charging information are displayed if offline charging is enabled; if not, an indication that offline charging is disabled is displayed:
	  • **Current service data container sequence number**—Sequence number of the current local service data container.
	  • **Current partial record sequence number**—Sequence number of the current partial record CDR.
	  • **Number of CDRs closed**—Number of closed CDRs generated.
	  • **Number of containers closed**—Number of containers closed.
		detail
		extensive

Table 18: show unified-edge ggsn-pgw subscribers Output Fields *(continued)*

Field Name	Field Description	Level of Output

Rating group information	The following information related to the rating group is displayed:
	• **Rating group**—Default rating group associated with the bearer.
	• **Service ID**—Service identifier of the rating group.
	• **Action ID**—(extensive only) Action identifier of the rating group.
	• **Trigger profile**—(extensive only) Trigger profile number associated with the rating group.
	• **Change condition bitmask**—(extensive only) Rating group trigger change condition bitmask.
	• **Action-id-bitmask**—(extensive only) Charging action ID bitmask.
	• **Signal bitmask**—(extensive only) Rating group trigger signal condition bitmask.
	• **Last signal bitmask**—(extensive only) Previous rating group trigger signal condition bitmask.
	• **Last statistics info**—(extensive only) The following information about the last statistics collected is displayed if statistics were collected; if not, an indication that no statistics were collected is displayed:
	  ◦ **Collection time**—Time when the last control plane recorded statistics for the subscriber.
	  ◦ **Uplink packets**—Number of packets handled in the uplink direction.
	  ◦ **Downlink packets**—Number of packets handled in the downlink direction.
	  ◦ **Uplink bytes**—Number of bytes handled in the uplink direction.
	  ◦ **Downlink bytes**—Number of bytes handled in the downlink direction.
		detail
		
		extensive

Sample Output

show unified-edge ggsn-pgw subscribers

```
user@host> show unified-edge ggsn-pgw subscribers
Gateway: PGW
    IMSI            MSISDN          Subscriber         Peer           APN
                                     Address          Address
 123213213123256      1926737745  20.20.4.1        200.6.88.2     jnpr-sunnyvale
```

show unified-edge ggsn-pgw subscribers detail

```
user@host> show unified-edge ggsn-pgw subscribers detail
Gateway: PGW

Subscriber Information:
  UE:
    IMSI: 123567213123256              IMEI: 1122334455667788
    RAT Type: E-UTRAN
  PDN Session:
    APN name: jnpr-sunnyvale
    IPv4 Address: 20.20.44.1           IPv6 Address: None
    GTP Version: 2                    Address Assignment: Local

    Local Control IP: 200.1.5.1        Remote Control IP: 200.1.6.1
    Local Control TEID: 0x25000000     Remote Control TEID: 0x15002c00
    Session PIC: 1 /1  (FPC/PIC)       PFE: 2 /2  (FPC/PIC)
    Service PIC: None/None (FPC/PIC)
    Session State: Established         Session Duration: 5:38
    Roaming Status: Visitor            Serving network: MCC: 123  MNC: 567
    Direct Tunnel: Disabled
```


Copyright © 2012, Juniper Networks, Inc.

```
    Negotiated APN AMBR: Downlink: 128 kbps        Uplink: 128  kbps
  Bearer:
    NSAPI/EBI: 5
    Local Data IP: 200.1.5.1           Remote Data IP: 200.1.6.1
    Local Data TEID: 0x3c150000        Remote Data TEID: 0x14250400
    Bearer State: Established
    Idle Timeout: 0   min              AAA Interim Interval: 0   min
    Negotiated QoS Parameters:
       QCI: 5                          ARP: 1 /0 /0   (PL/PVI/PCI)
       Forwarding Class:  None         Loss Priority:  None
    Charging information:
       Charging ID: 0x25000000
       Profile ID: 0
    Rating group information:
       Rating group: 0 Service id: 0
```

show unified-edge ggsn-pgw subscribers extensive (GTP Version 1 Subscribers)

```
user@host> show unified-edge ggsn-pgw subscribers extensive
Gateway: PGW1

Subscriber Information:
  UE:
    IMSI: 734444553443191              IMEI: 1122334455667790
    MSISDN: 34555557                   Time Zone: GMT     DST: None
    RAT Type: UTRAN
    User Location Info:
      MCC:  None   MNC:  None
      LAC: 0x0  CI: 0x0     SAC: 0x0  RAC: 0x0  TAC: 0x0  ECI: 0x0
  PDN Session:
    APN name: internet123
    IPv4 Address: 20.1.0.1             IPv6 Address: None
    GTP Version: 1                     Address Assignment: Local
    Local Control IP: 18.1.1.2         Remote Control IP: 30.1.1.2
    Local Control TEID: 0x12000000     Remote Control TEID: 0x1f9
    Selection mode: MS provided APN, subscription not verified
    Session PIC: 0 /0  (FPC/PIC)       PFE: 5 /0  (FPC/PIC)
    Service PIC: None/None (FPC/PIC)
    Session State: Established         Session Duration: 9
    Roaming Status: Visitor            Serving network: MCC: None MNC: None
    Direct Tunnel: Disabled
  Bearer:
    NSAPI/EBI: 5
    Local Data IP: 18.1.1.2            Remote Data IP: 30.1.1.2
    Local Data TEID: 0x14120000        Remote Data TEID: 0x1f8
    Bearer State: Established          Substate: None
    Idle Timeout: 0   min              AAA Interim Interval: 0   min
    Negotiated QoS Parameters:
       Traffic Class:Conversational       ARP: 1
       Traffic Handling Priority:0        Transfer Delay: 80
       MBR Uplink: 8640             kbps  MBR Downlink: 8640      kbps
       GBR Uplink: 4672             kbps   GBR Downlink: 4672      kbps
                                           Signaling Indicator: 0
       Forwarding Class:  None         Loss Priority:  None
    Requested QoS Parameters:
       Traffic Class: Conversational      ARP: 1
       Traffic Handling Priority: 0       Transfer Delay: 10
       MBR Uplink  : 8640           kbps  MBR Downlink: 8640      kbps
       GBR Uplink  : 4672           kbps  GBR Downlink: 4672      kbps
                                           Signaling Indicator: 0
    Charging information:
       Charging ID: 0x12000000
```

```
      Profile ID: 0
      State: Init                    Previous State: Init
      Profile selection criteria: None
    Offline charging information: Disabled
    Rating group information:
      Rating group: 0 Service id: 0
      Action ID: 0x0                    Trigger profile: 0
      Change condition bitmask: 0x0     Action-id-bitmask: 0x0
      Signal bitmask: 0x0               Last signal bitmask: 0x0
      Last statistics info:
        Collection time: None collected
```

show unified-edge ggsn-pgw subscribers extensive (GTP Version 2 Subscribers)

```
user@host> show unified-edge ggsn-pgw subscribers extensive
Gateway: PGW1

Subscriber Information:
  UE:
    IMSI: 324213213134030              IMEI: 1122334455667790
    MSISDN: 1926737867                 Time Zone: GMT     DST: None
    RAT Type: E-UTRAN
    User Location Info:
      MCC:  None   MNC: 180
      LAC: 0x22 CI: 0x0     SAC: 0x2b RAC: 0x0  TAC: 0x4  ECI: 0x0
  PDN Session:
    APN name: internet123
    IPv4 Address: 20.1.0.1             IPv6 Address: None
    GTP Version: 2                     Address Assignment: Local
    Local Control IP: 18.1.1.2         Remote Control IP: 30.1.1.2
    Local Control TEID: 0x14000000     Remote Control TEID: 0x113
    Peer CSID: 0                       Remote CSID: 0
    Selection mode: MS or network provided APN, subscription verified
    Session PIC: 0 /0  (FPC/PIC)       PFE: 5 /0  (FPC/PIC)
    Service PIC: None/None (FPC/PIC)
    Session State: Established         Session Duration: 10
    Roaming Status: Visitor            Serving network: MCC: 123  MNC: 567
    Direct Tunnel: None
    Negotiated APN AMBR: Downlink: 128 kbps        Uplink: 128  kbps
    Requested  APN AMBR: Downlink: 128 kbps        Uplink: 128  kbps
  Bearer:
    NSAPI/EBI: 5
    Local Data IP: 18.1.1.2            Remote Data IP: 30.1.1.2
    Local Data TEID: 0x14140000        Remote Data TEID: 0x114
    Bearer State: Established          Substate: None
    Idle Timeout: 0   min              AAA Interim Interval: 0   min
    Negotiated QoS Parameters:
      QCI: 5                           ARP: 2 /0 /0   (PL/PVI/PCI)
      Forwarding Class:  None          Loss Priority:  None
    Requested QoS Parameters:
      QCI: 5                           ARP: 2 /0 /0   (PL/PVI/PCI)
    Charging information:
      Charging ID: 0x14000000
      Profile ID: 0
      State: Init                      Previous State: Init
      Profile selection criteria: None
    Offline charging information: Disabled
    Rating group information:
      Rating group: 0 Service id: 0
      Action ID: 0x0                    Trigger profile: 0
      Change condition bitmask: 0x0     Action-id-bitmask: 0x0
      Signal bitmask: 0x0               Last signal bitmask: 0x0
```


Copyright © 2012, Juniper Networks, Inc.

```
Last statistics info:
  Collection time: None collected
```

show unified-edge ggsn-pgw subscribers traffic-class

Syntax

show unified-edge ggsn-pgw subscribers traffic-class (background | conversational | interactive | streaming)
<traffic-handling-priority *traffic-handling-priority*>

Release Information

Command introduced in Junos OS Mobility Release 11.4W.

Description

Display the subscribers information for the specified traffic class one or more Gateway GPRS Support Nodes (GGSNs) or Packet Data Network Gateways (P-GWs).

Options

traffic-class (background | conversational | interactive | streaming)—Display the subscriber information for the specified traffic class.

traffic-handling-priority *traffic-handling-priority*—(Optional) Display the subscriber information for the specified traffic handling priority. You can specify a traffic handling priority value of 1 through 3.

NOTE: **This field is applicable only if the traffic class is specified as interactive.**

Required Privilege Level

view

Related Documentation

- show unified-edge ggsn-pgw subscribers on page 174

List of Sample Output

show unified-edge ggsn-pgw subscribers traffic-class conversational on page 186
show unified-edge ggsn-pgw subscribers traffic-class interactive traffic—handling-priority 1 on page 187

Output Fields

The output fields for the **show unified-edge ggsn-pgw subscribers traffic-class** command are a subset of the output fields for the **show unified-edge ggsn-pgw subscribers** command. Refer to the explanation of the output fields for the **show unified-edge ggsn-pgw subscribers** command.

Sample Output

show unified-edge ggsn-pgw subscribers traffic-class conversational

```
user@host> show unified-edge ggsn-pgw subscribers traffic-class conversational
Gateway: PGW1

Subscriber Information:
  UE:
    IMSI: 734444553453197              IMEI: 1122334455677796
    RAT Type: UTRAN
  PDN Session:
    APN name: internet123
    IPv4 Address: 20.1.0.1             IPv6 Address: None
    GTP Version: 1                     Address Assignment: Local
    Local Control IP: 18.1.1.2         Remote Control IP: 30.1.1.2
```


Copyright © 2012, Juniper Networks, Inc.

```
    Local Control TEID: 0xb000000      Remote Control TEID: 0x5033
    Session PIC: 0 /0  (FPC/PIC)       PFE: 5 /0  (FPC/PIC)
    Service PIC: None/None (FPC/PIC)
    Session State: Established         Session Duration: 3:13
    Roaming Status: Visitor            Serving network: MCC: None MNC: None
    Direct Tunnel: Disabled
  Bearer:
    NSAPI/EBI: 5
    Local Data IP: 18.1.1.2            Remote Data IP: 30.1.1.2
    Local Data TEID: 0x130000          Remote Data TEID: 0x5032
    Bearer State: Established
    Idle Timeout: 0   min              AAA Interim Interval: 0   min
    Negotiated QoS Parameters:
       Traffic Class:Conversational       ARP: 1
       Traffic Handling Priority:0        Transfer Delay: 80
       MBR Uplink: 8640             kbps  MBR Downlink: 8640      kbps
       GBR Uplink: 4672             kbps   GBR Downlink: 4672      kbps
                                           Signaling Indicator: 0
       Forwarding Class:  None         Loss Priority:  None
    Requested QoS Parameters:
       Traffic Class: Conversational      ARP: 1
       Traffic Handling Priority: 0       Transfer Delay: 10
       MBR Uplink  : 8640           kbps  MBR Downlink: 8640      kbps
       GBR Uplink  : 4672           kbps  GBR Downlink: 4672      kbps
                                           Signaling Indicator: 0
    Charging information:
       Charging ID: 0xb000000
       Profile ID: 0
    Rating group information:
       Rating group: 0 Service id: 0
```

show unified-edge ggsn-pgw subscribers traffic-class interactive traffic–handling-priority 1

```
user@host> show unified-edge ggsn-pgw subscribers traffic-class interactive
traffic–handling-priority 1
Gateway: PGW1

Subscriber Information:
  UE:
    IMSI: 324213213134030              IMEI: 1122334455667790
    MSISDN: 1926737867                 Time Zone: GMT     DST: None
    RAT Type: E-UTRAN
    User Location Info:
      MCC:  None   MNC: 180
      LAC: 0x22 CI: 0x0     SAC: 0x2b RAC: 0x0  TAC: 0x4  ECI: 0x0
  PDN Session:
    APN name: internet123
    IPv4 Address: 20.1.0.1             IPv6 Address: None
    GTP Version: 2                     Address Assignment: Local
    Local Control IP: 18.1.1.2         Remote Control IP: 30.1.1.2
    Local Control TEID: 0x14000000     Remote Control TEID: 0x113
    Peer CSID: 0                       Remote CSID: 0
    Selection mode: MS or network provided APN, subscription verified
    Session PIC: 0 /0  (FPC/PIC)       PFE: 5 /0  (FPC/PIC)
    Service PIC: None/None (FPC/PIC)
    Session State: Established         Session Duration: 10
    Roaming Status: Visitor            Serving network: MCC: 123  MNC: 567
    Direct Tunnel: None
    Negotiated APN AMBR: Downlink: 128 kbps        Uplink: 128  kbps
    Requested  APN AMBR: Downlink: 128 kbps        Uplink: 128  kbps
  Bearer:
    NSAPI/EBI: 5
    Local Data IP: 18.1.1.2            Remote Data IP: 30.1.1.2
```

```
Local Data TEID: 0x14140000        Remote Data TEID: 0x114
Bearer State: Established          Substate: None
Idle Timeout: 0   min              AAA Interim Interval: 0   min
Negotiated QoS Parameters:
   QCI: 5                          ARP: 2 /0 /0   (PL/PVI/PCI)
   Forwarding Class:  None         Loss Priority:  None
Requested QoS Parameters:
   QCI: 5                          ARP: 2 /0 /0   (PL/PVI/PCI)
Charging information:
   Charging ID: 0x14000000
   Profile ID: 0
   State: Init                     Previous State: Init
   Profile selection criteria: None
Offline charging information: Disabled
Rating group information:
   Rating group: 0 Service id: 0
   Action ID: 0x0                     Trigger profile: 0
   Change condition bitmask: 0x0      Action-id-bitmask: 0x0
   Signal bitmask: 0x0                Last signal bitmask: 0x0
   Last statistics info:
     Collection time: None collected
```


Copyright © 2012, Juniper Networks, Inc.

PART 4

Index

- Index on page 191

Copyright © 2012, Juniper Networks, Inc.

Index

Symbols

#, comments in configuration statements....xiii
( ), in syntax descriptions....xiii
< >, in syntax descriptions....xii
[ ], in configuration statements....xiii
{ }, in configuration statements....xiii
| (pipe), in syntax descriptions....xiii

A

aggregate maximum bit rate *See* AMBR
aggregated-qos-control statement
  CoS policy profiles....91
allocation and retention priority *See* ARP
allocation-retention-priority statement
  CoS policy profiles....92
AMBR
  configuring
    downlink....31, 39
    uplink....31, 39
  overview....8, 12
ARP....9
  in 3G networks....8
  in 4G networks....8
  overview....8
  See also preemption

B

background traffic class
  description....5, 6
bandwidth pools....10
  configuring....24
    APN level....10
    downlink....44
    system level....10, 44
    uplink....44
  See also overview
bearer load
  configuring
    in 3G/4G networks....26
bearers
  configuring maximum number
    APN level....23
    system level....23
  initial QoS level....4
  managing load....11
  maximum number, at system or APN level....11
  preempting....11
  rejecting based on
    maximum traffic class....12
  upgrading based on
    AMBR....31, 39
    MBR....34, 35, 40, 41
bearers-load statement
  resource threshold profiles....93
braces, in configuration statements....xiii
brackets
  angle, in syntax descriptions....xii
  square, in configuration statements....xiii
Broadband Gateway
  configuring
    QoS, overview....18
broadband gateway
  QoS configuration example....49

C

CAC
  bandwidth pools....10
  enforcing....10
  maximum bearers....11
  overview....10
  preemption, enabling....25
  resource thresholds....11
call admission control *See* CAC
class-of-service statement....96
classifier profiles
  configuring
    for 3G and 4G networks....27
classifier-profile statement
  local policies....94
classifier-profiles statement
  CoS-CAC....95
  QoS....95
comments, in configuration statements....xiii
configuration example
  for QoS....49
conventions
  text and syntax....xii

conversational traffic class
description....5, 6
CoS policy profile
AMBR in....12
configuring
in 3G networks....32
in 3G/4G networks....37
in 4G networks....29
GBR in....13
maximum QCI in....12
maximum traffic class in....12
MBR in....12
overview....12
policer actions....13
cos-cac statement....98
cos-policy-profile statement
local policies....101
cos-policy-profiles statement
CoS-CAC....102
CPU
managing load 11
CPU load
configuring
in 3G/4G networks....26
cpu statement
resource threshold profiles....104
curly braces, in configuration statements....xiii
customer support....xiii
contacting JTAC....xiii

D

default settings
preemption....18
resource thresholds 11, 12
default-bearer-qci statement
CoS policy profiles....105
description statement
cos-classifier-profiles....106
cos-policy-profilees....106
local-policies....106
resource-threshold-profiles....106
diffserv model
QoS support on broadband gateway....4
dl-bandwidth-pool statement
local policies....108
documentation
comments on....xiii
downgrade-gtp-v1-gbr-bearers statement
guaranteed bit rate bandwidth pools....107
DSCP marking
subscriber packets....46, 47
dscp statement
egress rewrite rules
class of service....111
ingress rewrite rules
class of service....112
dscp-ipv6 statement
egress rewrite rules
class of service....109
ingress rewrite rules
class of service....110

E

edit unified-edge gateways statement
hierarchy....87
egress rewrite rules
configuring....45
overview
overview....14
exceed-action policer
overview....14
exceed-action statement
QoS policer action
CoS policy profiles....113

F

font conventions....xii
forwarding-class statement
QoS Class Identifier....114

G

GBR
overview....5, 13
GBR bearers....10
See also bandwidth pools
gbr-bandwidth-pools statement
CoS-CAC....115
QoS....115
gbr-bearer statement
QoS policer action
CoS policy profiles....116
guaranteed bit rate *See* GBR
guaranteed-bit-rate-downlink statement
PDP QoS control
CoS policy profiles....117
guaranteed-bit-rate-uplink statement
PDP QoS control
CoS policy profiles....119

Copyright © 2012, Juniper Networks, Inc.

H

high statement
- resource threshold profiles....121

I

inet-precedence statement
- egress rewrite rules
  - class of service....122
- ingress rewrite rules
  - class of service....123

information element (IE)
- initial QoS level....4

ingress rewrite rules
- configuring....45
- overview
  - overview....14

ingress-rewrite-rules statement
- class of service....124

interactive traffic class
- description....5, 6

interfaces
- mobile
  - applying rewrite rules....46, 47

interfaces statement
- class ofservice....125

L

local policies
- specifying
  - bandwidth pools....44
  - classifier profiles....43
  - policy profiles....43
  - resource thresholds....43

local policies profile
- configuring....43

local policy
- applying
  - system level....44

local-policies statement....126

local-policy-profile statement
- Broadband Gateway....127

loss-priority statement
- QoS Class Identifier....128

low statement
- resource threshold profiles....129

LTE *See* networks

M

manuals
- comments on....xiii

maximum bearers
- configuring
  - APN level....23
  - system level....23

maximum bit rate *See* MBR

maximum QCI
- overview....12

maximum traffic class
- overview....12

maximum-bandwidth statement
- guaranteed bit rate bandwidth pools....130

maximum-bearers statement
- Broadband Gateway....131

maximum-bit-rate-downlink statement
- aggregated QoS control
  - CoS policy profiles....132
- PDP QoS control
  - CoS policy profiles....134

maximum-bit-rate-uplink statement
- aggregated QoS control
  - CoS policy profiles....136
- PDP QoS control
  - CoS policy profiles....138

MBR
- configuring
  - downlink....34, 35, 40, 41
  - uplink....34, 35, 40, 41
- configuring in traffic classes....43
- overview....5, 12

memory
- managing load 11

memory load
- configuring
  - in 3G/4G networks....27

memory statement
- resource threshold profiles....139

mif statement
- class of service....140

mobile interface
- applying rewrite rules....14

mobile interfaces
- applying egress rewrite rules....47
- applying ingress rewrite rules....46

Copyright © 2012, Juniper Networks, Inc.

N

networks
- 3G
  - ARP....4
  - classifying subscriber traffic....4
  - GBR....4
  - MBR....4
  - QoS parameters....4
- 4G
  - AMBR....7
  - ARP....7
  - classifying subscriber traffic....7
  - QoS parameters....7

non-gbr-bearer statement
- QoS policer action
  - CoS policy profiles....141

P

parentheses, in syntax descriptions....xiii
PCI flags....9
PDP contexts
- GBR....5
- initial QoS level....4
- MBR....5

pdp-qos-control statement
- CoS policy profiles....142

policer action
- configuring
  - overview....13

policer configuration
- exceed-action....14
- overview....13
- violate-action....13, 14

policer-action statement
- CoS policy profiles....143

preemption
- capability....9
  - enabling....25
- enabling....25
- overview....9
- PCI flags....9
- PVI flags....9
- vulnerability....9, 25

preemption statement
- GGSN or P-GW....144

protocol statement
- egress rewrite rules
  - class of service....145

PVI flags....9

Q

QCI
- overview....7

qci statement
- PDP QoS control
  - CoS policy profiles....146

QoS
- class identifiers....7
- configuration example....49
- configuring
  - local policies....43
- configuring on Broadband Gateway
  - overview....18
- Differentiated Services model....4
- initial level assigned to bearer....4
- local policy
  - applying at apn level....44
  - applying at system level....44
- monitoring....161
- NQN flags and upgrade behavior....17
- overview....3
- traffic classes....4
- upgrade flags and upgrade behavior....17

QoS Class Identifier *See* QCI

QoS classifier profiles
- configuring
  - 3G/4G networks....27

QoS profiles
- configuring
  - classifier profile....27
  - CoS policy profile....37
  - CoS policy profile, in 3G networks....29, 32
  - local policy....43
  - resource threshold profile....26

qos-class-identifier statement
- classifier profiles....147

Quality of service *See* QoS

R

rejecting
- maximum active bearers....23

resource threshold profiles
- configuring
  - in 3G/4G networks....26

Copyright © 2012, Juniper Networks, Inc.

resource thresholds
default settings....11
managing load
bearer....11
CPU....11
memory....11
overview....11
preempting bearers....11
resource-threshold-profile statement
local policies....149
resource-threshold-profiles statement
CoS-CAC....148
QoS....148
rewrite rules
default DSCP marking
....46, 47
egress
applying to mobile interfaces....47
configuring....45
overview....14
ingress
applying to mobile interfaces....46
configuring....45
overview....14
overview....14
rewrite-rules statement
class ofservice....150
roamer-classifier-profile statement
local policies....151
roamer-cos-policy-profile statement
local policies....152

S

show unified-edge ggsn-pgw statistics traffic-class command....164
show unified-edge ggsn-pgw status command....166
show unified-edge ggsn-pgw status preemption-list command....171
show unified-edge ggsn-pgw subscribers command....174
show unified-edge ggsn-pgw subscribers traffic-class command....186
streaming traffic class
description....5, 6
subscriber packets
DSCP marking on....46, 47
subscriber traffic
policing....13
support, technical *See* technical support
syntax conventions....xii

T

technical support
contacting JTAC....xiii
traffic classes
overview....4

U

ul-bandwidth-pool statement
local policies....153
UMTS *See* networks
unit statement
mobile interface
class of service....154

V

violate-action policer
overview....13, 14
violate-action statement
QoS policer action
CoS policy profiles....155
visitor-classifier-profile statement
local policies....156
visitor-cos-policy-profile statement
local policies....157

Copyright © 2012, Juniper Networks, Inc.

Copyright © 2012, Juniper Networks, Inc.