



Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide

Version 12.1

Last Updated February 20, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23963-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

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

Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

About this Guide	V
Conventions Used	vi
Contacting Customer Support	viii
Additional Information	ix
Intelligent Policy Control Function Overview	11
Product Description	12
PCC Solution Elements	13
Intelligent Policy Control Function (IPCF)	13
Subscriber Service Controller (SSC)	15
Policy Provisioning Tool (PPT)	15
Licenses	15
Platform Requirements	16
Network Deployment and Interfaces	17
IPCF in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks	17
Standalone Deployment of IPCF	17
Co-located Deployment of IPCF	18
Supported Interfaces	19
Features and Functionality - Base Software	22
Event Notification Interface Support	22
Policy and Charging Control Function	22
Policy Definition Mapping Support	23
Policy Provisioning Tool Integration	23
System Management Features	23
Management System Overview	23
Bulk Statistics Support	25
Threshold Crossing Alerts (TCA) Support	26
ANSI T1.276 Compliance	26
Usage Monitoring and Control Support	27
Features and Functionality - Licensed Enhanced Feature Software	28
Session Recovery Support	28
Web Element Management System	29
How IPCF Works	30
IP-CAN Session Setup Procedure	30
AF Session Setup Procedure	33
Supported Standards	36
3GPP References	36
IETF References	36
Object Management Group (OMG) Standards	39
Understanding the Service Operation	41
Terminology	42
Contexts	42
Logical Interfaces	42
Bindings	44
Services and Networks	44

IPCF Node Configuration Procedures	47
Information Required for Configuring the System as an IPCF	48
Required Local Context Configuration Information	48
Required Source Context Configuration Information	49
Required Destination Context Configuration Information	52
Required AAA Context Configuration Information	53
IPCF Node Configuration	55
Local Interface Configuration	56
PCC-Service Configuration	56
Basic PCC-Service Configuration	57
PCC-QoS-Profile Configuration	58
PCC-Condition-Group Configuration	58
PCC-Action-Set Configuration	59
PCC-Service-Profile and Usage Monitoring Configuration	60
PCC-Policy-Service Configuration	61
PCC-Sp-Endpoint Configuration	61
Diameter Endpoint Configuration	62
Event Notification Interface Endpoint Configuration	63
Non-3GPP IP-CAN Session Configuration	64
Verifying IPCF Configuration	64
Logging Facility Configuration	66
Displaying Logging Facility	66
Congestion Control Configuration	68
Configuring the Congestion Control Threshold	68
Configuring Service Congestion Policies	68
Configuring New Call Policy	69
Alarm and Alert Trap Configuration	70
SNMP-MIB Traps for IPCF Node	71
Event IDs for IPCF Node	72
Monitoring the Service	73
Monitoring System Status and Performance	74
Monitoring Logging Facility	76
Clearing Statistics and Counters	77
Troubleshooting the Service	79
Test Commands	80
Using the Test IPCF Command	80
Checking Reachability of Node Using Ping	81
Using the Diameter Test Command	82
Engineering Rules	83
PCC Engineering Rules	84
Interface and Port Engineering Rules	85
Gx/Gxa Interface Rules	85
Rx Interface Rules	85
Sp Interface Rules	85
Service Engineering Rules	86

About this Guide





This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis.

This preface includes the following sections:

- [Conventions Used](#)
- [Contacting Customer Support](#)
- [Additional Information](#)

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a screen display	This typeface represents text that appears on your terminal screen, for example: Login:
Text represented as commands	This typeface represents commands that you enter at the CLI, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are <u>not</u> case sensitive.
Text represented as a command variable	This typeface represents a variable that is part of a command, for example: show card slot_number <i>slot_number</i> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New .

Command Syntax Conventions	Description
{ keyword or <i>variable</i> }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[keyword or <i>variable</i>]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
	<p>Some commands support alternative variables. These “options” are documented within braces or brackets by separating each variable with a vertical bar.</p> <p>These variables can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ nonce timestamp }</pre> <p>OR</p> <pre>[count number_of_packets size number_of_bytes]</pre>

Contacting Customer Support

Go to <http://www.cisco.com/cisco/web/support/> to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Cisco ASR 5000 Installation Guide*
- *Cisco ASR 5000 System Administration Guide*
- *Cisco ASR 5x00 CDMA Command Line Interface Reference*
- *Cisco ASR 5x00 eHRPD/LTE Command Line Interface Reference*
- *Cisco ASR 5x00 GPRS/UMTS Command Line Interface Reference*
- *Cisco ASR 5x00 Thresholding Configuration Guide*
- *Cisco ASR 5x00 SNMP MIB Reference*
- *Web Element Manager Installation and Administration Guide*
- *Cisco ASR 5x00 AAA Interface Administration and Reference*
- *Cisco ASR 5x00 GTPP Interface Administration and Reference*
- *Cisco ASR 5x00 Release Change Reference*
- *Cisco ASR 5x00 Statistics and Counters Reference*
- *Cisco ASR 5x00 Gateway GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 HRPD Serving Gateway Administration Guide*
- *Cisco ASR 5000 IP Services Gateway Administration Guide*
- *Cisco ASR 5x00 Mobility Management Entity Administration Guide*
- *Cisco ASR 5x00 Packet Data Network Gateway Administration Guide*
- *Cisco ASR 5x00 Packet Data Serving Node Administration Guide*
- *Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide*
- *Cisco ASR 5x00 Serving GPRS Support Node Administration Guide*
- *Cisco ASR 5x00 Serving Gateway Administration Guide*
- *Cisco ASR 5000 Session Control Manager Administration Guide*
- *Cisco ASR 5000 Packet Data Gateway/Tunnel Termination Gateway Administration Guide*
- Release notes that accompany updates and upgrades to the StarOS for your service and platform

Chapter 1

Intelligent Policy Control Function Overview

The Cisco ASR 5x00 Platform provides 3GPP PCC solution to network carrier operators with Intelligent Policy Control Function (IPCF) in UTRAN/E-UTRAN/cdma2000-1x/HRPD networks.

It offers an end-to-end Policy and Charging Control (PCC) solution that provides one of the highly intelligent and high performance solutions. Based on the 3rd Generation Partnership Project's (3GPP's) PCC standard (Rel-7 and Rel-8 compliant), the Cisco PCC solution allows operators to achieve real-time control of their network resources, control subscriber access to services, and proactively optimize network capacity, while offering compelling new services and applications. It intelligently extends it such as to simplify the complex and diverse requirements of policy and charging management for global operators.

Along with this solution operators can rapidly deploy a wide variety of standard services or new services to improve the quality of experience for their subscribers and generate additional revenue.

These benefits are achieved by the implementation and deployment of relevant PCRF functions in a core network with network function capabilities thereby reducing system hardware costs, and providing lower latency and a performance optimized PCC solution.

This overview provides general information about the Cisco PCC solution including:

- [Product Description](#)
- [Network Deployment and Interfaces](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - Licensed Enhanced Feature Software](#)
- [How IPCF Works](#)
- [Supported Standards](#)

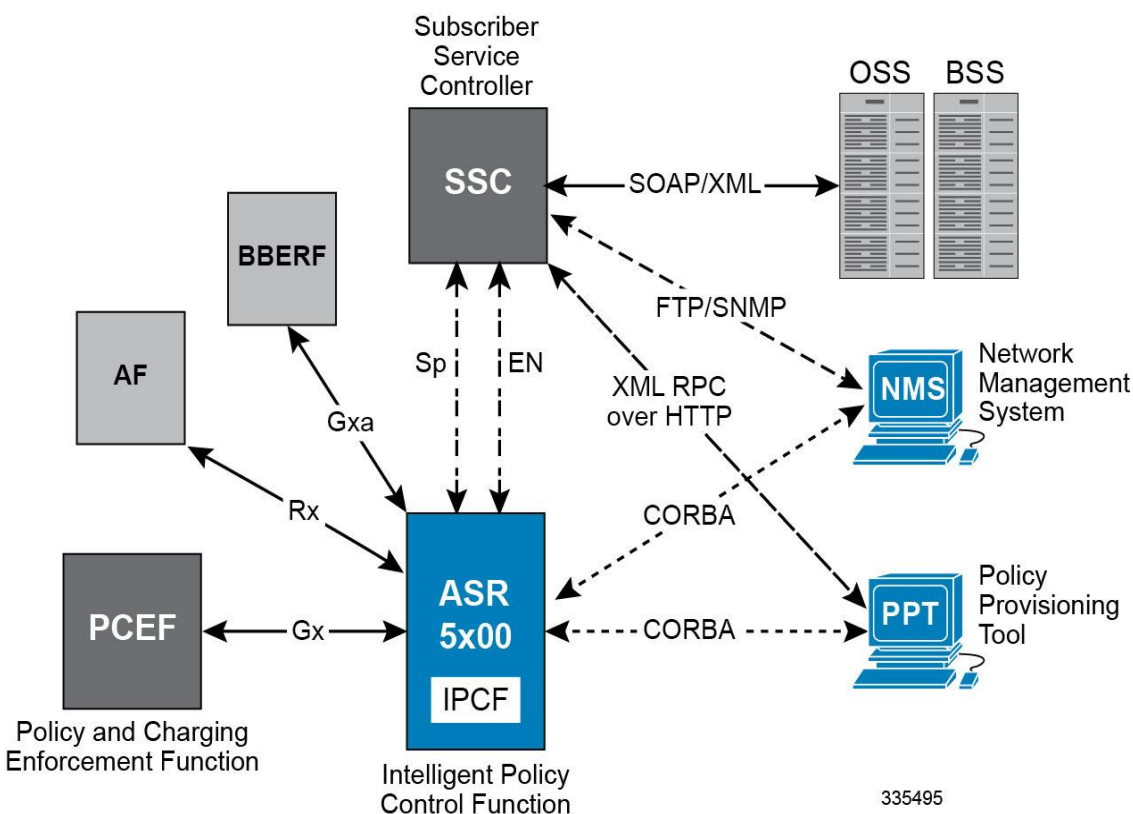
Product Description

This section provides an overview and describes the building blocks for the PCC solution.

The PCC solution comprises of Intelligent Policy Control Function (IPCF), which comprises of extended intelligent PCRF capabilities for policy control function and Subscriber Service Controller (SSC) having centralized PCRF function and Subscriber Profile Repository (SPR) functionality. It also includes a Web-based GUI tool, Policy Provisioning Tool (PPT) to implement and control the policy based subscriber access in the existing wireless network as well as service flow based charging implementation.

The figure given below describes a high level view of UTRAN/E-UTRAN/cdma2000-1x/HRPD network with IPCF and other components in a deployment scenario.

Figure 1. PCC Elements in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks



The IPCF is built around an intelligent rule configuration and execution system. The IPCF's policy rules engine is capable of acting on conditions such as the subscriber, the session state or network condition or even time and day, to decide upon the corresponding treatment to be given to the subscriber. All information and rules fetched by querying IPCF's subscription plan are stored in the SSC over **Sp** interface.

Cisco PCC solution is well compliant to 3GPP standard in operator's core network. Services available through Cisco PCC can be grouped in following categories:

- **Resource management:**
 - fair usage

- traffic optimization
- time-based differential charging policies
- **Personalization services:**
 - automated use notification
 - tiered services
 - parental control
 - roaming management policies
- **New services creation:**
 - turbo service for a dynamic upgrade
 - location based differential charging
 - on net preferential charging policies

Cisco PCC solution empowers operator to deploy a 3GPP Standards based solution ensuring maximum flexibility and derive and authorize the QoS information for the service data flow for session as well as bearer usage.



Important: Some of the features may not be available in this release. Kindly contact your local Cisco representative for more information on supported features.

PCC Solution Elements

This section provides the brief description and functionality of various network elements involved in the UTRAN/E-UTRAN/cdma2000-1x/HRPD network. The Policy and Charging Control includes the following functional entities:

- [Intelligent Policy Control Function \(IPCF\)](#)
- [Subscriber Service Controller \(SSC\)](#)
- [Policy Provisioning Tool \(PPT\)](#)

Intelligent Policy Control Function (IPCF)

Intelligent Policy Control Function (IPCF) provides policy control and charging rule functions in a core network.

Apart from standard capabilities, Cisco IPCF provides a unique possibility to deploy key functions in an integrated fashion collocated with the Policy and Charging Enforcement Function (PCEF) on a network function; i.e. GGSN, PDSN, P-GW. Such an integrated PCRF/PCEF capability allows for a further flattened and cost optimized network solution, leveraging Cisco ASR 5x00 platform performance and versatility.

IPCF along with SSC provide complete control of the policy and usage management for subscribers' data usage for any network. With SSC managing subscriber as well as policy related data, the IPCF performs the rules analysis and drives policy actions into the network. In case of PCEF-co-location model this basically translates to extending PCEF capabilities to support dynamic policy and charging functions with reduced latency in **Gx/Gxa/Rx** interface transactions.

IPCF acts as a PCRF functions supplemented with usage monitoring capability that enables policies around data consumption. IPCF interfaces with the PCEF over standard **Gx/Gxa/Rx** interface for policy management and optionally Volume Reporting over standard **Gx** (VRoGx) interface for getting the usage of IP Connectivity Access Network (IP-CAN) sessions.

Cisco IPCF is compliant in accordance with 3GPP standard in operator's core network. Some of the key functions of IPCF are to:

- Derive and authorize the QoS information for the service data flow for session as well as bearer usage
- Select the appropriate charging criteria and mechanism apt for the data usage
- Provides network control regarding the service data flow detection and gating
- Ensure the PCEF user plane traffic treatment is in accordance with the user's subscription profile
- Correlate service and charging information across PCEF and AF

PCC Rule and Charging Rule Report Handling

IPCF handles operation of PCC Rule and activate/deactivate/install/modify/remove the PCC rules at PCEF. PCC rule operation may fail on PCEF due to various reasons. In such failure cases PCEF sends back a Charging Rule Report containing PCC rules failed and corresponding failure cause.

The IPCF handles these charging rule reports and take appropriate actions based on configuration.

Charging Rule Report comes through CCA or RAA messages in a call flow used for handling the charging-rule-report.

IPCF supports following charging rule failure codes in report:

- Out-of-credit
- Reallocation-of-credit
- Unknown Rule Name
- Invalid Rating Group
- Invalid Service Identifier
- GW/PCEF Malfunction
- Limited Resources
- Max No. of Bearers Reached
- Unknown Bearer Id
- Missing Bearer Id
- Missing Flow Description
- Resource Allocation Failure
- QoS Validation Failure

Charging rule status can be any one of the following in this scenario:

- Active
- Inactive
- Temporarily Inactive

A charging rule report can occur in CCR message multiple times and maximum of 16 charging rule reports per CCR message is supported by IPCF.

Subscriber Service Controller (SSC)

SSC is the enhanced subscriber profile repository in Cisco PCC solution.

Based on standard platforms SSC provides following major functions:

- Subscriber profile storage
- Subscriber usage counters management
- Centralized network policy control
- Supports event manager module

SSC provides a number of additional PCC functions in the solution, including:

- an intelligent database function for the policy services (SPR), acting either as a standalone SPR or as a high-transaction SPR front-end for dynamic policy tracking
- a centralized Policy software application engine complementing the IPCF for advanced converged and correlated session handling where required
- an event notification module enabling user interaction via SMS and e-mail, and a policy events and statistics manager, which is key for operational monitoring and analysis of the end-user service usage.

The centralised policy handling capability set of the SSC is designed to enable session correlation not just across IPCFs, where needed, but also across network domains through coordinated interaction with other network domain policy nodes.

The SSC interacts with IPCF over **Sp** (a standard **Sh** protocol based) interface for given functionality. SSC also supports a proprietary **EN** interface, which is based on XML-RPC protocol, to receive event notification data from IPCF.

For more information on SSC function and supported interfaces, refer *Subscriber Service Controller Installation and Administration Guide*.

Policy Provisioning Tool (PPT)

Cisco Policy Provisioning Tool (PPT) is a Web-based client-server GUI application in PCC solution that helps the operator for subscriber policy provisioning and management.

It provides the user (network operator) a comprehensive use-case design experience. It enables the network operator to design a service plan and subscriber profile data modeling at a time with the help of use case design and configuration.

For more information on PPT function and supported interfaces, refer *Policy Provisioning Tool Installation and Administration Guide*.

Licenses

The IPCF is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Platform Requirements

The IPCF service runs on a Cisco® ASR 5x00 chassis running StarOS Rel. 10 or later. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the *Installation Guide* for the chassis and/or contact your Cisco account representative.

Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of IPCF and other components in a core network.

The following information is provided in this section:

- [IPCF in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks](#)
- [Supported Interfaces](#)

IPCF in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks

This section describes the deployment scenario of IPCF with Cisco PCC solution.

PCC elements can be deployed in various combinations but following are the most common scenarios for PCC deployment in UTRAN/E-UTRAN/cdma2000-1x/HRPD network:

- [Standalone Deployment of IPCF in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks](#)
- [Co-located Deployment of IPCF with PCEF in UTRAN/E-UTRAN/cdma2000-1x/HRPD Networks](#)

Standalone Deployment of IPCF

In standalone deployment, multiple PCEFs (GGSN/PDSN/P-GW) connect to a single IPCF through **Gx** interface and served by the PCC elements through IPCF.

The following figure displays simplified network overview of the IPCF deployment in an UTRAN/E-UTRAN Core Network to serve multiple PCEFs.

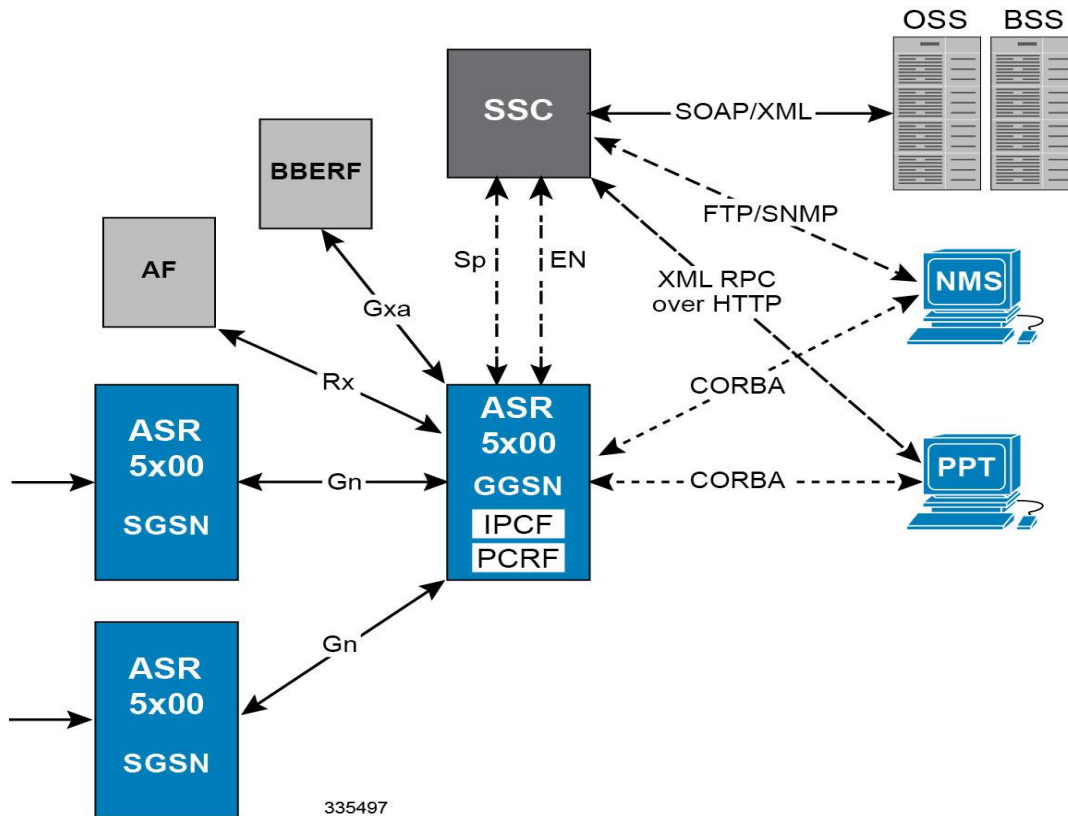
Figure 1 illustrates the network architecture, showing the interaction between various components. The diagram includes a central ASR 5x00 IPCF block, two ASR 5x00 GGSN PCEF blocks, two ASR 5x00 SGSN blocks, an AF block, a BBERF block, an SSC block, and external systems OSS, BSS, NMS, and PPT. The connections are as follows:

- ASR 5x00 SGSN blocks connect to ASR 5x00 GGSN PCEF blocks via Gn interfaces.
- ASR 5x00 GGSN PCEF blocks connect to the ASR 5x00 IPCF block via Gx interfaces.
- The ASR 5x00 IPCF block connects to the AF block via Rx and Gxa interfaces.
- The ASR 5x00 IPCF block connects to the BBERF block via Sp and EN interfaces.
- The ASR 5x00 IPCF block connects to the SSC block via Sp and EN interfaces.
- The SSC block connects to OSS and BSS blocks via SOAP/XML.
- The SSC block connects to the NMS block via FTP/SNMP and XML RPC over HTTP.
- The ASR 5x00 IPCF block connects to the NMS block via CORBA.
- The ASR 5x00 IPCF block connects to the PPT block via CORBA.

In co-located deployment IPCF is placed with PCEF on the same chassis. It interacts with PCEF through internal connection matching **Gx** reference and connects to other PCC elements over various interfaces.

Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide

Figure 3. IPCF in UTRAN/E-UTRAN Network with Multiple PCEFs



Supported Interfaces

The IPCF provides the following network interface support to connect to the various network elements in an UTRAN/E-UTRAN/cdma2000-1x/HRPD networks:

- **Gx:** This reference is an interface between IPCF and PCEF. It is a Diameter protocol-based interface over which the IPCF communicates with a PCEF for the provisioning of charging rules. The charging rules are based on the dynamic analysis of flows used for a 3GPP or Non-3GPP IP-CAN subscriber session.

This is the interface used by the IPCF to communicate with PCEF on the same Public Land Mobile Network (PLMN).

The **Gx** reference point enables an IPCF to have dynamic control over the policy and charging control behavior at a PCEF. The **Gx** reference supports the following functions:

- Request for policy and charging control decision from PCEF to IPCF
- Provision of policy and charging control decision from IPCF to PCEF
- Delivery of IP-CAN-specific parameters from IPCF to PCEF or from PCEF to IPCF
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/NW)
- Termination of **Gx** session (corresponding to an IP-CAN session) by PCEF or IPCF



Important: The IPCF decision to terminate an **Gx** session is based on situation like removal of a UE subscription etc.

One or more **Gx** interfaces can be configured per system context.

Cisco IPCF supports standard 3GPP Rel. 7, Rel. 8, and Rel. 9 **Gx** interface to support different access technologies.

To provide accessibility to PDSN as PCEF in CDMA/HRPD access network for 3GPP IP-CAN type session, **Gx** interface uses NAI and IMSI as subscriber Id and ESN and MEID for user equipment information.

- **Gxa:** This reference is an interface between IPCF and the Bearer Binding and Event Reporting Function (BBERF) at AN-GW. It is a Diameter protocol-based interface and enables an IPCF to have dynamic control over the BBERF behavior at AN-GW.

The **Gxa** reference point enables the signaling of QoS control decisions and it supports the following functions:

- Establishment of **Gxa** session by BBERF and termination of **Gxa** session by BBERF or IPCF
- Establishment of Gateway Control Session by the BBERF and termination of Gateway Control Session by the BBERF or IPCF
- Request for QoS decision from BBERF to IPCF and provision of QoS decision from IPCF to BBERF
- Delivery of IP-CAN-specific parameters from IPCF to BBERF or from BBERF to IPCF
- Negotiation of IP-CAN bearer establishment mode (UE-only and UE or network)

One or more **Gxa** interfaces can be configured per system context.

- **Sp:** This is a Diameter-based interface residing between Cisco IPCF and SSC. It is based on standard **Sh** interface.

This reference point allows the IPCF to request subscription information related to the IP-CAN transport level policies from the SSC based on a subscriber identifier and used by IPCF to retrieve subscriber service policy and subscription profile.

Only one **Sp** interface can be configured per system context.

- **Event Notification Interface (EN):** The **EN** interface supports uni-directional transfer of events from IPCF to SSC. This is an XML-RPC protocol based proprietary interface to send outbound event notifications to the SSC and forward these events to an event application module to generate mail/SMS notification to user/subscriber.

Only one **EN** interfaces can be configured per system context.

- **Rx:** This interface is the reference point between the Application Function (AF); i.e. IMS and the IPCF. This is a Diameter based interface.

The **Rx** reference point enables transport of application level session information from AF to IPCF. Such information includes:

- IP filter information to identify the service data flow for policy control and/or differentiated charging
- Media/application bandwidth requirements for QoS control

The **Rx** reference point enables the AF subscription to transport notifications on signaling path status of AF session in the IP-CAN.

One or more **Rx** interfaces can be configured per system context.

- **CORBA-based Interface:** IPCF supports the North-bound **CORBA** interfaces support for PPT and WEM management applications that can easily be integrated, using standards-based protocols (CORBA and

SNMPv1, v2), into higher-level management systems. It gives the ability to operator to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

Only one interface for WEM and one for PPT can be configured per system context.

Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on IPCF service.

IPCF along with SSC provide complete control of the policy and usage management for subscribers' data usage for any network. With SSC managing subscriber as well as policy related data, IPCF performs the rules analysis and drives policy actions into the network.

Following implemented features and supports are provided on Cisco IPCF for PCC function support:

- [Event Notification Interface Support](#)
- [Policy and Charging Control Function](#)
- [Policy Definition Mapping Support](#)
- [Policy Provisioning Tool Integration](#)
- [System Management Features](#)

Event Notification Interface Support

The Event Notification module residing at SSC handles the various interfaces that integrate with subscriber for providing notifications related to policy changes imposed by the PCC rules, for application integration, and real-time interactions.

IPCF's usage management and profile management module provide triggers along with related information to the SSC.

The event notification module supports an interface to deliver SMS notifications to subscriber using the subscriber ids from subscriber profile.

Policy and Charging Control Function

IPCF provides the following supports for PCC function:

- Predefined PCC Rule Support
- Dynamic PCC Rule Support
- Policy Re-authorization Support on Profile Modification
- Policy Evaluation Support for Session Conditions

This includes following session conditions for policy evaluation:

- Session Events: session setup, bearer setup/update, Policy modification etc.
- Network-based Events: Type of RAN, type of Access-Network etc.
- Time and Date: Time of day, specific date, specific week day
- Mobility: Home or roaming subscriber
- Usage based policies
- Single User Policy Management Support: It provides policy management across all sessions used by a single user.

Policy Definition Mapping Support

Policy definition mapping support is provided on IPCF to manage the PCC policy definition mapping based on subscriber/user identity. It supports policy mapping based on following identities:

- IMSI
- MSISDN
- APN name
- NAI
- SIP-URI

Policy Provisioning Tool Integration

Cisco Policy Provisioning Tool (PPT) is a Web-based client-server application which provides the user (network operator) a comprehensive use case design experience. It enables the network operator to design a service plan and subscriber profile data modeling at a time with the help of use case design and configuration.

The Cisco PPT provides the following major functionality to the network operator:

- to design highly flexible, easily expandable and manageable usecases.
- to build the provisioning components through libraries containing data related to APN, rules and traffic types.
- to configure the data plans that reside on SSC. In the data plans, the user can configure the usage limits and thresholds.
- to configure the e-mail and SMS templates that are sent to the subscribers when certain threshold is reached.

The PPT application has a very comprehensive and user-friendly interface to make the above listed configurations and services.

System Management Features

This section describes following features:

- [Management System Overview](#)
- [Bulk Statistics Support](#)
- [Threshold Crossing Alerts \(TCA\) Support](#)
- [ANSI T1.276 Compliance](#)

Management System Overview

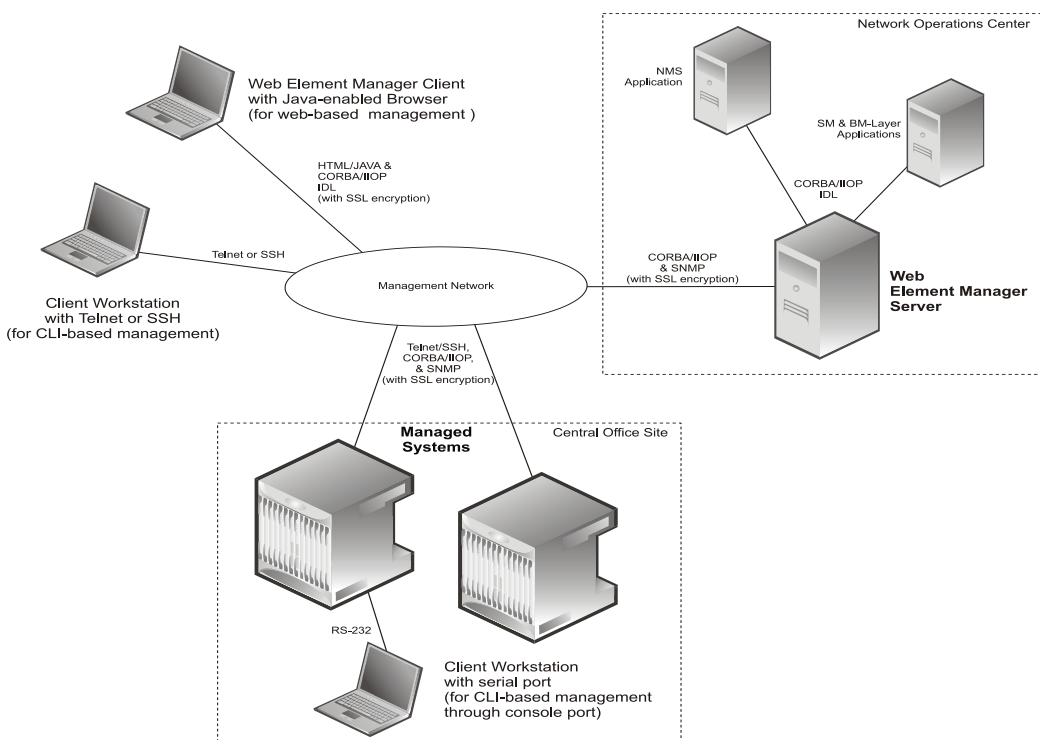
The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems - giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security reasons and to maintain system performance.


Operation and Maintenance module of ASR 5x00 offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces. These include:


- Using the command line interface (CLI).
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces.
- Local login through the Console port on SPIO card using an RS-232 serial connection.
- Using the Web Element Manager application.
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000.
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO.
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others).
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management.
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities.
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG's) Interface Definition Language (IDL).

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network:

Figure 4. Element Management System



 **Important:** System management functionality is enabled for console-based access by default. For GUI-based management support, refer *Web Element Management System*.

 **Important:** For more information on command line interface based management, refer *Command Line Interface Reference*.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a partial list of supported schemas:

- **System:** Provides system-level statistics.
- **Card:** Provides card-level statistics.
- **Port:** Provides port-level statistics.
- **PCC-AF:** Provides PCC Application Function related statistics.
- **PCC-Policy:** Provides PCC Policy related statistics.
- **PCC-Service:** Provides statistics collected for PCC service on a chassis endpoint in PCC service.
- **PCC-Sp-Endpoint:** Provides statistics collected at **Sp** interface endpoint in PCC service.

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the chassis or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, chassis host name, chassis uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, number of sessions etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps are created to indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists or a condition clear alarm is generated. “Outstanding” alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.



Important: For more information on threshold crossing alert configuration, refer *Thresholding Configuration Guide*.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5x00 Platforms and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a

variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

At IPCF, time monitoring over Gx feature enables it to monitor session time usage of a subscriber. With this feature available, IPCF is able to set time-base usage thresholds on Flow-level (PCC Rule level) or Session-Level Basis. The thresholds are communicated to PCEF over Gx interface. As per this implementation the time monitoring can be viewed as a natural extension to volume monitoring over Gx.

When a time-based usage reaches the provisioned threshold, then PCEF will report the usage to IPCF. If the subscriber session terminates before threshold is reached, PCEF will report the usage to IPCF while indicating the termination. The time threshold values provisioned to PCEF can be configured locally at IPCF or may come from SSC through Data Plans translated as Usage monitors at IPCF.

For time usage threshold and monitoring support the IPCF works in following manner:

1. IPCF receives data plan information along with threshold information from SSC.
2. Data plan information for a subscriber is treated as usage monitor information at IPCF.
3. Based on the operator configuration, IPCF can associate monitoring-key(s) with usage monitor(s). While this association is being done, IPCF also calculates the value of the threshold to be sent along with the monitoring key. As per operator configuration, IPCF decides if a particular monitoring-key is being used at Session-Level or PCC Rule-Level.
4. IPCF calculates and communicates the usage thresholds to PCEF over Gx interface.
5. IPCF can also enable an event trigger USAGE_REPORT over Gx interface so that it can receive the subscriber time usage information.
6. When USAGE_REPORT event-trigger is enabled, once a subscriber consumes time and the threshold is reached, then IPCF receives CCR-Update message with the monitoring key and the time consumed. IPCF updates this time usage in all the usage monitors that are associated with this monitoring key.
7. In order to continue usage counting at PCEF, PCRF sends back threshold values for the reported monitoring-keys in response.
8. In a case where subscriber session terminates before reaching the threshold, then IPCF will receive the time used in CCR-Termination message.
9. IPCF conveys the usage updates back to SSC over Sh.



Important: IPCF also have an operator configured policy based on the time usage. This policy can be defined based on the conditions on absolute time usage and the subscription limit of the usage monitor. Refer *IPCF Administration Guide* for more information on configuration of this support.

Usage Monitoring and Control Support

IPCF provides subscriber usage monitoring and control mechanism to operator based on different criteria and conditions. IPCF provides usage monitoring and control functions to support:

- multiple bearers and multiple sessions for a subscriber
- group of subscribers
- per service per plan usage thresholds
- configurable warning threshold
- usage counter reset on start of billing cycle

Features and Functionality - Licensed Enhanced Feature Software

This section describes the optional enhanced features and functions available for IPCF node.



Important: Some of the following features may require the purchase of an additional license to implement the functionality with the IPCF node.

This section describes following features:

- [Session Recovery Support](#)
- [Web Element Management System](#)

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of “standby mode” session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby packet processing card.

There are two modes for Session Recovery.

- **Task recovery mode:** Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby packet processing card. In this mode, recovery is performed by using the mirrored “standby-mode” session manager task(s) running on active packet processing cards. The “standby-mode” task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode:** Used when a packet processing card hardware failure occurs, or when a packet processing card migration failure happens. In this mode, the standby packet processing card is made active and the “standby-mode” session manager and AAA manager tasks on the newly activated packet processing card to perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processing cards to ensure task recovery.



Important: For more information on this feature, refer *Session Recovery* chapter in *System Administration Guide*.

Web Element Management System

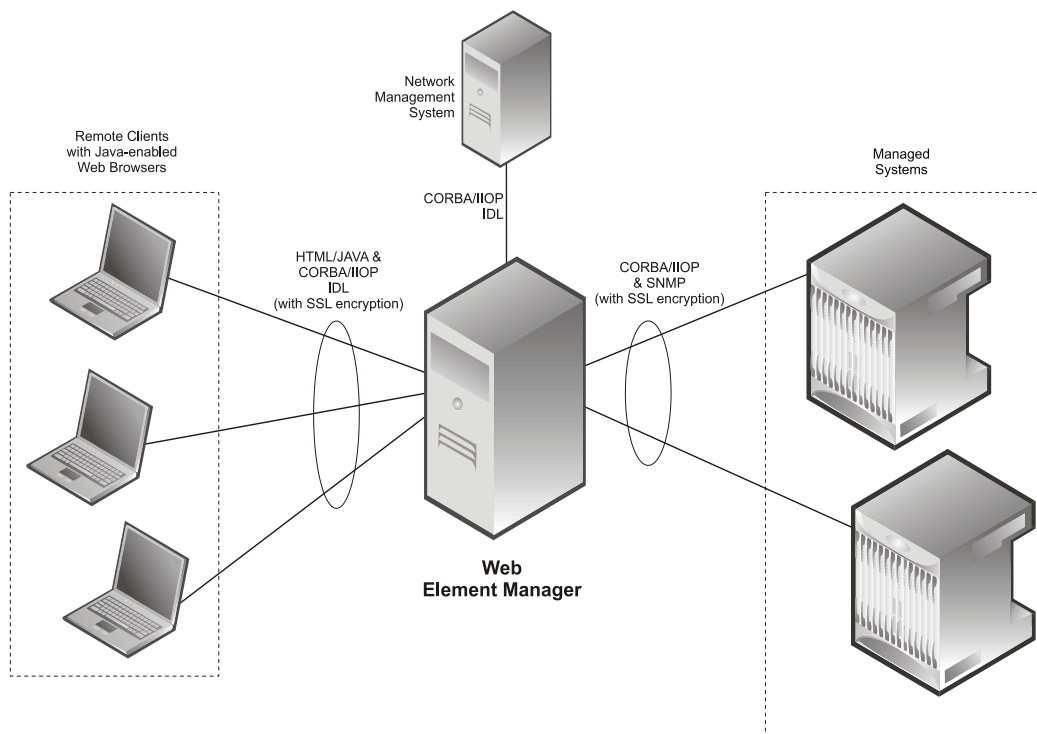
Provides a Graphical User Interface (GUI) for performing Fault, Configuration, Accounting, Performance, and Security (FCAPS) management of the ASR 5x00.

The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates various interfaces between the Cisco Web Element Manager and other network components.

Figure 5. Web Element Manager Network Interfaces



Important: For more information on WEM support, refer *WEM Installation and Administration Guide*.

How IPCF Works

This section provides information on the function and procedures of the IPCF in an PCC deployment scenario in an UTRAN/E-UTRAN/cdma2000-1x/HRPD network and presents message flows for different stages of session setup.

Every time a new IP-CAN session is established through PCEF's **Gx** interaction with IPCF, it queries SSC specifically to get subscriber's profile as well as the usage details during the current billing cycle. After receiving the subscriber profile, it forward the same to PCEF. For remaining duration of the session the subscriber policy profile remains cached with IPCF and no query performed over **Sp**.

Moreover, on any changes to the profile or to the subscription plan, SSC notifies IPCF over **Sp** interface, that is managing the session for the subscriber getting affected. IPCF ensures that the local repository has the most updated profile record for the subscriber at all times.

Once the subscriber policy profile details are available, IPCF's rule engine triggered by various interface events as well as internal events, determines the treatment to be given to the session in terms of the applicable QoS traffic management treatment and/or charging policy parameters.

In the case IPCF is also tracking the usage for deriving policy decision on the basis of same, it would appoint itself for pre-paid usage monitoring through **Gx** for usage control.

In the case where IPCF also performs usage monitoring via VRoGx interface, in addition to the session state triggers, additionally the usage can be monitored and operator can define various policy triggers around the usage thresholds for a session or even group of sessions. In the cases where usage is to be monitored across multiple sessions and PCEFs (from same or group of subscribers); e.g. for group policies, IPCF combined with SSC's usage monitor module, enable the PCC system to track and trigger appropriate treatments required for the multiple sessions. IPCF communicates with SSC over **Sp** interface which enables a synchronous fetch and update related to usage as well as asynchronous notifications from SSC to the IPCF, handling the sessions which may get impacted due to consumption reported by a session being tracked at a different IPCF.

The usage monitor at IPCF is capable of tracking aggregate volume and/or time consumption as well as on the basis of the service groups e.g. premium services, non-premium services in the network. This ensures that it is possible to apply different policy logic as well as different warning as well as usage thresholds on individual service or service-group basis, facilitating finer control over data consumption based policies. Further, the consumption during roaming scenarios can be counted differently from the home scenarios, if so desired by operator. The usage counter at IPCF in combination of SSC's usage manager performs intelligent allocation of usage based on the policy conditions that helps to avoid over usage in case usage policy breach conditions.

The following procedures are discussed in this section:

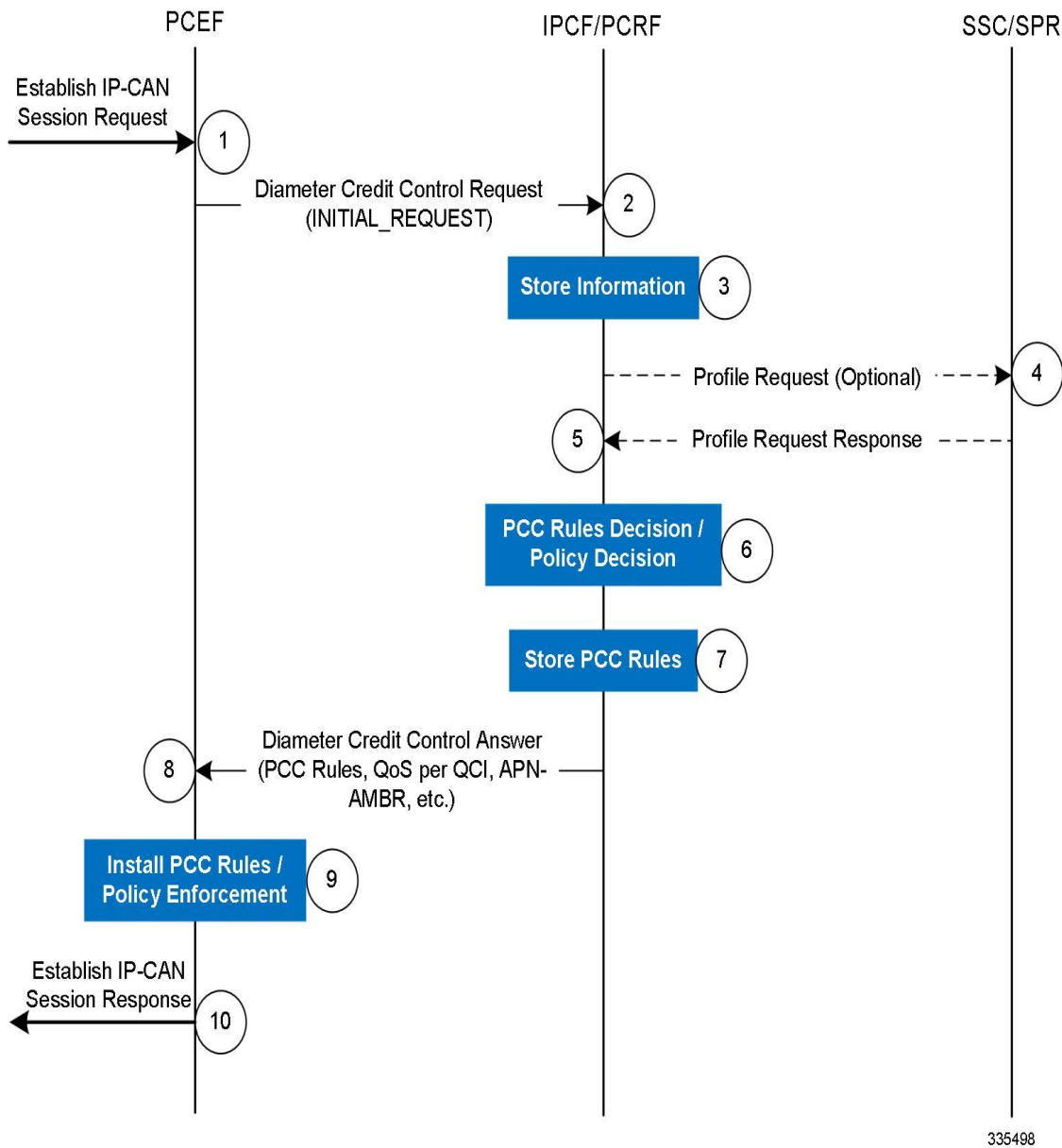
- [IP-CAN Session Setup Procedure](#)
- [AF Session Setup Procedure](#)

IP-CAN Session Setup Procedure

This section describes the call flow for IP-CAN session procedure.

The following figure and the text that follows describe the message flow for IP-CAN session setup procedure.

Figure 6. IP-CAN Session Setup Procedure Call Flow



1. The PCEF receives an Establish IP-CAN Session Request.
The form of the Establish IP-CAN Session Request depends upon the type of the IP-CAN. It can be the first Create PDP Context Request within an IP-CAN session for GPRS or an IPSec tunnel establishment request in an un-secured network.
2. PCEF informs the IPCF of the IP-CAN Session establishment request through Diameter Credit Control Request.
At this stage the PCEF initiates a new Gx session by sending a Diameter CCR to the IPCF and set the CC-Request-Type AVP to INITIAL_REQUEST.
In Diameter CC request, the PCEF provides the following information to IPCF if available:
 - UE identity information

- PDN identifier
- UE IPv4 address and/or UE IPv6 address prefix
- PDN connection identifier
- IP-CAN type
- RAT type
- default charging method
- Default-EPS-Bearer-QoS
- APN-AMBR
- types of IP-CAN, where the IPCF can be in control of IP-CAN Bearers; e.g. GPRS
- Bearer identifier and information about the requested bearer, such as QoS

In this procedure the IPCF associates the **Gx** session for the new IP-CAN session with the corresponding Gateway Control Session and maintains the aligned set of PCC and QoS rules in the PCEF as applicable for the case.

3. The IPCF stores the information received in the Diameter CC Request message.
4. *Optional.* If the IPCF needs subscription-related information and does not have it, the IPCF sends a Profile Request to the SSC in order to receive the information.
5. The SSC replies the Profile Request with the profile of subscriber which contains subscription related information; i.e., information about the allowed service(s), QoS information and PCC Rules information.
6. The IPCF selects or generates PCC Rule(s) based on received information in Profile Response to be installed. The IPCF can also take a policy decision by deriving an authorized QoS and by deciding whether service flows described in the PCC Rules are to be enabled or disabled.
7. The IPCF stores the selected PCC Rules and selects the Bearer Control Mode that will apply during the IP-CAN session if applicable for the particular IP-CAN.

Following scenarios are considered while IPCF stores the selected PCC rule:

- If the IPCF controls the binding of IP-CAN Bearers, the IPCF stores information about the IP-CAN Bearer to which the PCC Rules have been assigned.
 - If the BBERF/PCEF controls the binding of IP-CAN bearers, the IPCF may derive the QoS information per QCI applicable to that IP-CAN session for non-GBR bearers.
8. The IPCF provisions the PCC Rules to the PCEF using Diameter CC Answer. In Diameter CC Answer, the IPCF provides the following information to PCEF, if available:
 - Selected Bearer Control Mode for the particular IP-CAN
 - the QoS information per QCI
 - List of event triggers for which the IPCF desires PCC Rule Requests
 - authorized QoS (APN-AMBR, Default-EPS-Bearer-QoS, etc.)
 - User Location Information
 - usage monitoring status and applicable thresholds for usage monitoring control

If online charging is applicable then the PCEF requests credit information from the OCS over the **Gy** interface.

9. The PCEF installs the received PCC Rules. The PCEF also enforces the authorized QoS and enables or disables service flows according to the flow status of the corresponding PCC Rules. If QoS information is received per QCI, PCEF sets the upper limit accordingly for the MBR that the PCEF assigns to the non-GBR bearer(s) for that QCI.

10. The PCEF sends a response to the Establish IP-CAN Session Request.

For GPRS, the GGSN accepts the PDP Context Request based on the results of the authorization policy decision enforcement. If the requested QoS parameters do not correspond to the authorized QoS, the GGSN adjusts (downgrades/upgrades) the requested UMTS QoS parameters to the authorized values.

NOTE: The IPCF can reject the IP-CAN session establishment, e.g., the IPCF cannot obtain the subscription-related information from the SSC and the IPCF cannot make the PCC rule decisions.

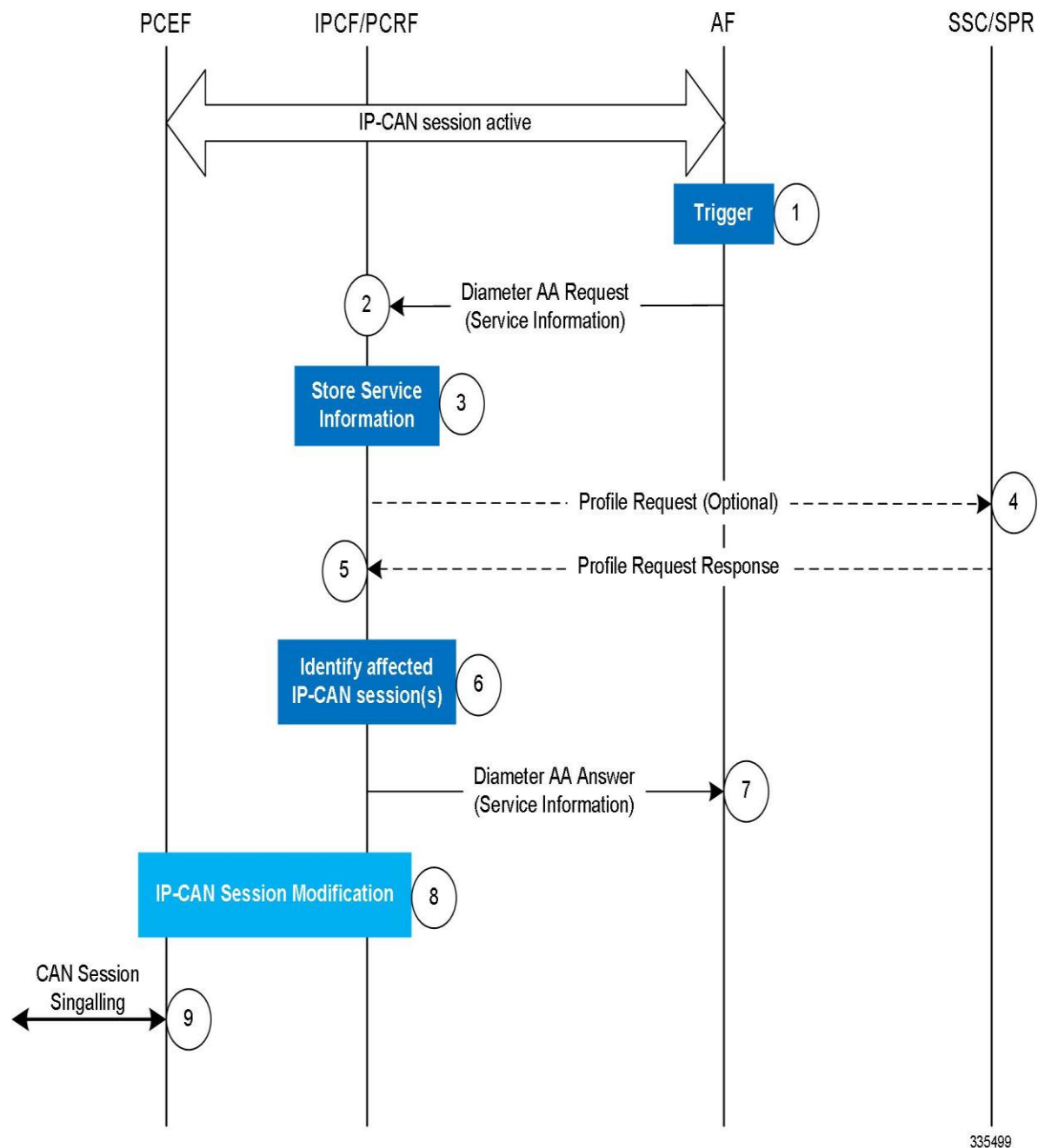
AF Session Setup Procedure

This section describes the Application Function session setup procedure between IPCF and AF.

This procedure is applicable for establishment of **Rx** connection between IPCF and AF (IMS) in core network.

The following figure and the text that follows describe the message flow for an **Rx** connection establishment procedure.

Figure 7. AF Session Setup Procedure Call Flow



335499

1. IP-CAN session is active and the AF receives an internal or external trigger to set-up a new AF session and provides Service Information; i.e., IP address of IP flow, Port numbers, media types, etc.
2. The AF forwards the Service Information to the IPCF by sending a Diameter AA Request for a new **Rx** Diameter session.
3. The IPCF stores the received Service Information.
4. *Optional*. If the IPCF needs subscription-related information and does not have it, the IPCF sends a Profile Request to the SSC in order to receive the information.

5. The SSC replies the Profile Request with the profile of subscriber which contains subscription related information; i.e. information about the allowed service(s), QoS information and PCC Rules information.
6. The IPCF identifies the affected established IP-CAN Session(s) using the information previously received from the PCEF/V-PCRF and the Service Information received from the AF.
7. The IPCF sends a Diameter AA Answer to the AF.
8. The IPCF interacts with the PCEF/V-PCRF and initiates IP-CAN Session Modification Procedure.
9. When **Gxa** does not apply for the IP-CAN session, IP-CAN bearer signaling is executed separately for each IP-CAN bearer under the following conditions:
 - All PCC rules bound to a bearer have been removed or deactivated
 - One or more bearers have to be modified
 - The PCEF needs to establish a new bearer

Supported Standards

The IPCF complies with the following standards for UTRAN/E-UTRAN/cdma2000-1x/HRPD networks services.

- [3GPP References](#)
- [IETF References](#)
- [Object Management Group \(OMG\) Standards](#)

3GPP References

- 3GPP TS 23.203 V8.6.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.4.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.4.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signaling flows and QoS parameter mapping; (Release 8)
- 3GPP TS 29.214 V8.5.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 8)
- 3GPP TS 29.215 V8.2.0 (2009-05): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over S9 reference point; (Stage 3) Release 8
- 3GPP TS 29.328 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Sh interface; Signaling flows and message contents (Release 8)

IETF References

- RFC-768, User Datagram Protocol (UDP), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991

- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC 1823, LDAPv2 Application Program Interface, August 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC 2131, Dynamic Host Configuration Protocol
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2328, OSPF Version 2, April 1998

- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol “L2TP”, August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC 2960, Stream Control Transmission Protocol, October 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000

- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- RFC 4511, Lightweight Directory Access Protocol (LDAP): The Protocol, June 2006

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

Chapter 2

Understanding the Service Operation

The IPCF provides wireless carriers with a flexible solution for providing extended and intelligent PCRF functionality for 3GPP Policy and Charging Control (PCC) solution.

The system functioning as IPCF is capable of supporting the following types of deployment scenario for IP-CAN sessions:

- **Standalone Deployment of IPCF in Networks**: In standalone deployment multiple PCEFs connects to a single IPCF through **Gx** interface and served by the PCC elements through IPCF.
- **Co-located Deployment of IPCF with PCEF Networks**: In co-located deployment IPCF sits with PCEF on the same chassis. It interacts with PCEF through internal connection matching **Gx** reference and connects to other PCC elements over various interfaces.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

Terminology

This section defines some of the terms used in the chapters that follow.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP interfaces, subscribers, etc. for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- **Source context:** Also referred to as the “ingress” context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a 3G UMTS network, the network function containing the PCEF would communicate with the PCF system via Gx/Gx-like interfaces configured within the source context as part of the PCC-service.
- **Destination context:** Also referred to as the “egress” context, this context is where a subscriber is provided connectivity to PCC elements (such as access to the SSC, AF etc.) as configured on PCC and related services. For example, the system's destination context would be configured with the **Sp** or **Rx** interfaces facilitating subscriber policy profile and charging rule data traffic to/from the PCC elements or other PDN (Mobile Data Service or Internet).
- **Local context:** This is the default context on the system used to provide out-of-band management functionality.

Logical Interfaces

This section describes the logical interface supported on PCC-PCF.

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that are used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a PCC-service, it will function as a Gx interface between the PCEF service and the PCF node.

The PCF provides the following network interface support to connect to the various network elements in an UTRAN/E-UTRAN/cdma2000-1x/HRPD networks:

- **Gx:** This reference is an interface between PCF and PCEF. It is a Diameter protocol-based interface over which the PCF communicates with a PCEF for the provisioning of charging rules. The charging rules are based on the dynamic analysis of flows used for a 3GPP or Non-3GPP IP-CAN subscriber session.

This is the interface used by the IPCF to communicate with PCEF on the same Public Land Mobile Network (PLMN).

The **Gx** reference point enables an IPCF to have dynamic control over the policy and charging control behavior at a PCEF. The **Gx** reference supports the following functions:

- Request for policy and charging control decision from PCEF to IPCF
- Provision of policy and charging control decision from IPCF to PCEF
- Delivery of IP-CAN-specific parameters from IPCF to PCEF or from PCEF to IPCF
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/NW)
- Termination of **Gx** session (corresponding to an IP-CAN session) by PCEF or IPCF



Important: The IPCF decision to terminate an **Gx** session is based on situation like removal of a UE subscription etc.

One or more **Gx** interfaces can be configured per system context.

Cisco IPCF supports standard 3GPP Rel. 7, Rel. 8, and Rel. 9 **Gx** interface to support different access technologies.

To provide accessibility to PDSN as PCEF in CDMA/HRPD access network for 3GPP IP-CAN type session, **Gx** interface uses NAI and IMSI as subscriber Id and ESN and MEID for user equipment information.

- **Gxa**: This reference is an interface between IPCF and the Bearer Binding and Event Reporting Function (BBERF) at AN-GW. It is a Diameter protocol-based interface and enables an IPCF to have dynamic control over the BBERF behavior at AN-GW.

The **Gxa** reference point enables the signaling of QoS control decisions and it supports the following functions:

- Establishment of **Gxa** session by BBERF and termination of **Gxa** session by BBERF or IPCF
- Establishment of Gateway Control Session by the BBERF and termination of Gateway Control Session by the BBERF or IPCF
- Request for QoS decision from BBERF to IPCF and provision of QoS decision from IPCF to BBERF
- Delivery of IP-CAN-specific parameters from IPCF to BBERF or from BBERF to IPCF
- Negotiation of IP-CAN bearer establishment mode (UE-only and UE or network)

One or more **Gxa** interfaces can be configured per system context.

- **Sp**: This is a Diameter-based interface residing between Cisco IPCF and SSC. It is based on standard **Sh** interface.

This reference point allows the IPCF to request subscription information related to the IP-CAN transport level policies from the SSC based on a subscriber identifier and used by IPCF to retrieve subscriber service policy and subscription profile.

Only one **Sp** interface can be configured per system context.

- **Event Notification Interface (EN)**: The **EN** interface supports uni-directional transfer of events from IPCF to SSC. This is an XML-RPC protocol based proprietary interface to send outbound event notifications to the SSC and forward these events to an event application module to generate mail/SMS notification to user/subscriber.

Only one **EN** interfaces can be configured per system context.

- **Rx:** This interface is the reference point between the Application Function (AF); i.e. IMS and the IPCF. This is a Diameter based interface.

The **Rx** reference point enables transport of application level session information from AF to IPCF. Such information includes:

- IP filter information to identify the service data flow for policy control and/or differentiated charging
- Media/application bandwidth requirements for QoS control

The Rx reference point enables the AF subscription to transport notifications on signaling path status of AF session in the IP-CAN.

One or more **Rx** interfaces can be configured per system context.

- **CORBA-based Interface:** IPCF supports the North-bound **CORBA** interface support for PPT and WEM management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems. It gives the ability to operator to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

Only one interface for WEM and one for PPT can be configured per system context.

Bindings

A binding is an association between “elements” within the system. There are two types of bindings: static and dynamic.

Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a PCC-service bound to a logical interface will cause the logical interface to take on the characteristics of a **Gx** interface within a 3GPP UMTS network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Services and Networks

This section describes the services configured on IPCF to support various functionality.

Services are configured within a context and enable certain functionality. The following services can be configured on the system:

- **PCC-services:** PCC-services are configured in Context configuration mode to support Policy Charging and Control Function. The PCC-service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of a **Gx** interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Gx interfaces.

It manages the policy logic for the networks. The authorization of resources for a subscriber’s data usage under various conditions and policies are defined in the PCC-service.

Only one PCC-service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

- **PCC-AF-Service:** PCC-AF-Service is configured in Context configuration mode to link, configure, and manage the Application Function endpoints and associated PCC-services over **Rx** interface for the IPCF services.

The PCC-AF service consolidates the provisioning and management required for the PCC-AF services being supported by the network that fall under the PCC regime. The application service handles the **Rx** interface over which the IPCF may receive media information for the application usage from AF.



Important: In case of absence of the **Rx** interface, the media information is available in the PCC-AF Service statically.

Multiple PCC-AF service instances can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

- **PCC-Policy-Service:** PCC-Policy Service configured in Context configuration mode to link, configure, and manage the policy authorization where IPCF acts as a policy server with PCEF/BBERF/AN-GW.

The PCC-Policy-service is mainly used to provide a mechanism to manage the external **Gx** or similar interfaces required for policy authorization purpose. It manages **Gx** and Gx-like interfaces such as **Gxa** which is based on the dictionary used for PCC-Policy-service.

Multiple instances of PCC-Policy-Service may exist in a system which could link with the same PCC-Service that controls the business logic. This service allows for configuration management for peers as well as services related to **Gx** like functions.

Multiple PCC-Policy service instances can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

- **PCC-Sp-Endpoint:** PCC-Sp endpoint configured in Context configuration mode to link, configure, and manage the **Sp** interface endpoints towards SSC for operational parameter configuration related to its peer.

An instance of PCC-Sp-endpoint represents a client end for SSC interactions and facilitates the configuration of the treatment required for the **Sp** interface as well as manage the connection and operational parameters related to its peer.

Only one PCC-Sp-endpoint across a chassis can be configured on a system.

- **Event-Notification Interface Endpoint:** Event notification endpoint configured in Context configuration mode to enable the event notification interface (Enctrl) mechanism on IPCF and to configure the Event Notification collection server endpoint related parameters.

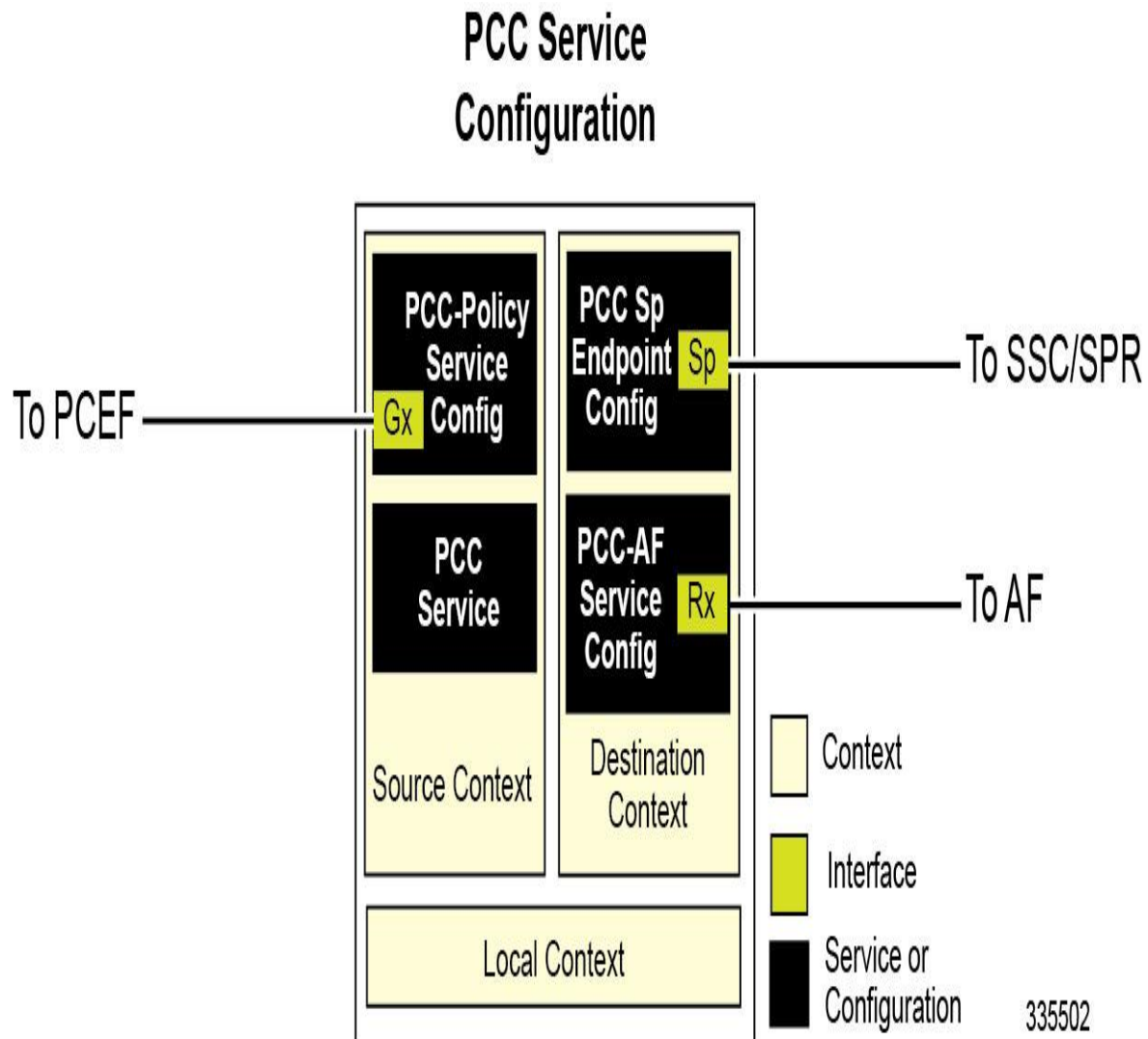
Only one Event Notification interface across a chassis can be configured on a system.

Following figure illustrates the relationship between services, interfaces, and contexts within the IPCF system for PCC service in 3G UMTS networks.



Important: ASR 5000 platform provides a highly flexible configuration model where any service/interface can be configured in any context. Example provided here is for illustration purpose only.

Figure 8. Service, Interface, and Context Relationship Within the System



The source context used to service a subscriber session is the same as the context in which the PCC related services are configured. Each PCC-Policy service is bound to an IP address in a source context. Once a PCEF has established a **Gx** session with a IPCF, the IPCF continues to use the same address as a **Gx** node.

The destination context is used to service the **Sp** interface session to connect with SSC.

Chapter 3

IPCF Node Configuration Procedures

This chapter is meant to be used in conjunction with the other chapters that describes the information needed to configure the IPCF to support PCRF functionality in UMTS networks.

It is recommended that you identify the options from the previous chapters that are required for your specific deployment. You can then use the procedures in this chapter to configure those options.

This chapter describes following:

- [Information Required to Configure the System as an IPCF](#)
- [IPCF Node Configuration](#)
- [Logging Facility Configuration](#)
- [Congestion Control Configuration](#)
- [Alarm and Alert Trap Configuration](#)
- [SNMP-MIB Traps for IPCF Node](#)
- [Event IDs for IPCF Node](#)



Important: At least one Packet Services Card (PSC/PSC2) must be made active prior to service configuration. Information and instructions for configuring PSCs/PSC2s to be active can be found in the Configuring System Settings chapter of the System Administration Guide.




Caution: While configuring any base-service or enhanced feature, it is highly recommended to take care of conflicting or blocked IP addresses and port numbers for binding or assigning. In association with some service steering or access control features, like Access Control List configuration, use of inappropriate port number may result in communication loss. Refer respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external network.

Information Required for Configuring the System as an IPCF

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an IPCF node in a test environment. Information provided in this section includes the following:

- [Required Local Context Configuration Information](#)
- [Required System-Level Configuration Information](#)
- [Required Source Context Configuration Information](#)
- [Required Destination Context Configuration Information](#)
- [Required AAA Context Configuration Information](#)

 **Important:** The following sections describe the minimum amount of information required to configure and make the IPCF operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

 **Important:** There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the IPCF in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an IPCF.

Table 1. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces are configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces are configured.
Physical port number	The physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.

Required Information	Description
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that is used to access the systems such as telnetd, sshd, and/or ftpd.

Required Source Context Configuration Information

The following table lists the information that is required to configure the Source context on an IPCF.

Table 2. Required Information for Source Context Configuration

Required Information	Description
VPN Context and Interface Configuration	
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the Source context is recognized by the system. Generally it is identified as source context.
Gx Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces are configured.
IP address and subnet	Local IPv4 addresses assigned to the interface to connect with PCEF or other components in network. Multiple addresses and subnets are needed if multiple interfaces are configured.
Physical port number	The physical port to which the interface is to be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
PCC-Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-service can be identified on the system. It is configured in Context configuration mode.
PCC-Policy-Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Policy service can be identified on the system. It is configured in Context configuration mode. Multiple names are needed if multiple PCC-Policy services are configured.
PCC-AF (Application Function) Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Application-Function-Service name can be identified on the system. It is configured in Context configuration mode.
PCC-Service Configuration	
Action-Set Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Action-Set can be identified on the system. It is configured in PCC-Service configuration mode. Multiple names are needed if multiple PCC-Action-Sets are configured.
PCC-Action-Set Configuration	

Required Information	Description
Monitoring Key	An integer value between 1 to 65535 to indicate the associated/disassociated Monitoring Key which is installed in PCEF for usage tracking. It is configured in PCC-Service configuration mode.
Rule name	An identification string between 1 to 63 characters (alpha and/or numeric) to indicate the configured rule on PCEF for activation of deactivation.
Rulebase name	An identification string between 1 to 63 characters (alpha and/or numeric) to indicate the configured rule on PCEF for activation of deactivation.
QoS Profile name	An identification string between 1 to 63 characters (alpha and/or numeric) to indicate the associated/disassociated QoS profile. It is configured in PCC-Service configuration mode.
QCI	An integer value between 1 to 255 to indicate the QoS Class Identifier associated with specific QoS profile.
Condition-Group Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Condition-Group can be identified on the system. It is configured in PCC-Service configuration mode. Multiple names are needed if multiple PCC-Condition-Groups are configured.
Data-Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Data-Service can be identified on the system. It is configured in PCC-Service configuration mode. Multiple names are needed if multiple PCC-Data Services are configured.
PCC-Map-Profile Priority	<p>An integer value between 1 to 1024 to identify the keys used to match the profile for a subscriber in a PCC-service instance for IPCF configuration. It is configured in PCC-Service configuration mode. The profile map is used when the subscriber session established. It is based on the priority of map and condition matches the corresponding named profile is used for the subscriber session. Map-Profile priority needs to match with specific profile policy and optionally with following options:</p> <ul style="list-style-type: none"> • APN name • Condition Group name • Missing SPR Profile • Subscription Attribute name and value <p>Multiple priority values are needed if multiple PCC-Map-Profile priorities are configured.</p>
PCC-Monitoring Key Value	An integer value between 1 to 65535 to configure the Monitoring Key with a configurable grant volume size from 1 through 4294967296 bytes. IPCF installs this Monitoring Key in PCEF for usage tracking. Multiple priority values are needed if multiple PCC-Monitoring Keys are configured.
Profile Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Profile can be identified on the system. It is configured in PCC-Service configuration mode. Multiple names are needed if multiple PCC-Profiles are configured.
PCC-Profile Configuration	
Evaluation Priority	An integer value between 1 to 1024 to identify the keys used to match the PCC-Condition Group with corresponding PCC-Action Set in a PCC-Service Profile instance. It is configured in PCC-Service configuration mode.
Condition-Group Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Condition-Group can be identified on the PCC-Profile instance to match with the PCC-Action Set with required evaluation priority. It is configured in PCC-Service configuration mode.

Required Information	Description
Action-SetName	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Action Set can be identified on the PCC-Profile instance to match with the PCC-Condition Group with required evaluation priority. It is configured in PCC-Service configuration mode.
QoS Profile name	An identification string between 1 to 63 characters (alpha and/or numeric) to indicate the associated/disassociated QoS profile. It is configured in PCC-Service configuration mode.
QCI	An integer value between 1 to 255 to indicate the QoS Class Identifier associated with specific QoS profile.
QoS Profile Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-QoS Profile can be identified on the system. It is configured in PCC-Service configuration mode. Multiple names are needed if multiple PCC-QoS Profiles are configured.
PCC-QoS Profile Configuration	
QCI	An integer value between 1 to 255 to indicate the QoS Class Identifier to associate with QoS profile instance.
Allocation and Retention Priority (ARP) value	An integer value between 1 to 15 to indicate the ARP value in QoS profile instance.
Guaranteed Bit Rate (GBR) value	An integer value between 0 to 104857600 to set the guaranteed bit rate in uplink/downlink direction in QoS profile instance.
Maximum Bit Rate (MBR) value	An integer between 0 to 104857600 to set the maximum bit rate in uplink/downlink direction in QoS profile instance.
PCC-Policy-Service Configuration	
PCC-Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) which is associated with PCC-Policy-Service on system. The name is a pre configured PCC-Service instance in Context configuration mode.
Diameter Origin Endpoint (Gxx) name	An identification string by which the Diameter endpoint towards PCEF is associated with PCC-Policy-Service on system. The name is a pre configured Diameter Endpoint instance for Gx/Gxa interface in Context configuration mode.
PCC-AF-Service Configuration	
PCC-Service Name	An identification string between 1 to 63 characters (alpha and/or numeric) which is associated with PCC-AF-Service on system. The name is a pre configured PCC-Service instance in Context configuration mode.
Diameter Origin Endpoint (Rx) name	An identification string by which the Diameter endpoint towards PCEF is associated with PCC-AF-Service on system. The name is a pre configured Diameter Endpoint instance for Rx interface in Context configuration mode.
Diameter Dictionary name	An identification string by which the Diameter dictionary is identified and used by AF service over Rx interface on system.

Required Destination Context Configuration Information

The following table lists the information that is required to configure the destination context.

Table 3. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	An identification string between 1 to 79 characters (alpha and/or numeric) by which the destination context is recognized by the system.
IP address and subnet	Local IPv4 addresses assigned to the interface to connect with SSC or other components in network. Multiple addresses and subnets are needed if multiple interfaces are configured.
Physical port number	The physical port to which the interface is to be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
PCC-Sp-Endpoint Name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the PCC-Sp interface endpoint name to serve with SSC can be identified on the system. It is configured in Context configuration mode. Multiple names are needed if multiple PCC-Sp interface endpoints are configured.
Event Notification Interface Endpoint Name	An identification string between 1 to 31 characters (alpha and/or numeric) by which the Event Notification Interface endpoint name to connect with Event Notification server can be identified on the system. It is configured in Context configuration mode. Multiple names are needed if multiple Event Notification interface endpoints are configured.
PCC-Sp-Endpoint Configuration	
Access Type	Defines the type of access used for SSC communication. By default it is "Diameter".
Diameter Origin Endpoint (Sp) name	An identification string by which the Diameter origin endpoint towards PCEF is associated with PCC-Sp-Endpoint on system. The name is a pre configured Diameter Endpoint instance for Sp interface in Context configuration mode.
Diameter Dictionary name	An identification string by which the Diameter dictionary is identified and used by PCC-Sp-Endpoint over Sp interface on system.
Event Notification Interface Endpoint Configuration	
IP address and subnet	This is the assigned IP address of the IPCF node on which it will communicate with Event Notification server. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Peer name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the peer (Event Notification Server) node is recognized by the IPCF.
Peer IP address and subnet	This is the assigned IP address of the Event Notification server on which IPCF communicates for event notification management. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Peer port number	This specifies the port number between 1 to 65535 on which Event Notification will be received by Event Notification server from IPCF.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the Diameter (AAA) context.


Table 4. Required Information for AAA Context Configuration

Required Information	Description
AAA context name	An identification string between 1 to 63 characters (alpha and/or numeric) by which the AAA context will be recognized by the system.
Diameter Endpoint Name Configuration	
Diameter Endpoint name (Gx)	An identification string by which the Diameter endpoint towards PCEF is recognized by the system. The name can be between 1 to 63 characters (alpha and/or numeric) and is not case sensitive. It may also contain dots (.) and/or dashes (-). This Diameter endpoint name will be associated with PCC-Policy Service configuration instance. Multiple names are needed if multiple Diameter Endpoints are used.
Diameter Endpoint name (Sp)	An identification string by which the Diameter endpoint towards SSC is recognized by the system. The name can be between 1 to 63 characters (alpha and/or numeric) and is not case sensitive. It may also contain dots (.) and/or dashes (-). This Diameter endpoint name will be associated with PCC-Sp-Endpoint configuration instance. Multiple names are needed if multiple Diameter Endpoints are used.
Diameter Endpoint name (Rx)	An identification string by which the Diameter endpoint towards AF is recognized by the system. The name can be between 1 to 63 characters (alpha and/or numeric) and is not case sensitive. It may also contain dots (.) and/or dashes (-). This Diameter endpoint name will be associated with PCC-AF-Service configuration instance. Multiple names are needed if multiple Diameter Endpoints are used.
Diameter Endpoint Name (Gx) Configuration	
Origin Realm name	This is an identification string between 1 to 63 characters (alpha and/or numeric) by which the Domain (Realm) of IPCF node is recognized by the PCEF.
Origin Host name	This is an identification string between 1 to 63 characters (alpha and/or numeric) by which the host (IPCF) node is recognized by the PCEF.
Origin Host IP address and subnet	This is the assigned IP address of the IPCF on which it will communicate with PCEF over Gx interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Origin Host port number	This specifies the port number between 1 to 65535 on which incoming traffic from PCEF will be accepted on IPCF.
Peer name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the peer (PCEF) node is recognized by the IPCF.
Peer IP address and subnet	This is the assigned IP address of the PCEF on which IPCF communicates over Gx interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Peer port number	This specifies the port number between 1 to 65535 from which incoming traffic from PCEF will be sent to IPCF.


Required Information	Description
Diameter Endpoint Name (Rx) Configuration	
Origin Realm name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the Domain (Realm) of IPCF node is recognized by the AF.
Origin Host name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the host (IPCF) node is recognized by the AF.
Origin Host IP address and subnet	This is the assigned IP address of the IPCF on which it will communicate with AF over Rx interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Origin Host port number	This specifies the port number between 1 to 65535 on which incoming traffic from AF will be accepted on IPCF.
Peer name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the peer (AF) node is recognized by the IPCF.
Peer IP address and subnet	This is the assigned IP address of the AF on which IPCF communicates over Rx interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Peer port number	This specifies the port number between 1 to 65535 from which incoming traffic from AF will be sent to IPCF.
Diameter Endpoint Name (Sp) Configuration	
Origin Realm name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the Domain (Realm) of IPCF node is recognized by the PCEF.
Origin Host name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the host (IPCF) node is recognized by the SSC.
Origin Host IP address and subnet	This is the assigned IP address of the IPCF on which it will communicate with SSC over Sp interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Origin Host port number	This specifies the port number between 1 to 65535 on which incoming and outgoing traffic from SSC will be processed by IPCF.
Peer name	This is an identification string between 1 to 79 characters (alpha and/or numeric) by which the peer (SSC) node is recognized by the IPCF.
Peer IP address and subnet	This is the assigned IP address of the SSC on which IPCF communicates over Sp interface.

IPCF Node Configuration

IPCF nodes are configured on system that allow the system to function as an IPCF in the 3G wireless data network.

 **Important:** This section provides the minimum instruction set for configuring an IPCF node that allows the system to process the IP-CAN session. Commands that configure additional properties are provided in the different chapters of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*.

 **Important:** Detailed procedure definition for step 1 to step 7 in following procedure is out of the scope of this guide. Kindly refer respective Administration Guides and References for more information.

To configure the system to work as IPCF node:

- Step 1** Make sure that PCEF/BBERF is configured with **Gx/Gxa** interface support as described in respective *Administration Guide*.
- Step 2** Make sure that Enhanced Charging Service Rules and Ruledefs are enabled on PCEF as described in *Enhanced Charging Service Administration Guide*.
- Step 3** *Optional.* Configure the subscriber threshold parameters for IP-CAN sessions by applying the example configuration in the *Thresholding Configuration Guide*.
- Step 4** *Optional.* Configure system to enable logging facilities for IP-CAN session subscribers and protocols by applying the example configuration in the *Logging Facility Configuration* section.
- Step 5** *Optional.* Configure congestion control parameters for IP-CAN session instances on system by applying the example configuration in the *Congestion Control Configuration* section.
- Step 6** *Optional.* Enable and configure the SNMP Traps to generate alarms and alerts from system for various events and thresholds for PCC related service instances by applying the example configuration in the *Alarm and Alert Trap Configuration* section.
- Step 7** Create and configure the local interfaces and bind it to IPCF node towards PCEF, SSC or any other component in network by applying the example configuration in the *Local Interface Configuration* section.
- Step 8** Create and configure the PCC-service and associate related parameters like policy profile, QoS profile, monitoring key, condition group, and action set on IPCF node by applying the example configuration in the *PCC-Service Configuration* section.
- Step 9** Create and configure the PCC-Policy service and associate related parameters to provide policy processing with PCEF over **Gx** interface in IP-CAN session by applying the example configuration in the *PCC-Policy-Service Configuration* section.
- Step 10** Create and configure the PCC-Sp-Endpoint and associate related parameters to provide SSC related processing with SSC over **Sp** interface for IP-CAN session by applying the example configuration in the *PCC-Sp-Endpoint Configuration* section.

- Step 11** Create and configure the Diameter Endpoint for **Gx** and **Sp** interface to connect with PCEF and SSC by applying the example configuration in the *Diameter Endpoint Configuration* section.
- Step 12** Create and configure the Event notification server node used to process event notification from IPCF by applying the example configuration in the *Event Notification Interface Endpoint Configuration* section.
- Step 13** *Optional.* If using Non-3GPP access technology, modify the PCC-Condition-Group configuration to connect with PDSN as PCEF over **Gx** interface by applying the example configuration in the *Non-3GPP IP-CAN Session Configuration* section.
- Step 14** Verify your IPCF configuration by following the steps in the *IPCF Service Configuration Verification* section.
- Step 15** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Local Interface Configuration

Use the following example to configure the interfaces in context to be used for PCEF and SSC or other nodes in network:

configure

```
context <vpn_ctxt_name> -noconfirm

interface <gx_intf_name>

  ip address <local_ip_address>/<mask>

  exit

exit

interface <sp_intf_name>

  ip address <local_ip_address>/<mask>

  end
```

Notes:

- <vpn_ctxt_name> is name of the source context in which IPCF service is to configure.
- <gx_intf_name> is name of the interface which is to use IP address <local_ip_address> for communication between IPCF node and PCEF or other components in network.
- <sp_intf_name> is name of the interface which is to use IP address <local_ip_address> for communication between IPCF node and SSC or other components like Event Notification Server in network.

PCC-Service Configuration

Use the following example to configure the PCC-service on system in context to provide the PCRF functionality in networks:



Important: This section provides the minimum instruction set for configuring an IPCF node that allows the system to process the IP-CAN session. Commands that configure additional properties are provided in the different chapters of *Command Line Interface Reference*.

- Step 1** Create and configure PCC-Service in context configuration mode with timeout duration, monitoring key, profile mapping and other common parameters by applying the example configuration in the *Basic PCC-Service Configuration* section.
- Step 2** Configure the QoS profile and parameters by applying the example configuration in the *PCC-QoS-Profile Configuration* section.
- Step 3** Configure the Condition Group and related parameters by applying the example configuration in the *PCC-Condition-Group Configuration* section.
- Step 4** Configure the Action set and related parameters by applying the example configuration in the *PCC-Action-Set Configuration* section.
- Step 5** Configure the Service-Profile and related parameters along with usage monitoring limits by applying the example configuration in the *PCC-Service-Profile and Usage Monitoring Configuration* section.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Basic PCC-Service Configuration

Use the following example to configure the basic parameters for PCC-service on system to provide PCRF functionality related processing for IP-CAN session in network.

```
configure

context <vpn_ctxt_name>

    pcc-service <pcc_svc_name> -noconfirm

        timeout idle <idle_dur [ action reauthorize ]

        timeout setup <setup_dur>

        timeout long-duration <ldt_timeout> [ action {detection | disconnect}]

        monitoring-key <mon_key> grant-size <volume>

        map-profile priority <priority_value> profile-policy name <prof_policy_name>

        multiple-pcef-per-subscriber

    end
```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <pcc_svc_name> is name of the PCC-service which is to be configured for IPCF functionality in network.

PCC-QoS-Profile Configuration

Use the following example to configure the parameters for PCC-QoS Profiles parameters like QCI, MBR, GBR etc. on system to provide PCRF functionality related processing for IP-CAN session in network.

```
configure

context <vpn_ctxt_name>

  pcc-service <pcc_svc_name>

    qos-profile <qos_prof_name>

      qci <qci_id>

      max-bitrate uplink <ulink_mbr> downlink <dlink_mbr>

      gauranteed-bitrate uplink <ulink_gbr> downlink <dlink_gbr>

      arp-priority <arp_prior_value> pre-emption {capable | not-capable} {not-
vulnerable | vulnerable}

    end
```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <pcc_svc_name> is name of the PCC-service which is to be configured for IPCF functionality in network.
- <qos_prof_name> is name of the PCC-QoS-Profile which is to be used to configure the QoS profiles for IPCF functionality in network. This command can be entered multiple times to configure multiple QoS profiles with other parameters, if required. For more information on available parameters for QoS Profile, refer *PCC-QoS-Profile Configuration Mode Commands* chapter in *Command Line Interface Reference*.

PCC-Condition-Group Configuration

Use the following example to configure the parameters for various condition parameters like threshold, RAT, event triggers etc. on system to provide PCRF functionality related processing for IP-CAN session in network.

```
configure

context <vpn_ctxt_name>

  pcc-service <pcc_svc_name>

    condition-group <cond_grp_name>

      threshold-condition usage-monitor <usage_mon_name> usage {= | !=} {absolute value
<volume> | subscription-limit | subscription-threshold <subs_thres_limit>}

      radio-access-technology { = | != } <RAT>

      event-trigger { = | != } {an-gw-change | bearer-qos-change | bearer-setup |
bearer-termination | default-eps-bearer-qos-change | ip-can-change | loss-of-bearer |
out-of-credit | pgw-trace-control | plmn-change | qos-change | qos-change-exceeding-
```

```

authorization | rai-change | rat-change | reallocation-of-credit | recover-of-bearer |
resource-modification-request | revalidation-timeout | session-setup | session-
termination | sgsn-change | successful-resource-allocation | tft-change | ue-ip-address-
allocate | ue-ip-address-release | ue-time-zone-change | user-location-change}

bearer-count { = | != | <= | >= } <num_bearer>

user-equipment-info eui64 {= | !=} <eui64>

user-equipment-info imeisv {= | !=} <imei_sv >

user-equipment-info mac {= | !=} <mac_value>

user-equipment-info modified-eui64 {= | !=} <meui64>

exit

```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <pcc_svc_name> is name of the PCC-service which is to be configured for IPCF functionality in network.
- <cond_grp_name> is name of the PCC-Condition-Group which is to be used to configure the session condition parameters for IPCF functionality in network. This command can be entered multiple times to configure multiple condition groups with other parameters, if required. For more information on available parameters for PCC-Condition-Group, refer *PCC-Condition-Group Configuration Mode Commands* chapter in *Command Line Interface Reference*.

PCC-Action-Set Configuration

Use the following example to configure the parameters for action-set parameters like rule activation, authorization, usage monitoring key association with PCC-Service etc. on system to provide PCRF functionality related processing for IP-CAN session in network.

```

configure

context <vpn_ctxt_name>

pcc-service <pcc_svc_name>

action-set <actionset_name>

rule-activate <rule_name>

associate monitoring-key <mon_key_id> usage-monitor <usage_mon_name>

authorize {apn-mbr | default-eps-bearer | qci} qos-profile <qos_prof_name>

end

```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <pcc_svc_name> is name of the PCC-service which is to be configured for IPCF functionality in network.

- `<actionset_name>` is name of the PCC-Action-set which is to be used to configure the set of action to initiate on the basis of condition parameters for IPCF functionality in network. This command can be entered multiple times to configure multiple action-sets with other parameters, if required. For more information on available parameters for Action-set, refer *PCC-Action-Set Configuration Mode Commands* chapter in *Command Line Interface Reference*.

PCC-Service-Profile and Usage Monitoring Configuration

Use the following example to configure the service profile and sets the parameters like usage limits, rulebase association, service-tag etc. on system to provide PCRF functionality related processing for IP-CAN session in network.

```
configure

context <vpn_ctxt_name>

    pcc-service <pcc_svc_name>

        profile <profile_name>

            eval-priority <priority_value> condition-group <cond_grp_name> action-set
            <actionset_name>

            associate monitoring-key <mon_key_id> usage-monitor <usage_mon_name>

            default-rulebase-name <rulebase_name>

            service-tag <svc_tag> {rule-name <rule_name> | rulebase-name <rulebase_name>}

            usage-monitor <usage_mon_name> -noconfirm

            usage-limit volume [downlink <dlink_volume> | total <total_volume> | uplink
            <uplink_volume>]

        end
```

Notes:

- `<vpn_ctxt_name>` is name of the source context in which PCC-service is configured.
- `<pcc_svc_name>` is name of the PCC-service which is to be configured for IPCF functionality in network.
- `<profile_name>` is name of the PCC-Service-Profile which is to be used to map in IP-CAN for IPCF functionality in network. This command can be entered multiple times to configure multiple Subscriber profiles with other parameters, if required. For more information on available parameters for Subscriber Profile, refer *PCC-Profile-Configuration Mode Commands* chapter in *Command Line Interface Reference*.
- `<usage_mon_name>` is name of the PCC-Usage-Monitor-Key which is to be used to monitor the usage in IP-CAN for IPCF functionality in network. This command can be entered multiple times to configure multiple PCC-Usage-Monitor-Key, if required. For more information on available parameters for PCC-Service-Profile, refer *PCC-Usage-Monitor Configuration Mode Commands* chapter in *Command Line Interface Reference*.

PCC-Policy-Service Configuration

Use the following example to configure the PCC-Policy-service on system in to provide the Gx interface functionality for Policy related processing with PCEF in network:

```
configure

context <vpn_ctxt_name>

    pcc-policy-service <pcc_policy_svc_name> -noconfirm

        associate <pcc_svc_name>

        diameter origin endpoint <gx_end_name>

        diameter dictionary {gxa-standard | r7-standard | standard}

        max policy-sessions <max_session>

        subscriber-binding-identifier {imsi | msisdn | nai | sip-uri}

        ehrpd-access-bcm {as-requested | ue-nw | ue-only}

        gprs-access-bcm {as-requested | ue-nw | ue-only}

    end
```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <pcc_policy_svc_name> is name of the Gx interface configuration instance which provides Gx interface functionality on IPCF node for subscriber policy processing with PCEF in IP-CAN session.
- <pcc_svc_name> is name of the PCC-Service which is to be associated with PCC-Policy service and configured in *PCC-Service Configuration* section.
- <gx_end_name> is name of the Diameter Endpoint node which is to be used as Gx interface node with PCEF and configured in *Diameter Endpoint Configuration* section.

PCC-Sp-Endpoint Configuration

Use the following example to configure the PCC-Sp-Endpoint on system to provide Sp interface functionality for subscriber profile related processing for IP-CAN session with SSC in network:

```
configure

context <vpn_ctxt_name>

    pcc-sp-endpoint <sp_endpoint_node> -noconfirm

        access-type {custom | diameter | ldap}

        diameter origin endpoint <sp_end_name>
```

```
diameter dictionary {sh-custom-starent | sh-standard}

profile-update-notification {allow | disallow}

spr subscriber identifier {imsi | msisdn

end
```

Notes:

- `<vpn_ctxt_name>` is name of the source context in which PCC-Sp-Endpoint is configured.
- `<sp_endpoint_node>` is name of the Sp interface configuration instance which provides Sp interface functionality on IPCF node for subscriber profile processing with SSCP in IP-CAN session.
- `<sp_end_name>` is name of the Diameter Endpoint node which is to be used as Sp interface node with SSC and configured in *Diameter Endpoint Configuration* section.

Diameter Endpoint Configuration

Use the following example to configure the Diameter Endpoints on IPCF node for **Gx/Gxa** and **Sp** interface to interact with PCEF and SCC respectively for IP-CAN session processing in network:

```
configure

context <vpn_ctxt_name>

    diameter endpoint <gx_end_name>

        origin realm <realm_ipcf>

        origin host <ipcf_host_name> address <local_ip_address> port <inbound_gx_port>
accept-incoming-connections

        no watchdog-timeout

        use-proxy server-mode demux-mode

        peer <pcef_peer_name> realm <pcef_realm_name> address <pcef_ip_address> port
<outbound_pcef_port>

        exit

    diameter endpoint <sp_end_name>

        origin realm <realm_ipcf>

        origin host <ipcf_host_name> address <local_ip_address> port <inbound_sp_port>

        no watchdog-timeout

        use-proxy

        connection timeout <dur>
```

```

connection retry-timeout <dur>

peer <ssc_peer_name> realm <ssc_realm_name> address <ssc_ip_address>

end

```

Notes:

- <vpn_ctxt_name> is name of the source context in which PCC-service is configured.
- <gx_end_name> is name of the Gx interface instance which is to be configured for subscriber policy processing over Gx interface in network with PCEF.
- <realm_ipcf> is name of the domain (Realm) in which IPCF node is located.
- <pcef_peer_name> is name of the PCEF (GGSN) node which is to be connected with IPCF for subscriber policy processing over Gx interface in network.
- <pcef_ip_address> is IP address of the PCEF (GGSN) node which is to be connected with IPCF for subscriber policy processing over Gx interface in network.
- <pcef_realm_name> is name of the domain (Realm) in which PCEF node is located.
- <sp_end_name> is name of the Sp interface instance which is to be configured for subscriber profile processing over Sp interface in network with SSC.
- <ssc_peer_name> is name of the SSC node which is to be connected with IPCF for subscriber profile processing over Sp interface in network.
- <ssc_realm_name> is name of the domain (Realm) in which SSC node is located.
- <ssc_ip_address> is IP address of the SSC node which is to be connected with IPCF for subscriber profile processing over Sp interface in network.

Event Notification Interface Endpoint Configuration

Use the following example to configure the Event Notification Interface Endpoint on IPCF node to interact with Event Notification server for event notification management during IP-CAN session in network:

```

configure

context <vpn_ctxt_name>

    event-notif-endpoint <event_notif_intc_name>

        address <local_ip_address>

        peer name <remote_server_name> address <remote_server_ip_address> port
<out_remote_serv_port>

    end

```

Notes:

- <vpn_ctxt_name> is name of the context in which PCC-service is configured.
- <event_notif_intc_name> is name of the Event notification interface instance on IPCF which is to be used for with remote Event notification server.

- `<local_ip_address>` is IP address of the IPCF node which configured in *Local Interface Configuration* section.
- `<remote_server_name>` is name of the remote Event Notification collection and processing server. Multiple peers can be configured in one Event Notification Interface.
- `<remote_server_ip_address>` is IP address of the remote Event notification collection processing server which is to be used for event notification management for IP-CAN session.

Non-3GPP IP-CAN Session Configuration

Use the following example to modify the PCC-Condition Group configuration to support the conditions to process CDMA UE subscribers coming from PDSN node over Gx interface where PDSN acts as PCEF with IPCF node for non-3GPP IP-CAN session in network:

```
configure
```

```
context <vpn_ctxt_name>
```

```
    pcc-service <pcc_svc_name>
```

```
        condition-group <cond_grp_name>
```

```
            base-station-id {[ sid {= | != | < | <= | > | >= } <sys_identifier> ] | range
<start_range> to <end_range>}] [ nid {= | != | < | <= | > | >= } <netwrk_identifier> ] |
range <start_range> to <end_range>}] [ cellid {= | != | < | <= | > | >= } <cell_identifier>
] | range <start_range> to <end_range> ]}]
```

```
            nai {= | !=} {username <user_name> [domain <domain>] | domain <domain>}
```

```
            user-equipment-info esn {= | !=} <esn>
```

```
            user-equipment-info meid {= | !=} <meid>
```

```
        end
```

Notes:

- `<vpn_ctxt_name>` is name of the context in which PCC-service is configured.
- Currently following are not supported for non-3GPP IP-CAN session support:
 - multiple bearer in single Non-3GPP IP-CAN session
 - Bearer control mode when initiated by both, the UE and Network
 - Network initiated bearer creation/modification/deletion
- `<cond_grp_name>` is a preconfigured PCC-Condition-Group which is to be used to configure the session condition parameters for IPCF functionality in network. For more information on initial configuration for PCC-Condition-Group, refer *PCC-Condition-Group Configuration* in *PCC-Service Configuration* section.

Verifying IPCF Configuration

This section shows the configuration parameters configured for IPCF service.

- Step 1** Verify that your PCC-service was created and configured properly by entering the following command in Exec Mode:

```
show pcc-service service-name <pcc_svc_name>
```

The output of this command shows a concise listing of PCC-service parameter settings.

- Step 2** Verify configuration errors of your PCC-service by entering the following command in Exec Mode:

```
show configuration errors section pcc-service verbose }
```

The output of this command displays current configuration errors and warning information for the target configuration file as specified for PCC-service.

- Step 3** Verify that your PCC-Policy service was created and configured properly by entering the following command in Exec Mode:

```
show pcc-policy service name <pcc_policy_svc_name>
```

The output of this command shows a concise listing of PCC-Policy service parameter settings.

- Step 4** Verify configuration errors of your PCC-Policy service by entering the following command in Exec Mode:

```
show configuration errors section pcc-policy-service verbose }
```


The output of this command displays current configuration errors and warning information for the target configuration file as specified for PCC-Policy service.



Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.

Logging Facility Configuration

Use the following example to configure the IPCF node system to enable the logging and debug facilities for IP-CAN session subscribers and related protocols.

 **Important:** This section provides the minimum instruction set for configuring logging facilities for system monitoring that allows the user to monitor the events and logging. Commands that configure additional logging facilities are provided in the *Exec Mode Command* chapter of *Command Line Interface Reference*.

```
configure

logging console

logging display event-verbosity {min | concise | full}

logging filter runtime facility bindmux { critical | error | warning | unusual | info |
trace | debug }

logging filter runtime facility diameter { critical | error | warning | unusual | info
| trace | debug }

logging filter runtime facility event-notif { critical | error | warning | unusual |
info | trace | debug }


logging filter runtime facility evlog { critical | error | warning | unusual | info |
trace | debug }

logging filter runtime facility pccmgr { critical | error | warning | unusual | info |
trace | debug }

logging filter runtime facility sprmgr { critical | error | warning | unusual | info |
trace | debug }

logging filter runtime facility threshold { critical | error | warning | unusual | info
| trace | debug }

end
```

 **Important:** Refer *System Administration Guide* for more information on logging facility configuration.

Displaying Logging Facility

This section shows the logging facility event logs for logging facilities enabled on IPCF node.

Step 1 Verify the logging facilities configured on IPCF node by entering the following command in Exec Mode:

```
show logging [ active | verbose]
```

The output of this command provides the display of event logs for configured logging facilities.

Congestion Control Configuration

To configure Congestion Control functionality:

- Step 1** Configure Congestion Control Threshold by applying the example configuration in the *Configuring the Congestion Control Threshold* section.
- Step 2** Configure Service Congestion Policies for PCC related services by applying the example configuration in the *Configuring Service Congestion Policies* section.
- Step 3** *Optional.* Operator can configure the system to reject the all new incoming call coming to specific or all PCC related service instances in a busy-out or planned maintenance or for troubleshooting by applying the example configuration in the *Configuring New Call Policy* section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring the Congestion Control Threshold

To configure congestion control threshold, apply the following example configuration:

```
configure

 congestion-control threshold max-sessions-per-service-utilization <percent>

 congestion-control threshold tolerance <percent>

end
```

Notes:

- There are several additional threshold parameters. See the *Global Configuration Mode* chapter of the *Command Line Interface Reference* for more information.
- The tolerance is the percentage under a configured threshold that dictates the point at which the condition is cleared.
- Repeat this configuration as needed for additional thresholds.

Configuring Service Congestion Policies

To create a congestion control policy for PCC related sessions, apply the following example configuration:

```
configure

 congestion-control policy {pcc-af-service | pcc-policy-service } action { drop | none
| reject }

end
```

Notes:

- For all IP-CAN session on PCC related services **none** is the default action, if this command is not configured.

Configuring New Call Policy

To create a new call policy in a busy hour or planned maintenance or other operator intervened scenario, apply the following example configuration:

```
newcall policy pcc-af-service [all | name <pcc_af_svc_name> ] reject
```

```
newcall policy pcc-policy-service [all | name <pcc_policy_svc_name> ] reject
```

Notes:

- For IP-CAN sessions **reject** is the default action for all new calls coming on a specific or all PCC related service instance.

Alarm and Alert Trap Configuration

To enable and configure the SNMP Traps to generate alarms and alerts from system for various events and thresholds in PCC related services, apply the following example configuration:

```
configure
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear] {ThreshPCCAFSessions |
ThreshPCCPolicySessions} [ target <trap_collector>]
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear]
{ThreshPerServicePCCAFSessions | ThreshPerServicePCCPolicySessions} [ target
<trap_collector>]
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear] {ThreshClearPCCAFSessions
| ThreshClearPCCPolicySessions} [ target <trap_collector>]
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear]
{ThreshClearPerServicePCCAFSessions | ThreshClearPerServicePCCPolicySessions} [ target
<trap_collector>]
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear] {PCCAFServiceStart |
PCCAFServiceStop} [ target <trap_collector>]
```

```
    snmp trap { enable | suppress} [Congestion CongestionClear] {PCCPolicyServiceStart |
PCCPolicyServiceStop} [ target <trap_collector>]
```

```
end
```

Notes:

- Repeat these configuration as needed for additional traps.
- There are several additional SNMP Traps which can be configured. Refer *Global Configuration Mode* chapter of the *Command Line Interface Reference* for more information.
- For more information on SNMP Traps, refer *System SNMP-MIB Reference*.

SNMP-MIB Traps for IPCF Node

SNMP traps are used to manage and monitor the service on IPCF node.

Supported SNMP traps and its id are indicated in the following table.

Table 5. SNMP Traps and Object Ids

Traps	Object Id
starPCCPolicyServiceStart	starentTraps 1127
starPCCPolicyServiceStop	starentTraps 1128
starPCCAFServiceStart	starentTraps 1131
starPCCAFServiceStop	starentTraps 1132
starSPRServerUnreachable	starentTraps 1133
starSPRServerReachable	starentTraps 1134
starNtfyIntfPeerUnreachable	starentTraps 1173
starNtfyIntfPeerReachable	starentTraps 1174



Important: For more information on SNMP trap configuration and supported object ids, refer *System SNMP-MIB Reference*.

Event IDs for IPCF Node

Identification numbers (IDs) are used to reference events as they occur when logging is enabled on the system. Logs are collected on a per facility basis.

Each facility possesses its own range of event IDs as indicated in the following table.



Important: Not all event IDs are used on all platforms. It depends on the platform type and the license(s) running.

For more information on logging facility configuration and event id, refer *Configuring and Viewing System Logs* chapter in *System Administration Guide*.

Table 6. System Event Facilities and ID Ranges

Facility	Event ID Range
Demux-Bindmux Facility Events	158200-158999
PCC Manager Facility Events	159000-159499
SPR Manager Facility Events	159500-159999
LDAP Request Facility Events	160000-160499
Event Notification Interface Facility Events	170000-170499
AAA Client Facility Events	6000-6999
Alarm Controller Facility Events	65000-65999
Card/Slot/Port (CSP) Facility Events	7000-7999
Command Line Interface Facility Events	30000-30999
Event Log Facility Events	2000-2999
Statistics Facility Events	31000-31999
System Facility Events	1000-1999
System Initiation Task (SIT) Main Facility Events	4000-4999
Threshold Facility Events	61000-61999
Virtual Private Network Facility Events	5000-5999

Chapter 4

Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These commands have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provide the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the Command Line Interface Reference.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference Guide* for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the *Counters and Statistics Reference*.

Table 7. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Subscriber Information	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the PCC-Service on system	<code>show subscribers pcc-service pccs_svc_name</code>
View information for a specific subscriber	<code>show subscribers pcc-service pccs_svc_name full</code>
View Recovered Session Information	
View session state information and session recovery status	<code>show subscriber debug-info { callid msid username }</code>
View Session Statistics and Information	
Display Historical Session Counter Information	
View all historical information for all sample intervals	<code>show session counters historical</code>
Display Session Duration Statistics	
View session duration statistics	<code>show session duration</code>
Display Session State Statistics	
View session state statistics	<code>show session progress</code>
Display Session Subsystem and Task Statistics	
Refer to the <i>System Software Task and Subsystem Descriptions</i> appendix of the <i>System Administration Guide</i> for additional information on the Session subsystem and its various manager tasks.	
View PCC Bind Demux Manager statistics	<code>show session subsystem facility bindmux all</code>
View Session Manager statistics	<code>show session subsystem facility sessmgr all</code>
View Demux Manager status showing detailed statistics for IMSI Manager	<code>show demux-mgr statistics imsimgr full</code>

To do this:	Enter this command:
View Subscriber Profile Repository (SSC) manager facility statistics	<code>show logs facility sprmgr</code>
View PCC Manager facility statistics	<code>show logs facility pccmgr</code>
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons</code>
Display a PCC-Service Information	
View all configured PCC-service configuration in detail	<code>show pcc-service all verbose</code>
View configuration errors in PCC-Service section in detail	<code>show configuration errors section pcc-service verbose</code>
Display a PCC-AF-Service Information	
View all configured PCC-Policy service configuration	<code>show pcc-af service all</code>
View PCC-Policy-Service statistics	<code>show pcc-af service statistics</code>
Display a PCC-Policy Service Information	
View all configured PCC-Policy-Service configuration in detail	<code>show pcc-policy service all verbose</code>
View configuration errors in PCC-Policy-Service section in detail	<code>show configuration errors section pcc-policy-service verbose</code>
Display Event-Notification-Endpoint Information	
View all configured Event Notification server configuration in detail	<code>show event-notif server all verbose</code>
View all configured Event Notification interface statistics	<code>show event-notif statistics</code>
Display a PCC-Sp-Endpoint Information	
View configured PCC-Sp-Endpoint configuration on system	<code>show pcc-sp-endpoint all</code>
View status of PCC-Sp-Endpoint connections between IPCF and SSC	<code>show pcc-sp-endpoint connection all</code>
View PCC-Sp-Endpoint interface statistics	<code>show pcc-sp-endpoint statistics all</code>

Monitoring Logging Facility

This section contains commands used to monitor the logging facility active for specific tasks, managers, applications and other software components in the system.

Table 8. Logging Facility Monitoring Commands

To do this:	Enter this command:
Monitor logging facility for specific session based on Call-id on system	<code>logging trace callid <i>call_id</i></code>
Monitor logging facility based on IP address used in session on system	<code>logging trace ipaddr <i>ip_address</i></code>
Monitor logging facility based on MS Identity used in session on system	<code>logging trace msid <i>ms_identifier</i></code>
Monitor logging facility based on user name used in session on system	<code>logging trace username <i>name</i></code>
Monitor BindDemuxManager logging facility for IPCF on system	<code>logging filter active facility bindmux { critical error warning unusual info trace debug }</code>
Monitor Diameter logging facility for interface related activity on system	<code>logging filter active facility diameter { critical error warning unusual info trace debug }</code>
Monitor EventNotification Interface logging facility on system	<code>logging filter active facility event-notif { critical error warning unusual info trace debug }</code>
Monitor EventLog logging facility on system	<code>logging filter active facility evlog { critical error warning unusual info trace debug }</code>
Monitor PCCManager logging facility on system	<code>logging filter active facility pccmgr { critical error warning unusual info trace debug }</code>
Monitor SSC logging facility on system	<code>logging filter active facility sprmgr { critical error warning unusual info trace debug }</code>
Monitor threshold logging facility for IPCF on system	<code>logging filter active facility threshold { critical error warning unusual info trace debug }</code>

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PCC-Service, PCC-Policy, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to *Command Line Interface Reference* for detailed information on using this command.

Chapter 5

Troubleshooting the Service

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during service operation.

All commands described in this chapter are available in Exec Mode only.

Test Commands

In the event that an issue was discovered with an installed application or line card, depending on the severity, it may be necessary to take corrective action.

The system provides several redundancy and fail-over mechanisms to address issues with application and line cards in order to minimize system downtime and data loss. These mechanisms are described in the sections that follow.

Using the Test IPCF Command

This command tests the status of IPCF BindMuxManager instance and also provides ability to start or stop the BindMuxManager instance on the chassis.



Important: This command must be executed from within the context in which at least one PCC service is configured.

The command has the following syntax:

```
test ipcf bindmux [start | stop]
```

Keyword/Variable	Description
start	Starts the IPCF BindMuxManager instance running on the chassis.
stop	Stops the IPCF BindMuxManager instance running on the chassis.

Checking Reachability of Node Using Ping

This command tests the reachability of network nodes from a chassis.

The command has the following syntax:

```
ping host_ip_address [broadcast] [count num_packets ] [pattern packet_pattern]
[size octet_count ] [src {src_host_name | src_host_ip_address} ] ]
```

Keyword/Variable	Description
<i>host_ip_address</i>	Identifies the remote node to which the ability to communicate with is to be verified. <i>host_ip_address</i> : specifies the remote node using the node's assigned IP address specified using the standard IPv4 dotted decimal notation.
broadcast	Sends ping packets to broadcast addresses.
count <i>num_packets</i>	Specifies the number of packets to send to the remote host for verification. <i>num_packets</i> must be within the range 1 through 10000.
pattern <i>packet_pattern</i>	Specifies a pattern to use to fill the internet control message protocol packets with. <i>packet_pattern</i> must be specified in hexadecimal format with a value in the range hexadecimal 0x0000 through 0xFFFF. <i>packet_pattern</i> must begin with a '0x' followed by up to 4 hexadecimal digits.
size <i>octet_count</i>	Specifies the number of bytes each IP datagram. <i>octet_count</i> must be a value in the range 40 through 18432.
src { <i>src_host_name</i> <i>src_host_ip_address</i> }	Specifies an IP address to use in the packets as the source node. <i>src_host_name</i> : specifies the source node using the node's logical host name which must be resolved via DNS lookup. <i>src_host_ip_address</i> : specifies the source node using the node's assigned IP address specified using the standard IPv4 dotted decimal notation.

Using the Diameter Test Command

This command disables a Diameter endpoint without removing the peer's configuration.

Use this command to perform a troubleshooting by resetting the Diameter endpoint.



Important: This command must be executed from within the context in which at least one Diameter node is configured.

The command has the following syntax:

```
diameter {disable | enable | reset connection} endpoint endpoint_name peer
peer_id
```

Keyword/Variable	Description
disable	Disables a Diameter endpoint and peer host configured in it before starting troubleshooting.
enable	Enables a Diameter endpoint and peer host configured in it after troubleshooting.
reset connection	Resets the connection between Diameter endpoint and peer host configured in it as a first attempt to resolve the issue before disabling it for troubleshooting.
endpoint <i>endpoint_name</i>	Specifies the endpoint in which the peer is configured. <i>endpoint_name</i> must be the name of the endpoint, and must be an alpha and/or numeric string of 1 through 63 characters in length.
peer <i>peer_id</i>	Specifies the peer id which is to be reset. <i>peer_id</i> must be the Diameter peer host name, and must be a string of 1 through 63 characters in length.

Appendix A

Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

This appendix describes following engineering rules for PCC service:

- [PCC Engineering Rules](#)
- [Interface and Port Engineering Rules](#)
- [Service Engineering Rules](#)

PCC Engineering Rules

The following engineering rules apply when the system is configured as an IPCF node:

- A maximum of 1 PCC service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.
- Multiple PCC-Policy services, but limited to maximum of 256 services (regardless of type), can be configured per system.
- Multiple PCC-AF services, but limited to maximum of 256 services (regardless of type), can be configured per system.
- A maximum of 1 PCC-Sp-Endpoint instance can be configured per system.
- A maximum of 1 Event Notification interface can be configured per system.

Interface and Port Engineering Rules

The rules discussed in this section pertain to both the Ethernet 10/100 and Ethernet 1000 Line Cards and the four-port Quad Gig-E Line Card and the type of interfaces they facilitate.

Gx/Gxa Interface Rules

When communicating PCEFs/BBERFs the system provides **Gx/Gxa** interface support and connects to the PCEFs/BBERFs over this interface.

The following engineering rules apply to the **Gx/Gxa** interface between the PCEF/BBERF and IPCF:

- A **Gx/Gxa** interface is created once a Diameter endpoint entity is bound to a PCC-Policy Service and respective dictionary is associated.

Rx Interface Rules

When communicating Application Functions (AFs) the system provides **Rx** interface support and connects to the AFs over this interface.

The following engineering rules apply to the **Rx** interface between the AF and IPCF:

- An **Rx** interface is created once a Diameter endpoint entity is bound to a PCC-AF Service.

Sp Interface Rules

When communicating SSC (SPR) the system provides **Sp** interface support and connects to the SSC over this interface.

The following engineering rules apply to the **Sp** interface between the SSC and IPCF:

- An **Sp** interface is created once a Diameter endpoint entity is bound to a PCC-Sp-Endpoint Service.

Service Engineering Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.



Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.
