

Policy and Charging Enforcement Function (PCEF) for GGSN/PDN Gateway



Published: 2013-06-02

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

Copyright © 2013, 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.

Policy and Charging Enforcement Function (PCEF) for GGSN/PDN Gateway

Copyright © 2013, 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	PCEF Overview	3
	Policy and Charging Enforcement Function Overview	3
	Policy and Charging Control Rules Overview	5
	Understanding Service Data Flow Filters	5
	Policy and Charging Control	7
	PCC Rules Under Static Policy Control	8
	PCC Rules Under Dynamic Policy Control	8
	Static-Gx Rules	9
	Policing of Subscriber Traffic	9
	Application-Aware Policy and Charging Control Rules Overview	9
	Understanding Application-Aware PCEF Services on the Broadband Gateway	10
	Use Case for Application-Aware PCEF Service	10
	Junos OS Services Package Requirements for Application-Aware PCEF	11
	APPID Feature Overview	11
	Application Tracking (AppTrack)	12
	Custom Application Signatures	12
	Signature Groups	13
	Heuristics-Based Detection	14
	Nested Application Identification	14
	Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned	15
	Understanding How Rules Are Provisioned on the Gx Interface	15
	Provisioning of Dynamic Policies	15
	Provisioning of Predefined Static Policies	17
	Bearer Binding Overview	17

	Understanding Event Triggers	19
	Implicit Event Triggers	19
	Configurable PCEF-Enabled Event Triggers	19
	MobileNext Broadband Gateway Support for Session Management Procedures	20
Part 2	Configuration	
Chapter 2	Configuration Tasks	25
	Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic	25
	Configuring Service Data Flow Filters (Flow Identifiers)	27
	Configuring Policy and Charging Control Action Profiles	28
	Configuring Layer 3 and Layer 4 Policy and Charging Control Rules	30
	Configuring Application-Aware Policy and Charging Control Rules	31
	Configuring a Policy and Charging Control Rulebase	32
	Configuring Event Trigger Profiles	33
	Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies	34
	Configuring a Policy and Charging Enforcement Function Profile for Static Policies	36
Chapter 3	Configuration Examples	39
	Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules	39
	Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules	57
Chapter 4	Configuration Statements	87
	[edit unified-edge pcef] Hierarchy Level	87
	[edit services service-set] Hierarchy Level	89
	[edit services pcef] Hierarchy Level	89
	activate-dedicated-bearers	90
	af-charging-identifier	90
	allocation-retention-priority (PCC Action Profiles)	91
	application-function-record-info	91
	application-groups (PCC Rules)	92
	applications (PCC Rules)	93
	charging (PCC Action Profiles)	94
	charging-method (PCC Action Profiles)	95
	diameter-profile (Gx)	96
	direction (Service Data Flow Filters)	96
	dynamic-policy-control	97
	event-trigger-profile	98
	event-trigger-profiles	99
	failure-action	100
	failure-handling	101
	flow-descriptions	102
	flows	103
	from (PCC Rules)	104

	gate-status	105
	guaranteed-bit-rate	106
	local-port-range	107
	local-ports	108
	maximum-bit-rate	109
	measurement-method (PCC Action Profiles)	110
	nested-applications (PCC Rules)	111
	no-send-to-ue	112
	pcc-action-profile	112
	pcc-action-profiles	113
	pcc-rule	114
	pcc-rulebases (PCEF Profile)	115
	pcc-rulebases (PCEF)	116
	pcc-rules (PCEF Profile)	117
	pcc-rules (PCEF)	118
	pcef	119
	pcef (Services)	121
	pcef-profile (Service Set)	122
	preemption-capability	123
	preemption-vulnerability	124
	priority-level (PCC Action Profiles)	125
	profile (Services PCEF)	126
	profiles (PCEF)	127
	protocol (Flow Descriptions)	128
	qci (PCC Action Profiles)	129
	rating-group (PCC Action Profile)	129
	release (PCEF Profile)	130
	remote-address	131
	remote-port-range	132
	remote-ports	133
	service-identifier	134
	service-id-level-reporting	134
	session-failover-not-supported (PCEF Profiles)	135
	static-policy-control	136
	then (PCC Rules)	137
	traceoptions (PCEF)	138
Part 3	Administration	
Chapter 5	Operational Commands	143
	clear unified-edge ggsn-pgw subscribers bearer	144
	show unified-edge ggsn-pgw subscribers policy	145
Part 4	Troubleshooting	
Chapter 6	Acquiring Troubleshooting Information	151
	Tracing PCEF Operations	151

Part 5	Index	
	Index	155

List of Figures

Part 1	Overview	
Chapter 1	PCEF Overview	3
	Figure 1: Architecture for Policy and Charging Enforcement Function	4
	Figure 2: Service Data Flow Filtering of Downlink IP Packets	7
	Figure 3: Message Flow for Push Mode	16
	Figure 4: Message Flow for Pull Mode	17
Part 2	Configuration	
Chapter 3	Configuration Examples	39
	Figure 5: Architecture for Policy and Charging Enforcement Function	40
	Figure 6: Architecture for Policy and Charging Enforcement Function	58

List of Tables

About the Documentation	xi
Table 1: Notice Icons	xii
Table 2: Text and Syntax Conventions	xii

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
- MX960
- MX480

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: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</code>

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 <i>(string1 string2 string3)</i>
# (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]
Indentation 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.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu 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>.

PART 1

Overview

- [PCEF Overview on page 3](#)

CHAPTER 1

PCEF Overview

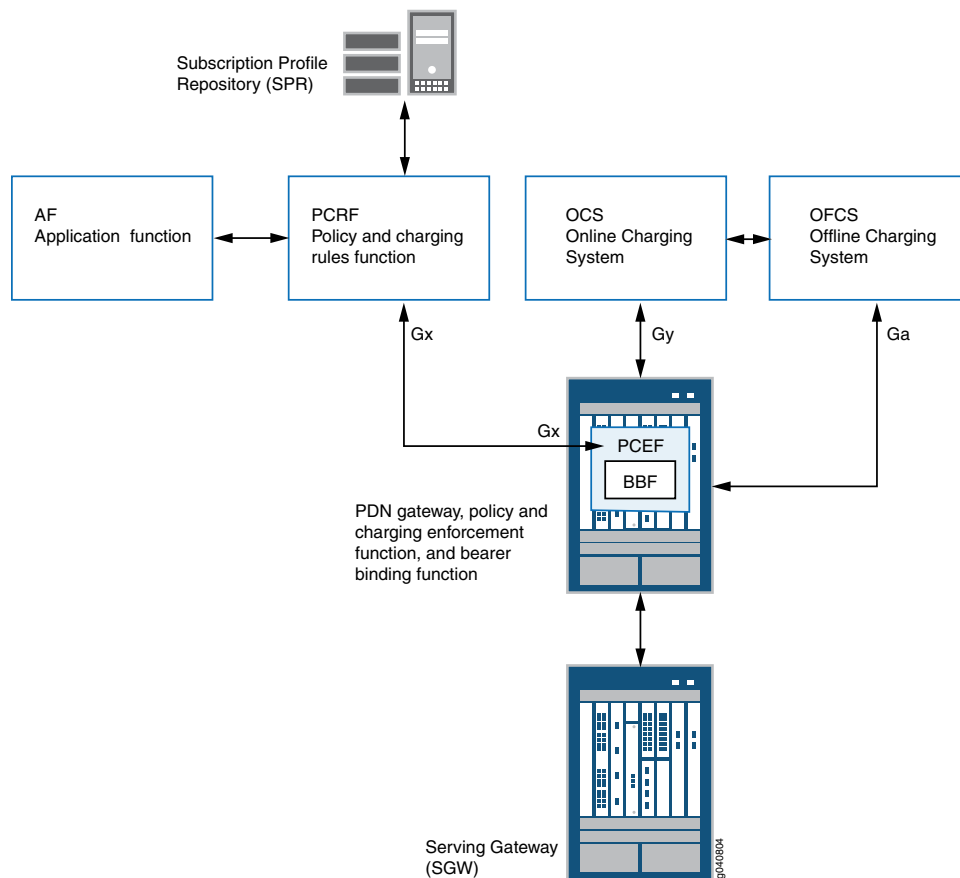
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Policy and Charging Control Rules Overview on page 5](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [APPID Feature Overview on page 11](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [Bearer Binding Overview on page 17](#)
- [Understanding Event Triggers on page 19](#)
- [MobileNext Broadband Gateway Support for Session Management Procedures on page 20](#)

Policy and Charging Enforcement Function Overview

The policy and charging enforcement function (PCEF) enforces policy decisions that are received from the policy and charging rules function (PCRF) and provides the PCRF with subscriber and access information over the Gx interface, which connects the PCEF and the PCRF. For dynamic policies, the PCEF can also act upon the messages received from the PCRF to install, modify, or remove Policy and Charging Control (PCC) rules. For static policies, the PCEF enforces policy decisions with no interaction from the PCRF and no Gx interface support.

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. The PCEF interacts with the internal charging function, which, in turn, interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS). [Figure 1 on page 4](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging.

Figure 1: Architecture for Policy and Charging Enforcement Function



A PCEF configuration on the MobileNext Broadband Gateway comprises the following filters, rules, and profiles:

- Service data flow filters—Provides detection of IP flows based on source IP, destination IP, source port, destination port, Layer 4 protocol (UDP and TCP), applications (for example, BitTorrent and HTTP), and nested applications (for example, YouTube and Facebook). A service data flow filter is specified in the **from** clause of the PCC rules to detect uplink service flows, downlink service flows, or both.
- PCC action profile—Defines the QoS, charging, and gating controls to apply to a bearer. A PCC action profile is specified in the **then** clause of the PCC rule.
- PCC rules—Defines the QoS, charging, and gating control for specified traffic flows between the Packet Data Network Gateway (P-GW) and the user equipment (UE). A PCC rules configuration includes service data flow filters and a PCC action profile.
- (Optional) PCC rulebase—Defines a group of PCC rules, each of which are assigned a precedence for specified traffic flows between the P-GW and the user equipment (UE).
- (Optional) Event-trigger profile—Provides event notification to the PCRF when an event-trigger event occurs on the network, such as radio access technology (RAT)

change, or Serving Gateway Support Node (SGSN) change. An event-trigger profile can be configured in the PCEF profile with dynamic policy control.

- PCEF profile—Defines either static policies or dynamic policies. A PCEF profile configured with static policy control requires predefined PCC rules, PCC rulebases, or both. A PCEF profile configured with dynamic policy control requires a Diameter Gx profile and, optionally, event-trigger profiles and predefined PCC rules, PCC rulebases, or both.

**Related
Documentation**

- [Policy and Charging Control Rules Overview on page 5](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [Understanding Event Triggers on page 19](#)

Policy and Charging Control Rules Overview

In the Policy and Charging Control (PCC) architecture, the policy and charging rule function (PCRF) is the central entity that makes policy and charging decisions based on input from different sources, including mobile operator configuration, user subscription information, services information, and so forth. The PCC decisions are then communicated to the policy and charging enforcement function in the form of PCC rules, which contain service data flow (SDF) information that allows identification of IP traffic, charging parameters that are used to charge this traffic, and quality-of-service (QoS) parameters to be applied to the IP traffic that the SDF filters identify. PCC rules can also be statically configured in the PCEF and then dynamically referenced by the PCRF through the Gx interface.

This topic includes the following sections:

- [Understanding Service Data Flow Filters on page 5](#)
- [Policy and Charging Control on page 7](#)
- [PCC Rules Under Static Policy Control on page 8](#)
- [PCC Rules Under Dynamic Policy Control on page 8](#)
- [Static-Gx Rules on page 9](#)
- [Policing of Subscriber Traffic on page 9](#)

Understanding Service Data Flow Filters

Service data flow (SDF) filters (flow identifiers) are configured in PCC rules to classify IP packets to a service data flow. SDF filters in the PCC rules enforce transport of uplink and downlink IP flows in the appropriate IP CAN bearer. If the IP packet matches the SDF filter, and the gate of the corresponding rule is open, the packet is forwarded to its destination.

To configure Layer 3 or Layer 4 SDF filters, you specify one or more of the following parameters to detect IP packet flows:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 4 protocol (UDP or TCP)

To configure application-aware SDF filters, you can specify one or more of the following parameters to detect IP packet flows:

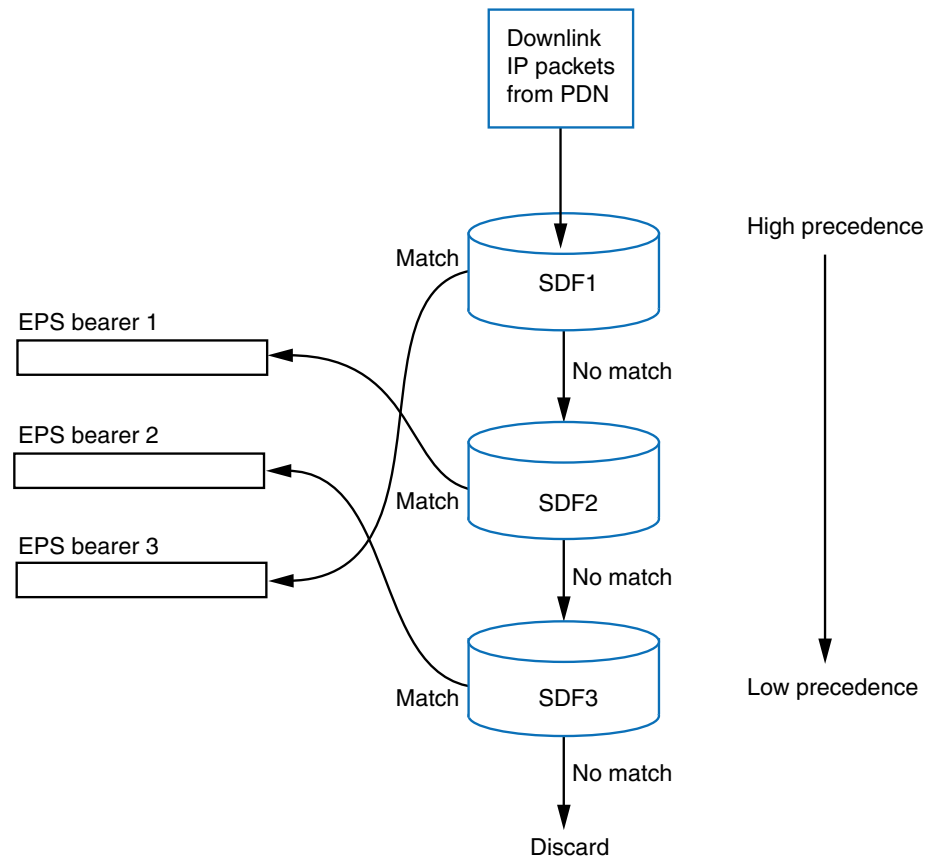
- application—Specifies the name of an application, for example, HTTP.
- nested-application—Specifies encapsulated application types (with different application signatures) that are running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but to identify them as two different applications, the application layer is divided into two layers: Layer 7 applications and Layer 7 protocols.
- application-group—Specifies the name of an application group, which can be used to process a number of applications or subgroups at the same time.



NOTE: Application-aware PCC rules that reference specified applications can include wildcard or specific Layer-3 SDF filters, Layer-4 SDF filters, or both.

All IP packets that match an SDF filter (flow identifier, application, nested-application, or application-group) are designated a service data flow. [Figure 2 on page 7](#) shows the process by which the configured SDF filters direct IP packets to an appropriate bearer.

Figure 2: Service Data Flow Filtering of Downlink IP Packets



SDF filters are evaluated in order of precedence assigned to the PCC rules within the session. For example, when multiple rules are associated with a bearer, the SDF filters in PCC rules of higher precedence are evaluated prior to the SDF filters in PCC rules of a lower precedence.



NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

Policy and Charging Control

A PCC rule configuration includes an action profile that defines the quality-of-service (QoS), charging, and gating control to apply to a service data flow. A PCC action profile can be configured and used in one or more PCC rules to provide the following functionality:

- **QoS control**—Allows the PCRF to specify the QoS treatment for an SDF. QoS can include QoS Class Identifier (QCI), allocation retention priority (ARP), maximum bit rate (MBR), guaranteed bit rate (GBR), and preemption vulnerability or capability. The PCEF enforces the QoS control by establishing or modifying bearers and enforcing bit rates for service sessions.
- **Charging control**—The PCRF determines whether online or offline charging is appropriate for a given service session. The PCEF, in turn, enforces that decision by interacting with the charging systems and collecting charging data. The PCRF also controls the measurement method (volume, duration, volume/duration, or event-based) to use.
- **Gating status**—Specifies whether IP packets associated with an SDF should be blocked or allowed. The PCEF allows or blocks IP packets associated with an SDF to ensure that the SDF does not violate the authorized QoS. The PCRF makes the gating decisions (open or closed), which the PCEF enforces on a per SDF basis.

PCC Rules Under Static Policy Control

Static PCC rules (policies) are provisioned by the PCEF with no interaction from the PCRF and no Gx interface support. Static policies can be predefined on the MobileNext Broadband Gateway and are activated by the PCEF when a PCEF profile is applied to an APN or service-selection profile.

PCC Rules Under Dynamic Policy Control

Dynamic PCC rules are provisioned by the PCRF to the PCEF and are carried over the Gx interface using Diameter AVPs. The PCRF is central in making policy and charging control decisions and can activate, modify, or deactivate a dynamic rule at any time. The PCRF can provision the complete PCC rules or provision the name of predefined rules (static-Gx policies).

The PCRF can make its policy and charging control decisions based different sources, including:

- Subscription information for a UE that is received from the SPR
- Operator configuration in the PCRF
- Information from the access network about the access technology

The broadband gateway supports the following operations for dynamic PCC rules:

- **Install or modify**—The **Charging-Rule-Install** AVP is used to install a PCC rule that is not already installed or modify an existing rule on the broadband gateway.
- **Remove**—The **Charging-Rule-Remove** AVP is used to remove a PCC rule that is already installed.

The containers for the PCC rules are named **Charging-Rule-Definition**. Multiple **Charging-Rule-Definition** containers can be sent within a **Charging-Rule-Install** or **Charging-Rule-Remove**, each of which is applied per bearer.

Static-Gx Rules

Static Gx PCC rules are configured on the PCEF but provisioned by the PCRF over the Gx interface using Diameter AVPs. The PCRF provides the name of the local PCC rule or group of PCC rules to be activated or deactivated. The broadband gateway supports the following operations for static Gx rules:

- Install or modify—**Charging-Rule-Install** AVP is used to install a PCC rule that has not been installed or modify an existing rule on the broadband gateway.
- Remove—**Charging-Rule-Remove** AVP is used to remove a PCC rule that is already installed.

Policing of Subscriber Traffic

For 3G and 4G GBR bearers, the maximum bit rate (MBR) and guaranteed bit rate (GBR) is applied per PCC rule.

For non-GBR bearers, the following behavior applies:

- For 3G Release 9 and 4G subscriber traffic, all non-GBR bearers associated with a session share the APN-AMBR value, which defines the total bit rate that is allowed for all non-GBR bearers associated with an APN.
- For 3G pre-Release 9 subscriber traffic, a specific QoS is associated with a bearer, and policing is performed at the bearer level.

Related Documentation

- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Understanding Event Triggers on page 19](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)

Application-Aware Policy and Charging Control Rules Overview

The policy and charging enforcement function (PCEF) supports Layer 3 and Layer 4 policy and charging control (PCC) rules as well as application-aware PCC rules that use deep packet inspection (DPI) to support policies for Layer 7 and higher-layer application traffic. For application-aware PCC rules, the PCRF can only refer PCC rules or rulebases (static Gx policies) that are statically configured on the MobileNext Broadband Gateway.

This topic covers:

- [Understanding Application-Aware PCEF Services on the Broadband Gateway on page 10](#)
- [Use Case for Application-Aware PCEF Service on page 10](#)
- [Junos OS Services Package Requirements for Application-Aware PCEF on page 11](#)

Understanding Application-Aware PCEF Services on the Broadband Gateway

To enforce Layer 3 and Layer 4 PCC rules, the Packet Forwarding Engine inspects uplink and downlink subscriber traffic on an access point name (APN). To enforce application-aware PCC rules, the policy and charging enforcement function (PCEF) is applied as a service on the APN (MIF interface) to indicate to the Packet Forwarding Engine that traffic should be directed to the Junos OS services PIC that hosts the PCEF service. When subscriber traffic is redirected to the services PIC, processing is completed and the appropriate policies are applied as a service on the MIF interface associated with an APN.

At the Junos OS services PIC, the application-identification engine inspects traffic to match against a database of application signatures, which are either imported from a Juniper intranet or extranet server or are configured from the command-line interface (CLI). An application signature typically identifies a unique type of application, for example, YouTube video, or a set of applications, for example, streaming audio.

The PCEF service takes information provided by the application-identification engine and retrieves the database of PCC rules to determine the appropriate policies and charging actions to apply to the specified application-aware traffic flow.

An application-aware service set must be configured (and applied on the APN interface) to link the application-identification engine and PCEF service together. For this release, a PCEF (services) profile includes no configurable attributes; however, to reference the PCEF service in a service set, you must configure the PCEF profile.

For mobile subscribers, the Packet Forwarding Engine handles GPRS Tunneling Protocol (GTP) encapsulation and decapsulation even when subscriber traffic might require processing by an application-aware service. In the uplink (Gn to Gi) direction, decapsulated subscriber traffic is sent to the services PIC. In the downlink (Gi to Gn) direction, the incoming Internet traffic is sent to the services PIC, and after the PCEF service, is redirected to the Packet Forwarding Engine for GTP encapsulation towards a Serving Gateway Support Node (SGSN) or Serving Gateway (SGW).

Use Case for Application-Aware PCEF Service

An application-aware PCEF service supports both online and offline charging, based on the application signatures. For example, you might configure an application-aware PCEF service to define different Internet walled-garden server URLs in the application-identification engine, and assign these URL signatures to different PCC rules to provide differentiated charging.

The following steps outline how an operator might configure an application-aware PCEF service to provide free access to social networking sites during off-peak hours:

- Define the URL signatures for the targeted social networking sites.
- Define the PCC rules by specifying different rating groups for these URL signatures.
- The Junos OS PCEF service reports charging data for traffic that matches the URL signatures to the internal charging system.

- The Junos OS PCEF service reports charging data for traffic that matches the URL signatures to the internal charging system.
- The internal charging system interacts with the Online Charging System (OCS) or Offline Charging System (OFCS) depending on the characteristics of the rating group.
- Operator billing infrastructure uses this rating group to bypass or apply a different billing rate to the subscriber traffic that is reported for the particular rating group.



NOTE: The Layer 3 or Layer 4 based PCEF on the Packet Forwarding Engine does not account for traffic that is redirected to the Junos OS services plane for application-aware inspection, so subscriber traffic is protected from being double accounted for both a Layer 3 or Layer 4 rule and application-aware rule or rating group.

Junos OS Services Package Requirements for Application-Aware PCEF

To provide application-aware policy enforcement on the network, the MobileNext Broadband Gateway uses the following services packages to perform deep packet inspection (DPI) on the Junos OS services plane (services PIC):

- `jservices-appid`—The application-identification engine on the SRX Series or MX Series platform, which inspects and detects application traffic.
- `jservices-mss`—The mobile subscriber services package on the MX platform, which provides mobile subscriber awareness and user equipment (UE) session information to the Junos OS services plane.
- `jservices-pcef`—The PCEF service package, which provides application-aware PCEF.

Related Documentation

- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [APPID Feature Overview on page 11](#)

APPID Feature Overview

The APPID (application identification) feature is a Junos OS feature that identifies applications as constituents of application groups in TCP/UDP/ICMP traffic.

The MobileNext Broadband Gateway supports the following APPID features:

- [Application Tracking \(AppTrack\) on page 12](#)
- [Custom Application Signatures on page 12](#)
- [Signature Groups on page 13](#)
- [Heuristics-Based Detection on page 14](#)
- [Nested Application Identification on page 14](#)

Application Tracking (AppTrack)

Juniper Networks provides predefined application signatures that detect TCP and UDP applications running on non-standard ports. Identifying these applications provides data for application tracking (AppTrack). A PCC rule that includes application-aware SDF filters also uses the application data to perform actions (charging, blocking, rate-limiting, redirecting) on the application traffic.



NOTE: The broadband gateway does not support Application Firewall (AppFw), Application QoS (AppQoS), Application DDoD, or Intrusion Detect Prevention (IDP).

Juniper Networks provides frequent updates to the predefined application signature package database and makes these updates available to subscribers on the Juniper Networks website. This package includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, quality of service prioritization, and IDP. The application signature package database contains application objects such as FTP and DNS as well as nested applications that operate over an HTTP protocol, such as Facebook, Kazaa, and instant messenger programs.

Before you configure application identification, application firewall policy, or AppTrack, you must download and install the application signature package, which is included in the default IDP installation and does not need to be downloaded separately.

If you do not plan to use application identification, you can execute the following commands to extract the application portion of the IDP signature database and install it as the application signature database:

- **request services application-identification download**
- **request services application-identification install**

Custom Application Signatures

Application identification supports user-defined custom application signatures, nested application signatures, and signature groups. Custom application signatures are unique to your environment and are not part of the predefined application package. When you update or uninstall the application package, the custom signatures and signature groups are not modified or removed.



NOTE: The uninstall operation will fail if any active security policies, custom application signatures, or signature groups reference predefined application signatures or signature groups in the Junos OS configuration.

To create custom application signatures, use the CLI to specify a name, the protocol and port where the application runs, the signature pattern, and match criteria. For ease of

use, copy a similar predefined application signature or group, and modify the characteristics so that it identifies the unique application running in your environment.

You can view application signatures and application signature groups by using the **show services application-identification application** and **show services application-identification group** commands.

You can copy a predefined application signature or signature group to use as a model by entering the **request services application-identification application copy** or the **request services application-identification group copy** command. With this command, your copy is automatically named by replacing the “junos” prefix with the prefix “my”. (The “junos” prefix is reserved for predefined application signatures and groups.) You can copy the same predefined application signature and signature group only once. Duplicate custom signatures and groups are not allowed. Rename your custom application signature or signature group to a unique name appropriate to your environment.

For additional information about MobileNext Broadband Gateway support for signature groups, see [Understanding Application Grouping for Junos OS Application Identification](#).

Signature Groups

In Junos OS, application grouping lets you group multiple applications under a single name to improve accuracy and consistency in policy definition. Both predefined and user-defined applications can be grouped together.

The hierarchy of application groups resembles a tree structure with associated applications as the leaf nodes. The group any refers to the root node. The group unassigned is always situated one level from the root and initially contains all applications. When a group is defined, applications are assigned from the unassigned group to the new group. When a group is deleted, its applications are moved back to the unassigned group

Applications can be assigned to a group or can remain unassigned, but they cannot be assigned to more than one group. There is no specific limitation on the number of applications assigned to a single group or on the number of application groups that can be configured for a device.

All predefined application groups have the prefix “junos” in the application group name to prevent naming conflicts with custom application groups. You cannot modify the list of applications within a predefined application group. However, you can copy a predefined application group to use it as a template for creating a custom application group.

To customize a predefined application group you must first disable the predefined group. Note that a disabled predefined application group remains disabled after an application database update. You can then use the operational command **request services application-identification group** to copy the disabled predefined application group. The copied group is placed in the configuration file, and the prefix “junos” is changed to “my”. At this point, you can modify the list of applications in “my” application group and rename the group with a unique name.

To reassign an application from one custom group to another, you must remove the application from its current custom application group, and then reassign it to the other.

See the *Junos OS CLI Reference* for information about using the **request services application-identification** commands.

Heuristics-Based Detection

Peer-to-peer applications such as Skype contain encrypted data packets. The SRX devices cannot identify the encrypted data packets with the current application signatures, which are based on regular expression patterns. Heuristics are used to detect such traffic and to improve the detection rate. To enable detection of encrypted peer-to-peer applications, you can use the following command:

```
set services application-identification enable-heuristics
```

Junos OS detects encrypted peer-to-peer traffic on TCP and UDP.

If a session cannot be identified as known encrypted peer-to-peer traffic, you can assign the session to a special application named *junos:unspecified-encrypted*. Application firewall can configure a policy on the application that is similar to other dynamic applications.

Nested Application Identification

Greater use of application protocol encapsulation requires support for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. In order to do this, the current application identification layer is split into two layers: Layer 7 nested applications and Layer 7 protocols.

The included predefined application signatures are created to detect the Layer 7 nested applications, whereas the existing Layer 7 protocol signatures, such as FTP and HTTP, still function in the same manner. You can use these predefined application signatures in attack objects.

The nested application identification module detects nested applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS).

Application identification can also extract the server name information or the server certification from the TLS or SSL sessions.

Related Documentation

- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25](#)

Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned

Located between the policy and charging rules function (PCRF) and policy control enforcement function (PCEF), the Gx interface is used to provision or remove Policy and Charging Control (PCC) rules from the PCRF to the PCEF, and provide notification of traffic-plane events from the PCEF to the PCRF.

This topic includes the following sections:

- [Understanding How Rules Are Provisioned on the Gx Interface on page 15](#)
- [Provisioning of Dynamic Policies on page 15](#)
- [Provisioning of Predefined Static Policies on page 17](#)

Understanding How Rules Are Provisioned on the Gx Interface

The Gx interface provides charging and policy control by applying attribute-value pairs (AVPs) relevant to the application.

The PCRF collects and compares subscriber and application data, authorizes quality-of-service resources, and provides instructions (the PCC rules) for transporting subscriber traffic, as follows:

1. To determine the policy decisions that form the policy rules, the PCRF evaluates session information, subscription data for user equipment (UE) from the Subscription Profile Repository (SPR), operator-defined service policies, and other information from the access network about the access technology.
2. The PCRF sends the PCC rules (either the rules or name of the rules) to the PCEF, which enforces policy decisions based on the rules that are received.



NOTE: If the PCC rules indicate that online charging will apply, the PCEF notifies the Online Charging System (OCS), via the Gy interface, and requests credit based on the measurement method that the PCC rules specifies. If the PCC rules indicate that offline charging will apply, the PCEF notifies the internal charging module, which will collect usage data that is then forwarded to the Offline Charging System (OFCS).

3. The PCEF installs the PCC rules and performs bearer binding to ensure that the traffic for this service receives the required QoS and charging treatment. Bearer operations (session modifications) might require a Create Bearer request or Modify Bearer request.
4. Data is transported across the network, and the PCEF performs service data flow (SDF) detection to detect the IP flow for this service.

Provisioning of Dynamic Policies

Dynamic policies include both *dynamic* policies, which are provisioned by the PCRF to the PCEF, and are carried over the Gx interface, and *static* Gx policies, which are predefined

rules (configured on the PCEF) that are dynamically controlled (activated and deactivated) by the PCRF. The PCRF is central in making Policy and Charging Control (PCC) decisions and can activate, modify, or deactivate a dynamic rule at any time.

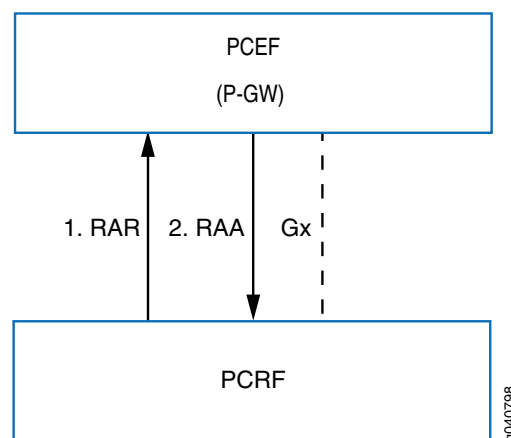


NOTE: The P-GW gives precedence to dynamic policies sent by the PCRF over static (predefined) policies that are configured on the PCEF.

The PCRF uses one of the following procedures to specify the PCC rules that the PCEF will apply:

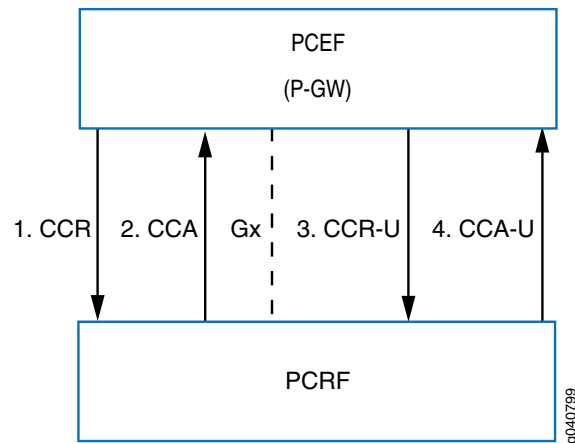
- **Push mode**—Applies when the PCRF decides to provision PCC rules without obtaining a request from the PCEF. The PCRF sends a Re-Authorization Request (RAR) to the PCEF based on information sent to the PCRF via the Rx interface or in response to a trigger within the PCRF. Because the PCC rules were not requested by the PCEF, the PCRF includes these PCC rules in a RAR message, and no Credit Control Request (CCR) or Credit Control Answer (CCA) messages are triggered by the RAR. [Figure 3 on page 16](#) shows the message flow for a push procedure.

Figure 3: Message Flow for Push Mode



- **Pull mode**—Applies when the PCEF requests PCC rules from the PCRF. The PCEF sends a Credit Control Request (CCR) message for PCC rules to the PCRF, and the PCRF provisions the appropriate PCC rules in the Credit Control Answer (CCA). [Figure 4 on page 17](#) shows the message flow for a pull procedure.

Figure 4: Message Flow for Pull Mode



A pull procedure is initiated during IP Connectivity Access Network (IP-CAN) session establishment (CCR-Init) or IP-CAN session modification (CCR-Update).

An IP-CAN session modification is initiated under the following conditions:

- A new IP-CAN bearer is being established, modified, or terminated.
- UE-initiated resource modification bearer is being established, modified, or terminated.
- An event-trigger event occurs, such as Radio Access Technology (RAT) change.

Provisioning of Predefined Static Policies

Static PCC rules are predefined rules that are provisioned by the PCEF with no interaction from the PCRF and no Gx interface support. Because a static policy is not controlled by the PCRF, a static policy is typically applied to all subscriber traffic on a given APN, and activated or deactivated locally on the P-GW.

- Related Documentation**
- [Policy and Charging Control Rules Overview on page 5](#)
 - [Understanding Event Triggers on page 19](#)

Bearer Binding Overview

Bearer binding refers to the association between a bearer and the Policy and Charging Control (PCC) rules. To ensure that subscriber packets receive the appropriate quality of service (QoS), charging, and gating control, a PCC rule is mapped to a corresponding bearer in the access network. Bearer binding is performed by the policy and charging enforcement function (PCEF).

When the policy and charging rules function (PCRF) provides details about the active PCC rules to the PCEF, the PCEF determines if an existing bearer in the access network can be used. If no bearer exists with the corresponding combination of QoS Class Identifier

(QCI) and allocation retention priority (ARP) values specified in the PCC rules, then the PCEF initiates the creation of new bearers.



NOTE: The ARP value specifies the priority level, preemption-vulnerability, and preemption-capability, so if the combination of ARP values specified in the PCC rules is not also specified in an existing bearer (with the same QCI) on the access network, a new bearer is installed or activated with the same QCI and ARP values.



NOTE: To provide a match with an application-aware PCC rule, the PCEF service must defer bearer binding until the HTTP (or relevant application layer) subscriber packets are detected on the service data flow. However, after the match is completed and the traffic is mapped to a dedicated bearer, the service data flow cannot be remapped to a different dedicated bearer.

The bearer binding function can trigger any combination of the following bearer requests:

- Create bearer requests—Triggered when a PCC rule arrives with unique QCI/ARP values (no existing bearer in the session has the same combination of QCI/ARP values).
- Update bearer requests can be triggered when the following changes occur:
 - Traffic flow template for the bearer has changed (SDF filters are added or removed).
 - Precedence for PCC rules has changed.
 - APN-AMBR is updated.
 - MBR/GBR values of a GBR bearer are modified.
- Delete bearer requests—Triggered when all PCC rules associated with a dedicated bearer are deleted.

**Related
Documentation**

- [Policy and Charging Control Rules Overview on page 5](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Understanding Event Triggers on page 19](#)

Understanding Event Triggers

You can configure event triggers on the policy and charging enforcement function (PCEF) so that the PCEF notifies the policy and charging rules function (PCRF) about changes in the access network. By default, the PCEF enables any event triggers that are received from the PCRF in a Credit Control Answer (CCA) or Re-Authorization Request (RAR) message. When you configure event triggers on the PCEF, the PCEF adds these PCEF configured event triggers to the PCRF provisioned event triggers.

When an event occurs that matches an event trigger configured on the PCEF or provisioned from the PCRF, the PCEF reports the event to the PCRF. In some circumstances, the PCRF might require information from the P-GW/GGSN or PCEF in order to make a policy decision, for example, when the access technology in use by the user equipment (UE) changes, or a subscriber leaves the home network and is roaming, or the authorized guaranteed bit rate (GBR) cannot be supported over the radio link.

The PCEF also supports the unconditional (implicit) event triggers, in which the PCEF unconditionally reports certain events to PCRF without any need for configuration of the event triggers on the PCEF or receipt of event triggers from the PCRF) in a Credit Control Answer (CCA) or Re-Auth Request (RAR) message.

This topic includes the following sections:

- [Implicit Event Triggers on page 19](#)
- [Configurable PCEF-Enabled Event Triggers on page 19](#)

Implicit Event Triggers

Implicit event triggers define the events that the PCEF must report to the PCRF, even though the PCRF does not explicitly subscribe to these events.

The MobileNext Broadband Gateway includes the following implicit event triggers:

- QOS_CHANGE
- LOSS_OF_BEARER
- RECOVERY_OF_BEARER
- DEFAULT_EPS_BEARER_QOS_CHANGE

Configurable PCEF-Enabled Event Triggers

To configure event triggers that identify the events that the PCEF must report to the PCRF, you must explicitly include the event triggers in an event-trigger profile. The following event triggers can be configured on the PCEF:

- IP_CAN_CHANGE
- PLMN_CHANGE
- RAT_CHANGE

- **RAI_CHANGE**
- **SSGN_CHANGE**
- **TFT_CHANGE**
- **UE_TIMEZONE_CHANGE**
- **USER_LOCATION_CHANGE**

**Related
Documentation**

- [Configuring Event Trigger Profiles on page 33](#)
- [Policy and Charging Control Rules Overview on page 5](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)

MobileNext Broadband Gateway Support for Session Management Procedures

The PGW/policy and charging enforcement function (PCEF) supports the following subset of session management procedures, as defined in the 3GPP technical specification 23.40, Section 5.4:

- IP-Can Session Initiation
- IP-Can Session Termination: UE Initiated
- IP-Can Session Termination: PCRF Initiated
- IP-Can Session Termination: PCEF Initiated
- IP-Can Session Modification: UE/MME Initiated Bearer Deletion
- IP-Can Session Modification: HSS Initiated Bearer Update
- IP-Can Session Modification: UE/HSS Initiated Bearer Update
- Network Initiated IP-Can Session Modification: Bearer Activation
- Network Initiated IP-Can Session Modification: Bearer Deactivation
- Network Initiated IP-Can Session Modification: Bearer Update
- Network Initiated IP-Can Session Modification: Failure 1
- Network Initiated IP-Can Session Modification: Failure 2
- RAR/CCA Leading to Multiple Bearer Operations
- Network Initiated Secondary PDP Context Creation for GTPv1
- Network Initiated Update PDP Context Request for GTPv1
- Network Initiated Delete PDP Context Request for GTPv1
- RAR/CCA leading to multiple PDP Context operations for GTPv1
- Handover from SGW to Gn/Gp SGSN
- Handover from Gn/Gp SGSN to SGW

The P-GW/PCEF does not support the following session management procedures:

- IP-Can Session Modification: UE Initiated Bearer Creation
- UE Initiated Bearer Resource Command Failure
- UE Initiated Secondary PDP Context Creation for GTPv1
- UE Initiated Update PDP Context Request for GTPv1
- UE Initiated Delete PDP Context Request for GTPv1

**Related
Documentation**

- [Policy and Charging Control Rules Overview on page 5](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)

PART 2

Configuration

- [Configuration Tasks on page 25](#)
- [Configuration Examples on page 39](#)
- [Configuration Statements on page 87](#)

CHAPTER 2

Configuration Tasks

- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25](#)
- [Configuring Service Data Flow Filters \(Flow Identifiers\) on page 27](#)
- [Configuring Policy and Charging Control Action Profiles on page 28](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)
- [Configuring Application-Aware Policy and Charging Control Rules on page 31](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)
- [Configuring Event Trigger Profiles on page 33](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36](#)

Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic

The MobileNext Broadband Gateway supports application-aware service data flows (SDFs) in Policy and Charging Control (PCC) rules to inspect traffic for mobile subscribers accessing Web-based services. Before you configure application-aware PCC rules, you must configure a PCEF profile as a service for an access point name (APN) so that all traffic flowing through the APN is inspected for application-aware based charging and policy enforcement.

Before you configure a PCEF profile as a service for a broadband gateway APN, complete the following tasks:

- Configure the chassis of the broadband gateway
- Configure the interfaces of the broadband gateway
- Configure the Packet Data Network Gateway (P-GW) parameters for the broadband gateway
- Configure the APN parameters for the specific APN
- Configure an application identification profile

For information about configuring application profiles, see [Configuring Application Profiles](#) in the Junos OS Application Identification feature documentation.

If the PCEF service interface configured is in the form **amsn**, then per-subscriber load balancing is performed. If the PCEF service interface configured is in the form **msn**, then no load balancing (or redundancy) is performed. In either case, the **interface** statement at the **system** hierarchy level of the P-GW is required for all subscriber-aware services because the subscriber is anchored on the services PIC interface.

To configure an application-aware PCEF service for an APN:

1. Configure a services PIC for the PCEF service.

```
[edit unified-edge gateways ggsn-pgw MBG1 system]
user@host# set service-pics interface ams0
```

2. Configure the PCEF profile by specifying a name for the PCEF profile.

```
[edit services pcef]
user@host# edit profile profile-name
```



NOTE: In this release, the PCEF profile is a placeholder profile with no configuration options, but must be created to provide future compatibility for PCEF services.

3. Define a service to use as an application-aware PCEF service.

```
[edit services service-set pcef-service-1]
user@host# set tcp-mss 1300
user@host# set service-set-options subscriber-awareness
user@host# set pcef-profile profile-name
user@host# set application-identification app-id-profile-name
user@host# set interface-service service-interface ams0
```

4. Apply the PCEF application-aware service to the mobile interface for the APN for both ingress and egress traffic so that all traffic arriving on the APN is inspected for application-based charging and policy.

```
[edit interfaces mif unit 0 family inet service]
user@host# set input service-set pcef-service-1
user@host# set output service-set pcef-service-1
```

5. Configure a Deep Packet Inspection (DPI) filter for application-aware traffic.

```
user@host# edit firewall family inet service-filter dpi-filter-1
user@host# set term dpi-flow from redirect-reason dpi
user@host# set term dpi-flow then service
```

6. Apply the DPI filter so that only application-aware traffic is forwarded to the services PIC.

```
[edit interfaces mif unit 5]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service service-filter dpi-filter-1
user@host# set family inet service output service-set dpi-service service-filter dpi-filter-1
```


7. Include the `jservice-appid`, `jservice-pcef`, and `jservice-mss` packages with the services PIC configuration.

```
[edit chassis fpc 3 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
```

**Related
Documentation**

- [Configuring Application-Aware Policy and Charging Control Rules on page 31](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)

Configuring Service Data Flow Filters (Flow Identifiers)

A service data flow (SDF) filter configured at `[edit unified-edge pcef flow-descriptions flow-identifier]` hierarchy level specifies one or more IP packet parameters (source IP, destination IP, source port, destination port, and protocol type) that the policy and charging enforcement function (PCEF) uses to detect IP packets that belong to a specific service session. An SDF filter configured as a flow identifier comprises all the IP packets that match the SDF filter.

A service data flow filter is specified in the **from** clause of a Policy and Charging Control (PCC) rules configuration.



NOTE: If you configure a flow identifier SDF for a remote-address, port, port-range, or protocol without specifying a corresponding value, then any value for the SDF filter type is accepted.

To configure Layer 3 and Layer 4 SDF filters:

1. Specify a name for the flow identifier that you want to configure to detect IP packets for a service data flow.

```
[edit unified-edge pcef]
user@host# set flow-descriptions flow-identifier
```

2. Specify the flow direction for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set direction (uplink | downlink | both)
```

3. Specify an IPv4 subnet for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set remote-address ipv4-address 10.11.12.14/32
```

4. Specify an IPv6 subnet for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set remote-address ipv6-address 2000:1.2.3::1/128
```

5. Specify a protocol (by number) for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set protocol 17
```

- Specify a local port for the SDF filter.

```
edit unified-edge pcef flow-descriptions flow-identifier
```

```
user@host# set local-ports 170
```



NOTE: You can configure a local port or local port range but not both in the same SDF filter.

- Specify from one to three remote ports for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set remote-ports 999
```



NOTE: You can configure a remote port or remote port range but not both in the same SDF filter.

- Specify a local port range for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set local-ports low 20 high 100
```

- Specify a remote port range for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set remote-ports low 20 high 100
```

- Specify that signaling information about the SDF filter is not sent to the user equipment (UE), for example, when an SDF filter is applied in the downlink direction only.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set no-send-ue
```

Related Documentation

- [Policy and Charging Control Rules Overview on page 5](#)

Configuring Policy and Charging Control Action Profiles

A Policy and Charging Control (PCC) action profile defines the quality-of-service (QoS) treatment and charging treatment to apply to a service data flow. A PCC action profile is specified in the **then** clause of a PCC rule.

To configure PCC action profiles:

- Specify a name for the PCC action profile.

```
[edit unified-edge pcef]
```

```
user@host# edit pcc-action-profiles profile-name
```

- Configure the QoS Class Identifier (QCI) by entering a QCI value from 1 through 9.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
```

```
user@host# set qci n
```

3. Configure the allocation and retention priority level by entering a priority level from 1 through 15.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set priority-level n
```

4. Configure the preemption capability.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set preemption-capability (enable | disable)
```

5. Configure the preemption vulnerability.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set preemption-vulnerability (enable | disable)
```

6. Configure the maximum bit-rate for uplink and downlink subscriber traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set maximum-bit-rate uplink n downlink n
```

7. Configure the guaranteed bit-rate values for uplink and downlink subscriber traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set guaranteed-bit-rate uplink n downlink n
```



NOTE: Guaranteed bit-rate values are only valid for GTP version 2 and GTP version 1 Release 9.

8. Configure the gating status by enabling or disabling the forwarding of service flow packets.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set gate-status (uplink | downlink | uplink-downlink | disable-both)
```

9. Configure the rating-group number for charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set rating-group n
```

10. Configure the service identifier number for online charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set service-identifier n
```

11. Configure the charging method.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set charging-method (online | offline | online-offline | none)
```



NOTE: If a charging-method is not configured, the bearer-level charging method applies. If the charging-method is configured with none, then no charging is applied for the PCC rules.

12. Configure the measurement method for charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set measurement-method (volume | time | volume-time)
```

13. Specify the application-function charging identifier for enabling charging correlation between the application and bearer layer, if the application layer has provided this information via the Rx interface.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging  
application-function-record-info]  
user@host# set af-charging-identifier identifier
```

14. Enable service-ID level reporting.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]  
user@host# set service-id-level-reporting
```

**Related
Documentation**

- [Policy and Charging Control Rules Overview on page 5](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)
- [pcc-action-profiles on page 113](#)
- [charging on page 94](#)

Configuring Layer 3 and Layer 4 Policy and Charging Control Rules

Before you configure Policy and Charging Control (PCC) rules for Layer 3 and Layer 4 traffic, you must do the following:

- Configure the flow identifiers that the PCC rules reference.
- Configure the PCC action profiles that the PCC rules reference.

To configure Layer 3 and Layer 4 PCC rules:

1. Specify a name for the PCC rules.

```
[edit unified-edge pcef]  
user@host# edit pcc-rules pcc-rule-name1
```

2. Specify one or more flow identifiers that define the Layer 3 and Layer 4 match conditions for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]  
user@host# set from flows flow-identifier1  
user@host# set from flows flow-identifier2  
user@host# set from flows flow-identifier3
```

3. Specify the PCC rules action profile that defines the quality of service (QoS), charging, and gating controls for the service data flow.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]  
user@host# set then pcc-action-profile action-profile-name1
```

**Related
Documentation**

- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)

- [Configuring Application-Aware Policy and Charging Control Rules on page 31](#)

Configuring Application-Aware Policy and Charging Control Rules

Before you configure application-aware Policy and Charging Control (PCC) rules, you must do the following:

- Configure the flow identifiers that the PCC rules reference.
- Configure the applications, application groups, and nested applications (not already included as predefined application signatures in the Junos OS) that you want to reference in application-aware PCC rules. You use the application identification feature to configure application signatures.
- Configure the PCC action profiles that the PCC rules reference.



NOTE: When specifying application-aware PCC rules in a PCEF profile, you must also configure a default Layer 3 or Layer 4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the policy (PCEF profile) that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

To configure application-aware PCC rules:

1. Specify a name for the PCC rules.

```
[edit unified-edge pcef ]
user@host# edit pcc-rules pcc-rule-name1
```

2. In a **from** statement, specify a flow identifier to use Layer 3 or Layer 4 match conditions for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]
user@host# set from flows flow-identifier1
```

3. Specify an application (defined in the application identification configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]
user@host# set from applications app-1
```

4. Group multiple applications instead of specifying each application separately, by specifying an application group (defined in the application identification configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]
user@host# set from application-groups app-group-name-1
```

5. Specify a nested application (defined in a Junos configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set from nested-applications nest-app-1
```

6. Specify the PCC rules action profile that defines the quality of service (QoS), charging, and gating controls for the application-level SDF filters.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set then pcc-action-profile action-profile-1
```

**Related
Documentation**

- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)

Configuring a Policy and Charging Control Rulebase

A Policy and Charging Control (PCC) rulebase contains a set of PCC rules. Each rule specified in the PCC rulebase is assigned a precedence to designate the priority in which PCC rules are evaluated for selection in a policy and charging enforcement function (PCEF) profile.

Before you configure a PCC rulebase, you must do the following:

- Configure service data flow filters.
- Configure PCC action profiles.
- Configure PCC rules.

To configure a PCC rulebase:

1. Specify a name for the rulebase.

```
[edit unified-edge pcef]  
user@host# edit pcc-rulebases rulebase-name
```

2. Specify the PCC rules that the rulebase references and a precedence value (1 through 65,535) for each rule.

```
[edit unified-edge pcef pcc-rulebases rulebase-name]  
user@host# set pcc-rule rule-name1 precedence 10  
user@host# set pcc-rule rule-name2 precedence 11  
user@host# set pcc-rule rule-name3 precedence 12
```

**NOTE:**

- The same rule can be configured in different rulebases and can have a different precedence.
- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

Related Documentation

- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)
- [pcc-rulebases \(PCEF\) on page 116](#)
- [pcc-rules \(PCEF\) on page 118](#)

Configuring Event Trigger Profiles

Event triggers are configured on the policy and charging enforcement function (PCEF) to notify the Policy and Charging Rule Function (PCRF) about changes in the access network. An event trigger profile contains one or more event triggers and can be referenced in a PCEF profile configured with dynamic policy control. The PCRF is notified by the PCEF about the event triggers that are configured in an event trigger profile.

To configure an event trigger profile:

1. Specify a name for the event trigger profile.

```
[edit unified-edge pcef]
user@host# edit pcef event-trigger-profiles event-trigger-name
```

2. Configure an event trigger to send notification to the PCRF when the broadband gateway or PCEF detects a change in the IP-CAN type.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]
user@host# set ip-can-change
```

3. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Traffic Flow Template (TFT) change at the bearer level.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]
user@host# set tft-change
```

4. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Public Land Mobile Network (PLMN) change.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]
user@host# set plmn-change
```

5. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the Routing Area Identity (RAI) of the Serving Gateway (S-GW) or Serving GPRS Support Node (SGSN) where the user equipment (UE) is registered.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set rai-change
```

6. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the Radio Access Technology (RAT) that is serving the user equipment.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set rat-change
```

7. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the user equipment has moved to a new S-GW or SGSN.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set sgsn-change
```

8. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the time zone in which the user equipment is located has changed.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set ue-timezone-change
```

9. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the user location.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set user-location-change
```

- Related Documentation**
- [Understanding Event Triggers on page 19](#)
 - [event-trigger-profiles on page 99](#)

Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies

When a policy and charging enforcement function (PCEF) profile is configured with dynamic policy control, the policy and charging rules function (PCRF) can provision both Policy and Charging Control (PCC) rules and PCC rule names over the Gx interface.

Before you configure a PCEF profile for dynamic policies, you must do the following:

- Configure a Diameter Gx profile.
- Configure service data flow (SDF) filters (optional).
- Configure a PCC action profile (optional).
- Configure PCC rules, PCC rulebases, or both (optional).
- Configure an event trigger profile (optional).



NOTE: When a PCEF profile includes application-aware PCC rules, you must also include a default Layer3 or Layer4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

1. To configure a PCEF profile, specify a name for the PCEF profile for dynamic policies.

```
[edit unified-edge pcef]
user@host# edit profiles pcef-dynamic-services-profile-name
```

2. Specify one or more PCC rules and a precedence for each rule.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name]
user@host# set dynamic-policy-control pcc-rules pcc-rule-name1 precedence 5
user@host# set dynamic-policy-control pcc-rules pcc-rule-name2 precedence 6
user@host# set dynamic-policy-control pcc-rules pcc-rule-name3 precedence 7
```

You can assign a precedence value from 1 through 65,535.



NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC profile has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

3. Specify one or more PCC rulebases.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name]
user@host# set dynamic-policy-control pcc-rulebases rulebase-name1
user@host# set dynamic-policy-control pcc-rulebases rulebase-name2
```



NOTE: The PCC rules and PCC rulebases configured in a PCEF profile should not overlap.

4. Specify the action to be initiated when the PCRF goes down.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# edit failure-action (continue | continue-and-retry | terminate)
```

5. If the **edit failure-action terminate** action is configured in the PCEF profile, specify the name of the PCC rule or PCC rulebase to apply to start a new session after the existing session terminates.

- To specify a PCC rule to apply to start a new session:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# set pcc-rules rule-name1 precedence 5
```

- To specify a PCC rulebase to apply to start a new session:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# set pcc-rulebases rulebase-name1
```

6. Specify a Diameter Gx profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# edit diameter-profile diameter-profile-name
```

7. Specify the release that the Gx interface uses at the PDN gateway (P-GW) so that the P-GW receives only the AVPs compliant to the release version configured.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# set release (rel8 | rel9)
```

8. Specify that online charging sessions should not fail over to an alternate server.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# edit session-failover-not-supported
```

Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)
- [dynamic-policy-control on page 97](#)
- [pcef on page 119](#)
- [Policy and Charging Control Rules Overview on page 5](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)

Configuring a Policy and Charging Enforcement Function Profile for Static Policies

A policy and charging enforcement function (PCEF) profile configured for static policy control specifies that Policy and Charging Control (PCC) rules are provisioned by the PCEF with no interaction from the policy and charging rules function (PCRF) and no Gx interface support.

Before you configure a PCEF profile for static policies, you must do the following:

- Configure service data flow filters for PCC rules.
- Configure PCC action profiles for PCC rules.

- Configure PCC rules.
- Configure PCC rulebases (optional).

To configure a PCEF profile:

1. Specify a name for the PCEF profile for static policies.

```
[edit unified-edge pcef]
user@host# edit profile pcef-static-services-profile-name
```

2. Specify one or more PCC rules and a precedence for each rule.

```
[edit unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set pcc-rules rule-name1 precedence 10
user@host# set pcc-rules rule-name2 precedence 11
user@host# set pcc-rules rule-name3 precedence 12
```

You can assign a precedence value from 1 through 65,535.



NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC profile has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

3. Specify one or more PCC rule bases.

```
[edit unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set pcc-rulebases rulebase-name1
user@host# set pcc-rulebases rulebase-name2
```

4. Specify that a Create Session request creates a dedicated bearer with the specified QCI value, in addition to the default bearer.

```
[set unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set activate-dedicated-bearers 5
```



NOTE: A dedicated bearer can be associated with any QoS Class Identifier (QCI) value (1 through 9). For each QCI value you configure with the `activate-dedicated-bearers` statement, a separate dedicated bearer is created.

Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34](#)
- [pcef on page 119](#)

- [Policy and Charging Control Rules Overview on page 5](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [static-policy-control on page 136](#)

CHAPTER 3

Configuration Examples

- [Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules on page 39](#)
- [Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules on page 57](#)

Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules

This example shows how to configure the policy and charging enforcement function (PCEF) on the MobileNext Broadband Gateway. The PCEF manages user-plane traffic handling control on the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) by providing service data flow detection, quality-of-service (QoS) control, charging control, and gating status.

- [Requirements on page 39](#)
- [Overview on page 40](#)
- [Configuration on page 41](#)
- [Verification on page 50](#)
- [Troubleshooting on page 55](#)

Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC.
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package.
- Correct configuration as a P-GW with corresponding interfaces.

Before you begin:

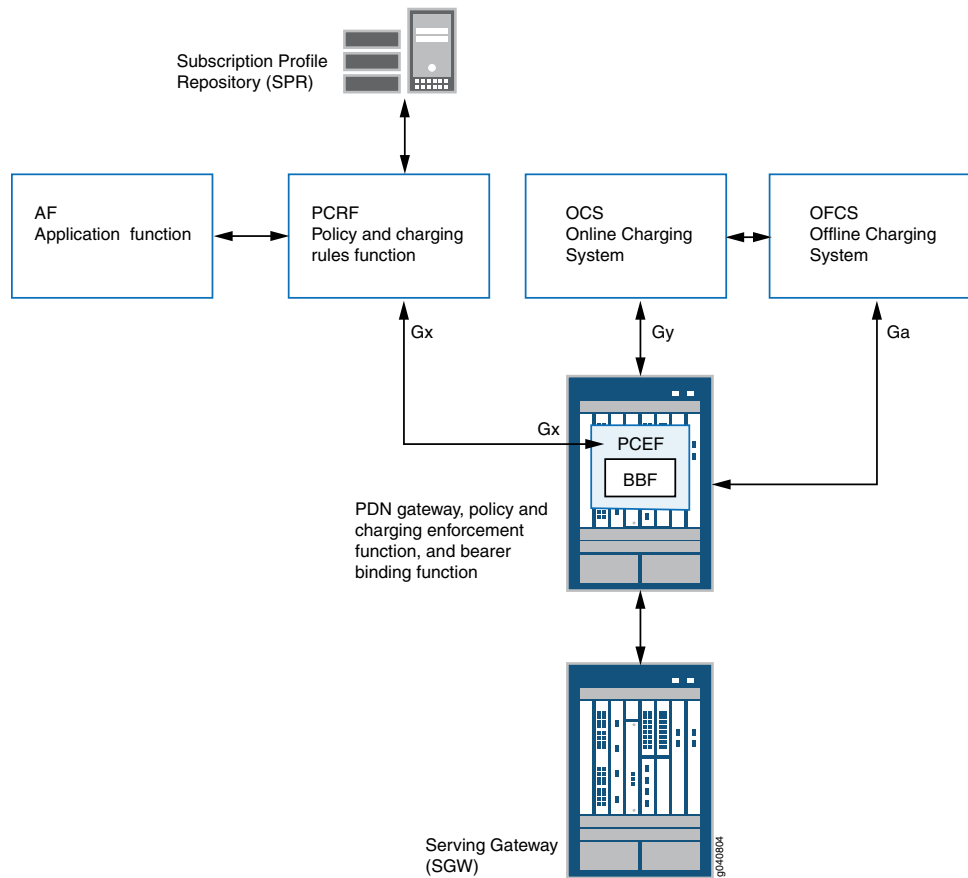
- Configure GTP and Diameter.
- Configure mobile interfaces for access point names (APNs).

- Configure APNs.
- Configure the policy and charging rule function (PCRF).

Overview

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. [Figure 5 on page 40](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging. The Gx interface connects the PCEF and the PCRF.

Figure 5: Architecture for Policy and Charging Enforcement Function



Topology

The topology for this PCEF example consists of mobile network nodes and the interfaces connecting them. The key component is the PCEF, which enforces policy decisions that are received from the PCRF and provides the PCRF with user and access information over the Gx reference point. The PCEF also interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS).

Configuration

To configure the PCEF on the P-GW, perform these tasks:

- [Configuring Service Data Flow Filters on page 41](#)
- [Configuring PCC Action Profiles on page 42](#)
- [Configuring PCC Rules on page 44](#)
- [Configuring a PCC Rulebase on page 46](#)
- [Configuring an Event Trigger Profile on page 46](#)
- [Configuring a Diameter Gx Profile for Dynamic Services on page 47](#)
- [Configuring a PCEF Profile for Dynamic Services on page 47](#)
- [Configuring a PCEF Profile for Static Services on page 48](#)
- [Applying a PCEF Policy for Dynamic Services to an APN on page 49](#)
- [Applying a PCEF Profile for Static Services to an APN on page 49](#)
- [Results on page 50](#)

Configuring Service Data Flow Filters

CLI Quick Configuration

To quickly configure the service data flow filters, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef flow-descriptions application-flow-1]
set direction both
set remote-ports 80
[edit unified-edge pcef flow-descriptions application2-flow-1]
set direction both
set remote-address ipv4-address 15.16.17.0/24
[edit unified-edge pcef flow-descriptions dns-flow-1]
set direction both
set remote-address ipv4-address 10.11.12.14/32
[edit unified-edge pcef flow-descriptions dns-flow-2]
set direction both
set remote-address ipv4-address 10.11.12.24/32
[edit unified-edge pcef flow-descriptions ipv6-gaming-flow]
set direction both
set remote-address remote-address ipv6-address 2000:1:2:3::1/128
[edit unified-edge pcef flow-descriptions sip-server-flow-1]
set remote-port-range low 5000 high 6000
set remote-address ipv4-address 12.13.14.16/32
[edit unified-edge pcef flow-descriptions video-svc-flow-1]
set direction both
set remote-address ipv4-address 11.12.13.14/32
[edit unified-edge pcef flow-descriptions video-svc-flow-2]
set direction both
set remote-address ipv4-address 11.12.13.15/32
```

Step-by-Step Procedure

To configure the service data flow filters:

1. Configure service data flow filters for HTTP traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions application-flow-1 direction
both remote-ports 80
user@host# set unified-edge pcef flow-descriptions application2-flow-1 direction
both remote-address ipv4-address 15.16.17.0/24
```

2. Configure service data flow filters for traffic going to Domain Name System (DNS) servers. For example, ensure that any mobile traffic going to the operator's own infrastructure (in this case, a DNS server) is not charged.

```
[edit]
user@host# set unified-edge pcef flow-descriptions dns-flow-1 direction both
remote-address ipv4-address 10.11.12.14/32
user@host# set unified-edge pcef flow-descriptions dns-flow-2 direction both
remote-address ipv4-address 10.11.12.24/32
```

3. Configure service data flow filters for real-time gaming traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions ipv6-gaming-flow direction
both remote-address ipv6-address 2000:1:2:3::1/128
```

4. Configure service data flow filters for VoIP traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions sip-server-flow-1
remote-port-range low 5000 high 6000
user@host# set unified-edge pcef flow-descriptions sip-server-flow-1 ipv4-address
12.13.14.16/32
```

5. Configure service data flow filters for streaming video traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions video-svc-flow-1 direction both
remote-address ipv4-address 11.12.13.14/32
```

6. Configure service data flow filters for interactive video traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions video-svc-flow-2 direction
both remote-address ipv4-address 11.12.13.15/32
```

Configuring PCC Action Profiles

CLI Quick Configuration To quickly configure the Policy and Charging Control (PCC) action profiles, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-action-profiles app1-action]
set qci 8
set allocation-retention-priority priority-level 12
set charging rating-group 5
set charging service-identifier 10
set charging charging-method offline
set charging measurement-method volume
[edit unified-edge pcef pcc-action-profiles app2-action]
set qci 8
set allocation-retention-priority priority-level 12
set charging rating-group 20
set charging service-identifier 30
```



```

set charging charging-method offline
set charging measurement-method volume
[edit unified-edge pcef pcc-action-profiles dns-action]
set qci 7
set allocation-retention-priority priority-level 15
set allocation-retention-priority preemption-capability disable
set allocation-retention-priority preemption-vulnerability enable
[edit unified-edge pcef pcc-action-profiles ipv6-gaming-action]
set qci 3
set maximum-bit-rate uplink 3000
set maximum-bit-rate downlink 5000
set charging rating-group 5
set charging charging-method online
set charging measurement-method time
[edit unified-edge pcef pcc-action-profiles sip-signalling-action]
set qci 5
set allocation-retention-priority priority-level 3
[edit unified-edge pcef pcc-action-profiles video-service-action]
set qci 4
set allocation-retention-priority priority-level 8
set maximum-bit-rate uplink 1000
set maximum-bit-rate downlink 10000
set guaranteed-bit-rate uplink 100
set guaranteed-bit-rate downlink 1000

```

Step-by-Step Procedure

To configure the PCC action profiles:

1. Configure the PCC action profiles for HTTP traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles app1-action qci 8
user@host# set unified-edge pcef pcc-action-profiles app1-action
allocation-retention-priority priority-level 12
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
rating-group 5
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
service-identifier 10
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
measurement-method volume
user@host# set unified-edge pcef pcc-action-profiles app2-action qci 8
user@host# set unified-edge pcef pcc-action-profiles app2-action
allocation-retention-priority priority-level 12
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
rating-group 20
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
service-identifier 30
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
measurement-method volume

```

2. Configure a PCC action profile for traffic directed to Domain Name System (DNS) servers. For example, ensure that any mobile traffic going to the operator's own infrastructure (in this case, a DNS server) is not charged.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles dns-action qci 7
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority priority-level 15
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority preemption-capability disable
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority preemption-vulnerability enable
```

3. Configure a PCC action profile for IPv6 real-time gaming traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action qci 3
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action
  maximum-bit-rate uplink 3000
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action
  maximum-bit-rate downlink 5000
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  rating-group 5
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  charging-method online
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  measurement-method time
```

4. Configure a PCC action profile for VoIP traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles sip-signalling-action qci 5
user@host# set unified-edge pcef pcc-action-profiles sip-signalling-action
  allocation-retention-priority priority-level 3
```

5. Configure a PCC action profile for streaming video and interactive video traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles video-service-action qci 4
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  allocation-retention-priority priority-level 8
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  maximum-bit-rate uplink 1000
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  maximum-bit-rate downlink 10000
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  guaranteed-bit-rate uplink 100
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  guaranteed-bit-rate downlink 1000
```

Configuring PCC Rules

CLI Quick Configuration

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

```
[edit unified-edge pcef pcc-rules app1-rule]
set from flows application-flow-1
set then pcc-action-profile app1-action
[edit unified-edge pcef pcc-rules app2-rule]
set from flows application2-flow-1
set then pcc-action-profile app2-action
```

```

[edit unified-edge pcef pcc-rules dns-rule]
set from flows dns-flow-1
set from flows dns-flow-2
set then pcc-action-profile dns-action
[edit unified-edge pcef pcc-rules ipv6-gaming-rule]
set from flows ipv6-gaming-flow
set then pcc-action-profile ipv6-gaming-action
[edit unified-edge pcef pcc-rules sip-signaling-rule]
set from flows sip-signaling-flow
set then pcc-action-profile sip-signaling-action
[edit unified-edge pcef pcc-rules video-service-rule]
set from flows video-svc-flow-1
set from flows video-svc-flow-2
set then pcc-action-profile video-service-action
[edit unified-edge pcef pcc-rulebases app-rule-base]
set pcc-rule app1-rule precedence 510
set pcc-rule app2-rule precedence 520
[edit unified-edge pcef profiles pcef-static-services-profile]
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]
set pcc-rules video-service-rule precedence 500
set pcc-rulebases app-rule-base
set diameter-profile gx1
[edit unified-edge pcef profiles pcef-dynamic-services-profile static-policy-control]
set pcc-rules sip-signalling-rule precedence 1000
set activate-dedicated-bearers 5
set pcc-rules ip v6-real-time-gaming precedence 1
set activate-dedicated-bearers 3

```

Step-by-Step Procedure

To configure PCC rules for the MobileNext Broadband Gateway:

1. Configure PCC rules for HTTP traffic (application 1).


```

[edit unified-edge pcef pcc-rules app1-rule]
user@host# set from flows application-flow-1
user@host# set then pcc-action-profile app1-action

```
2. Configure PCC rules for HTTP traffic (application 2).


```

[edit unified-edge pcef pcc-rules app2-rule]
user@host# set from flows application2-flow-1
user@host# set then pcc-action-profile app2-action

```
3. Configure PCC rules for Domain Name Server (DNS) traffic.


```

[edit unified-edge pcef pcc-rules dns-rule]
user@host# set from flows dns-flow-1
user@host# set from flows dns-flow-2
user@host# set then pcc-action-profile dns-action

```
4. Configure PCC rules for real-time gaming traffic.


```

[edit unified-edge pcef pcc-rules ipv6-gaming-rule]
user@host# set from flows ipv6-gaming-flow
user@host# set then pcc-action-profile ipv6-gaming-action

```
5. Configure PCC rules for IMS service (VoIP) traffic.


```

[edit unified-edge pcef pcc-rules sip-signaling-rule]
user@host# set from flows sip-signaling-flow

```

```
user@host# set then pcc-action-profile sip-signaling-action
```

6. Configure PCC rules for streaming video and interactive video traffic.

```
[edit unified-edge pcef pcc-rules video-service-rule]
user@host# set from flows video-svc-flow-1
user@host# set from flows video-svc-flow-2
user@host# set then pcc-action-profile video-service-action
```

Configuring a PCC Rulebase

CLI Quick Configuration To quickly configure a PCC rulebase, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-rulebases app-rule-base]
set pcc-rule app1-rule precedence 510
set pcc-rule app2-rule precedence 520
```

Step-by-Step Procedure

1. To configure a rulebase, specify a name for the rulebase.

```
[edit]
user@host# edit unified-edge pcef pcc-rulebases app-rule-base
```
2. Specify the PCC rules that the rulebase references and assign a precedence for each rule.

```
[edit unified-edge pcef pcc-rulebases app-rule-base]
user@host# set pcc-rule app1-rule precedence 510
user@host# set pcc-rule app2-rule precedence 520
```



NOTE: The higher the precedence value the lower the precedence and vice-versa. In this example, the PCC rule with precedence 510 is evaluated first and then the PCC rule with precedence 520 is evaluated.

Configuring an Event Trigger Profile

CLI Quick Configuration To quickly configure an event trigger profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef event-trigger-profiles evt-trigger1]
set rat-change
set sgsn-change
```

Step-by-Step Procedure

To configure an event trigger profile to include in a PCEF dynamic services profile:

1. Specify a name for the event-trigger profile.

```
[edit unified-edge pcef]
user@host# edit event-trigger-profiles evt-trigger1
```
2. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the air interface, communicated as the Radio Access Technology (RAT) type, has changed.

```
[edit unified-edge pcef]
user@host# set event-trigger-profiles evt-trigger1 rat_change
```

3. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that Serving Gateway Support Node (SGSN) or Serving Gateway (S-GW) has changed.

```
[edit unified-edge pcef]
user@host# set event-trigger-profiles evt-trigger1 sgsn_change
```

Configuring a Diameter Gx Profile for Dynamic Services

CLI Quick Configuration To quickly configure a Gx profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge diameter-profiles gx-profile gx1]
set targets pcef-dne1 destination-realm juniper.net
set targets pcef-dne1 priority 1
set targets pcef-dne1 network-element pcrf-dne1
set targets pcef-dne2 destination-realm juniper.net
set targets pcef-dne2 priority 1
set targets pcef-dne2 network-element pcrf-dne2
```

Step-by-Step Procedure To configure the Diameter Gx profile named *gx1* for the Gx application:

1. Specify a name for the Gx profile.

```
[edit unified-edge diameter-profiles]
user@host# edit gx-profile gx1
```

2. Configure the target named *pcef-dne1* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne1 destination-realm juniper.net
user@host# set targets pcef-dne1 priority 1
user@host# set targets pcef-dne1 network-element pcrf-dne1
```

3. Configure the target named *pcef-dne2* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne2 destination-realm juniper.net
user@host# set targets pcef-dne2 priority 1
user@host# set targets pcef-dne2 network-element pcrf-dne2
```

Configuring a PCEF Profile for Dynamic Services

CLI Quick Configuration To quickly configure a policy and charging enforcement function (PCEF) profile for dynamic policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]
set dynamic-policy-control pcc-rules video-service-rule precedence 500
set dynamic-policy-control pcc-rulebases app-rule-base
set dynamic-policy-control event-trigger evt-trigger1
```

```
set dynamic-policy-control diameter-profile gx1
```

**Step-by-Step
Procedure**

To configure a PCEF profile:

1. Specify a name for the PCEF profile.

```
[edit unified-edge pcef]  
user@host# edit profiles pcef-dynamic-services-profile
```

2. Specify the PCC rules and precedence.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]  
user@host# set dynamic-policy-control pcc-rules video-service-rule precedence  
500
```



NOTE: The PCRF will evaluate either the PCC rule base or PCC rules, but not both.

3. Specify a PCC rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]  
user@host# set dynamic-policy-control pcc-rulebases app-rule-base1
```

4. Specify an event trigger for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]  
user@host# set event-trigger evt-trigger1
```

5. Specify a diameter Gx profile for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]  
user@host# edit diameter-profile gx1
```

Configuring a PCEF Profile for Static Services

**CLI Quick
Configuration**

To quickly configure a PCEF profile for static policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-static-services-profile]  
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]  
set pcc-rules sip-signalling-rule precedence 1000  
set pcc-rules ipv6-gaming-rule precedence 1  
set activate-dedicated-bearers 5
```

**Step-by-Step
Procedure**

To configure a PCEF profile:

1. Specify a name for the PCEF profile.

```
[edit unified-edge]  
user@host# edit pcef profile pcef-static-services-profile
```

2. Specify the PCC rules and rule precedence.

```
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]  
user@host# set pcc-rules sip-signaling-rule precedence 1000  
user@host# set pcc-rules ip-v6-real-time-gaming precedence 1
```

- Specify that a Create Session request creates a dedicated bearer, in addition to the default bearer.

```
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]
user@host# set activate-dedicated-bearers 5
```

Applying a PCEF Policy for Dynamic Services to an APN

CLI Quick Configuration

To quickly apply the PCEF profile to an access point name (APN), copy the following commands and paste them into the router terminal window:

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns pcef-dynamic-services-apn]
set mobile-interface mif.1
set address-assignment local
set selection-mode from-ms
set pcef-profile pcef-dynamic-services-profile
```

Step-by-Step Procedure

To apply a PCEF policy:

- Configure an APN named `pcef-dynamic-services-apn` to use for the `mif.1` interface.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set mobile-interface mif.1
```

- Configure a `local` address assignment that uses the default mobile pool to assign the IP address. The default pool is configured in the routing instance that is associated with the mobile interface of the APN.

```
[unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set address-assignment local
```

- Configure the APN to allow a Create Session Request or Create Packet Data Protocol (PDP) Context message with the selection mode IE value of 1.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set selection-mode from-ms
```

- Configure the APN to use a PCEF dynamic policy to use real-time analysis of the service to assign PCC rules.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set pcef-profile pcef-dynamic-services-profile
```

Applying a PCEF Profile for Static Services to an APN

CLI Quick Configuration

To quickly apply the PCEF profile to an APN, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns pcef-static-services-apn]
mobile-interface mif.2
set mobile-interface mif.2
set address-assignment local
set selection-mode from-ms
```

```
set pcef-profile pcef-static-services-profile
```

**Step-by-Step
Procedure**

To apply a PCEF policy:

1. Configure an APN named `pcef-static-services-apn` to use for the `mif.2` interface.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set mobile-interface mif.2
```
2. Configure a **local** address assignment that uses the default mobile pool to assign the IP address. The default pool is configured in the routing instance that is associated with the mobile interface of the APN.

```
[unified-edge gateways ggsn-pgw PGW apn-services apns pcef-static-services-apn]  
user@host# set address-assignment local
```
3. Configure the APN to allow a Create Session Request or Create Packet Data Protocol (PDP) Context message with the selection mode IE value of 1.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set selection-mode from-ms
```
4. Configure the APN to use a PCEF static policy to assign PCC rules.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set pcef-profile pcef-static-services-profile
```

Results

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

For brevity, this **show** command output includes only the configuration that is relevant to this example.

```
[edit unified-edge gateways ggsn-pgw mbg-1 pcef]
```

Verification

To display Gx statistics and active bearer statistics to verify the PCEF configuration on the broadband gateway is working properly, you can perform the following tasks:

- [Verifying Control Plane Gx Statistics on the Gateway on page 50](#)
- [Verifying Active Bearers on the Gateway on page 51](#)
- [Verifying Control Plane Gx Statistics on the Gateway on page 52](#)
- [Verifying Control Plane GX Statistics on the APN on page 52](#)

Verifying Control Plane Gx Statistics on the Gateway

Purpose Verify the control plane statistics for the Gx interface on the P-GW.

Action user@host> show unified-edge ggsn-pgw statistics

Gateway: PGW

Control plane GTP statistics:

Session establishment attempts:	6	
Successful session establishments:	6	
MS/peer initiated session deactivations:	4	
Successful MS/peer initiated deactivations:	4	
Gateway initiated session deactivations:	0	
Successful gateway initiated deactivations:	0	

PCC Gx statistics:

Session attempts using dynamic policy:	6	Success: 6
Dedicated bearer activation attempts:	5	Success: 3
MS-Peer init dedicated bearer deactivations:	2	
Gateway init dedicated bearer deactivations:	0	
PCRF init dedicated bearer deactivations:	0	

Data plane global statistics:

Source address violation packets:	0
Non-existent TEID/TID packets:	0
GTP length error packets:	0
Non-existent UE address packets:	0
Mobile-to-mobile packets:	0

Data plane GTP statistics (Gn/S5/S8):

Input packets:	15
Input bytes:	1500
Output packets:	15
Output bytes:	1500
Discarded packets:	0

Data plane GTP statistics (Gi):

Input packets:	15
Input bytes:	1500
Output packets:	15
Output bytes:	1500
Discarded packets:	0

Meaning The `show unified-edge ggsn-pgw statistics` command displays all statistics at the gateway level for different interfaces.

Verifying Active Bearers on the Gateway

Purpose Verify the active bearers on the P-GW.

Action user@host> show unified-edge ggsn-pgw status

Gateway: PGW

Mobile gateway status:

Active Subscribers	:	2
Active Sessions	:	2
Active Bearers	:	3
Active GBR Bearers	:	1
Active Non-GBR Bearers	:	2
Active Prepaid bearers	:	0
Active Postpaid bearers	:	0
CPU Load (%)	:	0
Memory Load (%)	:	32

Meaning The `show unified-edge ggsn-pgw status` command displays the active subscribers, sessions, and bearers on the network.

Verifying Control Plane Gx Statistics on the Gateway

Purpose Verify the control plane Gx statistics on the P-GW.

Action `user@host> show unified-edge ggsn-pgw statistics gateway PGW`
Gateway: PGW
Control plane GTP statistics:
 Session establishment attempts: 6
 Successful session establishments: 6
 MS/peer initiated session deactivations: 4
 Successful MS/peer initiated deactivations: 4
 Gateway initiated session deactivations: 0
 Successful gateway initiated deactivations: 0
PCC Gx statistics:
 Session attempts using dynamic policy: 6 Success: 6
 Dedicated bearer activation attempts: 5 Success: 3
 MS-Peer init dedicated bearer deactivations: 2
 Gateway init dedicated bearer deactivations: 0
 PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
 Source address violation packets: 0
 Non-existent TEID/TID packets: 0
 GTP length error packets: 0
 Non-existent UE address packets: 0
 Mobile-to-mobile packets: 0
Data plane GTP statistics (Gn/S5/S8):
 Input packets: 15
 Input bytes: 1500
 Output packets: 15
 Output bytes: 1500
 Discarded packets: 0
Data plane GTP statistics (Gi):
 Input packets: 15
 Input bytes: 1500
 Output packets: 15
 Output bytes: 1500
 Discarded packets: 0

Meaning The `show unified-edge ggsn-pgw statistics gateway PGW` command displays gateway-level statistics.

Verifying Control Plane GX Statistics on the APN

Purpose Verify the control plane statistics for the Gx interface on the broadband gateway.

```

Action user@host> show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:                21
  Successful session establishments:              20
  MS/peer initiated session deactivations:       12
  Successful MS/peer initiated deactivations:    12
  Gateway initiated session deactivations:       2
  Successful gateway initiated deactivations:    2
  MS initiated modification attempts:            0
  Successful MS initiated modifications:          0
  PGW/GGSN initiated modification attempts:      1
  Successful PGW/GGSN initiated modifications:   1
  Redirect statistics:
    Successful apn redirects:                    0
    Attempted gateway redirects:                 0
    Successful gateway redirects:                0
  User authentication statistics:
    Authentication failures:                     0
    Attempted authentications:                   0
    Successful authentications:                  0
  Address allocation statistics:
    Dynamic IP allocation attempts:              21
    Dynamic IP allocation success:                21
  Charging statistics:
    Number of CDRs allocated:                    25
    Number of partial CDRs allocated:             0
    Number of CDRs closed:                      17
    Number of containers closed                   17
  Static policy statistics:
    Session establishment attempts using static policy: 0
    Session establishment success using static policy: 0
  DCCA-Gy Statistics:
    Online authorizations attempted:              0 Success : 0
    Online authorization timeouts:                0
    Quota threshold reauthorization requests sent: 0
    Gy Diameter msg statistics:
      CCR-Initial Sent : 0 Success : 0 Fail : 0
      CCR-Update Sent : 0 Success : 0 Fail : 0
      CCR-Terminate Sent : 0 Success : 0 Fail : 0
      RAR Received : 0 Answer : 0 Fail : 0
      ASR Received : 0 Answer : 0
      CCR Failure :
        Transient : 0
        Parameter : 0
        Permanent : 0
        Unknown code : 0
        Unknown session : 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
  PCC Gx statistics:
    Session attempts:                21 Success: 20
    MS-peer initiated APN-AMBR modification attempts: 0 Success: 0
    MS-peer initiated QoS modification attempts: 0 Success: 0

```

```

    PCRF initiated session deactivations:      0
    Gateway initiated session deactivations:    2
    MS-peer initiated session deactivations:    12
Gx modification statistics:
    Initiated by MS-peer: 0      Success: 0
    Initiated by PCRF: 8      Success: 0
Modification event reason:
    QoS change: 0      RAT change: 0
    SGSN change: 0      SGW change: 0
    PLMN change: 0      RAI change: 0
    ULI change: 0      IP-CAN change: 0
    TFT change (MS): 0      TFT change (Network): 0
    Bearer loss: 0      Bearer recovery: 0
    Resource allocation: 0      Revalidation Timeout: 0
    QoS exceeding auth: 0      Time-of-Day procedure: 0
    Change of Subscription: 0      AMBR change: 0
    ECGI change: 0      TAI change: 0
    Timezone change: 0      Default-EPS-QoS change: 0
Dedicated bearer statistics:
    MS-peer initiated activation attempts: 0      Success: 0
    Network initiated activation attempts: 7      Success: 5
    MS-peer initiated modification attempts: 0      Success: 0
    Network initiated modification attempts: 0      Success: 0
    MS-peer initiated deactivations: 5
    Network initiated deactivations: 0
    Gateway initiated deactivations: 0
Gx Failure Statistics:
    GBR dedicated bearer create failure due to CAC: 0
    Non-GBR dedicated bearer create failure due to CAC: 0
    Session terminations due to unreachable PCRF: 0
    Session terminations due to PCRF restart: 0
Gx diameter message statistics:
    CCR-I sent: 21      CCA-I received: 20
    CCR-U sent: 20      CCA-U received: 20
    CCR-T sent: 15      CCA-T received: 0
    RAR received: 8      RAA sent: 6
    RAA sent resource failure: 0
CCR failure reason:
    Transient failure: 0      Initial params error: 0
    Permanent failure: 0      Unknown code: 0
    Unknown session: 0
Gx rule statistics:
    Dynamic rule activations: 0      Deactivations: 0
    Static rules activations: 10      Deactivations: 10
    Dynamic rule modifications: 20
Rule failure statistics:
    Rule validation failure: 14
    Rule enforcement failure no resource: 2
    Rule activation failure no resource: 0
    Rule update procedure fail: 0
Handover Statistics:
    Inter-RAT Handover attempts: 0      Success: 0
    Intra-RAT Handover attempts: 0      Success: 0
Data plane statistics:
    Total packets violating MIF ACL: 0
    Total accepted mobile-to-mobile packets: 0
    Total accepted mobile-to-mobile bytes: 0
Miscellaneous Packet statistics:
    IPv6 Router Solicitations received: 0
    IPv6 Router Advertisement transmitted: 0
    IPv6 Neighbor Solicitations received: 0

```

```

IPv6 Neighbor Advertisement transmitted:    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 The `show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic` command displays the control plane Gx statistics for an APN. If the output shows that session attempts are successful, then the connection to the PCEF is functioning properly.

Troubleshooting

To troubleshoot the policy and charging enforcement function (PCEF) configuration, perform these tasks:

- [Connection is Down Between the PCEF and PCRF on page 55](#)
- [PCEF and PCRF Application Messages Are Not Sent or Received on page 56](#)

Connection is Down Between the PCEF and PCRF

Problem The connection between the PCEF and PCRF peers on the Gx interface appears to be down.

Solution To display Diameter peer status for the PCRF and PCEF:

1. From operational mode, enter the `show unified-edge ggsn-pgw diameter peer status` command.

```

user@host> show unified-edge ggsn-pgw diameter peer status
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:      6
  Successful session establishments:    6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy: 6      Success: 6
  Dedicated bearer activation attempts: 5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:      0
  Non-existent TEID/TID packets:        0
  GTP length error packets:             0
  Non-existent UE address packets:      0
  Mobile-to-mobile packets:             0

```

Data plane GTP statistics (Gn/S5/S8):

```
Input    packets:      15
Input    bytes:        1500
Output   packets:      15
Output   bytes:        1500
Discarded packets:     0
```

Data plane GTP statistics (Gi):

```
Input    packets:      15
Input    bytes:        1500
Output   packets:      15
Output   bytes:        1500
Discarded packets:     0
```

2. Check that status of the State field, which is displayed at the beginning of the output. When the connection between the Diameter peers (PCEF and PCRF) is up, the State status indicates **I-Open**.
3. Check that the status of the Watchdog State field, which is displayed near the beginning of the output. When Diameter peers are connected, the Watchdog State status indicates **okay**.

PCEF and PCRF Application Messages Are Not Sent or Received

Problem The PCRF and PCEF application messages (Re-Authorization Request/Re-Authorization Answer or Credit Control Request/Credit Control Answer) are not being sent or received.

Solution To display status of application messages for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer statistics** command.

```
user@host> show unified-edge ggsn-pgw diameter peer statistics
```

```
Peer: p1
```

Request Timeouts:	0	
Request Retransmissions:	0	
Messages	Transmitted	Received
-----	-----	-----
Total Messages	22	22
Credit Control Requests	14	0
Credit Control Answers	0	14
Re-Auth Requests	0	2
Re-Auth Answers	2	0
Abort Session Requests	0	0
Abort Session Answers	0	0
Capability Exchange Requests	2	0
Capability Exchange Answers	0	2
Device Watchdog Requests	4	0
Device Watchdog Answers	0	4
Disconnect Peer Requests	0	0
Disconnect Peer Answers	0	0

2. Check that for each message type, there are an equal number of messages for requests and answers.

Related Documentation • [Application-Aware Policy and Charging Control Rules Overview on page 9](#)

- [Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules on page 57](#)
- [Policy and Charging Control Rules Overview on page 5](#)
- [Policy and Charging Enforcement Function Overview on page 3](#)
- [Understanding Event Triggers on page 19](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 15](#)

Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules

This example shows how to configure the policy and charging enforcement function (PCEF) with application-aware policy and charging control (PCC) rules on the MobileNext Broadband Gateway. To enforce application-aware PCC rules, PCEF is applied as a service on the APN (the MIF interface) to indicate to the Packet Forwarding Engine that traffic should be directed to the Junos OS services PIC that hosts the PCEF service. When subscriber traffic is redirected to the services PIC, processing is completed and the appropriate policies are applied as a service on the MIF interface associated with an APN.

- [Requirements on page 57](#)
- [Overview on page 58](#)
- [Configuration on page 58](#)
- [Verification on page 78](#)
- [Troubleshooting on page 84](#)

Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package
- Correct configuration as a P-GW with corresponding interfaces

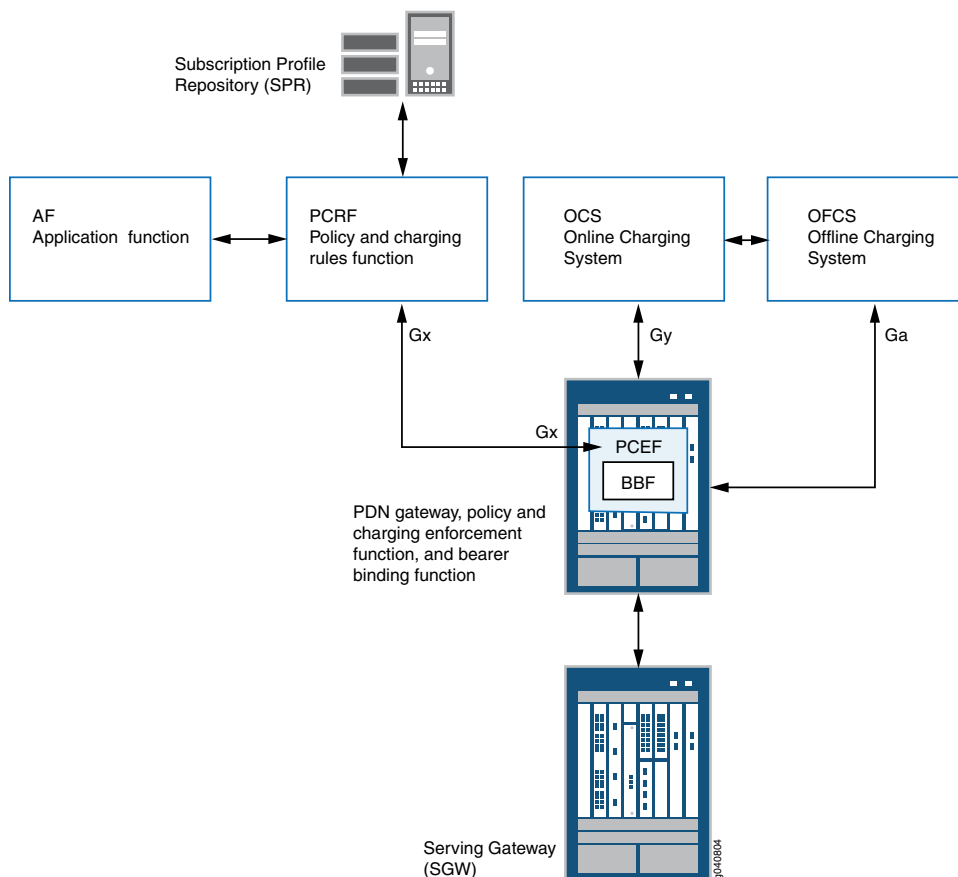
Before you begin:

- Configure GTP and Diameter.
- Configure mobile interfaces for access point names (APNs).
- Configure APNs.
- Configure the policy and charging rule function (PCRF).

Overview

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. The Gx interface connects the PCEF and the PCRF.

Figure 6: Architecture for Policy and Charging Enforcement Function



Topology

The topology for this PCEF example consists of mobile network nodes and the interfaces connecting them. The key component is the PCEF, which enforces policy decisions that are received from the PCRF and provides the PCRF with user and access information over the Gx reference point. The PCEF also interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS).

Configuration

To configure the PCEF on the P-GW, perform these tasks:

- [Configuring Application Signatures on page 59](#)
- [Configuring an Application Identification Profile on page 60](#)

- [Configuring PCEF Services for Application-Aware Traffic on page 60](#)
- [Configuring Service Data Flow Filters on page 62](#)
- [Configuring PCC Action Profiles on page 63](#)
- [Configuring Application-Aware PCC Rules on page 69](#)
- [Configuring PCC Rulebases on page 72](#)
- [Configuring a Diameter Gx Profile for Dynamic Services on page 73](#)
- [Configuring PCEF Profiles for Dynamic Policies on page 73](#)
- [Configuring PCEF Profiles for Static \(Local\) Services on page 75](#)
- [Applying PCEF Policies for Dynamic Services to APNs on page 77](#)
- [Applying a PCEF Profile for Static Services to an APN on page 77](#)
- [Results on page 78](#)

Configuring Application Signatures

CLI Quick Configuration

To quickly configure application signatures to detect Layer 7 nested applications, copy the following commands and paste them into the router terminal window:

```
[edit services application-identification]
set download url https://devdb.secteam.juniper.net/xmlexport.cgi
set nested-application reddy protocol HTTP
set nested-application reddy signature reddy member m01 context http-url-parsed
set nested-application reddy signature reddy member m01 pattern ".*\[reddy\].*"
set nested-application reddy signature reddy member m01 direction client-to-server
set nested-application reddy signature reddy maximum-transactions 1
```

Step-by-Step Procedure

The application identification (APPID) feature (supported on MX Series routers equipped with Multiservices DPCs) identifies applications as constituents of application groups in TCP, UDP, or ICMP traffic. For more information about defining the application signatures in the application identification engine, see “Configuring Application Identification for Nested Applications” in the Junos OS *Services Interfaces* guide.

1. Specify the URL to download the Junos OS application package:

```
[edit services application-identification]
user@host# set download url https://devdb.secteam.juniper.net/xmlexport.cgi
```

2. Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device.

```
[edit services application-identification nested-application]
user@host# set reddy protocol HTTP
user@host# set reddy signature reddy member m01 context http-url-parsed
user@host# set reddy signature reddy member m01 pattern ".*\[reddy\].*"
user@host# set reddy signature reddy member m01 direction client-to-server
user@host# set reddy signature reddy maximum-transactions 1
```

Configuring an Application Identification Profile

CLI Quick Configuration To quickly configure an application identification profile, copy the following commands and paste them into the router terminal window:

```
[edit services application-identification]
edit profile app-id-profile1
```

Step-by-Step Procedure You configure an application profile for use in a service set. The profile consists of one or more rule sets, but only one profile can be included per service set. For more information, see “Configuring Application Profiles” in the Junos OS *Services Interfaces* documentation.

1. Define an application profile for use in the *dpi-service-set-1* service set.

```
[edit services application-identification]
user@host# edit profile app-id-profile1
```

Configuring PCEF Services for Application-Aware Traffic

CLI Quick Configuration

```
[edit unified-edge gateways ggsn-pgw PGW1 system]
set service-pics interface ams0
[edit services pcef profile pcef-service-profile1]
[edit services service-set dpi-service-set-1]
set tcp-mss 1300
set service-set-options subscriber-awareness
set pcef-profile pcef-service-profile-1
set application-identification app-id-profile1
set interface-service service-interface ams0
[edit interfaces mif unit 0 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 1 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 2 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 3 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit firewall family inet service-filter dpi-filter-1]
set term dpi-flow-1 from redirect-reason dpi
set term dpi-flow-1 then service
[edit interfaces mif unit 0]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 1]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 2]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
```

```

set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 3]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1

```

Step-by-Step Procedure

To configure an application-aware PCEF service for an APN:

1. Configure a service PIC for the PCEF service.

```

[edit unified-edge gateways ggsn-pgw PGW1 system]
user@host# set service-pics interface ams0

```
2. Configure the PCEF services profile by specifying a name for the PCEF profile.

```

[edit ]
user@host# edit services pcef profile pcef-service-profile1

```



NOTE: In this release, the PCEF profile is a placeholder profile with no configuration options; however, you must create a PCEF profile to provide future compatibility for PCEF services.

3. Define a service to use as an application-aware PCEF service.

```

[edit services service-set dpi-service-set-1]
user@host# set tcp-mss 1300
user@host# set service-set-options subscriber-awareness
user@host# set pcef-profile pcef-service-profile1
user@host# set application-identification app-id-profile1
user@host# set interface-service service-interface ams1.1

```
4. Apply the PCEF application-aware service to the mobile interfaces for the APNs for both ingress and egress traffic so that all traffic arriving on the APN is inspected for application-based charging and policy.

```

[edit interfaces mif unit 0 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 1 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 2 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 3 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1

```
5. Configure a Deep Packet Inspection (DPI) filter for application-aware traffic.

```

[edit ]
user@host# edit firewall family inet service-filter dpi-filter-1
[edit firewall family inet service-filter dpi-filter-1]
user@host# set term dpi-flow-1 from redirect-reason dpi
user@host# set term dpi-flow-1 then service

```

6. Apply the DPI filter to the MIF interfaces so that only application-aware traffic is forwarded to the services PICs.

```
[edit interfaces mif unit 0]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 1]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 2]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 3]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
```

7. Include the `jservice-appid`, `jservice-pcef`, and `jservice-mss` packages with the services PIC configuration.

```
[edit chassis fpc 1 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
[edit chassis fpc 1 pic 1 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
```

Configuring Service Data Flow Filters

CLI Quick Configuration To quickly configure the service data flow filters, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef flow-descriptions allow_all]
set direction both
[edit unified-edge pcef flow-descriptions flow-tcp-1]
set direction both
set protocol 6
```

Step-by-Step Procedure To configure the service data flow filters:

1. Configure a service data flow filter to provide a wildcard PCC rule that permits all traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions allow_all direction both
```



NOTE: You can configure a wild-card service data flow filter in an application-aware PCC rule, so that any flows redirected to the PCEF service that do not match any of the configured application-aware PCC rules are appropriately handled and assigned a rating group.

2. Configure a service data flow filter to specify a protocol in an application-aware PCC rule.

```
[edit]
user@host# set unified-edge pcef flow-descriptions flow-tcp-1 direction both
user@host# set unified-edge pcef flow-descriptions flow-tcp-1 protocol 6
```

Configuring PCC Action Profiles

CLI Quick Configuration

To quickly configure the Policy and Charging Control (PCC) action profiles, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-action-profiles pap-1]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 10
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-2]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 11
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-11]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 20
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-12]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 21
set charging charging-method online
```

```
[edit unified-edge pcef pcc-action-profiles pap-6]
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status disable-both
set charging rating-group 15
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-7]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 16
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-16]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 25
set charging service-identifier 25
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-17]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 26
set charging service-identifier 26
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-3]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 12
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-13]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 22
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-4]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 13
```

```

set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-5]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 14
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-14]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 23
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-15]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 24
set charging charging-method online

```

Step-by-Step Procedure

To configure the PCC action profiles:

1. Configure the PCC action profiles for static (local) PCC rules for offline-charging traffic.


```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-1 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-1 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-1 set charging rating-group
10
user@host# set unified-edge pcef pcc-action-profiles pap-1 set charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles pap-2 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-2 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-2 set charging rating-group
11

```

```
user@host# set unified-edge pcef pcc-action-profiles pap-2 set charging  
charging-method offline
```

2. Configure the PCC action profiles for static PCC rules for online-charging traffic.

```
[edit]  
user@host# set unified-edge pcef pcc-action-profiles pap-11 qci 5  
user@host# set unified-edge pcef pcc-action-profiles pap-11  
allocation-retention-priority priority-level 1  
user@host# set unified-edge pcef pcc-action-profiles pap-11  
allocation-retention-priority preemption-capability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-11  
allocation-retention-priority preemption-vulnerability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-11 gate-status  
uplink-downlink  
user@host# set unified-edge pcef pcc-action-profiles pap-11 charging rating-group  
20  
user@host# set unified-edge pcef pcc-action-profiles pap-11 charging  
charging-method online  
user@host# set unified-edge pcef pcc-action-profiles pap-12 qci 5  
user@host# set unified-edge pcef pcc-action-profiles pap-12  
allocation-retention-priority priority-level 1  
user@host# set unified-edge pcef pcc-action-profiles pap-12  
allocation-retention-priority preemption-capability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-12  
allocation-retention-priority preemption-vulnerability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-12 gate-status  
uplink-downlink  
user@host# set unified-edge pcef pcc-action-profiles pap-12 charging rating-group  
21  
user@host# set unified-edge pcef pcc-action-profiles pap-12 charging  
charging-method online
```

3. Configure the PCC action profiles for static-Gx PCC rules for offline-charging traffic.

```
[edit]  
user@host# set unified-edge pcef pcc-action-profiles pap-6 qci 5  
user@host# set unified-edge pcef pcc-action-profiles pap-6  
allocation-retention-priority priority-level 1  
user@host# set unified-edge pcef pcc-action-profiles pap-6  
allocation-retention-priority preemption-capability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-6  
allocation-retention-priority preemption-vulnerability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-6 gate-status disable-both  
user@host# set unified-edge pcef pcc-action-profiles pap-6 charging rating-group  
15  
user@host# set unified-edge pcef pcc-action-profiles pap-6 charging  
charging-method offline  
user@host# set unified-edge pcef pcc-action-profiles pap-6  
user@host# set unified-edge pcef pcc-action-profiles pap-7 qci 5  
user@host# set unified-edge pcef pcc-action-profiles pap-7  
allocation-retention-priority priority-level 1  
user@host# set unified-edge pcef pcc-action-profiles pap-7  
allocation-retention-priority preemption-capability 0  
user@host# set unified-edge pcef pcc-action-profiles pap-7  
allocation-retention-priority preemption-vulnerability 0
```



```

user@host# set unified-edge pcef pcc-action-profiles pap-7 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-7 charging rating-group
16
user@host# set unified-edge pcef pcc-action-profiles pap-7 charging
charging-method offline

```

4. Configure the PCC action profiles for static-Gx PCC rules for online-charging traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-16 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-16 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging rating-group
25
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging
service-identifier 25
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging
charging-method online
user@host# set unified-edge pcef pcc-action-profiles pap-17 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-17 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging rating-group
26
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging
service-identifier 26
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging
charging-method online

```

5. Configure the PCC action profiles for wildcard rules for offline-charging traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-3 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-3 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-3 charging rating-group
12
user@host# set unified-edge pcef pcc-action-profiles pap-3 charging
charging-method offline

```

6. Configure the PCC action profiles for wildcard rules for online-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-13 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-13 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-13 charging rating-group
  22
user@host# set unified-edge pcef pcc-action-profiles pap-13 charging
  charging-method online
```

7. Configure the PCC action profiles for static rules for a rulebase for offline-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-4 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-4 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-4 charging rating-group
  13
user@host# set unified-edge pcef pcc-action-profiles pap-4 charging
  charging-method offline
user@host# set unified-edge pcef pcc-action-profiles pap-5 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-5 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-5 charging rating-group
  14
user@host# set unified-edge pcef pcc-action-profiles pap-5 charging
  charging-method offline
```

8. Configure the PCC action profiles for static rules for a rulebase for online-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-14 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-14
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-14
  allocation-retention-priority preemption-capability 0
```

```

user@host# set unified-edge pcef pcc-action-profiles pap-14
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-14 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-14 charging-rating-group
23
user@host# set unified-edge pcef pcc-action-profiles pap-14 charging
charging-method online
user@host# set unified-edge pcef pcc-action-profiles pap-15 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-15 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-15 charging-rating-group
24
user@host# set unified-edge pcef pcc-action-profiles pap-15 charging
charging-method online

```

Configuring Application-Aware PCC Rules

CLI Quick Configuration

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

```

[edit unified-edge pcef pcc-rules local-offline-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-2
[edit unified-edge pcef pcc-rules local-offline-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-3
[edit unified-edge pcef pcc-rules local-online-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-11
[edit unified-edge pcef pcc-rules local-online-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-12
[edit unified-edge pcef pcc-rules local-online-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-13
[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
set from flows allow_all

```

```
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-15
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set local-offline-rb-1 pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
[edit unified-edge pcef pcc-rules static-gx-offline-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-6
[edit unified-edge pcef pcc-rules static-gx-offline-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-7
[edit unified-edge pcef pcc-rules static-gx-offline-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-8
[edit unified-edge pcef pcc-rules static-gx-online-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-16
[edit unified-edge pcef pcc-rules static-gx-online-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-17
[edit set unified-edge pcef pcc-rules static-gx-online-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-18
```

**Step-by-Step
Procedure**

To configure application-aware PCC rules for the MobileNext Broadband Gateway:

1. Configure static PCC rules for offline-charging traffic.

```
[edit unified-edge pcef pcc-rules local-offline-rule-1]
```

```

user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-2

```

2. Configure static PCC rules to include in a rulebase for offline-charging traffic.

```

[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:LINKEDIN
user@host# set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:YAHOO-MAIL
user@host# set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-offline-rule-1]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-2

```

3. Configure a default Layer 3 or Layer 4 wildcard PCC rule for offline-charging traffic to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic.

```

[edit unified-edge pcef pcc-rules local-offline-wildcard-rule]
user@host# set from flows allow_all
user@host# set then pcc-action-profile pap-3

```



NOTE: The PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

4. Configure the static PCC rules for online traffic.

```

[edit unified-edge pcef pcc-rules local-online-rule-1]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-11
[edit unified-edge pcef pcc-rules local-online-rule-2]
user@host# set from flows flow-tcp-1

```

```
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-12
```

5. Configure static PCC rules to include in a rulebase for online traffic.

```
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications junos:LINKEDIN
user@host# set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications junos:YAHOO-MAIL
user@host# set then pcc-action-profile pap-15
```

6. Configure a default Layer 3 or Layer 4 wildcard PCC rule for online traffic to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic.

```
[edit unified-edge pcef pcc-rules local-online-wildcard-rule]
user@host# set from flows allow_all
user@host# set then pcc-action-profile pap-13
```

Configuring PCC Rulebases

CLI Quick Configuration

To quickly configure a PCC rulebase, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
```

Step-by-Step Procedure

To configure PCC rulebases:

1. Specify a name for the local rulebases you want to configure to manage online-charging traffic and offline-charging traffic.

```
[edit]
user@host# edit unified-edge pcef pcc-rulebases local-offline-rb-1
user@host# edit unified-edge pcef pcc-rulebases local-online-rb-1
```

2. Specify the PCC rules that each rulebase references and assign a precedence for each PCC rule.

```
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
user@host# set pcc-rule local-offline-rb-rule-1 precedence 3001
user@host# set pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
user@host# set pcc-rule local-online-rb-rule-1 precedence 3501
user@host# set pcc-rule local-online-rb-rule-2 precedence 3510
```



NOTE: The higher the precedence value the lower the precedence and vice-versa. In this example, the PCC rule with precedence 3001 is evaluated first and then the PCC rule with precedence 3010 is evaluated, and so on.

Configuring a Diameter Gx Profile for Dynamic Services

CLI Quick Configuration To quickly configure a Gx profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge diameter-profiles gx-profile gx1]
set targets pcef-dne1 destination-realm juniper.net
set targets pcef-dne1 priority 1
set targets pcef-dne1 network-element pcrf-dne1
set targets pcef-dne2 destination-realm juniper.net
set targets pcef-dne2 priority 1
set targets pcef-dne2 network-element pcrf-dne2
```

Step-by-Step Procedure To configure the Diameter Gx profile named *gx1* for the Gx application:

1. Specify a name for the Gx profile.

```
[edit unified-edge diameter-profiles]
user@host# edit gx-profile gx1
```
2. Configure the target named *pcef-dne1* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne1 destination-realm juniper.net
user@host# set targets pcef-dne1 priority 1
user@host# set targets pcef-dne1 network-element pcrf-dne1
```
3. Configure the target named *pcef-dne2* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne2 destination-realm juniper.net
user@host# set targets pcef-dne2 priority 1
user@host# set targets pcef-dne2 network-element pcrf-dne2
```

Configuring PCEF Profiles for Dynamic Policies

CLI Quick Configuration To quickly configure the PCEF profiles for dynamic policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof dynamic-policy-control]
set pcc-rules static-gx-offline-rule-1 precedence 10
set pcc-rules static-gx-offline-rule-2 precedence 50
set pcc-rules static-gx-offline-wildcard-rule precedence 1900
set diameter-profile gx1
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
```

```
set pcc-rules static-gx-online-rule-1 precedence 500
set pcc-rules static-gx-online-rule-2 precedence 510
set pcc-rules static-gx-online-wildcard-rule precedence 1950
set diameter-profile gx1
```

**Step-by-Step
Procedure**

To configure dynamic PCEF profiles to enforce policy decisions that are received from the PCRF and provide the PCRF with subscriber and access information over the Gx interface:

1. Configure a dynamic PCEF profile to handle traffic for offline charging:

- a. Specify a name for the PCEF profile.

```
user@host# edit unified-edge pcef profiles pcef-static-gx-offline-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# set dynamic-policy-control pcc-rules static-gx-offline-rule-1
precedence 10
user@host# set dynamic-policy-control pcc-rules static-gx-offline-rule-2
precedence 50
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# set dynamic-policy-control pcc-rules static-gx-offline-wildcard-rule
precedence 1900
```



NOTE: A PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

- d. Specify a diameter Gx profile for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# edit dynamic-policy-control diameter-profile gx1
```

2. Configure a dynamic PCEF profile to handle online-charging traffic:

- a. Specify a name for the PCEF profile.

```
user@host# edit unified-edge pcef profiles pcef-static-gx-online-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# set pcc-rules static-gx-online-rule-1 precedence 500
user@host# set pcc-rules static-gx-online-rule-2 precedence 510
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# set pcc-rules static-gx-online-wildcard-rule precedence 1950
```

- d. Specify a diameter Gx profile for the PCEF profile.


```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# edit diameter-profile gx1
```

Configuring PCEF Profiles for Static (Local) Services

CLI Quick Configuration

To quickly configure a PCEF profile for static policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
set static-policy-control pcc-rules local-offline-rule-1 precedence 2001
set static-policy-control pcc-rules local-offline-rule-2 precedence 2010
set static-policy-control pcc-rules local-offline-wildcard-rule precedence 3900
set static-policy-control pcc-rulebases local-offline-rb-1
[edit unified-edge pcef profiles pcef-local-online-prof]
set static-policy-control pcc-rules local-online-rule-1 precedence 2500
set static-policy-control pcc-rules local-online-rule-2 precedence 2510
set static-policy-control pcc-rules local-online-wildcard-rule precedence 3950
set static-policy-control pcc-rulebases local-online-rb-1
[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-15
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set local-offline-rb-1 pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
```

Step-by-Step Procedure

To configure PCEF profiles for static (local) services:

1. Configure a local PCEF profile to handle traffic for offline charging:
 - a. Specify a name for the PCEF profile.


```
user@host# edit unified-edge pcef profiles pcef-local-offline-prof
```
 - b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.


```
[edit unified-edge pcef profiles pcef-local-offline-prof]
```

```
user@host# set static-policy-control pcc-rules local-offline-rule-1 precedence
2001
user@host# set static-policy-control pcc-rules local-offline-rule-2 precedence
2010
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
user@host# set static-policy-control pcc-rules local-offline-wildcard-rule
precedence 3900
```



NOTE: A PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

- d. Specify a rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
user@host# set static-policy-control pcc-rulebases local-offline-rb-1
set
set diameter-profile gx1
```

2. Configure a local PCEF profile to handle traffic for online charging:

- a. Specify a name for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-local-online-prof]
set static-policy-control pcc-rules local-online-rule-1 precedence 2500
set static-policy-control pcc-rules local-online-rule-2 precedence 2510
set static-policy-control pcc-rules local-online-wildcard-rule precedence 3950
set static-policy-control pcc-rulebases local-online-rb-1

user@host# edit unified-edge pcef profiles pcef-local-online-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set pcc-rules local-online-rule-1 precedence 2500
user@host# set static-policy-control pcc-rules local-online-rule-2 precedence
2510
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set static-policy-control pcc-rules local-online-wildcard-rule
precedence 3950
```

- d. Specify a rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set static-policy-control pcc-rulebases local-online-rb-1
```

Applying PCEF Policies for Dynamic Services to APNs

- CLI Quick Configuration** To quickly apply each PCEF profile to an access point name (APN), copy the following commands and paste them into the router terminal window:
- ```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
set mobile-interface mif.0
set address-assignment allow-static-ip-address
set pcef-profile pcef-static-gx-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
set mobile-interface mif.1
set address-assignment allow-static-ip-address
set pcef-profile pcef-static-gx-online-prof
```
- Step-by-Step Procedure** To apply the dynamic PCEF policies to APNs:
1. Configure APNs to use for the MIF interfaces for the PCEF policies.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set mobile-interface mif.0
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set mobile-interface mif.1
```
  2. Configure the **allow-static-ip-address** address assignment for each APN so that the broadband gateway allows for a static IP address provided by the user equipment.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set address-assignment allow-static-ip-address
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set address-assignment allow-static-ip-address
```
  3. Configure APNs to use dynamic PCEF policies to use real-time analysis of the service to assign PCC rules.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set pcef-profile pcef-static-gx-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set pcef-profile pcef-static-gx-online-prof
```

### Applying a PCEF Profile for Static Services to an APN

- CLI Quick Configuration** To quickly apply the PCEF profile to an APN, copy the following commands and paste them into the router terminal window:
- ```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
set mobile-interface mif.0
set address-assignment allow-static-ip-address
set pcef-profile pcef-local-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
set mobile-interface mif.1
set address-assignment allow-static-ip-address
set pcef-profile pcef-local-online-prof
```
- Step-by-Step Procedure** To apply the static PCEF policies to APNs:
1. Configure APNs to use for the MIF interfaces.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
user@host# set mobile-interface mif.0
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set mobile-interface mif.1
```

2. Configure the **allow-static-ip-address** address assignment for each APN so that the broadband gateway allows for a static IP address provided by the user equipment.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
user@host# set address-assignment allow-static-ip-address
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set address-assignment allow-static-ip-address
```

3. Configure APNs to use local PCEF policies to assign PCC rules.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set pcef-profile pcef-local-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set pcef-profile pcef-local-online-prof
```

Results

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

For brevity, this **show** command output includes only the configuration that is relevant to this example.

Verification

To display Gx statistics and active bearer statistics to verify that the PCEF configuration on the broadband gateway is working properly, perform the following tasks:

- [Verifying Control Plane Gx Statistics on the Gateway on page 78](#)
- [Verifying Active Bearers on the Gateway on page 79](#)
- [Verifying Control Plane Gx Statistics on the Gateway on page 80](#)
- [Verifying Control Plane GX Statistics on the APN on page 80](#)
- [Verifying Application Identification Counter Statistics on page 83](#)
- [Verifying Application Signatures Counter Statistics on page 83](#)

Verifying Control Plane Gx Statistics on the Gateway

Purpose Verify the control plane statistics for the Gx interface on the P-GW.

```

Action user@host> show unified-edge ggsn-pgw statistics
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:          6
  Successful session establishments:        6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy:    6      Success: 6
  Dedicated bearer activation attempts:     5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:         0
  Non-existent TEID/TID packets:           0
  GTP length error packets:                0
  Non-existent UE address packets:         0
  Mobile-to-mobile packets:                0
Data plane GTP statistics (Gn/S5/S8):
  Input packets:                           15
  Input bytes:                             1500
  Output packets:                           15
  Output bytes:                             1500
  Discarded packets:                        0
Data plane GTP statistics (Gi):
  Input packets:                           15
  Input bytes:                             1500
  Output packets:                           15
  Output bytes:                             1500
  Discarded packets:                        0

```

Meaning The `show unified-edge ggsn-pgw statistics` command displays all statistics at the gateway level for different interfaces.

Verifying Active Bearers on the Gateway

Purpose Verify the active bearers on the P-GW.

```

Action user@host> show unified-edge ggsn-pgw status
Gateway: PGW
Mobile gateway status:
  Active Subscribers          :      2
  Active Sessions             :      2
  Active Bearers              :      3
  Active GBR Bearers          :      1
  Active Non-GBR Bearers      :      2
  Active Prepaid bearers      :      0
  Active Postpaid bearers     :      0
  CPU Load (%)                :      0
  Memory Load (%)             :     32

```

Meaning The `show unified-edge ggsn-pgw status` command displays the active subscribers, sessions, and bearers on the network.

Verifying Control Plane Gx Statistics on the Gateway

Purpose Verify the control plane Gx statistics on the P-GW.

Action `user@host> show unified-edge ggsn-pgw statistics gateway PGW`
Gateway: PGW
Control plane GTP statistics:
 Session establishment attempts: 6
 Successful session establishments: 6
 MS/peer initiated session deactivations: 4
 Successful MS/peer initiated deactivations: 4
 Gateway initiated session deactivations: 0
 Successful gateway initiated deactivations: 0
PCC Gx statistics:
 Session attempts using dynamic policy: 6 Success: 6
 Dedicated bearer activation attempts: 5 Success: 3
 MS-Peer init dedicated bearer deactivations: 2
 Gateway init dedicated bearer deactivations: 0
 PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
 Source address violation packets: 0
 Non-existent TEID/TID packets: 0
 GTP length error packets: 0
 Non-existent UE address packets: 0
 Mobile-to-mobile packets: 0
Data plane GTP statistics (Gn/S5/S8):
 Input packets: 15
 Input bytes: 1500
 Output packets: 15
 Output bytes: 1500
 Discarded packets: 0
Data plane GTP statistics (Gi):
 Input packets: 15
 Input bytes: 1500
 Output packets: 15
 Output bytes: 1500
 Discarded packets: 0

Meaning The `show unified-edge ggsn-pgw statistics gateway PGW` command displays gateway-level statistics.

Verifying Control Plane GX Statistics on the APN

Purpose Verify the control plane statistics for the Gx interface on the broadband gateway.

```

Action user@host> show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:                21
  Successful session establishments:              20
  MS/peer initiated session deactivations:       12
  Successful MS/peer initiated deactivations:    12
  Gateway initiated session deactivations:       2
  Successful gateway initiated deactivations:    2
  MS initiated modification attempts:            0
  Successful MS initiated modifications:         0
  PGW/GGSN initiated modification attempts:      1
  Successful PGW/GGSN initiated modifications:   1
  Redirect statistics:
    Successful apn redirects:                    0
    Attempted gateway redirects:                 0
    Successful gateway redirects:                0
  User authentication statistics:
    Authentication failures:                    0
    Attempted authentications:                  0
    Successful authentications:                 0
  Address allocation statistics:
    Dynamic IP allocation attempts:              21
    Dynamic IP allocation success:               21
  Charging statistics:
    Number of CDRs allocated:                   25
    Number of partial CDRs allocated:            0
    Number of CDRs closed:                      17
    Number of containers closed                  17
  Static policy statistics:
    Session establishment attempts using static policy: 0
    Session establishment success using static policy: 0
  DCCA-Gy Statistics:
    Online authorizations attempted:             0 Success : 0
    Online authorization timeouts:               0
    Quota threshold reauthorization requests sent: 0
  Gy Diameter msg statistics:
    CCR-Initial Sent : 0 Success : 0 Fail : 0
    CCR-Update Sent : 0 Success : 0 Fail : 0
    CCR-Terminate Sent : 0 Success : 0 Fail : 0
    RAR Received : 0 Answer : 0 Fail : 0
    ASR Received : 0 Answer : 0
    CCR Failure :
      Transient : 0
      Parameter : 0
      Permanent : 0
      Unknown code : 0
      Unknown session : 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
  PCC Gx statistics:
    Session attempts:                21 Success: 20
    MS-peer initiated APN-AMBR modification attempts: 0 Success: 0
    MS-peer initiated QoS modification attempts: 0 Success: 0

```

```

    PCRF initiated session deactivations:      0
    Gateway initiated session deactivations:   2
    MS-peer initiated session deactivations:   12
Gx modification statistics:
    Initiated by MS-peer: 0      Success: 0
    Initiated by PCRF: 8      Success: 0
Modification event reason:
    QoS change: 0      RAT change: 0
    SGSN change: 0      SGW change: 0
    PLMN change: 0      RAI change: 0
    ULI change: 0      IP-CAN change: 0
    TFT change (MS): 0      TFT change (Network): 0
    Bearer loss: 0      Bearer recovery: 0
    Resource allocation: 0      Revalidation Timeout: 0
    QoS exceeding auth: 0      Time-of-Day procedure: 0
    Change of Subscription: 0      AMBR change: 0
    ECGI change: 0      TAI change: 0
    Timezone change: 0      Default-EPS-QoS change: 0
Dedicated bearer statistics:
    MS-peer initiated activation attempts: 0      Success: 0
    Network initiated activation attempts: 7      Success: 5
    MS-peer initiated modification attempts: 0      Success: 0
    Network initiated modification attempts: 0      Success: 0
    MS-peer initiated deactivations: 5
    Network initiated deactivations: 0
    Gateway initiated deactivations: 0
Gx Failure Statistics:
    GBR dedicated bearer create failure due to CAC: 0
    Non-GBR dedicated bearer create failure due to CAC: 0
    Session terminations due to unreachable PCRF: 0
    Session terminations due to PCRF restart: 0
Gx diameter message statistics:
    CCR-I sent: 21      CCA-I received: 20
    CCR-U sent: 20      CCA-U received: 20
    CCR-T sent: 15      CCA-T received: 0
    RAR received: 8      RAA sent: 6
    RAA sent resource failure: 0
CCR failure reason:
    Transient failure: 0      Initial params error: 0
    Permanent failure: 0      Unknown code: 0
    Unknown session: 0
Gx rule statistics:
    Dynamic rule activations: 0      Deactivations: 0
    Static rules activations: 10      Deactivations: 10
    Dynamic rule modifications: 20
Rule failure statistics:
    Rule validation failure: 14
    Rule enforcement failure no resource: 2
    Rule activation failure no resource: 0
    Rule update procedure fail: 0
Handover Statistics:
    Inter-RAT Handover attempts: 0      Success: 0
    Intra-RAT Handover attempts: 0      Success: 0
Data plane statistics:
    Total packets violating MIF ACL: 0
    Total accepted mobile-to-mobile packets: 0
    Total accepted mobile-to-mobile bytes: 0
Miscellaneous Packet statistics:
    IPv6 Router Solicitations received: 0
    IPv6 Router Advertisement transmitted: 0
    IPv6 Neighbor Solicitations received: 0

```



```

IPv6 Neighbor Advertisement transmitted:    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 The `show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic` command displays the control plane Gx statistics for an APN. If the output shows that session attempts are successful, then the connection to the PCEF is functioning properly.

Verifying Application Identification Counter Statistics

Purpose Verify the application identification (APPID) statistics on the broadband gateway.

Action `user@host> show services application-identification counter`

```

Counter Statistics:
  pic: ams1
  Total sessions: 78537
  Total identified sessions: 78537
  Total un-identified sessions: 0
  Protocol Method
    Total identified-by-protocol sessions: 0
    Total un-identified-by-protocol sessions: 0
  Address Method
    Total identified-by-address sessions: 0
    Total un-identified-by-address sessions: 78537
  Port Method
    Total identified-by-port sessions: 2053
    Total un-identified-by-port sessions: 0
    Total identified-by-icmp sessions: 0
    Total un-identified-by-icmp sessions: 0
    Total identified-by-ip-protocol sessions: 0
    Total un-identified-by-ip-protocol sessions: 0
  Signature Method
    Total identified-by-signature sessions: 76484
    Total identified-by-signature uni-directional sessions: 0
    Total un-identified-by-signature sessions: 2053
    Total unspecified encrypted sessions: 0
    Total encrypted P2P sessions detected by heuristics: 0
    Total application system cache hits: 0
    Total application system cache misses: 0

```

Verifying Application Signatures Counter Statistics

Purpose Verify detailed information about a specified application signature, all application signatures, or a summary of the existing application signatures and nested application signatures. Both custom and predefined application signatures and nested application signatures can be displayed.

```
Action user@host> show services application-identification application detail junos:FACEBOOK-ACCESS
re0:
Application Name: junos:FACEBOOK-ACCESS
Application type: FACEBOOK-ACCESS
Description: This signature detects requests to Facebook.com, a social networking
Web site.
Application ID: 311
Disabled: No
Number of Parent Group(s): 1
Application Groups:
  junos:social-networking:facebook
Application Tags:
  characteristic      : Loss of Productivity
  characteristic      : Supports File Transfer
  characteristic      : Known Vulnerabilities
  characteristic      : Capable of Tunneling
  characteristic      : Can Leak Information
  risk                : 5
  subcategory         : Facebook
  category            : Social-Networking
Signature NestedApplication:FACEBOOK-ACCESS
Layer-7 Protocol: HTTP
Chain Order: Yes
Maximum Transactions: 20
Order: 33322
Member(s): 1
  Member 0
    Context: http-header-host
    Pattern: (.*\.)?(facebook\.com|fbcdn\.net)(:\d+)?
    Direction: CTS
```

Troubleshooting

To troubleshoot the policy and charging enforcement function (PCEF) configuration, perform these tasks:

- [Connection Is Down Between the PCEF and PCRF on page 84](#)
- [PCEF and PCRF Application Messages Are Not Sent or Received on page 85](#)

Connection Is Down Between the PCEF and PCRF

Problem The connection between the PCEF and PCRF peers on the Gx interface appears to be down.

Solution To display the Diameter peer status for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer status** command.

```
user@host> show unified-edge ggsn-pgw diameter peer status
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:          6
  Successful session establishments:        6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
```

```

    Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy:      6      Success: 6
  Dedicated bearer activation attempts:      5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:          0
  Non-existent TEID/TID packets:            0
  GTP length error packets:                 0
  Non-existent UE address packets:          0
  Mobile-to-mobile packets:                0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0

```

2. Check that status of the State field, which is displayed at the beginning of the output. When the connection between the Diameter peers (PCEF and PCRF) is up, the State status indicates **I-Open**.
3. Check that the status of the Watchdog State field, which is displayed near the beginning of the output. When Diameter peers are connected, the Watchdog State status indicates **okay**.

PCEF and PCRF Application Messages Are Not Sent or Received

Problem The PCRF and PCEF application messages (Re-Authorization Request/Re-Authorization Answer or Credit Control Request/Credit Control Answer) are not being sent or received.

Solution To display the status of application messages for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer statistics** command.

```

user@host> show unified-edge ggsn-pgw diameter peer statistics
Peer: p1
Request Timeouts:          0
Request Retransmissions:   0
Messages                   Transmitted      Received
-----
Total Messages             22              22
Credit Control Requests    14              0
Credit Control Answers     0              14
Re-Auth Requests           0              2
Re-Auth Answers            2              0
Abort Session Requests     0              0
Abort Session Answers       0              0
Capability Exchange Requests 2              0

```

Capability Exchange Answers	0	2
Device Watchdog Requests	4	0
Device Watchdog Answers	0	4
Disconnect Peer Requests	0	0
Disconnect Peer Answers	0	0

2. Check that for each message type, there are an equal number of messages for requests and answers.

**Related
Documentation**

- [Application-Aware Policy and Charging Control Rules Overview on page 9](#)
- [APPID Feature Overview on page 11](#)
- [Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules on page 39](#)

CHAPTER 4

Configuration Statements

- [\[edit unified-edge pcef\] Hierarchy Level on page 87](#)
- [\[edit services service-set\] Hierarchy Level on page 89](#)
- [\[edit services pcef\] Hierarchy Level on page 89](#)

[\[edit unified-edge pcef\] Hierarchy Level](#)

```
unified-edge {
  pcef {
    event-trigger-profiles profile-name {
      ip-can-change;
      plmn-change;
      rai-change;
      rat-change;
      sgsn-change;
      tft-change;
      ue-timezone-change;
      user-location-change;
    }
    flow-descriptions flow-identifier {
      direction (uplink | downlink | both);
      local-port-range {
        low lower-boundary high upper-boundary;
      }
      local-ports number;
      no-send-to-ue;
      protocol number;
      remote-address;
      remote-port-range {
        low lower-boundary high upper-boundary;
      }
      remote-ports number;
    }
    pcc-action-profiles profile-name {
      allocation-retention-priority {
        preemption-capability (enable | disable);
        preemption-vulnerability (enable | disable);
        priority-level value;
      }
      charging {
        application-function-record-info {
```

```

        af-charging-identifier identifier;
    }
    charging-method (online | offline | online-offline | none);
    measurement-method (volume | time | volume-time | event);
    rating-group number;
    service-identifier number;
    service-id-level-reporting;
}
gate-status (uplink | downlink | uplink-downlink | disable-both);
guaranteed-bit-rate uplink value downlink value;
maximum-bit-rate uplink value downlink value;
qci value;
}
pcc-rules rule-name {
    from {
        application-groups [application-name];
        applications [application-name];
        flows [flow-identifier];
        nested-applications [application-name];
    }
    then {
        pcc-action-profiles profile-name;
    }
}
pcc-rulebases rulebase-name {
    [pcc-rule rule-name number];
    profiles profile-name {
        dynamic-policy-control {
            diameter-profile gx-profile-name;
            event-trigger-profile profile-name;
            failure-handling {
                failure-action (continue | continue-and-retry | terminate);
                pcc-rules pcc-rule-name precedence precedence-number;
                pcc-rulebases pcc-rulebase-name;
            }
            pcc-rulebases [rulebase-name];
            pcc-rules [rule-name precedence-number];
            release (r8 | r9);
            session-failover-not-supported;
        }
        static-policy-control {
            activate-dedicated-bearers [[qci-value]];
            pcc-rules [rule-name number];
            pcc-rulebases [rulebase-name];
        }
    }
}
}
}

```

**Related
Documentation**

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

[edit services service-set] Hierarchy Level

```

service-set service-set-name {
  interface-service {
    load-balancing-options {
      hash-keys {
        egress-key (destination-ip | source-ip);
        ingress-key (destination-ip | source-ip);
        resource-triggered;
      }
    }
    service-interface interface-name.unit-number;
  }
  ip-reassembly-rules {
    [rule-name];
  }
  next-hop-service {
    inside-service-interface interface-name.unit-number;
    outside-service-interface interface-name.unit-number;
    outside-service-interface-type interface-type;
    service-interface-pool name;
  }
  [pcef-profile profile-name];
  [tag-rule-sets rule-set-name];
  [tag-rules rule-name];
  service-set-options {
    subscriber-awareness;
  }
}

```

Related
Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit services pcef] Hierarchy Level

```

pcef {
  [profile profile-name];
}

```

Related
Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

activate-dedicated-bearers

Syntax	activate-dedicated-bearers [<i>qci-value</i>];
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> static-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Configure the activate-dedicated-bearers statement so that a Create Session request creates one or more dedicated bearers, in addition to the default bearer. For each QoS Class Identifier (QCI) value you configure in the activate-dedicated-bearers statement, a dedicated bearer for that QCI value is created along with the default bearer.
Options	qci-value —A QCI value (1 through 9) for the dedicated bearer. To create multiple dedicated bearers, list the QCI values within square brackets ([]) and include a space between each value, for example, [4 5 6].
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• static-policy-control on page 136• Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36

af-charging-identifier

Syntax	af-charging-identifier <i>identifier</i> ;
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> charging application-function-record-info]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the application function charging identifier for enabling charging correlation between the application and bearer layer if the application function has provided this information via the Rx interface.
Options	identifier —The name of the application function charging identifier. Range: Up to 63 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	<ul style="list-style-type: none">• application-function-record-info on page 91• Configuring Policy and Charging Control Action Profiles on page 28


allocation-retention-priority (PCC Action Profiles)

Syntax	allocation-retention-priority { priority-level <i>priority-value</i> ; preemption-capability (enable disable); preemption-vulnerability (enable disable); }
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W
Description	<p>The configuration in this hierarchy determines the allocation and retention priority (ARP) for a Policy and Charging Control (PCC) action profile. This configuration provides the ARP value, preemption capability, and preemption vulnerability for the PCC rules, which, in turn, define the quality-of-service (QoS) for a bearer.</p> <p>The remaining statements are explained separately.</p>
Default	If this statement is not included, then the broadband gateway uses the ARP value sent in the PDP Context Request or Session Request message.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • pcc-action-profiles on page 113 • Configuring Policy and Charging Control Action Profiles on page 28


application-function-record-info

Syntax	application-function-record-info { af-charging-identifier <i>identifier</i> ; }
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	<p>The configuration in this hierarchy determines the application function charging identifier.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • charging on page 94 • pcc-action-profiles on page 113 • Configuring Policy and Charging Control Action Profiles on page 28

application-groups (PCC Rules)

Syntax	<code>application-groups [<i>application-group-name</i>];</code>
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rule-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	<p>An application group is defined in the application-identification engine from the [edit services application-identification] hierarchy level. Specify one or more application groups to define the match criteria for the Policy and Charging Control (PCC) rule. You can specify a maximum of 10 application groups in a PCC rule.</p> <div><p>NOTE: For any PCC rule, the subscriber must match the match conditions specified in a from statement. You must configure, at minimum, one flow identifier, application, application group, or nested application in the from statement of a PCC rule.</p></div>
Options	<p><i>application-group-name</i>—Name of an application group that is used to detect IP packet flows. The referenced application group must be defined.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• from on page 104• Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

applications (PCC Rules)

Syntax	<code>applications [<i>application-name</i>];</code>
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rule-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	An application is defined in the application-identification engine from the [edit services application-identification] hierarchy level. Specify one or more applications to define the match criteria for the Policy and Charging Control (PCC) rule. You can specify a maximum of 10 applications in a PCC rule.
	<div>  <p>NOTE: For any PCC rule, the subscriber must match the match conditions specified in a from statement. You must configure, at minimum, one flow identifier, application, application group, or nested application in the from statement of a PCC rule.</p> </div>
Options	<p>application-name—Name of an application that is used to detect IP packet flows. The referenced application must be defined.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • from on page 104 • Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

charging (PCC Action Profiles)

Syntax	<pre>charging { application-function-record-info { af-charging-identifier <i>identifier</i>; } charging-method (online offline online-offline none); measurement-method (volume time volume-time event); rating-group <i>number</i>; service-identifier <i>number</i>; service-id-level-reporting; }</pre>
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	<p>The configuration in this hierarchy determines the overall charging configuration for the Policy and Charging Control (PCC) rule that references the PCC action profile.</p> <p>The remaining statements are explained separately.</p>
Default	If the charging statement is not included in the PCC action profile, then the PCC rule that references the PCC action profile provides no charging information.
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• pcc-action-profiles on page 113• Configuring Policy and Charging Control Action Profiles on page 28

charging-method (PCC Action Profiles)

Syntax	charging-method (both offline online none);
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the default charging method in the PCC action profile. The broadband gateway uses the configured default charging method only when the policy and charging rules function (PCRF) or a static policy for the policy and charging enforcement function (PCEF) does not provide a charging method.
Default	If you do not include this statement, then the default charging method is set to offline charging (offline).
Options	<p>online—Use only the online charging method.</p> <p>offline—Use only the offline charging method.</p> <p>online-offline—Use both offline and online charging methods.</p> <p>none—No charging method is used.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging on page 94 • Configuring Policy and Charging Control Action Profiles on page 28

diameter-profile (Gx)

Syntax	diameter-profile <i>gx-profile-name</i> ;
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Specify the Gx interface Diameter parameters profile that the PCEF profile will use. A PCEF profile with dynamic policy control must reference a defined Diameter profile. The Gx Diameter profile must be correctly configured in the Diameter portion of the command-line interface (CLI).
Options	gx-profile-name —Name of the Gx Diameter profile to use with this dynamic policy control 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	<ul style="list-style-type: none">• dynamic-policy-control on page 97• Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34

direction (Service Data Flow Filters)

Syntax	direction (uplink downlink both);
Hierarchy Level	[edit unified-edge pcef flow-descriptions <i>flow-identifier</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the direction in which service data flow (SDF) filters will detect service flow IP packets and PCC rules are applied.
Default	If you do not configure the direction statement, the default direction is both .
Options	uplink —SDF filters are applied in the uplink direction. downlink —SDF filters are applied in the downlink direction. both —SDF filters are applied in both the uplink and downlink directions.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• Configuring Service Data Flow Filters (Flow Identifiers) on page 27

dynamic-policy-control

Syntax

```
dynamic-policy-control {
  failure-handling {
    failure-action (continue | continue-and-retry | terminate);
    pcc-rulebases pcc-rulebase-name;
    pcc-rules pcc-rule-name precedence precedence-number;
  }
  pcc-rules {
    [rule-name number];
  }
  pcc-rulebases {
    [rulebase-name];
  }
  diameter-profile gx-profile-name;
  event-trigger-profile profile-name;
  release (r8 | r9);
  session-failover-not-supported;
}
```

Hierarchy Level [edit unified-edge pcef profiles *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1W.

Description Configure the dynamic policy control for the PCC rules, PCC rulebases, or both in a PCEF profile. You can configure a maximum of 32 PCC rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.



NOTE: If you configure the `dynamic-policy-control` statement for a PCEF profile, you cannot configure the `static-policy-control` statement in the same 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

- [profiles on page 127](#)
- [static-policy-control on page 136](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36](#)

event-trigger-profile

Syntax	<code>event-trigger-profile <i>profile-name</i>;</code>
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Specify the event trigger profile that a policy and charging enforcement function (PCEF) profile configured with dynamic policy control will use. The event trigger profile must be correctly configured in the trigger profile portion of the command-line interface (CLI).
Default	By default, if this statement is not configured, then only implicit event triggers are enabled.
Options	profile-name —Name of the event trigger profile to use in a PCEF 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	<ul style="list-style-type: none">• dynamic-policy-control on page 97• Configuring Event Trigger Profiles on page 33

event-trigger-profiles

Syntax `event-trigger-profiles profile-name {
 ip-can-change;
 plmn-change;
 rai-change;
 rat-change;
 sgsn-change;
 tft-change;
 ue-timezone-change;
 user-location-change;
}`

Hierarchy Level [edit unified-edge pcef]

Release Information Statement introduced in Junos OS Release 12.1W.

Description Configure event trigger profiles to notify the policy and charging rules function (PCRF) about changes in the access network. When an event occurs that matches an event trigger configured on the policy and charging enforcement function (PCEF), the PCEF reports the event to the PCRF. If the PCRF determines that a change to its current policy is necessary, it can send new or updated PCC rules to the PCEF to address those changes.

After you configure an event trigger profile, you can include the event trigger profile in a PCEF profile configured with dynamic policy control.

Options The following event triggers can be configured in an event trigger profile:

profile-name—Name of the event trigger profile.

ip-can-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a IP Connectivity Access Network (IP-CAN) change.

plmn-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Public Land Mobile Network (PLMN) change.

rai-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Routing Area Identification (RAI) change.

rat-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Radio Access Technology (RAT) change.

sgsn-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Serving GPRS Support Node (SGSN) change.

tft-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Traffic Flow Template (TFT) change.

ue-time-zone-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a user equipment (UE) time zone change.

user-location-change—Configure an event trigger to send notification to the PCRF when the broadband gateway detects a user equipment (UE) location change.

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

Related Documentation

- [pcef on page 119](#)
- [Configuring Event Trigger Profiles on page 33](#)

failure-action

Syntax failure-action (continue | continue-and-retry | terminate);

Hierarchy Level [edit unified-edge pcef profiles *profile-name* dynamic-policy-control failure-handling]

Release Information Statement introduced in Junos OS Release 12.1W2.

Description Specify that when the policy and charging rules function (PCRF) goes down, one of the following actions is initiated:

- **continue**—Continue the existing Gx session with the dynamic rules and rulebases (if the rules are present), but the PCEF makes no retry attempts. Even when the link is up, no message is triggered towards the PCRF.
- **continue-retry**—Continue the existing Gx session and the PCEF will attempt to reconnect with the PCRF.
- **terminate**—Terminate the existing session and start a new session by applying the rule or rulebase that is configured in the failure-handling container in the PCEF 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

- [failure-handling on page 101](#)
- [dynamic-policy-control on page 97](#)
- [Configuring a Policy and Charging Control Rulebase on page 32](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)

failure-handling

Syntax	<pre>failure-handling { failure-action (continue continue-and-retry terminate); pcc-rulebases pcc-rulebase-name; pcc-rules pcc-rule-name precedence precedence-number; }</pre>
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W2.
Description	<p>The remaining statements are explained separately.</p> <p>Specify that when the policy and charging rules function (PCRF) goes down, one of the following actions is initiated:</p> <ul style="list-style-type: none"> Continue the existing session with the dynamic rules and rulebases (if the rules are present). Terminate the existing session and start a new session by applying the PCC rules or PCC rulebase specified in the failure-handling container in the PCEF profile. <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> dynamic-policy-control on page 97 Configuring a Policy and Charging Control Rulebase on page 32 Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

flow-descriptions

Syntax `flow-descriptions flow-identifier {
 direction (uplink | downlink | both);
 local-port-range {
 low lower-boundary high upper-boundary;
 }
 local-ports number;
 no-send-to-ue;
 protocol protocol-number;
 remote-address;
 remote-port-range {
 low lower-boundary high upper-boundary;
 }
 remote-ports number;
 }`

Hierarchy Level [edit unified-edge pcef]

Release Information Statement introduced in Junos OS Mobility Release 12.1W.

Description A service data flow (SDF) filter (flow identifier) includes one or more filtering parameters (address, protocol, and port) to identify the subscriber traffic that the SDF filter will detect. Flow identifiers are specified in a PCC rule to associate IP packet flows with bearers to apply the appropriate quality of service (QoS), charging, and gating control.



NOTE: A PCC rule must include at least one flow identifier and can include a maximum of 15 flow identifiers.

The remaining statements are explained separately.


Options **flow-identifier**—Name of the SDF filter.
Range: Up to 63 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

- [pcef on page 119](#)
- [Configuring Service Data Flow Filters \(Flow Identifiers\) on page 27](#)

flows

Syntax	<code>flows [<i>flow-identifier</i>];</code>
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rule-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the service data flow (SDF) filters (flow identifiers) that define the match criteria for the Policy and Charging Control (PCC) rule. You can configure a maximum of 15 flow identifiers in a flows statement.
<div>  <p>NOTE: For any PCC rule, the subscriber must match one of the flow-identifier, application, or application-group match conditions specified in a from statement. You must configure at minimum one flow identifier, application, or application group in the from statement of a PCC rule.</p> </div>	
Options	<p>flow-identifier—Name of an SDF filter that is used to detect IP packet flows. The referenced flow identifier must be defined.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • from on page 104 • Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

from (PCC Rules)

Syntax from {
 [application-groups](#) [*application-name*];
 [applications](#) [*application-name*];
 [flows](#) [*flow-identifier*];
 [nested-applications](#) [*application-name*];
 }

Hierarchy Level [edit unified-edge pcef pcc-rules *rule-name*]

Release Information Statement introduced in Junos OS Mobility Release 12.1W.

Description Specify the match criteria for the Policy and Charging Control (PCC) rules.



.....
NOTE: A PCC rule must include at least one flow identifier, application, application group, or nested application in the *from* statement.
.....

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 • [pcc-rules on page 118](#)
 • [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)


gate-status

Syntax	gate-status (uplink downlink uplink-downlink disable-both);
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Configure the gate status in a PCC action profile to enable or disable the forwarding of service flow packets. The gate status determines whether the uplink and downlink gates are opened or closed.
Default	By default, if this statement is not configured, forwarding of service data flow packets is enabled in both the uplink and downlink directions.
Options	<p>uplink—Enables forwarding of service data flow packets in the uplink direction.</p> <p>downlink—Enables forwarding of service data flow packets in the downlink direction.</p> <p>uplink-downlink—Enables forwarding of service data flow packets in the uplink and downlink directions.</p> <p>disable-both—Disables forwarding of service data flow packets in the uplink and downlink directions.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • pcc-action-profiles on page 113 • Configuring Policy and Charging Control Action Profiles on page 28


guaranteed-bit-rate

Syntax	<code>guaranteed-bit-rate uplink <i>gbr-uplink-value</i> downlink <i>gbr-downlink-value</i>;</code>
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	<p>Configure the guaranteed bit rate (GBR) for uplink and downlink traffic.</p> <p>The GBR specifies the total guaranteed bit rate for all GBR bearers associated with a specific gateway or access point name (APN).</p>
Default	If you configure the guaranteed-bit-rate statement but do not specify GBR values for uplink and downlink , the default value is 0.
Options	<p>gbr-uplink-value—Specify the GBR value in the uplink direction. Range: 1 through 256,000 kbps</p> <p>gbr-downlink-value—Specify the GBR value in the downlink direction. Range: 1 through 256,000 kbps</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• pcc-action-profiles on page 113• maximum-bit-rate on page 109• Configuring Policy and Charging Control Action Profiles on page 28

local-port-range

Syntax	<pre>local-port-range { low <i>low-value</i>; high <i>high-value</i>; }</pre>
Hierarchy Level	[edit unified-edge pcef flow-descriptions <i>flow-identifier</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the port range to identify the subscriber traffic that the service data flow (SDF) filter will detect.
<div>  <p>NOTE: You can specify either a port range or a list of ports, but not both.</p> </div>	
Default	If the local-port-range statement is not configured, the default is any range of local ports.
Options	<p><i>low-value</i>— Lower boundary for the port range. Range: 1 through 65,535</p> <p><i>high-value</i> — Upper boundary for the port range. Range: 1 through 65,535</p>
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • flow-descriptions on page 102 • local-ports on page 108 • Configuring Service Data Flow Filters (Flow Identifiers) on page 27

local-ports

Syntax	local-ports [<i>number</i>];
Hierarchy Level	[edit unified-edge pcef flow-description <i>flow-identifier</i>]
Description	Specify a port number or list of port numbers to identify the subscriber traffic that the service data flow (SDF) filter will detect.
	<div> NOTE: You can specify either a list of ports or a port range, but not both.</div>
Default	If the local-ports statement is not configured, the default is any local ports.
Options	number —A port number or list of port numbers. You can specify a maximum of three port numbers (separated by a space) in a list. Range: 1 through 65,535
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• local-port-range on page 107• Configuring Service Data Flow Filters (Flow Identifiers) on page 27


maximum-bit-rate

Syntax	maximum-bit-rate uplink <i>mbr-uplink-value</i> downlink <i>mbr-downlink-value</i> ;
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]
Description	<p>Configure the MBR for uplink and downlink traffic.</p> <p>The MBR specifies the total maximum bit rate (MBR) for all non-GBR bearers associated with a specific gateway or access point name (APN).</p>
Default	If you configure the maximum-bit-rate statement but do not specify MBR values for uplink and downlink , the default value is 0.
Options	<p>mbr-uplink-value—Specify the MBR value for the uplink direction. Range: 1 through 256,000 kbps</p> <p>mbr-downlink-value—Specify the MBR value for the downlink direction. Range: 1 through 256,000 kbps</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • pcc-action-profiles on page 113 • guaranteed-bit-rate on page 106 • Configuring Policy and Charging Control Action Profiles on page 28

measurement-method (PCC Action Profiles)

Syntax	measurement-method (volume time volume-time event);
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the usage measurement method used by the PCEF to support charging. The Online Charging System (OCS) provides credit management and grants credit to the PCEF based on volume, time, or both volume and time.
Default	By default, if this statement is not configured, the volume-time measurement method is enabled.
Options	<p>volume—Specify volume as the usage measurement method that the PCEF uses to support charging.</p> <p>time—Specify time as the usage measurement method that the PCEF uses to support charging.</p> <p>volume-time—Specify volume and time as the usage measurement method that the PCEF uses to support charging.</p> <p>event—Specify event as the usage measurement method that the PCEF uses to support charging.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• charging on page 94• Configuring Policy and Charging Control Action Profiles on page 28

nested-applications (PCC Rules)

Syntax	<code>nested-applications [<i>application-name</i>];</code>
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rule-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	A nested application is defined in the application-identification engine from the [edit services application-identification] hierarchy level. Specify one or more nested applications to define the match criteria for the Policy and Charging Control (PCC) rule. You can specify a maximum of 10 nested applications in a PCC rule.
	<div>  <p>NOTE: For any PCC rule, the subscriber must match the match conditions specified in a from statement. You must configure, at minimum, one flow identifier, application, application group, or nested application in the from statement of a PCC rule.</p> </div>
Options	<p><i>application-name</i>—Name of a nested application that is used to detect IP packet flows. The referenced nested application must be defined.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • from on page 104 • Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

no-send-to-ue

Syntax	no-send-to-ue;
Hierarchy Level	[edit unified-edge pcef flow-description <i>flow-identifier</i>]
Description	Specify that signaling information about the service data flow (SDF) filter is not sent to the user equipment (UE).
Default	By default, if this statement is not configured, signaling information about the SDF filter is sent to the UE.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• Configuring Service Data Flow Filters (Flow Identifiers) on page 27

pcc-action-profile

Syntax	pcc-action-profile <i>profile-name</i> ;
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rules-name</i> then]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	A pcc-action-profile statement specifies the name of the action profile to include in a Policy and Charging Control (PCC) rule configuration. The referenced action profile must be defined. The QoS, charging, and gating controls specified in the PCC action profile are applied to subscriber traffic that matches the SDF filters (flow identifiers) in the PCC rule.
Options	profile-name —Name of the PCC action profile that the PCC rule references. Range: Up to 63 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	<ul style="list-style-type: none">• pcc-rules on page 118• Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

pcc-action-profiles

```
Syntax  pcc-action-profiles profile-name {
        allocation-retention-priority {
            preemption-capability (enable | disable);
            preemption-vulnerability (enable | disable);
            priority-level value;
        }
        charging {
            application-function-record-info {
                af-charging-identifier identifier;
            }
            charging-method (online | offline | online-offline | none);
            gate-status (uplink | downlink | uplink-downlink | disable-both);
            guaranteed-bit-rate uplink value downlink value;
            maximum-bit-rate uplink value downlink value;
            measurement-method (volume | time | volume-time | event);
            rating-group number;
            service-identifier number;
            service-id-level-reporting;
        }
        qci value;
    }
```

Hierarchy Level [edit unified-edge pcef]

Release Information Statement introduced in Junos OS Mobility Release 12.1W.

Description A Policy and Charging Control (PCC) action profile defines the quality-of-service (QoS) control, charging control, and gating status for a PCC rule. The policy and charging enforcement function (PCEF) maps one or more PCC rules to a bearer in the access network to provide the QoS, charging, and gating treatment for IP packets.

The remaining statements are explained separately.

Options **profile-name**—Name of the PCC action profile.

Range: Up to 63 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

- [pcef on page 119](#)
- [Configuring Policy and Charging Control Action Profiles on page 28](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)

pcc-rule

Syntax	[pcc-rule <i>rule-name</i> precedence <i>precedence</i>];
Hierarchy Level	[edit unified-edge pcef pcc-rulebases <i>rulebase-name</i>]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Configure one or more Policy and Charging Control (PCC) rules and the rules precedence in a PCC rulebase.
Options	rule-name —Name of the previously configured PCC rule.



NOTE: The PCC rule must be previously configured at the [edit unified-edge pcef pcc-rules] hierarchy level.

Range: Up to 63 characters.

number—A precedence value assigned to the PCC rule.




NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

Range: 1 through 65,535

Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• pcc-rulebases (PCEF) on page 116• pcc-rules (PCEF) on page 118• Configuring a Policy and Charging Control Rulebase on page 32

pcc-rulebases (PCEF Profile)

Syntax	[pcc-rulebases <i>rulebase-name</i>];
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control] [edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control failure-handling] [edit unified-edge pcef profiles <i>profile-name</i> static-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Configure a Policy and Charging Control (PCC) rulebase for a dynamic or static policy control profile.
	<div>  <p>NOTE: The use of dynamic or static policy control is mutually exclusive. You can configure dynamic or static policy control for a profile, but not both.</p> </div>
Options	<i>rulebase-name</i> —Name of the PCC rulebase. The referenced PCC rulebase must be defined.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • dynamic-policy-control on page 97 • static-policy-control on page 136 • Configuring a Policy and Charging Control Rulebase on page 32 • Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

pcc-rulebases (PCEF)

Syntax	<code>pcc-rulebases <i>rulebase-name</i> { [pcc-rule <i>rule-name</i> precedence <i>number</i>]; }</code>
Hierarchy Level	[edit unified-edge pcef]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	<p>Configure a Policy and Charging Control (PCC) rulebase. You can specify from 1 to 4,000 rules in a rulebase.</p> <p>The remaining statements are explained separately.</p>
Options	<p>rulebase-name—Name of the PCC rulebase.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• pcc-rules on page 118• Configuring a Policy and Charging Control Rulebase on page 32

pcc-rules (PCEF Profile)

Syntax	<code>pcc-rules [rule-name precedence precedence];</code>
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control], [edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control failure-handling], [edit unified-edge pcef profiles <i>profile-name</i> static-policy-control]
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Specify the Policy and Charging Control (PCC) rules in a dynamic policy or static policy and assign a precedence to each PCC rule. You can configure up to 32 PCC rules in a PCEF profile.



NOTE: The use of dynamic or static policy control is mutually exclusive. You can configure dynamic or static policy control for a policy and charging enforcement function (PCEF) profile, but not both.

Options `rule-name`—Name of the previously configured PCC rule.



NOTE: The PCC rule must be previously configured at the [edit unified-edge pcef pcc-rules] hierarchy level.

`number`—A precedence value assigned to a PCC rule.



NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC profile has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

Range: 1 through 65,535

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 Policy and Charging Control Rulebase on page 32](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)
- [dynamic-policy-control on page 97](#)

- [failure-handling on page 101](#)
- [static-policy-control on page 136](#)

[pcc-rules \(PCEF\)](#)

Syntax `pcc-rules rule-name {
 from {
 applications [application-name];
 application-groups [application-name];
 flows [flow-identifier];
 nested-applications [application-name];
 }
 then {
 pcc-action-profile profile-name;
 }
 }`

Hierarchy Level `[edit unified-edge pcef]`

Release Information Statement introduced in Junos OS Release 12.1W.

Description Configure the Policy and Charging Control (PCC) rules. A PCC rule identifies the subscriber IP packets that are associated with a service data flow (SDF) and provides the quality-of-service (QoS) control, charging control, and gating status for a specified SDF. A PCC rule must include at least one flow identifier, application, or application group in the **from** statement and a PCC action profile in the **then** statement.

The remaining statements are explained separately.

Options **rule-name**—Name of the PCC rule.
 Range: Up to 63 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 • [pcef on page 119](#)
 • [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30](#)

pcef

```

Syntax  pcef {
    event-trigger-profiles profile-name {
        ip-can-change;
        plmn-change;
        rai-change;
        rat-change;
        sgsn-change;
        tft-change;
        ue-timezone-change;
        user-location-change;
    }
}
flow-descriptions flow-identifier {
    direction (uplink | downlink | both);
    local-port-range {
        low lower-boundary high upper-boundary;
    }
    local-ports number;
    no-send-to-ue;
    protocol number;
    remote-address;
    remote-port-range {
        low lower-boundary high upper-boundary;
    }
    remote-ports number;
}
pcc-action-profiles profile-name {
    allocation-retention-priority {
        preemption-capability (enable | disable);
        preemption-vulnerability (enable | disable);
        priority-level value;
    }
    charging {
        application-function-record-info {
            af-charging-identifier identifier;
        }
        charging-method (online | offline | online-offline | none);
        gate-status (uplink | downlink | uplink-downlink | disable-both);
        guaranteed-bit-rate uplink value downlink value;
        maximum-bit-rate uplink value downlink value;
        measurement-method (volume | time | volume-time | event);
        qci value;
        rating-group number;
        service-identifier number;
        service-id-level-reporting;
    }
}
pcc-rules rule-name {
    from {
        applications [application-name];
        application-groups [application-name];
        flows [flow-identifier];
    }
}

```

```

        nested-applications [application-name ];
    }
    then {
        pcc-action-profiles profile-name;
    }
}
pcc-rulebases rulebase-name {
    [pcc-rule rule-name precedence number];
}
profiles profile-name {
    dynamic-policy-control {
        diameter-profile profile-name;
        event-trigger-profile profile-name;
        failure-handling {
            failure-action (continue | continue-and-retry | terminate);
            pcc-rules pcc-rule-name precedence precedence-number;
            pcc-rulebases pcc-rulebase-name;
        }
        pcc-rules {
            [rule-name precedence number];
        }
        pcc-rulebases {
            [rule-base-name];
        }
        release (r8 | r9);
        session-failover-not-supported;
    }
    static-policy-control {
        activate-dedicated-bearers [[qci-value]];
        pcc-rulebases [rulebase-name];
        pcc-rules {
            [rule-name precedence number];
        }
    }
}
}
}

```

Hierarchy Level [edit unified-edge]

Release Information Statement introduced in Junos OS Mobility Release 12.1W.

Description The configuration in this hierarchy determines the overall policy and control enforcement function (PCEF) configuration.

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 | <ul style="list-style-type: none"> • Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34 • Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36 • Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30 • Configuring a Policy and Charging Control Rulebase on page 32 • Configuring Event Trigger Profiles on page 33 • Policy and Charging Enforcement Function Overview on page 3 • Policy and Charging Control Rules Overview on page 5 |
|------------------------------|--|

pcef (Services)

Syntax	<pre>pcef { profile profile-name; }</pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	<p>Configure a policy and charging enforcement function (PCEF) service to be referenced in a service set.</p> <p>The remaining statements are explained separately.</p>
Options	<p>profile-name—Name of the PCEF service profile.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>service-set (Aggregated Multiservices)</i> • Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25

pcef-profile (Service Set)

Syntax	<code>pcef-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit services service-set <i>service-set-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 12.1W2.
Description	Configure the PCEF parameters to be applied to the broadband gateway. <div><div></div><div><p>NOTE: The configuration in the <code>pcef-profile</code> statement is applicable only to PCEF on the services PIC.</p></div></div> <div><p>Specifies the service to use as the application-aware PCEF service. The PCEF profile you specify in a service set must reference a PCEF profile configured at the <code>[edit services]</code> hierarchy level.</p></div> <div><div></div><div><p>NOTE: The application-identification plugin and PCEF plugin must both be configured in the service set. The application-identification plugin is required for inspection of application-aware traffic, and the PCEF service uses the results of the inspection to apply policies (PCC rules) to subscriber traffic.</p></div></div>
Options	<p><i>profile-name</i>—The name of the PCEF plugin for policy and charging enforcement for all subscriber traffic.</p> <p>Range: Up to 63 characters.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><i>service-set (Aggregated Multiservices)</i>Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25


preemption-capability

Syntax	preemption-capability (enable disable);
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> allocation-retention-priority]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W
Description	Configure whether preemption capability should be enabled or disabled in the PCC action profile. Preemption aids in call admission control and enables the gateway to accommodate higher priority bearers over the lower priority bearers, based on the Preemption Capability Indicator (PCI) and Preemption Vulnerability Indicator (PVI).
Default	If you do not configure this statement, preemption capability is enabled by default.
Options	enable —Enable the preemption capability. disable —Disable the preemption capability.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• allocation-retention-priority on page 91• preemption-vulnerability on page 124• Configuring Policy and Charging Control Action Profiles on page 28

preemption-vulnerability

Syntax	preemption-vulnerability (enable disable);
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> allocation-retention-priority]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W
Description	Configure whether preemption vulnerability should be enabled or disabled in the PCC action profile. Preemption aids in call admission control and enables the gateway to accommodate higher priority bearers over the lower priority bearers, based on the Preemption Capability Indicator (PCI) and Preemption Vulnerability Indicator (PVI).
Default	If you do not configure this statement, preemption vulnerability is enabled by default.
Options	enable —Enable preemption vulnerability. disable —Disable preemption vulnerability.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• allocation-retention-priority on page 91• preemption-capability on page 123• Configuring Policy and Charging Control Action Profiles on page 28

priority-level (PCC Action Profiles)

Syntax	<code>priority-level <i>priority-value</i>;</code>
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> allocation-retention-priority]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Configure the allocation and retention priority (ARP) for the PCC action profile. This configuration is used in the establishment or modification of bearers when the bearer binding function (BBF) associates PCC rules with the bearers for a session.
Options	priority-value —Allocation retention priority used in the establishment or modification of bearers.
<div>  <p>NOTE: You must specify a value for the priority-level statement.</p> </div>	
Range: 1 through 15	
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • allocation-retention-priority on page 91 • Configuring Policy and Charging Control Action Profiles on page 28

profile (Services PCEF)

Syntax	<code>profile <i>profile-name</i>;</code>
Hierarchy Level	[edit services pcef]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	Before you configure application-aware PCC rules for Layer 7 traffic, you must configure a policy and charging enforcement function (PCEF) profile as a service. A PCEF profile configured at the [edit services pcef profile <i>profile-name</i>] hierarchy level refers to a plugin that specifies and enables PCEF functionality on the Junos OS services plane.
Options	<i>profile-name</i> —The name of a PCEF profile. Range: Up to 63 characters.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• pcef (Services) on page 121• Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 25

profiles (PCEF)

```
Syntax  profiles profile-name {
        dynamic-policy-control {
            diameter-profile gx-profile-name;
            event-trigger-profile profile-name;
            pcc-rulebases [rulebase-name];
            pcc-rules {
                [rule-name precedence number];
            }
            release (r8 | r9);
            session-failover-not-supported;
        }
        static-policy-control {
            activate-dedicated-bearers [[qci-values]];
            pcc-rules {
                [rule-name precedence number];
            }
            pcc-rulebases [rulebase-name];
        }
    }
```

Hierarchy Level [edit unified-edge pcef]

Release Information Statement introduced in Junos OS Release 12.1W.

Description A policy and charging enforcement function (PCEF) profile provides the overall PCEF configuration that can be applied to an APN or service-selection profile.



NOTE: You can configure either the `static-policy-control` statement or the `dynamic-policy-control` statement in a PCEF profile, but you cannot configure both statements in the same PCEF profile.



NOTE: When you configure the `dynamic-policy-control` statement in a PCEF profile, you must also specify a Diameter Gx profile from the `diameter-profile` statement.

You can configure a maximum of 32 Policy and Charging Control (PCC) rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.

Options *profile-name*—Name of the PCEF profile.

Range: Up to 63 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	<ul style="list-style-type: none">• pcef on page 119• Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34• Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36

protocol (Flow Descriptions)

Syntax	<code>protocol <i>number</i>;</code>
Hierarchy Level	<code>[edit unified-edge pcef flow-description <i>flow-identifier</i>]</code>
Description	Specify a protocol type to identify the subscriber traffic that the service data flow (SDF) filter will detect. If you specify the protocol statement, you must specify a protocol number.
Default	If you don't specify the protocol statement, the default is any protocol.
Options	number —A number that specifies the IP protocol type. Range: 1 through 255
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• Configuring Service Data Flow Filters (Flow Identifiers) on page 27


qci (PCC Action Profiles)

Syntax	<code>qci value;</code>
Hierarchy Level	<code>[edit unified-edge pcef pcc-action-profiles <i>profile-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Configure the QoS Class Identifier (QCI) to apply to a bearer when the bearer binding function associates the PCC rules (which references the PCC action profile) with a bearer. A QCI value must be specified.
Options	<p>value—The QCI value to apply to a bearer.</p> <p>Range: 1 through 9</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • pcc-action-profiles on page 113 • Configuring Policy and Charging Control Action Profiles on page 28

rating-group (PCC Action Profile)

Syntax	<code>rating-group number;</code>
Hierarchy Level	<code>[edit unified-edge pcef pcc-action-profile <i>profile-name</i> charging]</code>
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	<p>Specify a rating-group number for the PCC action profile. A rating-group number is associated with a charging trigger profile. A rating group represents a collection of services.</p> <p>If the rating-group statement is not configured, the rating group is picked up from the APN charging configuration.</p>
Options	<p>number—A number that identifies a particular rating group.</p> <p>Range: 0 through 4,294,967,294</p>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging on page 94 • rating-group (Trigger Profile) • Configuring Policy and Charging Control Action Profiles on page 28


release (PCEF Profile)

Syntax	release (r8 r9);
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W2.
Description	Specify the release (Release 8 or Release 9) that the Gx interface uses at the PDN gateway (P-GW) so that the P-GW will receive only the Attribute Value Pairs (AVPs) compliant to the release version configured.
Options	<p>r8—The P-GW sends one Supported Features AVP for Release 8 marked as Mandatory, ignores the Supported-Features AVP in the PCRF response, and behaves according to Release 8.</p> <p>r9—The P-GW sends two Supported Features AVPs, one each for Release 8 and Release 9 responses, and both are marked as Mandatory. The P-GW ignores the Supported-Features AVP in the PCRF response, and behaves according to Release 9.</p>
	<div> NOTE: If neither option is specified, the P-GW sends Release 8 as mandatory, and Release 9 as optional, in the respective Supported Features AVPs. The P-GW will use the Supported-Features AVP in the response from the PCRF to determine which release to use.</div>
Required Privilege Level	<p>unified-edge—To view this statement in the configuration.</p> <p>unified-edge-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• dynamic-policy-control on page 97• Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

remote-address

Syntax	<code>remote-address <i>ip-v4-address</i> <i>ip-v6-address</i>;</code>
Hierarchy Level	<code>[edit unified-edge pcef flow-description <i>flow-identifier</i>]</code>
Release Information	Statement introduced in Junos OS Release 12.1W.
Description	Specify an IP address for the service data flow (SDF) filter.
Options	<p><code>ipv4-address <i>address</i></code>—An IPv4 address.</p> <p><code>ipv6-address <i>address</i></code>—An IPv6 address.</p>
Required Privilege Level	<p><code>unified-edge</code>—To view this statement in the configuration.</p> <p><code>unified-edge-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• remote-ports on page 133• Configuring Service Data Flow Filters (Flow Identifiers) on page 27

remote-port-range

Syntax	remote-port-range { low <i>low-value</i> ; high <i>high-value</i> ; }
Hierarchy Level	[edit unified-edge pcef flow-descriptions <i>flow-identifier</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify the remote port range to identify the subscriber traffic that the service data flow (SDF) filter will detect.
	<div> NOTE: You can specify either a remote port range or a list of remote ports, but not both.</div>
Default	If you do not configure the remote-port-range statement, the default is any remote port range.
Options	low-value — Lower boundary for the remote port range. Range: 1 through 65,535 high-value — Upper boundary for the remote port range. Range: 1 through 65,535
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• flow-descriptions on page 102• remote-ports on page 133• Configuring Service Data Flow Filters (Flow Identifiers) on page 27

remote-ports

Syntax `remote-ports number;`

Hierarchy Level [edit unified-edge pcef flow-description *flow-identifier*]

Description Specify a remote port or list of remote ports to identify the subscriber traffic that the service data flow (SDF) filter will detect.



NOTE: You can specify either a list of remote ports or a remote port range, but not both.

Default If you don't configure the **remote-port** statement, the default is any remote port.

Options **number**—A port number or list of port numbers. You can specify a maximum of three port numbers in a list.

Range: 1 through 65,535

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

Related Documentation

- [flow-descriptions on page 102](#)
- [remote-port-range on page 132](#)
- [Configuring Service Data Flow Filters \(Flow Identifiers\) on page 27](#)

service-identifier

Syntax	<code>service-identifier <i>number</i>;</code>
Hierarchy Level	[edit unified-edge pcef pcc-action-profile <i>profile-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify a service identifier in a Policy and Charging Control (PCC) action profile that identifies a service.
Options	number —A number that identifies a particular service. Range: 0 through 4,294,967,294
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging on page 94• Configuring Policy and Charging Control Action Profiles on page 28

service-id-level-reporting

Syntax	<code>service-id-level-reporting;</code>
Hierarchy Level	[edit unified-edge pcef pcc-action-profiles <i>profile-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	When the service-id-level-reporting statement is configured, the policy and charging enforcement function (PCEF) reports usage at the service ID level to the Online Charging System (OCS). If service-id-level-reporting is not configured, then usage is reported at the Rating Group level to the OCS.
Required Privilege Level	unified-edge—To view this statement in the configuration. unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging on page 94• Configuring Policy and Charging Control Action Profiles on page 28

session-failover-not-supported (PCEF Profiles)

Syntax	session-failover-not-supported;
Hierarchy Level	[edit unified-edge pcef profiles <i>profile-name</i> dynamic-policy-control]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	Specify that online charging sessions should not fail over to an alternate server.
Default	If you do not include the session-failover-not-supported statement, the failover of online charging sessions to an alternate server is enabled by default. The alternate server is selected based on the configuration in the Diameter profile that is associated with the transport 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	<ul style="list-style-type: none">• dynamic-policy-control on page 97• Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34• Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36

static-policy-control

Syntax static-policy-control {
 pcc-rules {
 [rule-name precedence number];
 }
 pcc-rulebases {
 [rulebase-name];
 }
 activate-dedicated-bearers [qci-value];
 }

Hierarchy Level [edit unified-edge pcef profiles *profile-name*]

Release Information Statement introduced in Junos OS Release 12.1W.

Description Configure static policy control for the Policy and Charging Control (PCC) rules or PCC rulebase in a policy and charging enforcement function (PCEF) profile. You can configure a maximum of 32 PCC rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.



.....
NOTE: If you configure the **static-policy-control** statement for a PCEF profile, then you cannot configure the **dynamic-policy-control** statement in the same profile.
.....

Options 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

- [profiles on page 127](#)
- [dynamic-policy-control on page 97](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 36](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 34](#)

then (PCC Rules)

Syntax	<pre>then { pcc-action-profiles <i>profile-name</i>; }</pre>
Hierarchy Level	[edit unified-edge pcef pcc-rules <i>rule-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 12.1W.
Description	A then statement specifies the actions to be taken if the service data flow (SDF) filters in the from statement are matched. The actions specified in the Policy and Charging Control (PCC) action profile are applied to subscriber traffic that matches the SDF filters. A PCC rule configuration must include the then statement and a PCC action 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	<ul style="list-style-type: none">• pcc-rules on page 118• Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 30

tracoptions (PCEF)

Syntax tracoptions {
 file *file-name* <files *number*> <no-word-readable | world-readable> <size *size*>; flag *flag*;
 level (all | critical | error | info | notice | verbose | warning);
 no-remote-trace;
 }

Hierarchy Level [edit unified-edge pcef]

Release Information Statement introduced in Junos OS Mobility Release 12.1W.

Description Specify tracing options for policy and charging enforcement functions (PCEF).

Options file *file-name*—Name of the file to receive the output of the tracing operation.

 files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Range: 2 through 1000 files

Default: 3 files

 flag *flag*—Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.



.....
CAUTION: You might want to enable tracoptions only when you want to debug specific charging operations. Enabling the traceoption flags might have an impact on the system performance.
.....

- **all**—Trace all operations.
- **config**—Trace configuration events.
- **debug**—Trace debug internal events.
- **fsm**—Trace finite state machine events.
- **general**—Trace general events that do not fit in any specific traces.
- **high-availability**—Trace high-availability events.
- **init**—Trace initialization events.
- **tftmgr**—Trace tftmgr events.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **critical**—Match critical conditions.

- **error**—Match error conditions.
- **info**—Match informational messages
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the *size* option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.

Range: 10,240 through 1,073,741,824 bytes

Default: 128 KB

word-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace and unified-edge—To view this statement in the configuration.
Level	trace-control and unified-edge-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Tracing PCEF Operations on page 151 • pcef on page 119

PART 3

Administration

- [Operational Commands on page 143](#)

CHAPTER 5

Operational Commands

clear unified-edge ggsn-pgw subscribers bearer

Syntax	clear unified-edge ggsn-pgw subscribers bearer gateway gateway <ebi ebi> <imsi imsi> <msisdn msisdn> <qci qci>
Release Information	Command introduced in Junos OS Mobility Release 12.1W.
Description	Clear the bearers for subscribers on the specified Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW).
Options	gateway gateway —Clear the bearers for the specified GGSN or P-GW. ebi ebi —(Optional) Specify the Evolved Packet System Bearer ID (EBI) to clear the bearer. imsi imsi —(Optional) Clear the subscriber matching the specified International Mobile Subscriber Identity (IMSI). msisdn msisdn —(Optional) Clear the subscribers on the specified multiservices interface name. qci qci —(Optional) Specify the QoS Class Identifier (QCI) to clear the specified bearer.
Required Privilege Level	clear, unified-edge
Related Documentation	<ul style="list-style-type: none">• <i>clear unified-edge ggsn-pgw subscribers</i>• <i>show unified-edge ggsn-pgw subscribers</i>
List of Sample Output	clear unified-edge ggsn-pgw subscribers bearer on page 144
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

<code>clear unified-edge ggsn-pgw subscribers bearer</code>	<code>user@host> clear unified-edge ggsn-pgw subscribers bearer</code>
---	---

show unified-edge ggsn-pgw subscribers policy

Syntax	<code>show unified-edge ggsn-pgw subscribers policy gateway <i>gateway</i></code> <code><bearer-id <i>bearer-id</i>></code> <code><brief detail extensive></code> <code>imsi <i>imsi</i></code>
Release Information	Command introduced in Junos OS Mobility Release 12.1W.
Description	Display all policy details on the specified Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway</i>—Display the subscriber information for the specified gateway name.</p> <p>bearer-id <i>bearer-id</i>—(Optional) Display policy information for a specific bearer.</p> <p>brief detail extensive —(Optional) Display the specified level of output.</p> <p>imsi <i>imsi</i>—Display the subscriber information for the specified mobile station ISDN (MSISDN) number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show unified-edge ggsn-pgw subscribers
List of Sample Output	show unified-edge ggsn-pgw subscribers policy imsi 111213213188964 on page 145 show unified-edge ggsn-pgw subscribers policy imsi detail on page 146
Output Fields	Refer to the output fields for the <i>show unified-edge ggsn-pgw subscribers</i> command, which are the same as the output fields for the <i>show unified-edge ggsn-pgw subscribers policy</i> command.

Sample Output

```

show unified-edge ggsn-pgw subscribers user@host> show unified-edge ggsn-pgw subscribers policy imsi 111213213188964
Bearer:
      NSAPI/EBI: 5                      Charging ID: 0xa000401

```

policy imsi
111213213188964

```

Bearer State: Established      Bearer Type: 0
PCC Rule Information:
Rule Name: __default_wc_rule__
  Type: Static      Associated Rule Base: None
  Precedence: 65535  Status: Active
Bearer:
NSAPI/EBI: 6      Charging ID: 0xa000800
Bearer State: Established      Bearer Type: 0
PCC Rule Information:
Rule Name: "dynamic_rule_bronze"
  Type: Dynamic      Associated Rule Base: None
  Precedence: 100    Status: Active

```

show unified-edge
ggsn-pgw subscribers
policy imsi detail

```

user@host> show unified-edge ggsn-pgw subscribers policy imsi detail
Subscriber Information:
  IMSI: 111213213188964      IMEI: 1122334455667789
  MSISDN: 19267386          RAT Type: E-UTRAN
  Status: Visitor           MCC: 123      MNC: 234
PDN Session:
  APN name: apn-dynamic
  IPv4 Address: 30.30.8.1      IPv6 Address: None
  GTP Version: 2              Session State: Established
Bearer:
NSAPI/EBI: 5      Charging ID: 0xa000401
Bearer State: Established      Bearer Type: 0
PCC Rule Information:
Rule Name: __default_wc_rule__
  Type: Static      Associated Rule Base: None
  Precedence: 65535  Status: Active
QoS Attributes:
  QCI: 5      ARP: 1 /0 /0 (PL/PVI/PCI)
  Uplink GBR (kbps): 0      Downlink GBR (kbps): 0
  Uplink MBR (kbps): 0      Downlink MBR (kbps): 0
Charging Attributes:
  Rating Group : 0      Service Id: 0      Gating Status: enable
-both
  AF Charging Id: None      Charging Method: Unspecified Metering Method:
No
ne
  Filter Attributes:
  Remote IP/Mask: any/any      Protocol: any      Direction: Both
  Remote Port Range: any/any      Local Port Range: any/any

Bearer:
NSAPI/EBI: 6      Charging ID: 0xa000800
Bearer State: Established      Bearer Type: 0
PCC Rule Information:
Rule Name: "dynamic_rule_bronze"
  Type: Dynamic      Associated Rule Base: None
  Precedence: 100    Status: Active
QoS Attributes:
  QCI: 6      ARP: 1 /0 /0 (PL/PVI/PCI)
  Uplink GBR (kbps): 0      Downlink GBR (kbps): 0
  Uplink MBR (kbps): 0      Downlink MBR (kbps): 0
Charging Attributes:
  Rating Group : 1      Service Id: 10      Gating Status: enable
-downlink
  AF Charging Id: None      Charging Method: Unspecified Metering Method:
No
ne

```



```
ink      Filter Attributes:
         Remote IP/Mask: 99.88.77.1/32    Protocol: 1      Direction: Downl
         Remote Port Range:  any/any      Local Port Range: any/any
```


PART 4

Troubleshooting

- [Acquiring Troubleshooting Information on page 151](#)

Acquiring Troubleshooting Information

- [Tracing PCEF Operations on page 151](#)

Tracing PCEF Operations

To configure tracing operations for the policy and charging enforcement function (PCEF):

1. Specify that you want to configure tracing options for PCEF.

```
[edit unified-edge pcef]  
user@host# edit traceoptions
```

2. (Optional) Configure the name of the file used for the trace output.

```
[edit unified-edge pcef]  
user@host# set file filename
```

3. (Optional) Configure flags to filter the operations to be logged.

```
[edit unified-edge pcef]  
user@host# set flag flag
```

Flag	Description
all	Trace all operations
config	Trace configuration events
debug	Trace the debug internal events
fsm	Trace FSM
general	Trace general events that do not fit in any specific traces
high-availability	Trace high availability events
init	Trace initialization events
tftmgr	Trace tftmgr events

4. (Optional) Configure the level of tracing.

```
[edit unified-edge pcef]  
user@host# set level (all | critical | error | info | notice | verbose | warning)
```

Related • [traceoptions \(PCEF\) on page 138](#)
Documentation

PART 5

Index

- [Index on page 155](#)

Index

Symbols

#, comments in configuration statements.....	xiii
(), in syntax descriptions.....	xiii
< >, in syntax descriptions.....	xii
[], in configuration statements.....	xiii
[edit services pcef] hierarchy level.....	89
[edit services service-set] hierarchy level.....	89
[edit unified-edge] hierarchy level.....	87
{ }, in configuration statements.....	xiii
(pipe), in syntax descriptions.....	xiii

A

action profiles See PCC action profiles	
activate-dedicated-bearers statement	
PCEF.....	90
af-charging-identifier statement	
PCEF.....	90
allocation-retention-priority statement	
PCEF.....	91
application-function-record-info statement.....	91
applications statement	
PCC rules.....	93
applications-groups statement	
PCC rules.....	92, 111

B

bearer binding	
overview.....	17
triggering bearer requests.....	18
braces, in configuration statements.....	xiii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xiii

C

charging control	
overview.....	8
charging statement	
PCEF.....	94
charging-method statement	
PCEF.....	95

clear unified-edge ggsn-pgw subscribers bearer	
command.....	144
comments, in configuration statements.....	xiii
conventions	
text and syntax.....	xii
curly braces, in configuration statements.....	xiii
customer support.....	xiii
contacting JTAC.....	xiii

D

diameter-profile statement	
PCEF.....	96
direction statement (SDF filters)	
PCEF.....	96
documentation	
comments on.....	xiii
dynamic policies See policy and charging	
enforcement function	
overview.....	15
provisioning	
pull mode.....	16
push mode.....	16
dynamic-policy-control statement	
PCEF.....	97

E

event trigger reporting	
understanding.....	19
event triggers	
configurable triggers.....	19
configuring.....	33
implicit.....	19
overview.....	19
event-trigger-profile statement	
PCEF.....	98
event-trigger-profiles statement	
PCEF.....	99

F

failure-handling statement	
PCEF.....	100, 101
flow identifiers See service data flow filters	
flow-descriptions statement	
PCEF.....	102
flows statement	
PCEF.....	103, 130
font conventions.....	xii
from statement (PCC rules)	
PCEF.....	104

G

gate-status statement	
PCEF.....	105
gating control	
overview.....	8
GBR bearers	
behavior.....	9
guaranteed-bit-rate statement	
PCEF.....	106
Gx interface	
provisioning of rules	
overview.....	15

L

local-port-range statement	
PCEF.....	107
local-ports statement	
PCEF.....	108

M

manuals	
comments on.....	xiii
maximum-bit-rate statement	
PCEF.....	109
measurement-method statement	
PCEF.....	110

N

no-send-to-ue statement	
PCEF.....	112
non-GBR bearers	
behavior.....	9

P

parentheses, in syntax descriptions.....	xiii
PCC action profiles	
configuring.....	28
PCC rulebase	
configuring.....	32
PCC rules	
action profiles	
configuring.....	28
configuring.....	30, 31
dynamic policies	
overview.....	15
static policies	
overview.....	17
pcc-action-profile statement	
PCC rules.....	112

pcc-action-profiles statement	
PCEF.....	113
pcc-rule statement	
PCEF.....	114
pcc-rulebases statement	
PCEF.....	115, 116
pcc-rules statement	
PCEF.....	117
pcc-rules statement (predefined policies)	
PCEF.....	118
PCEF operations	
troubleshooting.....	151
PCEF profile for dynamic services	
applying to an APN.....	49, 77
PCEF profile for static services	
applying to an APN.....	49, 77
PCEF session management procedures	
supported.....	20
unsupported.....	21
pcef statement	
PCEF.....	119
services.....	121
pcef-profile statement	
service-set.....	122
policing, subscriber traffic.....	9
Policy and Charging Control	
overview.....	7, 9
rules	
dynamic policies.....	8, 10
provisioning.....	15
static policies.....	8
policy and charging control rules	
application-aware services.....	25
policy and charging enforcement function	
configuration	
overview.....	4
configuration example.....	39, 57
dynamic policies	
configuring.....	34
event triggers	
configuring.....	33
flow identifiers	
configuring.....	27
Layer 7 rules	
static policies.....	11
operations	
troubleshooting.....	151
overview.....	3

PCC rulebase		
configuring.....	32	
PCC rules		
configuring.....	30, 31	
PCEF profile		
applying to an APN.....	49, 77	
PCEF profile for dynamic policies		
configuring.....	34	
PCEF profile for static policies		
configuring.....	36	
service data flow filters		
configuring.....	27	
static policies		
configuring.....	36	
predefined static policies		
overview.....	17	
preemption-capability statement		
PCEF.....	123	
preemption-vulnerability statement		
PCEF.....	124	
priority-level statement (PCC)		
PCEF.....	125	
profile statement		
services, PCEF.....	126	
profiles statement		
PCEF.....	127	
protocol statement		
PCEF.....	128	
Q		
qci statement		
PCEF.....	129	
quality of service (QoS) control		
overview.....	8	
R		
rating-group statement		
PCEF.....	129	
remote-address statement		
PCEF.....	131	
remote-port-range statement		
PCEF.....	132	
remote-ports statement		
PCEF.....	133	
S		
service data flow filters		
configuring.....	27	
overview.....	5	
service-id-level-reporting statement		
PCEF.....	134	
service-identifier statement		
PCEF.....	134	
services		
application-aware policy and charging control		
rules.....	25	
session-failover-not-supported statement		
PCEF.....	135	
show unified-edge ggsn-pgw subscribers		
policy.....	145	
static Gx policy		
overview.....	15	
static Gx rules See Policy and Charging Control,		
dynamic policies		
static policies See policy and charging enforcement		
function See Policy and Charging Control		
static-policy-control statement		
PCEF.....	136	
support, technical See technical support		
syntax conventions.....	xii	
T		
technical support		
contacting JTAC.....	xiii	
then statement (PCC rules)		
PCEF.....	137	
traceoptions statement		
PCEF.....	138	

