Cisco ASR 5x00 Serving Gateway
Administration Guide

Version 15.0

Last Updated October 31, 2014

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
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 noninfringement 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 5x00 Serving Gateway Administration Guide

© 2014 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## About this Guide
- Conventions Used
- Supported Documents and Resources
- Related Common Documentation
- Related Product Documentation
- Obtaining Documentation
- Contacting Customer Support

## Serving Gateway Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Description</td>
<td>13</td>
</tr>
<tr>
<td>Platform Requirements</td>
<td>14</td>
</tr>
<tr>
<td>Licenses</td>
<td>16</td>
</tr>
<tr>
<td>Network Deployment(s)</td>
<td>16</td>
</tr>
<tr>
<td>Serving Gateway in the E-UTRAN/EPC Network</td>
<td>17</td>
</tr>
<tr>
<td>Supported Logical Network Interfaces (Reference Points)</td>
<td>17</td>
</tr>
<tr>
<td>Features and Functionality - Base Software</td>
<td>18</td>
</tr>
<tr>
<td>ANSI T1.276 Compliance</td>
<td>23</td>
</tr>
<tr>
<td>APN-level Traffic Policing</td>
<td>24</td>
</tr>
<tr>
<td>Bulk Statistics Support</td>
<td>24</td>
</tr>
<tr>
<td>Circuit Switched Fall Back (CSFB) Support</td>
<td>25</td>
</tr>
<tr>
<td>Closed Subscriber Group Support</td>
<td>25</td>
</tr>
<tr>
<td>Congestion Control</td>
<td>26</td>
</tr>
<tr>
<td>Downlink Delay Notification</td>
<td>26</td>
</tr>
<tr>
<td>Value Handling</td>
<td>26</td>
</tr>
<tr>
<td>Throttling</td>
<td>27</td>
</tr>
<tr>
<td>EPS Bearer ID and ARP Support</td>
<td>27</td>
</tr>
<tr>
<td>Dynamic GTP Echo Timer</td>
<td>27</td>
</tr>
<tr>
<td>Event Reporting</td>
<td>27</td>
</tr>
<tr>
<td>Idle-mode Signaling Reduction Support</td>
<td>28</td>
</tr>
<tr>
<td>IP Access Control Lists</td>
<td>28</td>
</tr>
<tr>
<td>IPv6 Capabilities</td>
<td>28</td>
</tr>
<tr>
<td>LIPA Support</td>
<td>29</td>
</tr>
<tr>
<td>Location Reporting</td>
<td>29</td>
</tr>
<tr>
<td>Management System Overview</td>
<td>29</td>
</tr>
<tr>
<td>Multiple PDN Support</td>
<td>31</td>
</tr>
<tr>
<td>Node Functionality GTP Echo</td>
<td>31</td>
</tr>
<tr>
<td>Online/Offline Charging</td>
<td>31</td>
</tr>
<tr>
<td>Online: Gy Reference Interface</td>
<td>32</td>
</tr>
<tr>
<td>Offline: Gz Reference Interface</td>
<td>32</td>
</tr>
<tr>
<td>Offline: Rt Reference Interface</td>
<td>32</td>
</tr>
<tr>
<td>Operator Policy Support</td>
<td>32</td>
</tr>
<tr>
<td>Peer GTP Node Profile Configuration Support</td>
<td>33</td>
</tr>
<tr>
<td>P-GW Restart Notification Support</td>
<td>33</td>
</tr>
<tr>
<td>QoS Bearer Management</td>
<td>34</td>
</tr>
<tr>
<td>Rf Diameter Accounting</td>
<td>34</td>
</tr>
<tr>
<td>Subscriber Level Trace</td>
<td>35</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>IMEI-Profile (SGSN only)</td>
<td>89</td>
</tr>
<tr>
<td>APN Remap Table</td>
<td>89</td>
</tr>
<tr>
<td>Operator Policies</td>
<td>90</td>
</tr>
<tr>
<td>IMSI Ranges</td>
<td>90</td>
</tr>
<tr>
<td>How It Works</td>
<td>92</td>
</tr>
<tr>
<td>Operator Policy Configuration</td>
<td>93</td>
</tr>
<tr>
<td>Call Control Profile Config.</td>
<td>94</td>
</tr>
<tr>
<td>Configuring the Call Control Profile for an SGSN</td>
<td>94</td>
</tr>
<tr>
<td>Configuring the Call Control Profile for an MME or S-GW</td>
<td>94</td>
</tr>
<tr>
<td>APN Profile Configuration</td>
<td>95</td>
</tr>
<tr>
<td>IMEI Profile Configuration - SGSN only</td>
<td>95</td>
</tr>
<tr>
<td>APN Remap Table Configuration</td>
<td>96</td>
</tr>
<tr>
<td>Operator Policy Configuration</td>
<td>96</td>
</tr>
<tr>
<td>IMSI Range Configuration</td>
<td>97</td>
</tr>
<tr>
<td>Configuring IMSI Ranges on the MME or S-GW</td>
<td>97</td>
</tr>
<tr>
<td>Configuring IMSI Ranges on the SGSN</td>
<td>97</td>
</tr>
<tr>
<td>Associating Operator Policy Components on the MME</td>
<td>98</td>
</tr>
<tr>
<td>Configuring Accounting Mode for S-GW</td>
<td>99</td>
</tr>
<tr>
<td>Verifying the Feature Configuration</td>
<td>100</td>
</tr>
<tr>
<td>Monitoring the Service</td>
<td>101</td>
</tr>
<tr>
<td>Monitoring System Status and Performance</td>
<td>102</td>
</tr>
<tr>
<td>Clearing Statistics and Counters</td>
<td>104</td>
</tr>
<tr>
<td>Configuring Subscriber Session Tracing</td>
<td>105</td>
</tr>
<tr>
<td>Introduction</td>
<td>106</td>
</tr>
<tr>
<td>Supported Functions</td>
<td>107</td>
</tr>
<tr>
<td>Supported Standards</td>
<td>109</td>
</tr>
<tr>
<td>Subscriber Session Trace Functional Description</td>
<td>110</td>
</tr>
<tr>
<td>Operation</td>
<td>110</td>
</tr>
<tr>
<td>Trace Session</td>
<td>110</td>
</tr>
<tr>
<td>Trace Recording Session</td>
<td>110</td>
</tr>
<tr>
<td>Network Element (NE)</td>
<td>110</td>
</tr>
<tr>
<td>Activation</td>
<td>110</td>
</tr>
<tr>
<td>Management Activation</td>
<td>111</td>
</tr>
<tr>
<td>Signaling Activation</td>
<td>111</td>
</tr>
<tr>
<td>Start Trigger</td>
<td>111</td>
</tr>
<tr>
<td>Deactivation</td>
<td>111</td>
</tr>
<tr>
<td>Stop Trigger</td>
<td>111</td>
</tr>
<tr>
<td>Data Collection and Reporting</td>
<td>111</td>
</tr>
<tr>
<td>Trace Depth</td>
<td>111</td>
</tr>
<tr>
<td>Trace Scope</td>
<td>112</td>
</tr>
<tr>
<td>Network Element Details</td>
<td>112</td>
</tr>
<tr>
<td>MME</td>
<td>112</td>
</tr>
<tr>
<td>S-GW</td>
<td>112</td>
</tr>
<tr>
<td>P-GW</td>
<td>113</td>
</tr>
<tr>
<td>Subscriber Session Trace Configuration</td>
<td>114</td>
</tr>
<tr>
<td>Enabling Subscriber Session Trace on EPC Network Element</td>
<td>114</td>
</tr>
<tr>
<td>Trace File Collection Config.</td>
<td>115</td>
</tr>
<tr>
<td>Verifying Your Configuration</td>
<td>116</td>
</tr>
<tr>
<td>Intelligent RAT Paging for ISR on the S-GW</td>
<td>119</td>
</tr>
<tr>
<td>Feature Description</td>
<td>120</td>
</tr>
<tr>
<td>Relationships to Other Features (optional)</td>
<td>120</td>
</tr>
<tr>
<td>How it Works</td>
<td>121</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>Direct Tunnel ............................................. 127</td>
<td></td>
</tr>
<tr>
<td>S-GW Event Reporting ........................................ 139</td>
<td></td>
</tr>
<tr>
<td>Rf Interface Support ......................................... 147</td>
<td></td>
</tr>
</tbody>
</table>

**Direct Tunnel**
- Direct Tunnel Feature Overview .................................. 128
- Direct Tunnel Configuration ........................................ 132
  - Configuring Direct Tunnel Support on the SGSN ............. 132
  - Enabling Setup of GTP-U Direct Tunnels ..................... 133
  - Enabling Direct Tunnel per APN ................................ 133
  - Enabling Direct Tunnel per IMEI ................................ 134
  - Enabling Direct Tunnel to Specific RNCs ..................... 134
  - Verifying the SGSN Direct Tunnel Configuration .......... 135
- Configuring S12 Direct Tunnel Support on the S-GW ........ 137

**S-GW Event Reporting**
- Event Record Triggers ........................................... 140
- Event Record Elements ........................................... 141
- Active-to-Idle Transitions ...................................... 143
- 3GPP 29.274 Cause Codes ........................................ 144

**Rf Interface Support**
- Introduction ....................................................... 148
  - Offline Charging Architecture ................................ 148
  - Charging Collection Function .................................. 150
  - Charging Trigger Function ...................................... 150
  - Dynamic Routing Agent .......................................... 150
- License Requirements .............................................. 150
- Supported Standards ............................................... 150
- Features and Terminology ........................................ 152
  - Offline Charging Scenarios .................................... 152
    - Basic Principles ............................................... 152
    - Event Based Charging ........................................ 153
    - Session Based Charging ..................................... 153
  - Diameter Base Protocol ......................................... 154
  - Timer Expiry Behavior ......................................... 155
  - Rf Interface Failures/Error Conditions ...................... 155
    - DRA/CCF Connection Failure ................................ 155
    - No Reply from CCF ........................................... 155
    - Detection of Message Duplication .......................... 155
    - CCF Detected Failure .......................................... 155
    - Rf-Gy Synchronization Enhancements ....................... 156
- How it Works ...................................................... 157
- Configuring Rf Interface Support ............................... 159
  - Enabling Rf Interface in Active Charging Service .......... 159
  - Configuring GGSN / P-GW Rf Interface Support ............. 160
  - Configuring HSGW Rf Interface Support ....................... 167
  - Configuring P-CSCF/S-CSCF Rf Interface Support .......... 177
  - Enabling Charging for SIP Methods .......................... 178
  - Configuring S-GW Rf Interface Support ....................... 179
  - Gathering Statistics ........................................... 190
S-GW Engineering Rules .................................................................195
  Interface and Port Rules .............................................................. 196
  Assumptions .................................................................................. 196
  S1-U/S11 Interface Rules ............................................................... 196
  S5/S8 Interface Rules .................................................................... 196
  MAG to LMA Rules ........................................................................ 197
  S-GW Service Rules ...................................................................... 198
  S-GW Subscriber Rules ................................................................. 199
About this Guide

This preface describes the Cisco ASR 5x00 Serving Gateway Administration Guide, how it is organized, and its document conventions.

This preface includes the following sections:

- Conventions Used
- Supported Documents and Resources
- Contacting Customer Support
## Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Info" /></td>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

### Typeface Conventions

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

Related Common Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following common documents are available:

- Hardware Installation Guide (hardware dependent)
- System Administration Guide (hardware dependent)
- Cisco ASR 5x00 Command Line Interface Reference
- 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 SNMP MIB Reference
- Cisco ASR 5x00 Statistics and Counters Reference
- Cisco ASR 5x00 Thresholding Configuration Guide
- Cisco MURAL Software Installation Guide
- Cisco MURAL User Guide
- Web Element Manager Installation and Administration Guide

Related Product Documentation

The following product documents are also available and work in conjunction with the S-GW:

- Cisco ASR 5x00 HRPD Serving Gateway Administration Guide
- Cisco ASR 5x00 Mobility Management Entity Administration Guide
- Cisco ASR 5x00 Packet Data Network Gateway Administration Guide
- Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide
- Cisco ASR 5000 Session Control Manager Administration Guide

Obtaining Documentation

The most current Cisco documentation is available on the following website:
http://www.cisco.com/cisco/web/psa/default.html

Use the following path selections to access the S-GW documentation:
Products > Wireless > Mobile Internet> Network Functions > Cisco SGW Serving Gateway
Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
Serving Gateway Overview

The Cisco® ASR 5x00 core platform provides wireless carriers with a flexible solution that functions as a Serving Gateway (S-GW) in Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks. This overview provides general information about the S-GW including:

- Product Description
- Network Deployment(s)
- Features and Functionality - Base Software
- Features and Functionality - External Application Support
- Features and Functionality - Optional Enhanced Feature Software
- How the Serving Gateway Works
- Supported Standards
Product Description

The Serving Gateway routes and forwards data packets from the UE and acts as the mobility anchor during inter-eNodeB handovers. Signals controlling the data traffic are received on the S-GW from the MME which determines the S-GW that will best serve the UE for the session. Every UE accessing the EPC is associated with a single S-GW.

Figure 1. S-GW in the Basic E-UTRAN/EPC Network

The S-GW is also involved in mobility by forwarding down link data during a handover from the E-UTRAN to the eHRPD network. An interface from the eAN/ePCF to an MME provides signaling that creates a GRE tunnel between the S-GW and the eHRPD Serving Gateway.
The functions of the S-GW include:

- packet routing and forwarding.
- providing the local mobility anchor (LMA) point for inter-eNodeB handover and assisting the eNodeB reordering function by sending one or more “end marker” packets to the source eNodeB immediately after switching the path.
- mobility anchoring for inter-3GPP mobility (terminating the S4 interface from an SGSN and relaying the traffic between 2G/3G system and a PDN gateway.
- packet buffering for ECM-IDLE mode downlink and initiation of network triggered service request procedure.
- replicating user traffic in the event that Lawful Interception (LI) is required.
- transport level packet marking.
- user accounting and QoS class indicator (QCI) granularity for charging.
- uplink and downlink charging per UE, PDN, and QCI.
- reporting of user location information (ULI).
- support of circuit switched fallback (CSFB) for re-using deployed CS domain access for voice and other CS domain services.
Platform Requirements

The S-GW service runs on a Cisco® ASR 5x00 Series chassis running StarOS. 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.

Licenses

The S-GW 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.
Network Deployment(s)

This section describes the supported interfaces and the deployment scenarios of a Serving Gateway.

Serving Gateway in the E-UTRAN/EPC Network

The following figure displays the specific network interfaces supported by the S-GW. Refer to Supported Logical Network Interfaces (Reference Points) for detailed information about each interface.

Figure 3. Supported S-GW Interfaces in the E-UTRAN/EPC Network

The following figure displays a sample network deployment of an S-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.
**Supported Logical Network Interfaces (Reference Points)**

The S-GW provides the following logical network interfaces in support of the E-UTRAN/EPC network:

**S1-U Interface**

This reference point provides bearer channel tunneling between the eNodeB and the S-GW. It also supports eNodeB path switching during handovers. The S-GW provides the local mobility anchor point for inter-eNodeB handovers. It provides inter-eNodeB path switching during handovers when the X2 handover interface between base stations cannot be used. The S1-U interface uses GPRS tunneling protocol for user plane (GTP-U v1). GTP encapsulates all end user IP packets and it relies on UDP/IP transport. The S1-U interface also supports IPSec IKEv2. This interface is defined in 3GPP TS 23.401.

**Supported protocols:**

- Transport Layer: UDP, TCP
S4 Interface

This reference point provides tunneling and management between the S-GW and a 3GPP S4 SGSN. The interface facilitates soft hand-offs with the EPC network by providing control and mobility support between the inter-3GPP anchor function of the S-GW. This interface is defined in 3GPP TS 23.401.

Supported protocols:
- Transport Layer: UDP
- Tunneling:
  - GTP: IPv4 or IPv6 GTP-C (GTPv2 control/signaling channel) and GTP-U (GTPv1 user/bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-
roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

**Supported protocols:**

- Transport Layer: UDP, TCP
- Tunneling: GTP: GTPv2-C (signaling channel), GTPv1-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**S11 Interface**

This reference point provides GTP-C control signal tunneling between the MME and the S-GW. One GTP-C tunnel is created for each mobile terminal between the MME and S-GW. This interface is defined in 3GPP TS 23.401.

**Supported protocols:**

- Transport Layer: UDP
- Tunneling: IPv4 or IPv6 GTPv2-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**S12 Interface**
This reference point provides GTP-U bearer/user direct tunneling between the S-GW and a UTRAN Radio Network Controller (RNC), as defined in 3GPP TS 23.401. This interface provides support for inter-RAT handovers between the 3G RAN and EPC allowing a direct tunnel to be initiated between the RNC and S-GW, thus bypassing the S4 SGSN and reducing latency.

**Supported protocols:**
- Transport Layer: UDP
- Tunneling: IPv4 or IPv6 GTP-U (GTPv1 bearer/user channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

---

### Gxc Interface

This signaling interface supports the transfer of policy control and charging rules information (QoS) between the Bearer Binding and Event Reporting Function (BBERF) on the S-GW and a Policy and Charging Rules Function (PCRF) server.

**Supported protocols:**
- Transport Layer: TCP or SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

---

### Gz Interface
The Gz reference interface enables offline accounting functions on the S-GW. The S-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage. The Gz interface and offline accounting functions are used primarily in roaming scenarios where the foreign P-GW does not support offline charging.

**Supported protocols:**
- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

---

**Rf Interface**

The Diameter Rf interface (3GPP 32.240) is used for offline (post-paid) charging between the Charging Trigger Function (CTF, S-GW) and the Charging Data Function (CDF). It follows the Diameter base protocol state machine for accounting (RFC 3588) and includes support for IMS specific AVPs (3GPP TS 32.299)

**Supported protocols:**
- Transport Layer: TCP or SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet
Features and Functionality - Base Software

This section describes the features and functions supported by default in the base software for the S-GW service and do not require any additional licenses to implement the functionality.

**Important:** To configure the basic service and functionality on the system for the S-GW service, refer to the configuration examples provided in the *Serving Gateway Administration Guide*.

The following features are supported and brief descriptions are provided in this section:

- ANSI T1.276 Compliance
- APN-level Traffic Policing
- Bulk Statistics Support
- Circuit Switched Fall Back (CSFB) Support
- Closed Subscriber Group Support
- Congestion Control
- Downlink Delay Notification
- Dynamic GTP Echo Timer
- Event Reporting
- Idle-mode Signaling Reduction Support
- IP Access Control Lists
- IPv6 Capabilities
- LIPA Support
- Location Reporting
- Management System Overview
- Multiple PDN Support
- Node Functionality GTP Echo
- Online/Offline Charging
- Operator Policy Support
- Peer GTP Node Profile Configuration Support
- P-GW Restart Notification Support
- QoS Bearer Management
- Rf Diameter Accounting
- Subscriber Level Trace
- Threshold Crossing Alerts (TCA) Support
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 Platform 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.

APN-level Traffic Policing

The S-GW now supports traffic policing for roaming scenarios where the foreign P-GW does not enforce traffic classes. Traffic policing is used to enforce bandwidth limitations on subscriber data traffic. It caps packet bursts and data rates at configured burst size and data rate limits respectively for given class of traffic.

Traffic Policing is based on RFC2698 - A Two Rate Three Color Marker (trTCM) algorithm. The trTCM meters an IP packet stream and marks its packets green, yellow, or red. A packet is marked red if it exceeds the Peak Information Rate (PIR). Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the Committed Information Rate (CIR). The trTCM is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

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
- **MAG**: Provides MAG service statistics
- **S-GW**: Provides S-GW node-level service statistics
- **IP Pool**: Provides IP pool statistics
- **APN**: Provides Access Point Name statistics
The system supports the configuration of up to four 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 system 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, system host name, system 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.

The Cisco Web Element Manager 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 its PostgreSQL database. It can also generate XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, the Bulk Statistics server can archive files to an alternative directory on the server. The directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

**Important:** For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

**Circuit Switched Fall Back (CSFB) Support**

Circuit Switched Fall Back (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switchover to the circuit switched (CS) domain or other CS-domain services (for example, Location Services (LCS) or supplementary services). Additionally, SMS delivery via the CS core network is realized without CSFB. Since LTE EPC networks were not meant to directly anchor CS connections, when any CS voice services are initiated, any PS based data activities on the EUTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

CSFB provides an interim solution for enabling telephony and SMS services for LTE operators that do not plan to deploy IMS packet switched services at initial service launch.

The S-GW supports CSFB messaging over the S11 interface over GTP-C. Supported messages are:

- Suspend Notification
- Suspend Acknowledge
- Resume Notification
- Resume Acknowledgement

The S-GW forwards Suspend Notification messages towards the P-GW to suspend downlink data for non-GBR traffic; the P-GW then drops all downlink packets. Later, when the UE finishes with CS services and moves back to E-UTRAN, the MME sends a Resume Notification message to the S-GW which forwards the message to the P-GW. The downlink data traffic then resumes.

**Closed Subscriber Group Support**

The S-GW supports the following Closed Subscriber Group (CSG) Information Elements (IEs) and Call Detail Record:

- User CSG Information (UCI) IE in S5/S8
- CSG Information Reporting Action IE and functionality in S5/S8
• An SGW-CDR that includes a CSG record

Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact on the system’s ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

• **Congestion Condition Thresholds**: Thresholds dictate the conditions for which congestion control is enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operational thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated. A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  • **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.

  • **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

• **Service Congestion Policies**: Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

**Important**: For more information on congestion control, refer to the *Congestion Control* appendix in the *System Administration Guide*.

Downlink Delay Notification

This feature is divided between the following:

• Value Handling
• Throttling
• EPS Bearer ID and ARP Support

Value Handling

This feature provides for the handling of delay value information elements (IEs) at the S-GW. When a delay value is received at the S-GW from a particular MME, the S-GW delays sending data notification requests for all idle calls belonging to that particular MME. Once the timer expires, requests can be sent. The delay value at the S-GW is determined by the factor received in the delay value IE (as a part of either a Modify Bearer Request or a Data Downlink Notification Request) and a hard-coded base factor of 50 ms at the S-GW.
Throttling

This feature provides additional controls allowing the S-GW to set factors that “throttle” the continuous sending and receiving of DDN messages. A single command configures the throttling parameters supporting this feature.

A description of the `ddn throttle` command is located in the S-GW Service Configuration Mode Commands chapter in the Command Line Interface Reference.

EPS Bearer ID and ARP Support

This feature allows support for Priority Paging support in the network. This is mainly needed for MPS subscriber support. The paging priority in the paging message is set by MME based on ARP received in Downlink Data Notification message.

In order to support MPS requirement for Priority Paging in the network for MPS subscriber, DDN message has been enhanced to support passing ARP and EBI information. When the S-GW sends a Downlink Data Notification message, it shall include both EPS Bearer ID and ARP. If the Downlink Data Notification is triggered by the arrival of downlink data packets at the S-GW, the S-GW shall include the EPS Bearer ID and ARP associated with the bearer on which the downlink data packet was received. If the Downlink Data Notification is triggered by the arrival of control signaling, the S-GW shall include the EPS Bearer ID and ARP, if present in the control signaling. If the ARP is not present in the control signaling, the S-GW shall include the ARP in the stored EPS bearer context. If multiple EPS Bearers IDs are reported in the Downlink Data Notification message, the S-GW shall include all the EBI values and the ARP associated with the bearer with the highest priority (lowest ARP value). For more information, see TS 23.401 (section 5.3.4.3) and 29.274 (section 7.2.11). Details are discussed in CR-859 of 3GPP specifications.

Dynamic GTP Echo Timer

The Dynamic GTP Echo Timer enables the eGTP and GTP-U services to better manage GTP paths during network congestion. As opposed to the default echo timer which uses fixed intervals and retransmission timers, the dynamic echo timer adds a calculated round trip timer (RTT) that is generated once a full request/response procedure has completed. A multiplier can be added to the calculation for additional support during congestion periods.

For more information, refer to the Configuring the GTP Echo Timer section located in the Configuring Optional Features on the eGTP S-GW section of the Serving Gateway Configuration chapter.

Event Reporting

The S-GW can be configured to send a stream of user event data to an external server. As users attach, detach, and move throughout the network, they trigger signaling events, which are recorded and sent to an external server for processing. Reported data includes failure reasons, nodes selected, user information (IMSI, IMEI, MSISDN), APN, failure codes (if any) and other information on a per PDN-connection level. Event data is used to track the user status via near real time monitoring tools and for historical analysis of major network events.

The S-GW Event Reporting appendix at the end of this guide describes the trigger mechanisms and event record elements used for event reporting.

The SGW sends each event record in comma separated values (CSV) format. The record for each event is sent to the external server within 60 seconds of its occurrence. The `session-event-module` command in the Context Configuration mode allows an operator to set the method and destination for transferring event files, as well as the format and handling characteristics of event files. For a detailed description of this command, refer to the Command Line Interface Reference.
Idle-mode Signaling Reduction Support

The S-GW now supports Idle-mode Signaling Reduction (ISR) allowing for a control connection to exist between an S-GW and an MME and S4-SGSN. The S-GW stores mobility management parameters from both nodes while the UE stores session management contexts for both the EUTRAN and GERAN/UTRAN. This allows a UE, in idle mode, to move between the two network types without needing to perform racking area update procedures, thus reducing the signaling previously required. ISR support on the S-GW is embedded and no configuration is required however, an optional feature license is required to enable this feature.

ISR support on the S-GW is embedded and no configuration is required, however, an optional feature license must be purchased to enable this feature.

IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

**Important:** The S-GW supports interface-based ACLs only. For more information on IP access control lists, refer to the IP Access Control Lists appendix in the System Administration Guide.

IPv6 Capabilities

IPv6 enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The S-GW platform offers the following IPv6 capabilities:

**IPv6 Connections to Attached Elements**

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gxc policy signaling interface
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

**Routing and Miscellaneous Features**

- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (for example, ECS, P2P detection, Stateful Firewall, etc.)

**LIPA Support**

A LIPA (Local IP Access) PDN is a PDN Connection for local IP access for a UE connected to a HeNB. The LIPA architecture includes a Local Gateway (LGW) acting as an S-GW GTPv2 peer. The LGW is collocated with HeNB in the operator network behaves as a PGW from SGW perspective. Once the default bearer for the LIPA PDN is established, then data flows directly to the LGW and from there into the local network without traversing the core network of the network operator.

In order to support millions of LIPA GTPC peers, S-GW memory management has been enhanced with regards to GTPv2 procedures and as well as to support the maintenance of statistics per peer node. Establishment of LIPA PDN follows a normal call flow similar to that of a normal PDN as per 23.401; the specification does not distinguish between a LGW and a PGW call. As a result, the S-GW supports a new configuration option to detect a LIPA peer. As a fallback mechanism, heuristic detection of LIPA peer based on data flow characteristics of a LIPA call is also supported.

Whenever a peer is detected as a LIPA peer, the S-GW will disable GTPC echo mechanism towards that particular peer and stop maintaining some statistics for that peer.

A configuration option in APN profile explicitly indicates that all the PDN’s for that APN are LIPA PDN’s, so all GTPC peers on S5 for that APN are treated as LGW, and thus no any detection algorithm is applied to detect LGW.

**Location Reporting**

Location reporting can be used to support a variety of applications including emergency calls, lawful intercept, and charging. This feature reports both user location information (ULI).

ULI data reported in GTPv2 messages includes:
- **TAI-ID**: Tracking Area Identity
- **MCC: MNC**: Mobile Country Code, Mobile Network Code
- **TAC**: Tracking Area Code

The S-GW stores the ULI and also reports the information to the accounting framework. This may lead to generation of Gz and Rf Interim records. The S-GW also forwards the received ULI to the P-GW. If the S-GW receives the UE time zone IE from the MME, it forwards this IE towards the P-GW across the S5/S8 interface.

**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 and to maintain system performance.

Cisco's O+M module 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 the SPIO card via 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 (such as, Microsoft Internet Explorer v6.0 and above or 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 5. Element Management Methods**
Important: P-GW management functionality is enabled by default for console-based access. For GUI-based management support, refer to the Web Element Manager section in this chapter.

Important: For more information on command line interface based management, refer to the Command Line Interface Reference and P-GW Administration Guide.

### Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or offdeck content services.

The Mobile Access Gateway (MAG) function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 (PMIP) tunnel for all user sessions toward the Local Mobility Anchor (LMA) function of the P-GW.

When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMAs. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default and dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.

Important: Up to 11 multiple PDN connections are supported.

### Node Functionality GTP Echo

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new “node features” IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node’s supported features. S-GW’s supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

### Online/Offline Charging

The Cisco EPC platforms support offline charging interactions with external OCS and CGF/CDF servers. To provide subscriber level accounting, the Cisco EPC platform supports integrated Charging Transfer Function (CTF) and Charging Data Function (CDF) / Charging Gateway Function (CGF). Each gateway uses Charging-IDs to distinguish between default and dedicated bearers within subscriber sessions.
The ASR 5x00 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it also possible to enable file compression using protocols such as GZIP.

The offline charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighboring CGF within the configurable polling interval, it will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

**Online: Gy Reference Interface**

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct Online Charging System (OCS) servers. The Gy interface provides a standardized Diameter interface for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Gy interface provides an online charging interface that works with the ECS Deep Packet Inspection feature. With Gy, customer traffic can be gated and billed. Both time- and volume-based charging models are supported.

**Offline: Gz Reference Interface**

The Cisco P-GW and S-GW support 3GPP Release 8 compliant offline charging as defined in TS 32.251, TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally when Gn/Gp interworking with SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW supports integrated Charging Transfer Function (CTF) and Charging Data Function (CDF). Each gateway uses Charging-IDs to distinguish between default and dedicated bearers within subscriber sessions.

The Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP or SFTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to transfer charging records between the CDF and CGF serve via FTP or SFTP. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc.

**Offline: Rf Reference Interface**

Cisco EPC platforms also support the Rf reference interface to enable direct transfer of charging files from the CTF function of the S-GW to external CDF or CGF servers. This interface uses Diameter Accounting Requests (Start, Stop, Interim, and Event) to transfer charging records to the CDF/CGF. Each gateway relies on triggering conditions for reporting chargeable events to the CDF/CGF. Typically as EPS bearers are activated, modified or deleted, charging records are generated. The EPC platforms include information such as Subscription-ID (IMSI), Charging-ID (EPS bearer identifier) and separate volume counts for the uplink and downlink traffic.

**Operator Policy Support**

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.
An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

The operator policy configuration to be applied to a subscriber is selected on the basis of the selection criteria in the subscriber mapping at attach time. A maximum of 1,024 operator policies can be configured. If a UE was associated with a specific operator policy and that policy is deleted, the next time the UE attempts to access the policy, it will attempt to find another policy with which to be associated.

A default operator policy can be configured and applied to all subscribers that do not match any of the per-PLMN or IMSI range policies.

The S-GW uses operator policy to set the Accounting Mode - GTP (default), RADIUS/Diameter or none. However, the accounting mode configured for the call-control profile will override this setting.

Changes to the operator policy take effect when the subscriber re-attaches and subsequent EPS Bearer activations.

**Peer GTP Node Profile Configuration Support**

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer.

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of S-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with S-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

**P-GW Restart Notification Support**

This procedure optimizes the amount of signaling involved on S11/S4 interface when P-GW failure is detected.

P-GW Restart Notification Procedure is a standards-based procedure supported on S-GW to notify detection of P-GW failure to MME/S4-SGSN. P-GW failure detection will be done at S-GW when it detects that the P-GW has restarted (based on restart counter received from the restarted P-GW) or when it detects that P-GW has failed but not restarted (based on path failure detection). When an S-GW detects that a peer P-GW has restarted, it shall locally delete all PDN connection table data and bearer contexts associated with the failed P-GW and notify the MME via P-GW Restart Notification. S-GW will indicate in the echo request/response on S11/S4 interface that the P-GW Restart Notification procedure is supported.

P-GW Restart Notification Procedure is an optional procedure and is invoked only if both the peers, MME/S4-SGSN and S-GW, support it. This procedure optimizes the amount of signaling involved on S11/S4 interface when P-GW failure is detected. In the absence of this procedure, S-GW will initiate the Delete procedure to clean up all the PDNs anchored at that failed P-GW, which can lead to flooding of GTP messages on S11/S4 if there are multiple PDNs using that S-GW and P-GW.
QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFTs) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco P-GW offers all of the following bearer-level aggregate constructs:

**QoS Class Identifier (QCI):** An operator provisioned value that controls bearer level packet forwarding treatments (for example, scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). Cisco EPC gateways also support the ability to map the QCI values to DiffServ codepoints in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.

**Important:** The S-GW does not support non-standard QCI values. QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203; the S-GW supports these standard values.

**Guaranteed Bit Rate (GBR):** A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

**Maximum Bit Rate (MBR):** The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given dedicated EPS bearer.

**Aggregate Maximum Bit Rate (AMBR):** AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

**Policing and Shaping:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDF’s) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority. When traffic shaping is enabled the P-GW enqueues the non-conforming session to the provisioned memory limit for the user session. When the allocated memory is exhausted, the inbound/outbound traffic for the user can be transmitted or policed in accordance with operator provisioned policy.

Rf Diameter Accounting

Provides the framework for offline charging in a packet switched domain. The gateway support nodes use the Rf interface to convey session related, bearer related or service specific charging records to the CGF and billing domain for enabling charging plans.
The Rf reference interface enables offline accounting functions on the HSGW in accordance with 3GPP Release 8 specifications. In an LTE application the same reference interface is also supported on the S-GW and P-GW platforms. The Cisco gateways use the Charging Trigger Function (CTF) to transfer offline accounting records via a Diameter interface to an adjacent Charging Data Function (CDF) / Charging Gateway Function (CGF). The HSGW and Serving Gateway collect charging information for each mobile subscriber UE pertaining to the radio network usage while the P-GW collects charging information for each mobile subscriber related to the external data network usage.

The S-GW collects information per-user, per IP CAN bearer or per service. Bearer charging is used to collect charging information related to data volumes sent to and received from the UE and categorized by QoS traffic class. Users can be identified by MSISDN or IMSI.

Flow Data Records (FDRs) are used to correlate application charging data with EPC bearer usage information. The FDRs contain application level charging information like service identifiers, rating groups, IMS charging identifiers that can be used to identify the application. The FDRs also contain the authorized QoS information (QCI) that was assigned to a given flow. This information is used to correlate charging records with EPC bearers.

**Subscriber Level Trace**

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the S-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S1-U, S11, S5/S8, and Gxc. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal

Note: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5x00 platform. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over an FTP or secure FTP (SFTP) connection. In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Once a subscriber level trace request is activated it can be propagated via the S5/S8 signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S11 : Create Session Request
- S11 : Trace Session Activation
- S11 : Modify Bearer Request

As subscriber level trace is a CPU intensive activity the maximum number of concurrently monitored trace sessions per Cisco P-GW or S-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.
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, IP pool addresses, 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. The alert is generated and/or sent at the end of the 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. The alert is generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and 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. As with other system facilities, logs are 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 to the *Thresholding Configuration Guide*. 
Features and Functionality - External Application Support

This section describes the features and functions of external applications supported on the S-GW. These services require additional licenses to implement the functionality.

- Web Element Management System
- InTracer

Web Element Manager

The Web Element Manager (WEM) provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management of the ASR 5x00 platform.

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

Figure 6. Web Element Manager Network Interfaces

---

Important: For more information on WEM support, refer to the WEM Installation and Administration Guide.
InTracer

Cisco InTracer is a high-performance troubleshooting and monitoring solution for subscribers. It performs call tracing, control data acquisition, processing and analysis of both active and historical subscriber sessions.

Cisco InTracer provides a framework for operators to analyze and investigate call flows and call events for subscriber sessions in real time.

Cisco InTracer consists of two modules:

- The InTracer Client module:
  Enables and configures on the Cisco gateway (to start sending subscriber traces (control plane information for sessions) to InTracer Server module

- The InTracer Server module:
  The InTracer Server module runs on an external box sitting close to the gateway to process and store subscriber traces

**Important:** External applications are now supported by the Cisco MITG RHEL v5.9 OS on selected Cisco UCS servers. The Cisco MITG RHEL v5.9 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications, for example, in this case Cisco InTracer. Users must not install any other applications on servers running the Cisco MITG RHEL v5.9 OS. For detailed software compatibility information, refer to the “Cisco MITG RHEL v5.9 OS Application Note.”
Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the S-GW service. Each of the following features require the purchase of an additional license to implement the functionality with the S-GW service.

This section describes following features:

- Always-On Licensing
- Direct Tunnel
- Intelligent Paging for ISR
- Inter-Chassis Session Recovery
- IP Security (IPSec) Encryption
- Lawful Intercept
- Layer 2 Traffic Management (VLANs)
- Overcharging Protection Support
- Session Recovery Support

Always-On Licensing

Use of Always-On Licensing requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Traditionally, transactional models have been based on registered subscriber sessions. In an “always-on” deployment model, however, the bulk of user traffic is registered all of the time. Most of these registered subscriber sessions are idle a majority of the time. Therefore, Always-On Licensing charges only for connected-active subscriber sessions.

A connected-active subscriber session would be in “ECM Connected state,” as specified in 3GPP TS 23.401, with a data packet sent/received within the last one minute (on average). This transactional model allows providers to better manage and achieve more predictable spending on their capacity as a function of the Total Cost of Ownership (TCO).

Direct Tunnel

In accordance with standards, one tunnel functionality enables the SGSN to establish a direct tunnel at the user plane level - a GTP-U tunnel, directly between the RAN and the S-GW.
In effect, a direct tunnel reduces data plane latency as the tunnel functionality acts to remove the SGSN from the data plane and limit the SGSN to the control plane for processing. This improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services). Additionally, direct tunnel functionality implements the standard SGSN optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

Typically, the SGSN establishes a direct tunnel at PDP context activation using an Update PDP Context Request towards the S-GW. This means a significant increase in control plane load on both the SGSN and S-GW components of the packet core. Hence, deployment requires highly scalable S-GWs since the volume and frequency of Update PDP Context messages to the S-GW will increase substantially. The ASR 5x00 platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

For more information on Direct Tunnel configuration, refer to the Direct Tunnel Configuration appendix in this guide.

**Intelligent Paging for ISR**

In case of Idle-mode Signaling Reduction (ISR) active and UE is idle, the S-GW will send Downlink Data Notification (DDN) Message to both the MME and the S4-SGSN if it receives the downlink data or network initiated control message for this UE. In turn, the MME and the S4-SGSN would do paging in parallel consuming radio resources.

To optimize the radio resource, the S-GW will now perform intelligent paging. When configured at S-GW service level for each APN, the S-GW will page in a semi-sequential fashion (one by one to peer MME or S4-SGSN based on last known RAT type) or parallel to both the MME and S4-SGSN.
Inter-Chassis Session Recovery

The ASR 5x00 platform provides industry-leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 PSC hardware redundancy, if a catastrophic PSC failure occurs all affected calls are migrated to the standby PSC if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint.
- If the Session Recovery feature is enabled, any total PSC failure will cause a PSC switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the MME Inter-Chassis Session Recovery (ICSR) feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

ICSR allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a proprietary TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

Interchassis Communication

Chassis configured to support ICSR communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis’ peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a proprietary TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

Checkpoint Messages

Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.

**Important:** For more information on inter-chassis session recovery support, refer to the Interchassis Session Recovery appendix in System Administration Guide.
IP Security (IPSec) Encryption

Enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

The Cisco S-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.

**Important:** You must purchase an IPSec license to enable IPSec. For more information on IPSec support, refer to the Cisco StarOS IP Security (IPSec) Reference.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the S-GW. Lawful Intercept is a licensed-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

Layer 2 Traffic Management (VLANs)

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as tags on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.

**Important:** For more information on VLAN support, refer to the VLANs appendix in the System Administration Guide.

Overcharging Protection Support

Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.

P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer
overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn’t desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.

Once the criterion to signal “stop charging” is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. MBReq will have a new private extension IE to send “stop charging” and “start charging” indication to P-GW.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume sending downlink packets after receiving “stop charging” request when either of these conditions is met:

- When the S-GW (which had earlier sent “stop charging” in MBReq) sends “start charging” in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).

Session Recovery Support

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.

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. StarOS has the ability to support stateful intra-chassis session recovery (ICSR) for S-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active packet services card during the upgrade process.

**Important:** For more information on session recovery support, refer to the Session Recovery appendix in the System Administration Guide.
How the Serving Gateway Works

This section provides information on the function of the S-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The S-GW supports the following network flows:

- GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network

GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network

The following topics and procedure flows are included:

- Subscriber-initiated Attach (initial)
- Subscriber-initiated Detach

Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.
Table 1. Subscriber-initiated Attach (initial) Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.</td>
</tr>
<tr>
<td>2</td>
<td>The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an MME selection function. The eNodeB forwards the Attach Request message to the new MME contained in a SI-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.</td>
</tr>
</tbody>
</table>
## How the Serving Gateway Works

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.</td>
</tr>
<tr>
<td>4</td>
<td>The UE responds with Identity Response (IMSI).</td>
</tr>
<tr>
<td>5</td>
<td>If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.</td>
</tr>
<tr>
<td>6</td>
<td>The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.</td>
</tr>
<tr>
<td>7</td>
<td>The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the EPS subscribed QoS profile for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.</td>
</tr>
<tr>
<td>8</td>
<td>The MME selects an S-GW using the Serving GW selection function and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause PDN GW selection function. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.</td>
</tr>
<tr>
<td>9</td>
<td>The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.</td>
</tr>
<tr>
<td>10</td>
<td>If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.</td>
</tr>
<tr>
<td>11</td>
<td>The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.</td>
</tr>
<tr>
<td>12</td>
<td>The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.</td>
</tr>
<tr>
<td>13</td>
<td>The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.</td>
</tr>
<tr>
<td>14</td>
<td>The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.</td>
</tr>
<tr>
<td>15</td>
<td>The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.</td>
</tr>
<tr>
<td>16</td>
<td>The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.</td>
</tr>
<tr>
<td>17</td>
<td>The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>18</td>
<td>The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW.</td>
</tr>
<tr>
<td>19</td>
<td>The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.</td>
</tr>
<tr>
<td>20</td>
<td>The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.</td>
</tr>
<tr>
<td>21</td>
<td>The S-GW sends its buffered downlink packets.</td>
</tr>
<tr>
<td>22</td>
<td>After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.</td>
</tr>
<tr>
<td>23</td>
<td>The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.</td>
</tr>
<tr>
<td>24</td>
<td>Bidirectional data is passed between the UE and PDN.</td>
</tr>
</tbody>
</table>

**Subscriber-initiated Detach**

This section describes the procedure of detachment from the EPC network by a subscriber.

**Figure 9. Subscriber-initiated Detach Call Flow**

![Subscriber-initiated Detach Call Flow Diagram]

**Table 2. Subscriber-initiated Detach Call Flow Description**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.</td>
</tr>
<tr>
<td>2</td>
<td>The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.</td>
</tr>
<tr>
<td>3</td>
<td>The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.</td>
</tr>
</tbody>
</table>
## How the Serving Gateway Works

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The P-GW acknowledges with a Delete Bearer Response (TEID) message.</td>
</tr>
<tr>
<td>5</td>
<td>The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.</td>
</tr>
<tr>
<td>6</td>
<td>The S-GW acknowledges with a Delete Bearer Response (TEID) message.</td>
</tr>
<tr>
<td>7</td>
<td>If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.</td>
</tr>
<tr>
<td>8</td>
<td>The MME releases the S1-MME signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.</td>
</tr>
</tbody>
</table>
Supported Standards

The S-GW service complies with the following standards.

- 3GPP References
- 3GPP2 References
- IETF References
- Object Management Group (OMG) Standards

3GPP References

Release 10 Supported Standards

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

Release 9 Supported Standards

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2 (Release 9)
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 9)
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 33.106: 3G Security; Lawful Interception Requirements
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

Release 8 Supported Standards

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture Enhancements for non-3GPP accesses
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 29.210. Gx application
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.214: Policy and Charging Control over Rx reference point
- 3GPP TS 29.274 V8.1.1 (2009-03): 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 8)
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.2.0 (both versions are intentional)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols, version 8.1.0
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 33.106: 3G Security; Lawful Interception Requirements
- 3GPP TS 36.107: 3G security; Lawful interception architecture and functions
- 3GPP TS 36.300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description
- 3GPP TS 36.412. EUTRAN S1 signaling transport
- 3GPP TS 36.413: Evolved Universal Terrestrial Radio Access (E-UTRA); S1 Application Protocol (S1AP)
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

**3GPP2 References**

- XP0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

**IETF References**

Supported Standards

- RFC 791: Internet Protocol (STD 5)
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3588: Diameter Base Protocol
- RFC 3775: Mobility Support in IPv6
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5213: Proxy Mobile IPv6
- Internet-Draft: Proxy Mobile IPv6
- Internet-Draft: GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft: Binding Revocation for IPv6 Mobility, work in progress

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group
Chapter 2
Serving Gateway Configuration

This chapter provides configuration information for the Serving Gateway (S-GW).

![Important:](image) Information about all commands in this chapter can be found in the Command Line Interface Reference.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the S-GW product are located in the Command Line Interface Reference.

The following procedures are located in this chapter:

- Configuring the System as a Standalone eGTP S-GW
- Configuring Optional Features on the eGTP S-GW
Configuring the System as a Standalone eGTP S-GW

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

- Information Required
- How This Configuration Works
- eGTP S-GW Configuration

Information Required

The following sections describe the minimum amount of information required to configure and make the S-GW operational on the network. To make the process more efficient, you should have this information available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the S-GW 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 eGTP S-GW.

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Interface Configuration</td>
<td>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Interface name</td>
<td>IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>The physical port to which the interface will 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.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the management interface(s) to a specific network.</td>
</tr>
<tr>
<td>Security administrator name</td>
<td>The name or names of the security administrator with full rights to the system.</td>
</tr>
<tr>
<td>Security administrator password</td>
<td>Open or encrypted passwords can be used.</td>
</tr>
</tbody>
</table>
## Required S-GW Ingress Context Configuration Information

The following table lists the information that is required to configure the S-GW ingress context on an eGTP S-GW.

**Table 4. Required Information for S-GW Ingress Context Configuration**

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-GW ingress context name</td>
<td>An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW ingress context is recognized by the system.</td>
</tr>
<tr>
<td>Accounting policy name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy is recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.</td>
</tr>
</tbody>
</table>

### S1-U/S11 Interface Configuration (To/from eNodeB/MME)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>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 will be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>The physical port to which the interface will 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.</td>
</tr>
</tbody>
</table>

| Gateway IP address           | Used when configuring static IP routes from the interface(s) to a specific network.                                                                                                                   |
| Gateway IP address           | Used when configuring static IP routes from the interface(s) to a specific network.                                                                                                                   |

### GTP-U Service Configuration

<table>
<thead>
<tr>
<th>GTP-U service name (for S1-U/S11 interface)</th>
<th>An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service bound to the S1-U/S11 interface will be recognized by the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>S1-U/S11 interface IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>

### S-GW Service Configuration

| S-GW service name | An identification string from 1 to 63 characters (alpha and/or numeric) by which the S-GW service is recognized by the system. Multiple names are needed if multiple S-GW services will be used. |

### eGTP Ingress Service Configuration
Configuring the System as a Standalone eGTP S-GW

Required Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGTP S1-U/S11 ingress service name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP S1-U/S11 ingress service is recognized by the system.</td>
</tr>
</tbody>
</table>

Required S-GW Egress Context Configuration Information

The following table lists the information that is required to configure the S-GW egress context on an eGTP S-GW.

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-GW egress context name</td>
<td>An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW egress context is recognized by the system.</td>
</tr>
</tbody>
</table>

S5/S8 Interface Configuration (To/from P-GW)

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>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 will be configured.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>The physical port to which the interface will 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.</td>
</tr>
</tbody>
</table>

Gateway IP address

Used when configuring static IP routes from the interface(s) to a specific network.

GTP-U Service Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTP-U service name (for S5/S8 interface)</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service bound to the S5/S8 interface will be recognized by the system.</td>
</tr>
<tr>
<td>IP address</td>
<td>S5/S8 interface IPv4 or IPv6 address.</td>
</tr>
</tbody>
</table>

eGTP Egress Service Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGTP Egress Service Name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP egress service is recognized by the system.</td>
</tr>
</tbody>
</table>

How This Configuration Works

The following figure and supporting text describe how this configuration with a single ingress and egress context is used by the system to process a subscriber call.
1. A subscriber session from the MME is received by the S-GW service over the S11 interface.
2. The S-GW service determines which context to use to access PDN services for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.
3. S-GW uses the configured egress context to determine the eGTP service to use for the outgoing S5/S8 connection.
4. The S-GW establishes the S5/S8 connection by sending a create session request message to the P-GW.
5. The P-GW responds with a Create Session Response message that includes the PGW S5/S8 Address for control plane and bearer information.
6. The S-GW conveys the control plane and bearer information to the MME in a Create Session Response message.
7. The MME responds with a Create Bearer Response and Modify Bearer Request message.
8. The S-GW sends a Modify Bearer Response message to the MME.

**eGTP S-GW Configuration**

To configure the system to perform as a standalone eGTP S-GW, review the following graphic and subsequent steps.
Step 1  Set system configuration parameters such as activating PSCs by applying the example configurations found in the System Administration Guide.

Step 2  Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the Initial Configuration section of this chapter.

Step 3  Configure the system to perform as an eGTP S-GW and set basic S-GW parameters such as eGTP interfaces and an IP route by applying the example configurations presented in the eGTP Configuration section.

Step 4  Verify and save the configuration by following the instruction in the Verifying and Saving the Configuration section.

Initial Configuration

Step 1  Set local system management parameters by applying the example configuration in the Modifying the Local Context section.

Step 2  Create an ingress context where the S-GW and eGTP ingress service will reside by applying the example configuration in the Creating an S-GW Ingress Context section.

Step 3  Create an eGTP ingress service within the newly created ingress context by applying the example configuration in the Creating an eGTP Ingress Service section.

Step 4  Create an S-GW egress context where the eGTP egress services will reside by applying the example configuration in the Creating an S-GW Egress Context section.
Step 5  Create an eGTP egress service within the newly created egress context by applying the example configuration in the Creating an eGTP Egress Service section.

Step 6  Create a S-GW service within the newly created ingress context by applying the example configuration in the Creating an S-GW Service section.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
context local
  interface <lcl_cntxt_intrfc_name>
    ip address <ip_address> <ip_mask>
  exit
  server ftpd
  exit
  server telnetd
  exit
  subscriber default
  exit
  administrator <name> encrypted password <password> ftp
  ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
  exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
end
```

Creating an S-GW Ingress Context

Use the following example to create an S-GW ingress context and Ethernet interfaces to an MME and eNodeB, and bind the interfaces to configured Ethernet ports.

```
configure
  context <ingress_context_name> -noconfirm
  subscriber default
```
exit
interface <slu-s11_interface_name>
  ip address <ipv4_address_primary>
  ip address <ipv4_address_secondary>
  exit
  ip route 0.0.0.0 0.0.0.0 <next_hop_address> <sgw_interface_name>
  exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <slu-s11_interface_name> <ingress_context_name>
end

Notes:
- This example presents the S1-U/S11 connections as a shared interface. These interfaces can be separated to support a different network architecture.
- The S1-U/S11 interface IP address(es) can also be specified as IPv6 addresses using the \texttt{ipv6 address} command.

Creating an eGTP Ingress Service

Use the following configuration example to create an eGTP ingress service:

```text
configure
  context <ingress_context_name>
    egtp-service <egtp_ingress_service_name> -noconfirm
end
```

Creating an S-GW Egress Context

Use the following example to create an S-GW egress context and Ethernet interface to a P-GW and bind the interface to configured Ethernet ports.

```text
configure
  context <egress_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <address>
      tunnel-mode ipv6ip
```
source interface <name>
  destination address <ipv4 or ipv6 address>
end

configure
  port ethernet <slot_number/port_number>
    no shutdown
  bind interface <s5s8_interface_name> <egress_context_name>
end

Notes:
- The S5/S8 interface IP address can also be specified as an IPv4 address using the `ip address` command.

Creating an eGTP Egress Service

Use the following configuration example to create an eGTP egress service in the S-GW egress context:

```
configure
  context <egress_context_name>
    egtp-service <egtp_egress_service_name> -noconfirm
end
```

Creating an S-GW Service

Use the following configuration example to create the S-GW service in the ingress context:

```
configure
  context <ingress_context_name>
    sgw-service <sgw_service_name> -noconfirm
end
```

**eGTP Configuration**

**Step 1**  Set the system’s role as an eGTP S-GW and configure eGTP service settings by applying the example configuration in the Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings section.

**Step 2**  Configure the S-GW service by applying the example configuration in the Configuring the S-GW Service section.

**Step 3**  Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring an IP Route section.

**Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings**
Use the following configuration example to set the system to perform as an eGTP S-GW and configure the GTP-U and eGTP services:

```
configure
  context <sgw_ingress_context_name>
    gtppp group default
    exit
  gtpu-service <gtpu_ingress_service_name>
    bind ipv4-address <s1-u_s11_interface_ip_address>
    exit
  egtp-service <egtp_ingress_service_name>
    interface-type interface-sgw-ingress
    validation-mode default
    associate gtpu-service <gtpu_ingress_service_name>
    gtpc bind address <s1u-s11_interface_ip_address>
    exit
  exit
  context <sgw_egress_context_name>
    gtpu-service <gtpu_egress_service_name>
    bind ipv4-address <s5s8_interface_ip_address>
    exit
  egtp-service <egtp_egress_service_name>
    interface-type interface-sgw-egress
    validation-mode default
    associate gtpu-service <gtpu_egress_service_name>
    gtpc bind address <s5s8_interface_ip_address>
  end
```

Notes:
- The **bind** command in the GTP-U ingress and egress service configuration can also be specified as an IPv6 address using the **ipv6-address** command.

**Configuring the S-GW Service**
Use the following example to configure the S-GW service:

```bash
configure

context <ingress_context_name>

sgw-service <sgw_service_name> -noconfirm
associate ingress egtp-service <egtp_ingress_service_name>
associate egress-proto gtp egress-context <egress_context_name>
qci-qos-mapping <map_name>

end
```

**Configuring an IP Route**

Use the following example to configure an IP Route for control and user plane data communication with an eGTP PDN Gateway:

```bash
configure

context <egress_context_name>

ip route <pgw_ip_addr/mask> <sgw_next_hop_addr> <sgw_intrfc_name>

end
```

**Verifying and Saving the Configuration**

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 Optional Features on the eGTP S-GW**

The configuration examples in this section are optional and provided to cover the most common uses of the eGTP S-GW in a live network. The intent of these examples is to provide a base configuration for testing.

The following optional configurations are provided in this section:

- Configuring the GTP Echo Timer
- Configuring GTPP Offline Accounting on the S-GW
- Configuring Diameter Offline Accounting on the S-GW
- Configuring APN-level Traffic Policing on the S-GW
- Configuring X.509 Certificate-based Peer Authentication
- Configuring Dynamic Node-to-Node IP Security on the S1-U and S5 Interfaces
- Configuring ACL-based Node-to-Node IP Security on the S1-U and S5 Interfaces
- Configuring S4 SGSN Handover Capability
Configuring the GTP Echo Timer

The GTP echo timer on the ASR5x00 S-GW can be configured to support two different types of path management: default and dynamic. This timer can be configured on the GTP-C and/or the GTP-U channels.

Default GTP Echo Timer Configuration

The following examples describe the configuration of the default eGTP-C and GTP-U interface echo timers:

eGTP-C

```plaintext
configure
  context <context_name>
    egtp-service <egtp_service_name>
    gtpc echo-interval <seconds>
    gtpc echo-retransmission-timeout <seconds>
    gtpc max-retransmissions <num>
end
```

Notes:

- This configuration can be used in either the ingress context supporting the S1 -U and/or S11 interfaces with the eNodeB and MME respectively; and the egress context supporting the S5/S8 interface with the P-GW.
- The following diagram describes a failure and recovery scenario using default settings of the three `gtpc` commands in the example above:
- The multiplier (x2) is system-coded and cannot be configured.

**GTP-U**

```bash
configure

context <context_name>

gtpu-service <gtpu_service_name>

  echo-interval <seconds>

  echo-retransmission-timeout <seconds>

  max-retransmissions <num>

end
```

**Notes:**
- This configuration can be used in either the ingress context supporting the S1-U interfaces with the eNodeB and the egress context supporting the S5/S8 interface with the P-GW.
The following diagram describes a failure and recovery scenario using default settings of the three GTP-U commands in the example above:

- The multiplier (x2) is system-coded and cannot be configured.

**Dynamic GTP Echo Timer Configuration**

The following examples describe the configuration of the dynamic eGTP-C and GTP-U interface echo timers:

**eGTP-C**

```
configure

context <context_name>

egtp-service <egtp_service_name>

gtpc echo-interval <seconds> dynamic smooth-factor <multiplier>

gtpc echo-retransmission-timeout <seconds>

gtpc max-retransmissions <num>
```
Notes:

- This configuration can be used in either the ingress context supporting the S1-U and/or S11 interfaces with the eNodeB and MME respectively; and the egress context supporting the S5/S8 interface with the P-GW.

- The following diagram describes a failure and recovery scenario using default settings of the three `gtpc` commands in the example above and an example round trip timer (RTT) of six seconds:

- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

**GTP-U**
context <context_name>

gtpu-service <gtpu_service_name>
  echo-interval <seconds> dynamic smooth-factor <multiplier>
  echo-retransmission-timeout <seconds>
  max-retransmissions <num>
end

Notes:

- This configuration can be used in either the ingress context supporting the S1-U interfaces with the eNodeB and the egress context supporting the S5/S8 interface with the P-GW.
- The following diagram describes a failure and recovery scenario using default settings of the three gtpc commands in the example above and an example round trip timer (RTT) of six seconds:
- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

**Configuring GTPP Offline Accounting on the S-GW**

By default the S-GW service supports GTPP accounting. To provide GTPP offline charging during, for example, scenarios where the foreign P-GW does not, configure the S-GW with the example parameters below:

```plaintext
configure
gtpp single-source
context <ingress_context_name>
subscriber default
```
accounting mode gtpp
exit
gtpp group default
gtpp charging-agent address <gz_ipv4_address>
gtpp echo-interval <seconds>
gtpp attribute diagnostics
gtpp attribute local-record-sequence-number
gtpp attribute node-id-suffix <string>
gtpp dictionary <name>
gtpp server <ipv4_address> priority <num>
gtpp server <ipv4_address> priority <num> node-alive enable
exit

policy accounting <gz_policy_name>
  accounting-level {type}
  operator-string <string>
  cc profile <index> buckets <num>
  cc profile <index> interval <seconds>
  cc profile <index> volume total <octets>
  exit

sgw-service <sgw_service_name>
  accounting context <ingress_context_name> gtpp group default
  associate accounting-policy <gz_policy_name>
  exit
  exit
context <ingress_context_name>
  interface <gz_interface_name>
    ip address <address>
    exit
  exit
exit
port ethernet <slot_number/port_number>
  no shutdown
bind interface <gz_interface_name> <ingress_context_name>
end

Notes:
- `gtpp single-source` is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- `gtpp` is the default option for the `accounting mode` command.
- An accounting mode configured for the call-control profile will override this setting.
- `accounting-level` types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the Accounting Profile Configuration Mode Commands chapter in the Command Line Interface Reference for more information on this command.

Configuring Diameter Offline Accounting on the S-GW

By default the S-GW service supports GTPP accounting. You can enable accounting via RADIUS/Diameter (Rf) for the S-GW service. To provide Rf offline charging during, for example, scenarios where the foreign P-GW does not, configure the S-GW with the example parameters below:

```
configure
  operator-policy name <policy_name>
    associate call-control-profile <call_cntrl_profile_name>
    exit
  call-control-profile <call_cntrl_profile_name>
    accounting mode radius-diameter
    exit
  lte-policy
    subscriber-map <map_name>
      precendence <number> match-criteria all operator-policy-name <policy_name>
      exit
    exit
  context <ingress_context_name>
    policy accounting <rf_policy_name>
      accounting-level {type}
```
operator-string <string>
exit

sgw-service <sgw_service_name>
  associate accounting-policy <rf_policy_name>
  associate subscriber-map <map_name>
exit

aaa group <rf-radius_group_name>
  radius attribute nas-identifier <id>
  radius accounting interim interval <seconds>
  radius dictionary <name>
  radius mediation-device accounting server <address> key <key>
  diameter authentication dictionary <name>
  diameter accounting dictionary <name>
  diameter accounting endpoint <rf_cfg_name>
  diameter accounting server <rf_cfg_name> priority <num>
exit

diameter endpoint <rf_cfg_name>
  use-proxy
  origin realm <realm_name>
  origin host <name> address <rf_ipv4_address>
  peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
  route-entry peer <rf_cfg_name>
exit
exit

context <ingress_context_name>
  interface <rf_interface_name>
    ip address <rf_ipv4_address>
exit
exit
port ethernet <slot_number/port_number>
   no shutdown
bind interface <rf_interface_name> <ingress_context_name>
end

Notes:
- accounting-level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the Accounting Profile Configuration Mode Commands chapter in the Command Line Interface Reference for more information on this command.
- The Rf interface IP address can also be specified as an IPv6 address using the ipv6 address command.

Configuring APN-level Traffic Policing on the S-GW

To enable traffic policing for scenarios where the foreign subscriber’s P-GW doesn’t enforce it, use the following configuration example:

configure

apn-profile <apn_profile_name>
   qos rate-limit downlink non-gbr-qci committed-auto-readjust duration <seconds> exceed-action {action} violate-action {action}
   qos rate-limit uplink non-gbr-qci committed-auto-readjust duration <seconds> exceed-action {action} violate-action {action}
   exit
operator-policy name <policy_name>
   apn default-apn-profile <apn_profile_name>
   exit
lte-policy
   subscriber-map <map_name>
      precedence <number> match-criteria all operator-policy-name <policy_name>
      exit
sgw-service <sgw_service_name>
   associate subscriber-map <map_name>
end

Notes:
- For the qos rate-limit command, the actions supported for violate-action and exceed-action are: drop, lower-ip-precedence, and transmit.
Configuring X.509 Certificate-based Peer Authentication

The configuration example in this section enables X.509 certificate-based peer authentication, which can be used as the authentication method for IP Security on the S-GW.

**Important:** Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration example enables X.509 certificate-based peer authentication on the S-GW.

In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure
  certificate name <cert_name> pem url <cert_pem_url> private-key pem url <private_key_url>
  ca-certificate name <ca_cert_name> pem url <ca_cert_url>
end
```

Notes:
- The `certificate name` and `ca-certificate list ca-cert-name` commands specify the X.509 certificate and CA certificate to be used.
- The PEM-formatted data for the certificate and CA certificate can be specified, or the information can be read from a file via a specified URL as shown in this example.

When creating the crypto template for IPSec in Context Configuration Mode, bind the X.509 certificate and CA certificate to the crypto template and enable X.509 certificate-based peer authentication for the local and remote nodes, as follows:

```
configure
  context <sgw_context_name>
    crypto template <crypto_template_name> ikev2-dynamic
      certificate name <cert_name>
      ca-certificate list ca-cert-name <ca_cert_name>
      authentication local certificate
      authentication remote certificate
    end
```

Notes:
- A maximum of sixteen certificates and sixteen CA certificates are supported per system. One certificate is supported per service, and a maximum of four CA certificates can be bound to one crypto template.
- The `certificate name` and `ca-certificate list ca-cert-name` commands bind the certificate and CA certificate to the crypto template.
• The *authentication local certificate* and *authentication remote certificate* commands enable X.509 certificate-based peer authentication for the local and remote nodes.

### Configuring Dynamic Node-to-Node IP Security on the S1-U and S5 Interfaces

The configuration example in this section creates IPSec/IKEv2 dynamic node-to-node tunnel endpoints on the S1-U and S5 interfaces.

**Important**: Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration examples are included in this section:

- Creating and Configuring an IPSec Transform Set
- Creating and Configuring an IKEv2 Transform Set
- Creating and Configuring a Crypto Template
- Binding the S1-U and S5 IP Addresses to the Crypto Template

#### Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure

context <sgw_context_name>

ipsec transform-set <ipsec_transform-set_name>

  encryption aes-cbc-128

  group none

  hmac sha1-96

  mode tunnel

end
```

**Notes:**

- The encryption algorithm, *aes-cbc-128*, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The *group none* command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The *hmac* command configures the Encapsulating Security Payload (ESP) integrity algorithm. The *sha1-96* keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
• The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header, including the IP header. This is the default setting for IPSec transform sets configured on the system.

### Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```plaintext
configure
  context <sgw_context_name>
  ikev2-ikesa transform-set <ikev2_transform-set_name>
    encryption aes-cbc-128
    group 2
    hmac shal-96
    lifetime <sec>
    prf shal
  end
```

**Notes:**

• The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.

• The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.

• The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **shal-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

• The **lifetime** command configures the time the security key is allowed to exist, in seconds.

• The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **shal** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

### Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```plaintext
configure
  context <sgw_context_name>
  crypto template <crypto_template_name> ikev2-dynamic
```
ikev2-ikesa transform-set list <name1> . . . <name6>

ikev2-ikesa rekey

payload <name> match childsa match ipv4

ipsec transform-set list <name1> . . . <name4>

rekey

end

Notes:
- The `ikev2-ikesa transform-set list` command specifies up to six IKEv2 transform sets.
- The `ipsec transform-set list` command specifies up to four IPSec transform sets.

**Binding the S1-U and S5 IP Addresses to the Crypto Template**

The following example configures the binding of the S1-U and S5 interfaces to the crypto template.

```
configure

color <sgw_ingress_context_name>

gtpu-service <gtpu_ingress_service_name>

bind ipv4-address <s1-u_interface_ip_address> crypto-template <enodeb_crypto_template>

exit

egtp-service <egtp_ingress_service_name>

interface-type interface-sgw-ingress

associate gtpu-service <gtpu_ingress_service_name>

gtpc bind address <s1u_interface_ip_address>

exit

exit

color <sgw_egress_context_name>

gtpu-service <gtpu_egress_service_name>

bind ipv4-address <s5_interface_ip_address> crypto-template <enodeb_crypto_template>

exit

egtp-service <egtp_egress_service_name>
```
interface-type interface=sgw-egress
associate gtpu-service <gtpu_egress_service_name>
gtpc bind address <s5_interface_ip_address>
exit
exit
context <sgw_ingress_context_name>
sgw-service <sgw_service_name> -noconfirm
    egtp-service ingress service <egtp_ingress_service_name>
    egtp-service egress context <sgw_egress_context_name>
end

Notes:
- The bind command in the GTP-U ingress and egress service configuration can also be specified as an IPv6 address using the ipv6-address command.

Configuring ACL-based Node-to-Node IP Security on the S1-U and S5 Interfaces

The configuration example in this section creates IKEv2/IPSec ACL-based node-to-node tunnel endpoints on the S1-U and S5 interfaces.

**Important:** Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration examples are included in this section:
- Creating and Configuring a Crypto Access Control List
- Creating and Configuring an IPSec Transform Set
- Creating and Configuring an IKEv2 Transform Set
- Creating and Configuring a Crypto Map

Creating and Configuring a Crypto Access Control List

The following example configures a crypto ACL (Access Control List), which defines the matching criteria used for routing subscriber data packets over an IPSec tunnel:

```
configure
    context <sgw_context_name>
    ip access-list <acl_name>
```
permit tcp host <source_host_address> host <dest_host_address> 
end

Notes:
- The `permit` command in this example routes IPv4 traffic from the server with the specified source host IPv4 address to the server with the specified destination host IPv4 address.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set which is used to define the security association that determines the protocols used to protect the data on the interface:

```configure
context <sgw_context_name>
  ipsec transform-set <ipsec_transform-set_name>
    encryption aes-cbc-128
    group none
    hmac sha1-96
    mode tunnel
end
```

Notes:
- The encryption algorithm, `aes-cbc-128`, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The `group none` command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The `hmac` command configures the Encapsulating Security Payload (ESP) integrity algorithm. The `sha1-96` keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The `mode tunnel` command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```configure
context <sgw_context_name>
  ikev2-ikesa transform-set <ikev2_transform-set_name>
```

Notes:
encryption aes-cbc-128
group 2
hmac sha1-96
lifetime <sec>
prf sha1
end

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map and applies it to the S1-U interface:

```plaintext
configure
  context <sgw_ingress_context_name>
  crypto map <crypto_map_name> ikev2-ipv4
    match address <acl_name>
    peer <ipv4_address>
    authentication local pre-shared-key key <text>
    authentication remote pre-shared-key key <text>
    ikev2-ikesa transform-set list <name1> ... <name6>
    payload <name> match ipv4
    lifetime <seconds>
```
ipsec transform-set list <name1> . . . <name4>
exit
exit
interface <s1-u_intf_name>
ip address <ipv4_address>
crypto-map <crypto_map_name>
exit
exit
port ethernet <slot_number/port_number>
no shutdown
bind interface <s1_u_intf_name> <sgw_ingress_context_name>
end

Notes:
- The type of crypto map used in this example is IKEv2-IPv4 for IPv4 addressing. An IKEv2-IPv6 crypto map can also be used for IPv6 addressing.
- The `ipsec transform-set list` command specifies up to four IPSec transform sets.

The following example configures an IKEv2 crypto map and applies it to the S5 interface:

```
context <sgw_egress_context_name>
crypto-map <crypto_map_name> ikev2-ipv4
match address <acl_name>
peer <ipv4_address>
authentication local pre-shared-key key <text>
authentication remote pre-shared-key key <text>
payload <name> match ipv4
   lifetime <seconds>
ipsec transform-set list <name1> . . . <name4>
exit
exit
interface <s5_intf_name>
```
ip address <ipv4_address>
crypto map <crypto_map_name>
ext
exit

port ethernet <slot_number/port_number>
no shutdown
bind interface <s5_intf_name> <sgw_egress_context_name>
end

Notes:
- The type of crypto map used in this example is IKEv2-IPv4 for IPv4 addressing. An IKEv2-IPv6 crypto map can also be used for IPv6 addressing.
- The `ipsec transform-set list` command specifies up to four IPSec transform sets.

### Configuring S4 SGSN Handover Capability

This configuration example configures an S4 interface supporting inter-RAT handovers between the S-GW and a S4 SGSN.

Use the following example to configure this feature:

```
configure
  context <ingress_context_name> -noconfirm
  interface <s4_interface_name>
    ip address <ipv4_address_primary>
    ip address <ipv4_address_secondary>
  exit
  exit
  port ethernet <slot_number/port_number>
  no shutdown
  bind interface <s4_interface_name> <ingress_context_name>
  exit
  context <ingress_context_name> -noconfirm
  gtpu-service <s4_gtpu_ingress_service_name>
  bind ipv4-address <s4_interface_ip_address>
```
exit
egtp-service <s4_egtp_ingress_service_name>
    interface-type interface--sgw-ingress
    validation-mode default
    associate gtpu-service <s4_gtpu_ingress_service_name>
    gtpc bind address <s4_interface_ip_address>
exit
sgw-service <sgw_service_name> -noconfirm
    associate ingress egtp-service <s4_egtp_ingress_service_name>
end

Notes:

- The S4 interface IP address(es) can also be specified as IPv6 addresses using the \texttt{ipv6 address} command.
Chapter 3
Operator Policy

The proprietary concept of an operator policy, originally architected for the exclusive use of an SGSN, is non-standard and currently unique to the ASR 5x00. This optional feature empowers the carrier with flexible control to manage functions that are not typically used in all applications and to determine the granularity of the implementation of any operator policy: to groups of incoming calls or to simply one single incoming call.

The following products support the use of the operator policy feature:

- MME (Mobility Management Entity - LTE)
- SGSN (Serving GPRS Support Node - 2G/3G/LTE)
- S-GW (Serving Gateway - LTE)

This document includes the following information:

- What Operator Policy Can Do
- The Operator Policy Feature in Detail
  - Call Control Profile
  - APN Profile
  - IMEI-Profile (SGSN only)
  - APN Remap Table
  - Operator Policies
  - IMSI Ranges
- How It Works
- Operator Policy Configuration
- Verifying the Feature Configuration
What Operator Policy Can Do

Operator policy enables the operator to specify a policy with rules governing the services, facilities and privileges available to subscribers.

A Look at Operator Policy on an SGSN

The following is only a sampling of what working operator policies can control on an SGSN:

- APN information included in call activation messages are sometimes damaged, misspelled, missing. In such cases, the calls are rejected. The operator can ensure calls aren't rejected and configure a range of methods for handling APNs, including converting incoming APNs to preferred APNs and this control can be used in a focused fashion or defined to cover ranges of subscribers.

- In another example, it is not unusual for a blanket configuration to be implemented for all subscriber profiles stored in the HLR. This results in a waste of resources, such as the allocation of the default highest QoS setting for all subscribers. An operator policy provides the opportunity to address such issues by allowing fine-tuning of certain aspects of profiles fetched from HLRs and, if desired, overwrite QoS settings received from HLR.

A Look at Operator Policy on an S-GW

The S-GW operator policy provides mechanisms to fine tune the behavior for subsets of subscribers. It also can be used to control the behavior of visiting subscribers in roaming scenarios by enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

The S-GW uses operator policy in the SGW service configuration to control the accounting mode. The default accounting mode is GTPP, but RADIUS/Diameter and none are options. The accounting mode value from the call control profile overrides the value configured in SGW service. If the accounting context is not configured in the call control profile, it is taken from SGW service. If the SGW service does not have the relevant configuration, the current context or default GTPP group is assumed.
The Operator Policy Feature in Detail

This flexible feature provides the operator with a range of control to manage the services, facilities and privileges available to subscribers.

Operator policy definitions can depend on factors such as (but not limited to):

- roaming agreements between operators,
- subscription restrictions for visiting or roaming subscribers,
- provisioning of defaults to override standard behavior.

These policies can override standard behaviors and provide mechanisms for an operator to circumvent the limitations of other infrastructure elements such as DNS servers and HLRs in 2G/3G networks.

By configuring the various components of an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

**Re-Usable Components** - Besides enhancing operator control via configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration lines needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- call control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- operator policies
- IMSI ranges

Each of these components is configured via a separate configuration mode accessed through the Global Configuration mode.

**Call Control Profile**

A call control profile can be used by the operator to fine-tune desired functions, restrictions, requirements, and/or limitations needed for call management on a per-subscriber basis or for groups of callers across IMSI ranges. For example:

- setting access restriction cause codes for rejection messages
- enabling/disabling authentication for various functions such as attach and service requests
- enabling/disabling ciphering, encryption, and/or integrity algorithms
- enabling/disabling of packet temporary mobile subscriber identity (P-TMSI) signature allocation (SGSN only)
- enabling/disabling of zone code checking
- allocation/retention priority override behavior (SGSN only)
Operator Policy

The Operator Policy Feature in Detail

- enabling/disabling inter-RAT, 3G location area, and 4G tracking area handover restriction lists (MME and S-GW only)
- setting maximum bearers and PDNs per subscriber (MME and S-GW only)

Call control profiles are configured with commands in the Call Control Profile configuration mode. A single call control profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet services cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following call control profile configuration rules should be considered:

- 1 (only one) - call control profile can be associated with an operator policy
- 1000 - maximum number of call control profiles per system (e.g., an SGSN).
- 15 - maximum number of equivalent PLMNs for 2G and 3G per call control profile
  - 15 - maximum number of equivalent PLMNs for 2G per ccprofile.
  - 15 - maximum number of supported equivalent PLMNs for 3G per ccprofile.
- 256 - maximum number of static SGSN addresses supported per PLMN
- 5 - maximum number of location area code lists supported per call control profile.
- 100 - maximum number of LACs per location area code list supported per call control profile.
- unlimited - number of zone code lists can be configured per call control profile.
- 100 - maximum number of LACs allowed per zone code list per call control profile.
- 2 - maximum number of integrity algorithms for 3G per call control profile.
- 3 - maximum number of encryption algorithms for 3G per call control profile.

APN Profile

An APN profile groups a set of access point name (APN)-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile will be applied.

For example:

- enable/disable a direct tunnel (DT) per APN. (SGSN)
- define charging characters for calls associated with a specific APN.
- identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.
- restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

APN profiles are configured with commands in the APN Profile configuration mode. A single APN profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards and 2G, 3G, 4G, and/or dual access, the following APN profile configuration rules should be considered:

- 50 - maximum number of APN profiles that can be associated with an operator policy.
- 1000 - maximum number of APN profiles per system (e.g., an SGSN).
• 116 - maximum gateway addresses (GGSN addresses) that can be defined in a single APN profile.

IMEI-Profile (SGSN only)

The IMEI is a unique international mobile equipment identity number assigned by the manufacturer that is used by the network to identify valid devices. The IMEI has no relationship to the subscriber.

An IMEI profile group is a set of device-specific parameters that control SGSN behavior when one of various types of Requests is received from a UE within a specified IMEI range. These parameters control:

- Blacklisting devices
- Identifying a particular GGSN to be used for connections for specified devices
- Enabling/disabling direct tunnels to be used by devices

IMEI profiles are configured with commands in the IMEI Profile configuration mode. A single IMEI profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following IMEI profile configuration rules should be considered:

- 10 - maximum number of IMEI ranges that can be associated with an operator policy.
- 1000 - maximum number of IMEI profiles per system (such as an SGSN).

APN Remap Table

APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This atypical level of control enables operators to deal with situations such as:

- An APN is provided in the Activation Request that does not match with any of the subscribed APNs; either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN would reject the Activation Request. It is possible to correct the APN, creating a valid name so that the Activation Request is not rejected.
- In some cases, an operator might want to force certain devices/users to use a specific APN. For example, all iPhone4 users may need to be directed to a specific APN. In such situations, the operator needs to be able to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table will be applied. For example, an APN remap table allows configuration of the following:

- APN aliasing - maps incoming APN to a different APN based on partial string match (MME and SGSN) or matching charging characteristic (MME and SGSN).
- Wildcard APN - allows APN to be provided by the SGSN when wildcard subscription is present and the user has not requested an APN.
- Default APN - allows a configured default APN to be used when the requested APN cannot be used – for example, the APN is not part of the HLR subscription.
APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following APN remap table configuration rules should be considered:

- 1 – maximum number of APN remap tables that can be associated with an operator policy.
- 1000 – maximum number of APN remap tables per system (such as an SGSN).
- 100 – maximum remap entries per APN remap table.

**Operator Policies**

The profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. An operator policy binds the various configuration components together. It associates APNs, with APN profiles, with an APN remap table, with a call control profile, and/or an IMEI profile (SGSN only) and associates all the components with filtering ranges of IMSIs.

In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers.

Operator policies are configured and the associations are defined via the commands in the Operator Policy configuration mode.

The IMSI ranges are configured with the command in the SGSN-Global configuration mode.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following operator policy configuration rules should be considered:

- 1 – maximum number of call control profiles associated with a single operator policy.
- 1 – maximum number of APN remap tables associated with a single operator policy.
- 10 – maximum number of IMEI profiles associated with a single operator policy (SGSN only)
- 50 – maximum number of APN profiles associated with a single operator policy.
- 1000 – maximum number of operator policies per system (e.g., an SGSN); this number includes the single default operator policy.
- 1000 – maximum number of IMSI ranges defined per system (e.g., an SGSN).

**Important:** SGSN operator policy configurations created with software releases prior to Release 11.0 are not forward compatible. Such configurations can be converted to enable them to work with an SGSN running Release 11.0 or higher. Your Cisco Account Representative can accomplish this conversion for you.

**IMSI Ranges**

Ranges of international mobile subscriber identity (IMSI) numbers, the unique number identifying a subscriber, are associated with the operator policies and used as the initial filter to determine whether or not any operator policy would be applied to a call. The range configurations are defined by the MNC, MCC, a range of MSINs, and optionally the PLMN ID. The IMSI ranges must be associated with a specific operator policy.
IMSI ranges are defined differently for each product supporting the operator policy feature.
How It Works

The specific operator policy is selected on the basis of the subscriber’s IMSI at attach time, and optionally the PLMN ID selected by the subscriber or the RAN node's PLMN ID. Unique, non-overlapping, IMSI + PLMN-ID ranges create call filters that distinguish among the configured operator policies.

The following flowchart maps out the logic applied for the selection of an operator policy:

Figure 12. Operator Policy Selection Logic
Operator Policy Configuration

This section provides a high-level series of steps and the associated configuration examples to configure an operator policy. By configuring an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers within a defined IMSI range.

Most of the operator policy configuration components are common across the range of products supporting operator policy. Differences will be noted as they are encountered below.

**Important:** This section provides a minimum instruction set to implement operator policy. For this feature to be operational, you must first have completed the system-level configuration as described in the *System Administration Guide* and the service configuration described in your product’s administration guide.

The components can be configured in any order. This example begins with the call control profile:

**Step 1** Create and configure a call control profile, by applying the example configuration presented in the Call Control Profile Configuration section.

**Step 2** Create and configure an APN profile, by applying the example configuration presented in the APN Profile Configuration section.

**Important:** It is not necessary to configure both an APN profile and an IMEI profile. You can associate either type of profile with a policy. It is also possible to associate one or more APN profiles with an IMEI profile for an operator policy (SGSN only).

**Step 3** Create and configure an IMEI profile by applying the example configuration presented in the IMEI Profile Configuration section (SGSN only).

**Step 4** Create and configure an APN remap table by applying the example configuration presented in the APN Remap Table Configuration section.

**Step 5** Create and configure an operator policy by applying the example configuration presented in the Operator Policy Configuration section.

**Step 6** Configure an IMSI range by selecting and applying the appropriate product-specific example configuration presented in the IMSI Range Configuration sections below.

**Step 7** Associate the configured operator policy components with each other and a network service by applying the example configuration in the Operator Policy Component Associations section.

**Step 8** 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*.

**Step 9** Verify the configuration for each component separately by following the instructions provided in the Verifying the Feature Configuration section of this chapter.
Call Control Profile Configuration

This section provides the configuration example to create a call control profile and enter the configuration mode. Use the call control profile commands to define call handling rules that will be applied via an operator policy. Only one call control profile can be associated with an operator policy, so it is necessary to use (and repeat as necessary) the range of commands in this mode to ensure call-handling is sufficiently managed.

Configuring the Call Control Profile for an SGSN

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure

call-control-profile <profile_name>>

    attach allow access-type umts location-area-list instance <list_id>

    authenticate attach

    location-area-list instance <instance> area-code <area_code>

    sgsn-number <E164_number>

end
```

Notes:

- Refer to the Call Control Profile Configuration Mode chapter in the Command Line Interface Reference for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Configuring the Call Control Profile for an MME or S-GW

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure

call-control-profile <profile_name>>

   associate hss-peer-service <service_name> s6a-interface

   attach imei-query-type imei verify-equipment-identity

   authenticate attach

   dns-pgw context <mme_context_name>

   dns-sgw context <mme_context_name>

end
```
Notes:

- Refer to the *Call Control Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.

- This profile will only become valid when it is associated with an operator policy.

**APN Profile Configuration**

This section provides the configuration example to create an APN profile and enter the apn-profile configuration mode. Use the `apn-profile` commands to define how calls are to be handled when the requests include an APN. More than one APN profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```bash
configure

apn-profile <profile_name>

gateway-address 123.123.123.1 priority <1> (SGSN only)
direct-tunnel not-permitted-by-ggsn (SGSN only)
idle-mode-acl ipv4 access-group station7 (S-GW only)

end
```

Notes:

- All of the parameter defining commands in this mode are product-specific. Refer to the *APN Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.

- This profile will only become valid when it is associated with an operator policy.

**IMEI Profile Configuration - SGSN only**

This section provides the configuration example to create an IMEI profile and enter the imei-profile configuration mode. Use the `imei-profile` commands to define how calls are to be handled when the requests include an IMEI in the defined IMEI range. More than one IMEI profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```bash
configure

imei-profile <profile_name>
ggsn-address 211.211.123.3
direct-tunnel not-permitted-by-ggsn (SGSN only)
associate apn-remap-table remap1
```
Notes:

- It is optional to configure an IMEI profile. An operator policy can include IMEI profiles and/or APN profiles.
- This profile will only become valid when it is associated with an operator policy.

**APN Remap Table Configuration**

This section provides the configuration example to create an APN remap table and enter the `apn-remap-table` configuration mode.

Use the `apn-remap-table` commands to define how APNs are to be handled when the requests either do or do not include an APN.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure

apn-remap-table <table_name>

  apn-selection-default first-in-subscription

  wildcard-apn pdp-type ipv4 network-identifier <apn_net_id>

  blank-apn network-identifier <apn_net_id> (SGSN only)

end
```

Notes:

- The `apn-selection-default first-in-subscription` command is used for APN redirection to provide “guaranteed connection” in instances where the UE-requested APN does not match the default APN or is missing completely. In this example, the first APN matching the PDP type in the subscription is used. The first-in-selection keyword is an MME feature only.

- Some of the commands represented in the example above are common and some are product-specific. Refer to the APN-Remap-Table Configuration Mode chapter in the Command Line Interface Reference for command details and variable options.

- This profile will only become valid when it is associated with an operator policy.

**Operator Policy Configuration**

This section provides the configuration example to create an operator policy and enter the operator policy configuration mode.

Use the commands in this mode to associate profiles with the policy, to define and associate APNs with the policy, and to define and associate IMEI ranges. Note: IMEI ranges are supported for SGSN only.

The example below includes sample variable that you will replace with your own values.

```
configure
```
operator-policy <policy_name>  
associate call-control-profile <profile_name>  
apn network-identifier <apn-net-id_1> apn-profile <apn_profile_name_1>  
apn network-identifier <apn-net-id_2> apn-profile <apn_profile_name_1>  
imei range <imei_number> to <imei_number> imei-profile name <profile_name>  
associate apn-remap-table <table_name>  
end

Notes:
• Refer to the Operator-Policy Configuration Mode chapter in the Command Line Interface Reference for command details and variable options.
• This policy will only become valid when it is associated with one or more IMSI ranges (SGSN) or subscriber maps (MME and S-GW).

IMSI Range Configuration

This section provides IMSI range configuration examples for each of the products that support operator policy functionality.

Configuring IMSI Ranges on the MME or S-GW

IMSI ranges on an MME or S-GW are configured in the Subscriber Map Configuration Mode. Use the following example to configure IMSI ranges on an MME or S-GW:

configure
subscriber-map <name>

lte-policy

precedence <number> match-criteria imsi mcc <mcc_number> mnc <mnc_number> msin first <start_range> last <end_range> operator-policy-name <policy_name>
end

Notes:
• The precedence number specifies the order in which the subscriber map is used. 1 has the highest precedence.
• The operator policy name identifies the operator policy that will be used for subscribers that match the IMSI criteria and fall into the MSIN range.

Configuring IMSI Ranges on the SGSN

The example below is specific to the SGSN and includes sample variables that you will replace with your own values.
configure

sgsn-global

  imsi-range mcc 311 mnc 411 operator-policy oppolicy1
  imsi-range mcc 312 mnc 412 operator-policy oppolicy2
  imsi-range mcc 313 mnc 413 operator-policy oppolicy3
  imsi-range mcc 314 mnc 414 operator-policy oppolicy4
  imsi-range mcc 315 mnc 415 operator-policy oppolicy5

end

Notes:

- Operator policies are not valid until IMSI ranges are associated with them.

## Associating Operator Policy Components on the MME

After configuring the various components of an operator policy, each component must be associated with the other components and, ultimately, with a network service.

The MME service associates itself with a subscriber map. From the subscriber map, which also contains the IMSI ranges, operator policies are accessed. From the operator policy, APN remap tables and call control profiles are accessed.

Use the following example to configure operator policy component associations:

configure

  operator-policy <name>
      associate apn-remap-table <table_name>
      associate call-control-profile <profile_name>

exit

lte-policy

  subscriber-map <name>
      precedence match-criteria all operator-policy-name <policy_name>

exit

exit

context <mme_context_name>

  mme-service <mme_svc_name>
      associate subscriber-map <name>
Notes:

- The `precedence` command in the subscriber map mode has other `match-criteria` types. The `all` type is used in this example.

## Configuring Accounting Mode for S-GW

The `accounting mode` command configures the mode to be used for the S-GW service for accounting, either GTPP (default), RADIUS/Diameter, or None.

Use the following example to change the S-GW accounting mode from GTPP (the default) to RADIUS/Diameter:

```
configure
context <sgw_context_name>
    sgw-service <sgw_srv_name>
        accounting mode radius-diameter
    end
end
```

Notes:

- An accounting mode configured for the call control profile will override this setting.
Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a .cfg file as described in the *System Administration Guide*.

**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

**Step 1**  
Verify that the operator policy has been created and that required profiles have been associated and configured properly by entering the following command in Exec Mode:

```
show operator-policy full name oppolicy1
```

The output of this command displays the entire configuration for the operator policy configuration.

```
[local]asr5x00# show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1

Call Control Profile Name: ccprofile1
  Validity: Valid

APN Remap Table Name: remap1
  Validity: Valid

IMEI Range 711919739 to 711919777

IMEI Profile Name: imeiprof1
Include/Exclude: Include
  Validity: Valid

APN NI homer51

APN Profile Name: apn-profile1
  Validity: Valid
```

**Notes:**
- If the profile name is shown as “Valid”, the profile has actually been created and associated with the policy. If the Profile name is shown as “Invalid”, the profile has not been created/configured.
- If there is a valid call control profile, a valid APN profile and/or valid IMEI profile, and a valid APN remap table, the operator policy is valid and complete if the IMSI range has been defined and associated.
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 command 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 provided 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 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 *Statistics and Counters Reference*.

### Table 6. System Status and Performance Monitoring Commands

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Congestion-Control Information</strong></td>
<td></td>
</tr>
<tr>
<td>View Congestion-Control Statistics</td>
<td>`show congestion-control statistics { allmgr</td>
</tr>
<tr>
<td><strong>View Subscriber Information</strong></td>
<td></td>
</tr>
<tr>
<td>View session resource status</td>
<td><code>show resources session</code></td>
</tr>
<tr>
<td>Display Subscriber Configuration Information</td>
<td></td>
</tr>
<tr>
<td>View locally configured subscriber profile settings (must be in context where subscriber resides)</td>
<td><code>show subscribers configuration username subscriber_name</code></td>
</tr>
<tr>
<td>View remotely configured subscriber profile settings</td>
<td><code>show subscribers aaa-configuration username subscriber_name</code></td>
</tr>
<tr>
<td><strong>View Subscribers Currently Accessing the System</strong></td>
<td></td>
</tr>
<tr>
<td>View a listing of subscribers currently accessing the system</td>
<td><code>show subscribers all</code></td>
</tr>
<tr>
<td><strong>View Statistics for Subscribers using S-GW Services on the System</strong></td>
<td></td>
</tr>
<tr>
<td>View statistics for subscribers using any S-GW service on the system</td>
<td><code>show subscribers sgw-only full</code></td>
</tr>
<tr>
<td>View statistics for subscribers using a specific S-GW service on the system</td>
<td><code>show subscribers sgw-service service_name</code></td>
</tr>
<tr>
<td><strong>View Statistics for Subscribers using MAG Services on the System</strong></td>
<td></td>
</tr>
<tr>
<td>View statistics for subscribers using any MAG service on the system</td>
<td><code>show subscribers mag-only full</code></td>
</tr>
<tr>
<td>View statistics for subscribers using a specific MAG service on the system</td>
<td><code>show subscribers mag-service service_name</code></td>
</tr>
<tr>
<td><strong>View Session Subsystem and Task Information</strong></td>
<td></td>
</tr>
<tr>
<td>Display Session Subsystem and Task Statistics</td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong> Refer to the System Software Task and Subsystem Descriptions appendix in the <em>System Administration Guide</em> for additional information on the Session subsystem and its various manager tasks.</td>
<td></td>
</tr>
<tr>
<td>View AAA Manager statistics</td>
<td><code>show session subsystem facility aaamgr all</code></td>
</tr>
</tbody>
</table>
### To do this:

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>View AAA Proxy statistics</td>
<td><code>show session subsystem facility aaaproxy all</code></td>
</tr>
<tr>
<td>View Session Manager statistics</td>
<td><code>show session subsystem facility sessmgr all</code></td>
</tr>
<tr>
<td>View MAG Manager statistics</td>
<td><code>show session subsystem facility magmgr all</code></td>
</tr>
<tr>
<td><strong>View Session Recovery Information</strong></td>
<td></td>
</tr>
<tr>
<td>View session recovery status</td>
<td><code>show session recovery status [ verbose ]</code></td>
</tr>
<tr>
<td><strong>View Session Disconnect Reasons</strong></td>
<td></td>
</tr>
<tr>
<td>View session disconnect reasons with verbose output</td>
<td><code>show session disconnect-reasons</code></td>
</tr>
<tr>
<td><strong>View S-GW Service Information</strong></td>
<td></td>
</tr>
<tr>
<td>View S-GW service statistics</td>
<td><code>show sgw-service statistics all</code></td>
</tr>
<tr>
<td>Verify S-GW services</td>
<td><code>context sgw_context_name</code> \ `show sgw-service all</td>
</tr>
<tr>
<td><strong>View GTP Information</strong></td>
<td></td>
</tr>
<tr>
<td>View eGTP-C service statistics for a specific service</td>
<td><code>show egtpc statistics egtpc-service name</code></td>
</tr>
<tr>
<td>View eGTP-C service information for a specific service</td>
<td><code>show egtpc-service name</code></td>
</tr>
<tr>
<td>View GTP-U service statistics for all GTP-U data traffic on the system</td>
<td><code>show gtpu statistics</code></td>
</tr>
<tr>
<td>View eGTP-U service information for a specific service</td>
<td><code>show gtpu-service name</code></td>
</tr>
<tr>
<td><strong>View QoS/QCI Information</strong></td>
<td></td>
</tr>
<tr>
<td>View QoS Class Index to QoS mapping tables</td>
<td><code>show qci-qos-mapping table all</code></td>
</tr>
</tbody>
</table>
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 (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI `clear` command. Refer to the *Command Line Reference* for detailed information on using this command.
Chapter 5
Configuring Subscriber Session Tracing

This chapter provides information on subscriber session trace functionality to allow an operator to trace subscriber activity at various points in the network and at various level of details in EPS network. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

This chapter discusses following topics for feature support of Subscriber Session Tracing in LTE service:

- Introduction
- Supported Standards
- Subscriber Session Tracing Functional Description
- Subscriber Session Trace Configuration
- Verifying Your Configuration
Introduction

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an LTE environment.

In general, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The EPC network entities like MME, S-GW, P-GW support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal

**Important:** Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the chassis. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

**Important:** Only Maximum Trace Depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:
All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

**Supported Functions**

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)
- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity
  - Support up to 32 simultaneous session traces per NE
  - Capacity to activate/deactivate TBD trace sessions per second
  - Each NE can buffer TBD bytes of trace data locally
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
- MME: S1, S3, S6a, S10, S11
- S-GW: S4, S5, S8, S11, Gxc
- PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Collection Entity (TCE) Support
  - Active pushing of files to the TCE
  - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager
Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)
Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session on EPC nodes:

Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

Trace Session

A trace session is the time between trace activation and trace deactivation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently, subscriber session trace is not supported for co-located network elements in the EPC network.

Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber or UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.
Management Activation

With a management-initiated activation, the WEM sends an activation request directly to the NE where the trace is to be initiated. The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

Signaling Activation

With a signaling-based activation, the trace session is indicated to the NE across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active).

Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Data Collection and Reporting

Subscriber session trace functionality supports data collection and reporting system to provide historical usage and event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09)

Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages.
(specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

**Important:** Only Maximum Trace Depth is supported in the current release.

**Trace Scope**

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

**Network Element Details**

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

**MME**

The MME support tracing of the following interfaces with the following trace capabilities:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Remote Device</th>
<th>Trace Signaling (De)Activation RX</th>
<th>Trace Signaling (De)Activation TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1a</td>
<td>eNodeB</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>S3</td>
<td>SGSN</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S6a</td>
<td>HSS</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S10</td>
<td>MME</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>S11</td>
<td>S-GW</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

**S-GW**

The S-GW support tracing of the following interfaces with the following trace capabilities:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Remote Device</th>
<th>Trace Signaling (De)Activation RX</th>
<th>Trace Signaling (De)Activation TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-U</td>
<td>eNodeB</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S4</td>
<td>SGSN</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>S5</td>
<td>P-GW (Intra-PLMN)</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S8</td>
<td>P-GW (Inter-PLMN)</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>S11</td>
<td>MME</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S12</td>
<td>RNC</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
### Interface Name
### Remote Device
### Trace Signaling (De)Activation RX
### Trace Signaling (De)Activation TX

**Gxc**
- Policy Server
- RX: Y
- TX: N

---

## P-GW

The P-GW support tracing of the following interfaces with the following trace capabilities:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Remote Device</th>
<th>Trace Signaling (De)Activation RX</th>
<th>Trace Signaling (De)Activation TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>S2abc</td>
<td>Various NEs</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>S5</td>
<td>S-GW (Intra-PLMN)</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S6b</td>
<td>AAA Server/Proxy</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>S8</td>
<td>S-GW (Inter-PLMN)</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Gx</td>
<td>Policy Server</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>SGi</td>
<td>IMS</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
Subscriber Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements in LTE/EPC networks.

**Important:** This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC networks. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

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

To configure the system to support subscriber session trace collection and trace file transport on a system:

**Step 1** Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC Network Element* section.

**Step 2** Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.

**Step 3** 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*.

**Step 4** Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

Enabling Subscriber Session Trace on EPC Network Element

This section provides the configuration example to enable the subscriber session trace on a system at the Exec mode:

```
session trace subscriber network-element { ggsn | mme | pgw | sgw } { imei <imei_id> } { imsi <imsi_id> } { interface { all | <interface> } } trace-ref <trace_ref_id> collection-entity <ip_address>
```

Notes:
- `<interface>` is the name of the interfaces applicable for specific NE on which subscriber session traces have to be collected. For more information, refer to the `session trace subscriber` command in the *Command Line Interface Reference*.
- `<trace_ref_id>` is the configured Trace Id to be used for this trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+TraceId (3 byte octet string).
- `<ip_address>` is the IP address of Trace collection Entity in IPv4 notation.
Trace File Collection Configuration

This section provides the configuration example to configure the trace file collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

```plaintext
configure

    session trace subscriber network-element { all | ggsn | mme | pgw | sgw } [ collection-timer <dur> ] [ tce-mode { none | push transport { ftp | sftp } path <string> username <name> { encrypted password <enc_pw> } | password <password> } ]

end
```

Notes:

- `<string>` is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer to the `session trace` command in the Command Line Interface Reference.
Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the System Administration Guide and also to retrieve errors and warnings within an active configuration for a service.

**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the Subscriber Session Trace configuration.

**Step 1** Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:

```plaintext
show session trace statistics
```

The output of this command displays the statistics of the session trace instance.

- Num current trace sessions: 5
- Total trace sessions activated: 15
- Total Number of trace session activation failures: 2
- Total Number of trace recording sessions triggered: 15
- Total Number of messages traced: 123
- Number of current TCE connections: 2
- Total number of TCE connections: 3
- Total number of files uploaded to all TCEs: 34

**Step 2** View the session trace references active for various network elements in an EPC network by entering the following command in Exec Mode:

```plaintext
show session trace trace-summary
```

The output of this command displays the summary of trace references for all network elements:

- **MME**
  - Trace Reference: 310012012345
  - Trace Reference: 310012012346

- **SGW**
  - Trace Reference: 310012012345
  - Trace Reference: 310012012346

- **PGW**
Trace Reference: 310012012347
Chapter 6
Intelligent RAT Paging for ISR on the S-GW

This chapter provides detailed feature information for the Intelligent RAT Paging for Idle Mode Signaling Reduction (ISR) feature on the S-GW.

- Feature Description
- How it Works
- Configuring Intelligent RAT Paging for ISR on the S-GW
Feature Description

This section describes the Intelligent RAT Paging for ISR feature on the S-GW.

When Idle Mode Signaling Reduction (ISR) is active, and a UE is in idle mode with control plane connections to both the MME and the S4-SGSN, and the S-GW receives downlink data for that UE, it sends Downlink-Data-Notification-Requests (requests to page UEs) to both the S4-SGSN and MME in parallel. This scenario causes the following problems:

- Both the MME and S4-SGSN perform paging in parallel, thereby resulting in an overuse of radio resources. The UE can be camped on either the MME or S4-SGSN, and respond to the paging of either the MME or S4-SGSN, so the radio resource of one node is not used effectively.
- If the S-GW tries to send DDN messages to both nodes sequentially, there can be a delay in call setup and establishment.

The Intelligent RAT Paging for ISR feature reduces both the radio resource usage due to paging and the internal load on the MME/S4-SGSN nodes.

The S-GW intelligently determines when to perform sequential paging as opposed to parallel paging by identifying the APN and its configuration (in the apn-profile configuration) for the downlink packet for which paging is originated. This provides the following benefits:

- More efficient utilization of radio resources used for paging when the incoming packet is not delay sensitive.
- Reduction in the delay of call establishment due to parallel paging when the incoming packet is delay sensitive.

This feature is useful for ISR enabled Networks to reduce the radio resource usage due to paging.

Relationships to Other Features (optional)

Before configuring the Intelligent RAT Paging for ISR feature on the S-GW, be aware of the following requirements and relationships to other features:

- This feature is useful if the peer MME and S4-SGSN also support ISR.
- If operators want to have the ISR paging method recovered for a given PDN, the Session Recovery feature must be configured on the S-GW.
How it Works

Intelligent RAT Paging for ISR on the S-GW

Depending on the situation, the S-GW uses one of two methods to perform Intelligent RAT Paging for ISR:

- **Sequential Paging** (pages both nodes one after the other). This method optimizes radio resource utilization. If quick call setup time is not indicated, the S-GW will perform sequential paging and it will page the S4-SGSN and MME one after the other. It first will page to the node of the last known RAT type of the UE.

- **Parallel Paging** (pages both the nodes in parallel). This method results in quick paging response time and faster call setup time. If the DDN is initiated for an APN that requires the quick call setup time (for example, VoLTE APN) then the S-GW performs parallel paging.

For intelligent paging, the S-GW has to determine whether to perform radio resource optimization or to use a quick call establishment procedure. The S-GW makes the decision to determine whether to perform sequential paging or parallel paging based on the configuration of the APN (through apn-profile applied for the APN).

The S-GW finds the APN of the particular bearer, and it checks to see if it received the downlink data. If isr-sequential-paging is configured for this APN on the S-GW, the S-GW initiates a DDN message to one node (MME or S4-SGSN) and waits for the service request procedure from that node within a configured time. If the S-GW does not receive the service request procedure within configured time, it initiates the DDN message towards the other node.

The node which was last sent the Modify Bearer Request to the S-GW (that is, the last known RAT type) is selected first to send the DDN messages.

Intelligent RAT Paging for ISR requires manual configuration through the Command Line Interface.

Licenses

Intelligent RAT Paging for ISR is a licensed Cisco feature. A separate feature license 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.

Limitations

The Intelligent RAT Paging for ISR feature has the following restrictions and limitations:

1. The S-GW performs sequential paging (if configured) only for Downlink data triggered Downlink Data Notification (DDN) messages. All control event triggered DDN messages are treated as high priority DDN messages and the S-GW always performs parallel paging for control event triggered DDN messages. No DDN-Throttling and DDN-Delay shall be applicable only to Downlink data triggered DDN messages.

2. S-GW Intelligent RAT Paging for ISR is supported on the S-GW only. It is not supported on the SAE-GW.

Flows

This section provides descriptive call flows for the Intelligent RAT Paging for ISR feature. It includes call flows for both sequential and parallel paging procedures.
**How it Works**

### Intelligent RAT Paging for ISR: Sequential Paging Procedure

**Figure 14.** Intelligent RAT Paging for ISR: Sequential Paging Procedure

**Table 7.** Intelligent RAT Paging for ISR: Sequential Paging Procedure Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The S-GW receives the downlink data packet for an idle UE which has ISR active and the S-GW is configured to initiate sequential paging for this APN. The Last known RAT Type for this UE is E-UTRAN.</td>
</tr>
<tr>
<td>2</td>
<td>The S-GW initiates Downlink Data Notification towards the MME and starts the timer $t_p$.</td>
</tr>
<tr>
<td>3</td>
<td>The MME replies with a Downlink Data Notification Ack message. If the MME initiates the service request procedure for this UE within time $t_p$, then the S-GW will stop the timer $t_p$ and process the service request procedure. The S-GW will not initiate the Downlink Data Notification towards S4-SGSN (in a different RAT). Therefore, the system saves the paging attempt and the radio resource of the S4-SGSN.</td>
</tr>
<tr>
<td>4</td>
<td>If the MME does not initiates the service request procedure for this UE within time $t_p$ then upon expiry of timer $t_p$, the S-GW will initiate the Downlink Data Notification towards the S4-SGSN.</td>
</tr>
<tr>
<td>5</td>
<td>The S4-SGSN replies with a Downlink Data Notification Ack message. The S4-SGSN attempts to page the UE. The S-GW will receive the service request procedure from S4-SGSN.</td>
</tr>
</tbody>
</table>
How it Works

Figure 15. Intelligent RAT Paging for ISR: Parallel Paging Procedure

Table 8. Intelligent RAT Paging for ISR: Parallel Paging Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The S-GW receives the downlink data packet for an ISR active, Idle UE. The S-GW is configured to initiate parallel paging for this APN.</td>
</tr>
<tr>
<td>2</td>
<td>The S-GW initiates Downlink Data Notification towards the MME.</td>
</tr>
<tr>
<td>3</td>
<td>The S-GW initiates Downlink Data Notification towards the S4-SGSN.</td>
</tr>
<tr>
<td>4</td>
<td>The MME replies with a Downlink Data Notification Ack message.</td>
</tr>
<tr>
<td>5</td>
<td>The S4-SGSN replies with a Downlink Data Notification Ack message.</td>
</tr>
<tr>
<td>6</td>
<td>The MME and S4-SGSN attempt to page the UE. The S-GW will receive the service request procedure from either the MME or S4-SGSN.</td>
</tr>
</tbody>
</table>
Configuring Intelligent RAT Paging for ISR on the S-GW

This section describes how to configure the Intelligent RAT Paging for ISR feature on the S-GW. It also describes how to verify the configuration and to monitor the feature’s performance.

Configuring the Intelligent RAT Paging for ISR Feature

Configuration of the Intelligent RAT Paging for ISR feature on the S-GW includes enabling ISR sequential paging in the APN profile context and configuring the DDN ISR sequential paging delay time in the S-GW service context.

Use the example configuration below to configure the Intelligent RAT Paging for ISR feature.

```
config
    apn-profile apn_profile_name
      isr-sequential-paging
    end

Notes:
- `apn_profile_name` is the name of the APN profile to be used for Intelligent RAT ISR Paging on this S-GW.
- `isr-sequential-paging` enables Intelligent RAT ISR Paging in this APN profile.
- To disable `isr-sequential-paging`, enter the `remove isr-sequential-paging` command.

config
    context sgw_context_name
      sgw-service sgw-service_name
        ddn isr-sequential-paging delay time duration_msecs

Notes:
- `sgw_context_name` is the name of the context in which the S-GW service is configured.
- `sgw_service_name` is the name of the configured S-GW service.
- `ddn isr-sequential-paging delay time` specifies the time delay between the paging of different RAT types. This value is entered in increments of 100 milliseconds (where 1 = 100 milliseconds). Valid entries are from 1 to 255. The default setting is 10 (1 second).
```

Verifying the Intelligent RAT Paging for ISR Configuration

This section describes how to verify the Intelligent RAT Paging for ISR configuration settings.
To verify that Intelligent RAT Paging for ISR is enabled in the APN profile for this S-GW, enter the following command from Exec Mode:

```
[local]asr5000#show apn-profile full name apn_profile_name
...
LIPA-APN :Disabled
**ISR-SEQUENTIAL-PAGING** :Enabled
Local Offload :Disabled
Overcharging protection :Disabled
...
```

To verify that the ISR sequential delay time is configured properly, enter the following command from Exec Mode:

```
[local]asr5000#show sgw-service name sgw_service_name
...
Service name
...
    GTPU Error Indication Handling:
...
    S4U-Interface: local-purge
        ddn failure-action pkt-drop-time: 300
        **ddn isr-sequential-paging delay-time**: 1
    Idle timeout :n/a
...
```
Appendix A
Direct Tunnel

This chapter briefly describes the 3G/4G UMTS direct tunnel (DT) feature, indicates how it is implemented on various systems on a per call basis, and provides feature configuration procedures.

Products supporting direct tunnel include:

- 3G devices (per 3GPP TS 23.919 v8.0.0):
  - the Serving GPRS Support Node (SGSN)
  - the Gateway GPRS Support Node (GGSN)
- LTE devices (per 3GPP TS 23.401 v8.3.0):
  - Serving Gateway (S-GW)
  - PDN Gateway (P-GW)

**Important:** Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. 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.

The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN and S-GW are the only products that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

This chapter provides the following information:

- Direct Tunnel Feature Overview
- Direct Tunnel Configuration
Direct Tunnel Feature Overview

The direct tunnel architecture allows the establishment of a direct *user plane* (GTP-U) tunnel between the radio access network equipment (RNC) and the GGSN/P-GW.

Once a direct tunnel is established, the SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDN context activation.

A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN/S-GW to handle the user plane processing.

A direct tunnel is achieved upon PDN context activation in the following ways:

- **3G network**: The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN, using an Updated PDN Context Request toward the GGSN.
1. Direct Tunneling - 3G Network

- **LTE network**: When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality. The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN/P-GW, using an Update PDN Context Request toward the GGSN/P-GW.

2. Direct Tunneling - LTE Network, GTP-U Tunnel

- **LTE network**: The SGSN establishes a user plane tunnel (GTP-U tunnel over an S12 interface) directly between the RNC and the S-GW, using an Update PDN Context Request toward the S-GW.
A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

The following figure illustrates the logic used within the SGSN/S-GW to determine if a direct tunnel will be setup.
Figure 17. Direct Tunneling - Establishment Logic

- IMSI check
- Matched operator policy for MS? NO
  - DT permitted by operator policy? NO
  - Matched APN or IMEI profile for PDP context? NO
  - DT restricted by RNC config? NO
  - DT restricted by SGTP service config? NO
- Direct Tunnel
- Matched operator policy for MS? YES
  - DT permitted by operator policy? YES
  - Matched APN or IMEI profile for PDP context? YES
  - DT restricted by APN profile? YES
- No Direct Tunnel
Direct Tunnel Configuration

The following configurations are provided in this section:

- Configuring Direct Tunnel Support on the SGSN
- Configuring S12 Direct Tunnel Support on the S-GW

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the system operator policy named default.

By default, direct tunnel support is

- disallowed on the SGSN/S-GW
- allowed on the GGSN/P-GW.

**Important:** If direct tunnel is allowed in the default operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel allowed.

For more information about operator policies and configuration details, refer to Operator Policy.

Configuring Direct Tunnel Support on the SGSN

The following is a high-level view of the steps, and the associated configuration examples, to configure the SGSN to setup a direct tunnel.

Before beginning any of the following procedures, you must have completed (1) the basic service configuration for the SGSN, as described in the Cisco ASR Serving GPRS Support Node Administration Guide, and (2) the creation and configuration of a valid operator policy, as described in the Operator Policy chapter in this guide.

**Step 1** Configure the SGSN to setup GTP-U direct tunnel between an RNC and an access gateway by applying the example configuration presented in the Enabling Setup of GTP-U Direct Tunnels section below.

**Step 2** Configure the SGSN to allow GTP-U direct tunnels to an access gateway, for a call filtered on the basis of the APN, by applying the example configuration presented in the Enabling Direct Tunnel per APN section below.

**Important:** It is only necessary to complete either step 2 or step 3 as a direct tunnel cannot be setup on the basis of call filtering matched with both an APN profile and an IMEI profile.

**Step 3** Configure the SGSN to allow GTP-U direct tunnels to a GGSN, for a call filtered on the basis of the IMEI, by applying the example configuration presented in the Enabling Direct Tunnel per IMEI section below.

**Step 4** Configure the SGSN to allow GTP-U direct tunnel setup from a specific RNC by applying the example configuration presented in the Enabling Direct Tunnel to Specific RNCs section below.

**Step 5** *(Optional)* Configure the SGSN to disallow direct tunnel setup to a single GGSN that has been configured to allow it in the APN profile. This command allows the operator to restrict use of a GGSN for any reason, such as load balancing. Refer to the direct-tunnel-disabled-ggsn command in the SGTP Service Configuration Mode chapter of the Command Line Interface Reference.
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.

Step 7 Check that your configuration changes have been saved by using the sample configuration found in the Verifying the SGSN Direct Tunnel Configuration section in this chapter.

Enabling Setup of GTP-U Direct Tunnels

The SGSN determines whether a direct tunnel can be setup and by default the SGSN doesn’t support direct tunnel.

Example Configuration

Enabling direct tunnel setup on an SGSN is done by configuring direct tunnel support in a call-control profile.

```plaintext
config
  call-control-profile <policy_name>
    direct-tunnel attempt-when-permitted
  end
```

Notes:
- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the Operator Policy chapter in this guide.
- Direct tunnel is now allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel per APN

In each operator policy, APN profiles are configured to connect to one or more GGSNs and to control the direct tunnel access to that GGSN based on call filtering by APN. Multiple APN profiles can be configured per operator policy.

By default, APN-based direct tunnel functionality is allowed so any existing direct tunnel configuration must be removed to return to default and to ensure that the setup has not been restricted.

Example Configuration

The following is an example of the commands used to ensure that direct tunneling, to a GGSN(s) identified in the APN profile, is enabled:

```plaintext
config
  apn-profile <profile_name>
    remove direct tunnel
  end
```

Notes:
• An APN profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the Operator Policy chapter in this guide.
• Direct tunnel is now allowed for the APN but will only setup if also allowed on the RNC.

Enabling Direct Tunnel per IMEI

Some operator policy filtering of calls is done on the basis of international mobile equipment identity (IMEI) so the direct tunnel setup may rely upon the feature configuration in the IMEI profile.
The IMEI profile basis its permissions for direct tunnel on the RNC configuration associated with the IuPS service.
By default, direct tunnel functionality is enabled for all RNCs.

Example Configuration

The following is an example of the commands used to enable direct tunneling in the IMEI profile:

```plaintext
config

imei-profile <profile_name>

direct-tunnel check-iups-service

end
```

Notes:
• An IMEI profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the Operator Policy chapter in this guide.
• Direct tunnel is now allowed for calls within the IMEI range associated with the IMEI profile but a direct tunnel will only setup if also allowed on the RNC.

Enabling Direct Tunnel to Specific RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service.
Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC.
By default, direct tunnel functionality is enabled for all RNCs.

Example Configuration

The following is an example of the commands used to ensure that restrictive configuration is removed and direct tunnel for the RNC is enabled:

```plaintext
config

context <ctx_name>

iups-service <service_name>

rnc id <rnc_id>
```
default direct-tunnel
end

Notes:
- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the Command Line Interface Reference.

Verifying the SGSN Direct Tunnel Configuration

Enabling the setup of a GTP-U direct tunnel on the SGSN is not a straightforward task. It is controlled by an operator policy with related configuration in multiple components. Each of these component configurations must be checked to ensure that the direct tunnel configuration has been completed. You need to begin with the operator policy itself.

Verifying the Operator Policy Configuration

For the feature to be enabled, it must be allowed in the call-control profile and the call-control profile must be associated with an operator policy. As well, either an APN profile or an IMEI profile must have been created/configured and associated with the same operator policy. Use the following command to display and verify the operator policy and the association of the required profiles:

```
show operator-policy full name <policy_name>
```

The output of this command displays profiles associated with the operator policy.

```
[local]asr5x00# show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name : ccprofile1
  Validity : Valid
IMEI Range 99999999999990 to 999999999999995
  IMEI Profile Name : imeiprofile1
  Validity : Invalid
APN NI homers1
  APN Profile Name : apnprofile1
  Validity : Valid
APN NI visitors2
  APN Profile Name : apnprofile2
  Validity : Invalid
```

Notes:
Direct Tunnel Configuration

- Validity refers to the status of the profile. Valid indicates that profile has been created and associated with the policy. Invalid means only the name of the profile has been associated with the policy.
- The operator policy itself will only be valid if one or more IMSI ranges have been associated with it - refer to the Operator Policy chapter, in this guide, for details.

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

```
show call-control-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

Call Control Profile Name = ccprofile1

```
... Re-Authentication : Disabled
Direct Tunnel       : Not Restricted
GTPU Fast Path     : Disabled
```

Verifying the APN Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the APN profile:

```
show apn-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified APN profile.

Call Control Profile Name = apnprofile1

```
... IP Source Validation : Disabled
Direct Tunnel          : Not Restricted
Service Restriction for Access Type > UMTS : Disabled
```

Verifying the IMEI Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the IMEI profile:

```
show imei-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified IMEI profile.

IMEI Profile Name = imeiprofile1
Black List : Disabled
GGSN Selection : Disabled
Direct Tunnel : Enabled

Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

```
show iups-service name <service_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name : iups1
...
Available RNC:
  Rnc-Id : 1
  Direct Tunnel : Not Restricted
```

Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the S4 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the MME over the S3 interface. The MME forwards the FTEID to the S-GW over the S11 interfaces. The S-GW responds with it’s own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

Use the following example to configure this feature:

```
configure
  context <egress_context_name> -noconfirm
    interface <s12_interface_name>
      ip address <s12_ipv4_address_primary>
      ip address <s12_ipv4_address_secondary>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s12_interface_name> <egress_context_name>
```

Cisco ASR 5x00 Serving Gateway Administration Guide
exit
context <egress_context_name> -noconfirm
gtpu-service <s12_gtpu_egress_service_name>
   bind ipv4-address <s12_interface_ip_address>
   exit
gtp-service <s12_egtp_egress_service_name>
   interface-type interface-sgw-egress
   validation-mode default
   associate gtpu-service <s12_gtpu_egress_service_name>
gtpc bind address <s12_interface_ip_address>
   exit
sgw-service <sgw_service_name> -noconfirm
   associate egress,proto gtp egress-context <egress_context_name> egtp-service <s12_egtp_egress_service_name>
end

Notes:

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the `ipv6 address` command.
Appendix B
S-GW Event Reporting

This appendix describes the record content and trigger mechanisms for S-GW event reporting. When enabled the S-GW write a record of session events and sends the resulting event files to an external file server for processing. Each event is sent to the server within 60 seconds of its occurrence.

The following topics are covered in this appendix:

- Event Record Triggers
- Event Record Elements
- Active-to-Idle Transitions
- 3GPP 29.274 Cause Codes
Event Record Triggers

When properly configured, the S-GW creates and sends a record in CSV format as the session events listed below occur:

- ID 1: Session Creation
- ID 2: Session Deletion
- ID 3: Bearer Creation
- ID 4: Bearer Deletion
- ID 5: Bearer Modification
  - suppress intra-system handover
  - configurable enable active to idle transition event reporting
- ID 6: Bearer Update

The following guidelines apply to the above session events:

- A session refers to a PDN connection and the default bearer associated with it.
- Bearer events refer to dedicated bearers that have been created/deleted/updated/modified.
- Bearer modifications that are intra-S-GW and intra-MME are not be reported.
- Bearers and sessions that fail to setup are reported once in a session/bearer creation record with the result code set to failure.
Event Record Elements

Each event record includes the information documented in the table below in comma separated value (CSV) ASCII format. The elements are listed in the order in which they will appear. All record elements are not available for all event triggers. If a record element cannot be populated due to incomplete information, the element is omitted and the comma separation maintained.

The following guidelines apply to record elements:

- Byte/packet counters shall not be sent in session or bearer creation messages
- Byte/packet counters include packets and bytes sent or received since the last record created for that session or bearer.
- The S-GW will attempt to populate all record elements. Values that are unavailable will not be populated.

<table>
<thead>
<tr>
<th>Event Number</th>
<th>Description</th>
<th>Format</th>
<th>Size (bytes)</th>
<th>Applicable Event Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Event identity (ID 1 – ID 6)</td>
<td>Integer [1-6]</td>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Event Result (3GPP 29.274 Cause Code)</td>
<td>Integer [1-255]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>IMSI</td>
<td>Integer (15 digits)</td>
<td>15</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>IMEISV</td>
<td>Integer (16 digits)</td>
<td>16</td>
<td>All</td>
</tr>
<tr>
<td>5</td>
<td>Start Time (GMT)</td>
<td>MM/DD/YYYY-HH:MM:SS:MS(millisecond accuracy)</td>
<td>18</td>
<td>All</td>
</tr>
<tr>
<td>6</td>
<td>End Time (GMT)</td>
<td>MM/DD/YYYY-HH:MM:SS:MS(millisecond accuracy)</td>
<td>18</td>
<td>2, 4</td>
</tr>
<tr>
<td>7</td>
<td>Protocol (GTPv2)</td>
<td>String</td>
<td>5</td>
<td>All</td>
</tr>
<tr>
<td>8</td>
<td>Disconnect code (ASR 5x00)</td>
<td>Integer [1-999]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>9</td>
<td>Trigger Event (3GPP 29.274 request cause code)</td>
<td>Integer [1-15]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>10</td>
<td>Origination Node</td>
<td>String (CLLI)</td>
<td>10</td>
<td>All</td>
</tr>
<tr>
<td>11</td>
<td>Origination Node Type</td>
<td>String (SGW</td>
<td>HSGW</td>
<td>PGW</td>
</tr>
<tr>
<td>12</td>
<td>EPS Bearer ID(Default)</td>
<td>Integer [0-15]</td>
<td>1 or 2</td>
<td>All</td>
</tr>
<tr>
<td>13</td>
<td>APN Name</td>
<td>String</td>
<td>34 to 255</td>
<td>All</td>
</tr>
<tr>
<td>14</td>
<td>PGW IP Address</td>
<td>IPv4 or IPv6 address</td>
<td>7 to 55</td>
<td>All</td>
</tr>
<tr>
<td>15</td>
<td>UE IPv4 Address</td>
<td>IPv4 address</td>
<td>7 to 15</td>
<td>All</td>
</tr>
<tr>
<td>16</td>
<td>UE IPv6 Address</td>
<td>IPv6 address</td>
<td>3 to 55</td>
<td>All</td>
</tr>
<tr>
<td>Event Number</td>
<td>Description</td>
<td>Format</td>
<td>Size (bytes)</td>
<td>Applicable Event Numbers</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------</td>
<td>-------------------------------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Uplink AMBR</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>18</td>
<td>Downlink AMBR</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>19</td>
<td>TAI - MCC/MNC/TAC</td>
<td>String (MCC;MNC;TAC)</td>
<td>14</td>
<td>All</td>
</tr>
<tr>
<td>20</td>
<td>Cell ID (ECI)</td>
<td>String (28 bits)</td>
<td>8</td>
<td>All</td>
</tr>
<tr>
<td>21</td>
<td>EPS Bearer ID (dedicated)</td>
<td>Integer (0-15)</td>
<td>1 or 2</td>
<td>21</td>
</tr>
<tr>
<td>22</td>
<td>Result Code (success/fail)</td>
<td>0=fail 1=success</td>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>23</td>
<td>QCI</td>
<td>Integer[1-255]</td>
<td>1 to 3</td>
<td>All</td>
</tr>
<tr>
<td>24</td>
<td>Uplink MBR (bps)</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>25</td>
<td>Downlink MBR (bps)</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>26</td>
<td>Uplink GBR (bps)</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>27</td>
<td>Downlink GBR (bps)</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>28</td>
<td>Downlink Packets Sent (interval)</td>
<td>Integer (0-4000000000)</td>
<td>1 to 10</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>29</td>
<td>Downlink Bytes Sent (interval)</td>
<td>Integer (0-5000000000000)</td>
<td>1 to 12</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>30</td>
<td>Downlink Packets Dropped (interval)</td>
<td>Integer (0-5000000000000)</td>
<td>1 to 12</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>31</td>
<td>Uplink Packets Sent (interval)</td>
<td>Integer (0-5000000000000)</td>
<td>1 to 12</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>32</td>
<td>Uplink Bytes Sent (interval)</td>
<td>Integer (0-5000000000000)</td>
<td>1 to 12</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>33</td>
<td>Uplink Packets Dropped (interval)</td>
<td>Integer (0-400000000000)</td>
<td>1 to 10</td>
<td>2, 4, 5, 6</td>
</tr>
<tr>
<td>34</td>
<td>MME S11 IP Address</td>
<td>IPv4 or IPv6 address</td>
<td>7 to 55</td>
<td>All</td>
</tr>
<tr>
<td>35</td>
<td>S1u IP Address of eNodeB</td>
<td>IPv4 or IPv6 address</td>
<td>7 to 55</td>
<td>All</td>
</tr>
</tbody>
</table>
**Active-to-Idle Transitions**

This figure and table below describes how active-to-idle transitions generate event records.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UE becomes Active (via UE or NW initiated service request)</td>
</tr>
<tr>
<td>2</td>
<td>Session becomes idle.</td>
</tr>
<tr>
<td>3</td>
<td>S-GW acknowledges idle session.</td>
</tr>
</tbody>
</table>
| 4    | Bearer modification event record is created, with the following fields:  
  • Start Time: Use the start time of the idle-to-active transition  
  • End Time: Use the timestamp of the idle time  
  • Bytes up/Bytes down: Amount of data sent between transitions  
  • Packets up/Packets down: Number of packets sent between transitions |
3GPP 29.274 Cause Codes

The following table lists some of the most commonly implemented cause codes identified in Record Element 2 – Event Result.

Table 11. 3GPP 29.274 Cause Codes

<table>
<thead>
<tr>
<th>Cause Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request</strong></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Local Detach</td>
</tr>
<tr>
<td>3</td>
<td>Complete</td>
</tr>
<tr>
<td>4</td>
<td>RAT changed from 3GPP to Non-3GPP</td>
</tr>
<tr>
<td>5</td>
<td>ISR deactivation</td>
</tr>
<tr>
<td>6</td>
<td>Error Indication received from RNC/eNodeB</td>
</tr>
<tr>
<td><strong>Accept</strong></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Request accepted</td>
</tr>
<tr>
<td>17</td>
<td>Request accepted partially</td>
</tr>
<tr>
<td>18</td>
<td>New PDN type due to network preference</td>
</tr>
<tr>
<td>19</td>
<td>New PDN type due to single address bearer only</td>
</tr>
<tr>
<td><strong>Reject</strong></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Context Not Found</td>
</tr>
<tr>
<td>65</td>
<td>Invalid Message Format</td>
</tr>
<tr>
<td>66</td>
<td>Version not supported by nextpeer</td>
</tr>
<tr>
<td>67</td>
<td>Invalid length</td>
</tr>
<tr>
<td>68</td>
<td>Service not supported</td>
</tr>
<tr>
<td>69</td>
<td>Mandatory IE incorrect</td>
</tr>
<tr>
<td>70</td>
<td>Mandatory IE missing</td>
</tr>
<tr>
<td>71</td>
<td>Reserved</td>
</tr>
<tr>
<td>72</td>
<td>System failure</td>
</tr>
<tr>
<td>73</td>
<td>No resources available</td>
</tr>
<tr>
<td>74</td>
<td>Semantic error in the TFT operation</td>
</tr>
<tr>
<td>75</td>
<td>Syntactic error in the TFT operation</td>
</tr>
<tr>
<td>76</td>
<td>Semantic errors in packet filter(s)</td>
</tr>
<tr>
<td>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>77</td>
<td>Syntactic errors in packet filter(s)</td>
</tr>
<tr>
<td>78</td>
<td>Missing or unknown APN</td>
</tr>
<tr>
<td>79</td>
<td>Unexpected repeated IE</td>
</tr>
<tr>
<td>80</td>
<td>GRE key not found</td>
</tr>
<tr>
<td>81</td>
<td>Relocation failure</td>
</tr>
<tr>
<td>82</td>
<td>Denied in RAT</td>
</tr>
<tr>
<td>83</td>
<td>Preferred PDN type not supported</td>
</tr>
<tr>
<td>84</td>
<td>All dynamic addresses are occupied</td>
</tr>
<tr>
<td>85</td>
<td>UE context without TFT already activated</td>
</tr>
<tr>
<td>86</td>
<td>Protocol type not supported</td>
</tr>
<tr>
<td>87</td>
<td>UE not responding</td>
</tr>
<tr>
<td>88</td>
<td>UE refuses</td>
</tr>
<tr>
<td>89</td>
<td>Service denied</td>
</tr>
<tr>
<td>90</td>
<td>Unable to page UE</td>
</tr>
<tr>
<td>91</td>
<td>No memory available</td>
</tr>
<tr>
<td>92</td>
<td>User authentication failed</td>
</tr>
<tr>
<td>93</td>
<td>APN access denied - no subscription</td>
</tr>
<tr>
<td>94</td>
<td>Request rejected</td>
</tr>
<tr>
<td>95</td>
<td>P-TMSI Signature mismatch</td>
</tr>
<tr>
<td>96</td>
<td>IMSI not known</td>
</tr>
<tr>
<td>97</td>
<td>Semantic error in the TAD operation</td>
</tr>
<tr>
<td>98</td>
<td>Syntactic error in the TAD operation</td>
</tr>
<tr>
<td>99</td>
<td>Reserved Message Value Received</td>
</tr>
<tr>
<td>100</td>
<td>Remote peer not responding</td>
</tr>
<tr>
<td>101</td>
<td>Collision with network initiated request</td>
</tr>
<tr>
<td>102</td>
<td>Unable to page UE due to Suspension</td>
</tr>
<tr>
<td>103</td>
<td>Conditional IE missing</td>
</tr>
<tr>
<td>104</td>
<td>APN Restriction type Incompatible with currently active PDN connection</td>
</tr>
<tr>
<td>105</td>
<td>Invalid overall length of the triggered response message and a piggybacked initial message</td>
</tr>
<tr>
<td>106</td>
<td>Data forwarding not supported</td>
</tr>
<tr>
<td>107</td>
<td>Invalid reply from remote peer</td>
</tr>
<tr>
<td>116 to 239</td>
<td>Spare. This value range is reserved for Cause values in rejection response message.</td>
</tr>
</tbody>
</table>
### Cause Codes

<table>
<thead>
<tr>
<th>Cause Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sub-Causes</strong></td>
<td></td>
</tr>
<tr>
<td>NO_INFORMATION</td>
<td></td>
</tr>
<tr>
<td>ABORTED_BY_SESSION_DELETION</td>
<td></td>
</tr>
<tr>
<td>NO_RESPONSE_FROM_MME</td>
<td></td>
</tr>
<tr>
<td>INTERNALLY_TRIGGERED</td>
<td></td>
</tr>
<tr>
<td>BEARERS_IN_MULTIPLE_PDN_CONNECTIONS</td>
<td></td>
</tr>
<tr>
<td>EXPECTED_BEARERS_MISSING_IN_MESSAGE</td>
<td></td>
</tr>
<tr>
<td>UNEXPECTED_BEARERS_PRESENT_IN_MESSAGE</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C
Rf Interface Support

This chapter provides an overview of the Diameter Rf interface and describes how to configure the Rf interface. Rf interface support is available on the Cisco system running StarOS 10.0 or later releases for the following products:

- Gateway GPRS Support Node (GGSN)
- HRPD Serving Gateway (HSGW)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)
- Serving Gateway (S-GW)

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

This chapter describes the following topics:

- Introduction
- Features and Terminology
- How it Works
- Configuring Rf Interface Support
Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, S-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/HRPD offline charging is based on 3GPP TS 32.299 V8.6.0, 3GPP TS 32.251 V8.5.0 and other 3GPP specifications. The Rf interface specification for IP Multimedia Subsystem (IMS) offline charging is based on 3GPP TS 32.260 V8.12.0 and 3GPP TS 32.299 V8.13.0.

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows the CTF (Diameter client) to issue offline charging events to a Charging Data Function (CDF) (Diameter server). The charging events can either be one-time events or may be session-based.

The system provides a Diameter Offline Charging Application that can be used by deployed applications to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on chassis to act as CTF to a configured CDF.

In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

The CCF with the CDF and Charging Gateway Function (CGF) will be implemented as part of the core network application. The CDF function collects and aggregates Rf messages from the various CTFs and creates CDRs. The CGF collects CDRs from the CDFs and generates charging data record files for the data mediation/billing system for billing.

Offline Charging Architecture

The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, S-GW, HSGW, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).
Figure 18. Charging Architecture

The following figure shows the Rf interface between CTF and CDF.

Figure 19. Logical Offline Charging Architecture

The Rf offline charging architecture mainly consists of three network elements — CCF, CTF and Diameter Dynamic Routing Agent (DRA).
**Charging Collection Function**

The CCF implements the CDF and CGF. The CCF will serve as the Diameter Server for the Rf interface. All network elements supporting the CTF function should establish a Diameter based Rf Interface over TCP connections to the DRA. The DRA function will establish Rf Interface connection over TCP connections to the CCF.

The CCF is primarily responsible for receipt of all accounting information over the defined interface and the generation of CDR (aka UDRs and FDRs) records that are in local storage. This data is then transferred to the billing system using other interfaces. The CCF is also responsible for ensuring that the format of such CDRs is consistent with the billing system requirements. The CDF function within the CCF generates and CGF transfers the CDRs to the billing system.

The CDF function in the CCF is responsible for collecting the charging information and passing it on to the appropriate CGF via the GTP' based interface per 3GPP standards. The CGF passes CDR files to billing mediation via SCP.

**Charging Trigger Function**

The CTF will generate CDR records and passes it onto CCF. When a P-GW service is configured as CTF, then it will generate Flow Data Record (FDR) information as indicated via the PCRF. The P-GW generates Rf messages on a per PDN session basis. There are no per UE or per bearer charging messages generated by the P-GW.

The service data flows within IP-CAN bearer data traffic is categorized based on a combination of multiple key fields (Rating Group, Rating Group and Service-Identifier). Each Service-Data-Container captures single bi-directional flow or a group of single bidirectional flows as defined by Rating Group or Rating Group and Service-Identifier.

Similarly, when S-GW service is configured as CTF, it will generate Usage Data Record (UDR) information configurable on a per PDN basis QCI basis. Note that per bearer charging and per UE charging are no longer required. The Diameter charging sessions to the CCF are setup on a per PDN connection basis.

**Dynamic Routing Agent**

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a CCF to the CTF.

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

**License Requirements**

The Rf interface support is a licensed Cisco feature. A separate feature license 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.

**Supported Standards**

Rf interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)
Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in 3GPP TS 32.240.

Basic Principles

The Diameter client and server must implement the basic functionality of Diameter accounting, as defined by the RFC 3588 — Diameter Base Protocol.

For offline charging, the CTF implements the accounting state machine as described in RFC 3588. The CDF server implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588, i.e. there is no order in which the server expects to receive the accounting information.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the following ACR event types:

Table 12. Rf ACR Event Types

<table>
<thead>
<tr>
<th>Request</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>START</td>
<td>Starts an accounting session</td>
</tr>
<tr>
<td>INTERIM</td>
<td>Updates an accounting session</td>
</tr>
<tr>
<td>STOP</td>
<td>Stops an accounting session</td>
</tr>
<tr>
<td>EVENT</td>
<td>Indicates a one-time accounting event</td>
</tr>
</tbody>
</table>

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.

Important: The ACR Event Type "EVENT" is supported in Rf CDRs only in the case of IMS specific Rf implementation.

The following table describes all possible ACRs that might be sent from the IMS nodes i.e. a P-CSCF and S-CSCF.

Table 13. Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

<table>
<thead>
<tr>
<th>Diameter Message</th>
<th>Triggering SIP Method/ISUP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR [Start]</td>
<td>SIP 200 OK acknowledging an initial SIP INVITE</td>
</tr>
</tbody>
</table>
### Diameter Message | Triggering SIP Method/ISUP Message
---|---
ISUP:ANM (applicable for the MGCF)
ACR [Interim] | SIP 200 OK acknowledging a SIP
| RE-INVITE or SIP UPDATE [e.g. change in media components]
| Expiration of AVP [Acct-Interim-Interval]
| SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE
ACR [Stop] | SIP BYE message (both normal and abnormal session termination cases)
| ISUP:REL (applicable for the MGCF)
ACR [Event] | SIP 200 OK acknowledging non-session related SIP messages, which are:
| • SIP NOTIFY
| • SIP MESSAGE
| • SIP REGISTER
| • SIP SUBSCRIBE
| • SIP PUBLISH
| SIP 200 OK acknowledging an initial SIP INVITE
| SIP 202 Accepted acknowledging a SIP REFER or any other method
| SIP Final Response 2xx (except SIP 200 OK)
| SIP Final/Redirection Response 3xx
| SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up
| SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
| SIP CANCEL, indicating abortion of a SIP session set-up

### Event Based Charging
In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

In this scenario, CTF asks the CDF to store event related charging data.

### Session Based Charging
Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

In this scenario, CTF asks the CDF to store session related charging data.
Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based.

In order for the application to be compliant with the specification, state machines should be implemented at some level within the implementation.

Diameter Base supports the following Rf message commands that can be used within the application.

<table>
<thead>
<tr>
<th>Table 14. Diameter Rf Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Name</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Accounting-Request</td>
</tr>
<tr>
<td>Accounting-Answer</td>
</tr>
</tbody>
</table>

There are a series of other Diameter messages exchanged to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other.
  - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
  - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.
- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is considered to be down.

  **Important:** DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- Device Watchdog Answer (DWA): This is the response to the DWR message from the server. This is used to monitor the connection state.
- Disconnect Peer Request (DPR): This message is sent to the peer to inform to shutdown the connection. There is no capability currently to send the message to the Diameter server.
- Disconnect Peer Answer (DPA): This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to “DO NOT WANT TO TALK TO YOU” state and there is no way to get the connection back except for reconfiguring the peer again.

  A timeout value for retrying the disconnected peer must be provided.
**Timer Expiry Behavior**

Upon establishing the Diameter connection, an accounting interim timer (AII) is used to indicate the expiration of a Diameter accounting session, and is configurable at the CTF. The CTF indicates the timer value in the ACR-Start, in the Acct-Interim-Interval AVP. The CDF responds with its own AII value (through the DRA), which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. An instance of the AII timer is started in the CCF at the beginning of the accounting session, reset on the receipt of an ACR-Interim and stopped on the receipt of the ACR-Stop. After expiration of the AII timer, ACR INTERIM message will be generated and the timer will be reset and the accounting session will be continued.

**Rf Interface Failures/Error Conditions**

The current architecture allows for primary and secondary connections or Active-Active connections for each network element with the CDF elements.

**DRA/CCF Connection Failure**

When the connection towards one of the primary/Active DRAs in CCF becomes unavailable, the CTF picks the Secondary/Active IP address and begins to use that as a Primary.

If no DRA (and/or the CCF) is reachable, the network element must buffer the generated accounting data in non-volatile memory. Once the DRA connection is up, all accounting messages must be pulled by the CDF through offline file transfer.

**No Reply from CCF**

In case the CTF/DRA does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the CTF/DRA sends the ACRs to the secondary/alternate DRA/CCF.

**Detection of Message Duplication**

The Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in RFC 3588.

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

**CCF Detected Failure**

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behavior of the CCF is operator configurable.
Rf-Gy Synchronization Enhancements

Both Rf (OFCS) and Gy (OCS) interfaces are used for reporting subscriber usage and billing. Since each interface independently updates the subscriber usage, there are potential scenarios where the reported information is not identical. Apart from Quota enforcement, OCS is utilized for Real Time Reporting (RTR), which provides a way to the user to track the current usage and also get notifications when a certain threshold is hit.

In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers “Service Data Volume Limit” and “Service Data Time Limit”.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U. In 16.0 and later releases, the containers are closed only after receiving CCA-U successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

For more information on the command associated with this feature, see the Accounting Policy Configuration Mode Commands chapter of the Command Line Interface Reference.
How it Works

This section describes how offline charging for subscribers works with Rf interface support in GPRS/eHRPD/LTE/IMS networks.

The following figure and table explain the transactions that are required on the Diameter Rf interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

![Rf Call Flow for Event Based Charging](image)

**Table 15. Rf Call Flow Description for Event Based Charging**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The network element (CTF) receives indication that service has been used/delivered.</td>
</tr>
<tr>
<td>2</td>
<td>The CTF (acting as Diameter client) sends Accounting-Request (ACR) with Accounting-Record-Type AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as Diameter server).</td>
</tr>
<tr>
<td>3</td>
<td>The CDF receives the relevant service charging parameters and processes accounting request.</td>
</tr>
<tr>
<td>4</td>
<td>The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.</td>
</tr>
</tbody>
</table>

The following figure and table explain the simple Rf call flow for session based charging.
Figure 21. Rf Call Flow for Session Based Charging

Table 16. Rf Call Flow Description for Session Based Charging

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The CTF receives a service request. The service request may be initiated either by the user or the other network element.</td>
</tr>
<tr>
<td>2</td>
<td>In order to start accounting session, the CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to START_RECORD to the CDF.</td>
</tr>
<tr>
<td>3</td>
<td>The session is initiated and the CDF opens a CDR for the current session.</td>
</tr>
<tr>
<td>4</td>
<td>The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.</td>
</tr>
<tr>
<td>5</td>
<td>When either AII elapses or charging condition changes are recognized at CTF, the CTF sends an Accounting-Request (ACR) with Accounting-Record-Type AVP set to INTERIM_RECORD to the CDF.</td>
</tr>
<tr>
<td>6</td>
<td>The CDF updates the CDR in question.</td>
</tr>
<tr>
<td>7</td>
<td>The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.</td>
</tr>
<tr>
<td>8</td>
<td>The service is terminated.</td>
</tr>
<tr>
<td>9</td>
<td>The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.</td>
</tr>
<tr>
<td>10</td>
<td>The CDF updates the CDR accordingly and closes the CDR.</td>
</tr>
<tr>
<td>11</td>
<td>The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.</td>
</tr>
</tbody>
</table>
Configuring Rf Interface Support

To configure Rf interface support:

1. Configure the core network service as described in this Administration Guide.
2. Enable Active Charging Service (ACS) and create ACS as described in the Enhanced Charging Services Administration Guide.

**Important:** The procedures in this section assume that you have installed and configured your chassis including the ECS installation and configuration as described in the Enhanced Charging Services Administration Guide.

3. Enable Rf accounting in ACS as described in the Enabling Rf Interface in Active Charging Service section.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN P-GW Rf Interface Support
   - Configuring HSGW Rf Interface Support
   - Configuring P-CSCFS-CSCF Rf Interface Support
   - Configuring S-GW Rf Interface Support
5. 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.

**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

Enabling Rf Interface in Active Charging Service

To enable the billing record generation and Rf accounting, use the following configuration:

```bash
configure

active-charging service <service_name>

rulebase <rulebase_name>

billing-records rf

active-charging rf { rating-group-override | service-id-override }

end
```

Notes:
Prior to creating the Active Charging Service (ACS), the `require active-charging` command should be configured to enable ACS functionality.

The `billing-records rf` command configures RF record type of billing to be performed for subscriber sessions. RF accounting is applicable only for dynamic and predefined ACS rules.

For more information on the rules and its configuration, refer to the ACS Charging Action Configuration Mode Commands chapter in the Command Line Interface Reference.

The `active-charging rf` command is used to enforce a specific rating group/service identifier on all PCC rules, predefined ACS rules, and static ACS rules for RF-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

For more information on this command, refer to the ACS Rulebase Configuration Mode Commands chapter in the Command Line Interface Reference.

### Configuring GGSN / P-GW RF Interface Support

To configure the standard RF interface support for GGSN/P-GW, use the following configuration:

```bash
configure
  context <context_name>
    apn <apn_name>
      associate accounting-policy <policy_name>
    exit
  policy accounting <policy_name>
    accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change } action { interim | stop-start }
    accounting-keys qci
    accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
    cc profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } | serving-nodes num | tariff time1 min hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } }
    max-containers { containers | fill-buffer }
  end
```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting levels/policies/modes/event triggers, refer to the Accounting Policy Configuration Mode Commands chapter in the Command Line Interface Reference.
• Depending on the triggers configured, the containers will either be cached or released. In the case of GGSN/P-GW, the containers will be cached when the event trigger is one of the following:
  • QOS_CHANGE
  • FLOW_INFORMATION_CHANGE
  • LOCATION_CHANGE
  • SERVING_NODE_CHANGE
  • SERVICE_IDLE
  • SERVICE_DATA_VOLUME_LIMIT
  • SERVICE_DATA_TIME_LIMIT
  • IP_FLOW_TERMINATION
  • TARIFF_CHANGE
If the event trigger is one of the following, the containers will be released:
  • VOLUME_LIMIT
  • TIME_LIMIT
  • RAT_CHANGE
  • TIMEZONE_CHANGE
  • PLMN_CHANGE

---

**Important:** Currently, SDF and flow level accounting are supported in P-GW.

The following assumptions guide the behavior of P-GW, GGSN, S-GW, HSGW and CCF for Change-Condition triggers:

• Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).

• All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target S-GW/HSGW/Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

• When multiple change conditions occur, the precedence of reporting change conditions is as follows for S-GW and HSGW only:
  • Normal/Abnormal Release (Stop)
  • Management Intervention (Stop)
  • RAT Change
  • UE Timezone Change
  • Serving Node PLMN Change
  • Max Number of Changes in Charging conditions
  • Volume Limit
  • Time Limit
- Service Data Volume Limit
- Service Data Time Limit
- Service Idled out
- Serving Node Change
- User Location Change
- QoS Change

Even though Accounting Interim Interval (AII) timer expiration trigger is not a Change-Condition, AII timer trigger has the lowest precedence among the above triggers. The AII timer will be reset when a ACR Interim for any of the above triggers is sent.

For P-GW and GGSN, Service-Data-Container grouped AVP has the Change-Condition AVP as multiple occurrence AVP sending all the Change-Conditions that occur at a point in time, so the above precedence is not needed.

Table 17. P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/E-HRPD/GGSN

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>CC Level Population</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partial FDR</td>
<td>Final FDR</td>
</tr>
<tr>
<td>Stop</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>CC Level Population</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partial FDR</td>
<td>Final FDR</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>QoS-Change</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Interim</td>
<td>Volume Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Interim</td>
<td>Time Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger.

For PDN/IP Session Volume Limit. The Volume Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>CC Level Population</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Serving Node Change</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>Interim</td>
<td>Serving Node PLMN Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>User Location Change</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>Interim</td>
<td>RAT Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Interim</td>
<td>UE Timezone Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Tariff Time Change</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.

This is BSID Change in eHRPD. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.

This is not applicable for eHRPD.

Triggered when Tariff Time changes. Tariff Time Change requires an online charging side change. The implementation of this Change Condition is dependent on implementation of Online Charging update.
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>CC Level Population</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Service Idled Out</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Service Data Volume Limit</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Service Data Time Limit</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>
## Configuring RF Interface Support

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>CC Level Population</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Stop</td>
<td>Management Intervention</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>
### Configuring HSGW Rf Interface Support

To configure HSGW Rf interface support, use the following configuration:

```bash
configure

context <context_name>

hsgw-service <service_name>

    associate accounting-policy <policy_name>

    exit

exit

p

olicy accounting <policy_name>

    accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change } action { interim | stop-start }

    accounting-keys qci

    accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }

    cc profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } | serving-nodes num | tariff time1 min hrs | time2 min hrs...time4 min hrs | volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } }

    max-containers { containers | fill-buffer }

    exit

end
```
Notes:

- The policy can be configured in any context.
- For information on configuring accounting policies/modes/event triggers, refer to the *Accounting Policy Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For an HSGW session, the containers will be cached when the event trigger is one of the following:
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
  - SERVING_NODE_CHANGE

Similarly, if the event trigger is one of the following, the containers will be released:

- VOLUME_LIMIT
- TIME_LIMIT

Table 18. HSGW and CCF Behavior for Change-Condition in ACR[Stop] and ACR[Interim] for eHRPD

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting(PDN Session based accounting)</th>
<th>EPS bearer level reporting(PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>YE S</td>
<td>Normal Release for all bearers</td>
</tr>
</tbody>
</table>

When PDN session/PDN Session per QCI is closed, C-C in both level will have Normal Release.
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partia l UDR</td>
<td>Fina l UDR</td>
<td>C-C on PS Information Level</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>Abnormal Release</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Abnormal Release</td>
<td>YES NO NO N/A</td>
<td>Abnormal Release for the specific bearer that is released. N/A N/A</td>
<td>This is for FFS. This is applicable for per PDN Session based accounting only. This is when a bearer is closed abnormally in a PDN Session accounting charging session. TDV is populated and the container is added to the record. The container for this change condition will be cached by the HSGW and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.</td>
<td></td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>QoS-Change</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Volume Limit</td>
<td>YES</td>
<td>YES NO Volume Limit for all bearers</td>
<td>Volume Limit for all bearers</td>
<td>Volume Limit for all bearers</td>
</tr>
</tbody>
</table>

The Volume Limit is configured as part of the Charging profile and the Charging Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to HSGW through various interfaces. The charging profile will be provisioned in the HSS.
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim</td>
<td>Time Limit</td>
<td>YES</td>
<td>YES NO</td>
<td>Time Limit for all bearers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions ).</td>
<td>Serving Node Change</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>N/A</td>
<td>Serving Node PLMN Change</td>
<td>N/A N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>User Location Change</td>
<td>YES NO NO N/A</td>
<td>ULI Change added to TDV for all bearers, ACR sent when MaxCCC is reached (if MaxCC is configured)</td>
<td>N/A</td>
<td>ULI Change added to TDV, ACR sent when MaxCCC is reached (if MaxCC is configured)</td>
</tr>
<tr>
<td>N/A</td>
<td>RAT Change</td>
<td>N/A N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>UE Timezone Change</td>
<td>N/A N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Tariff Time Change</td>
<td>N/A N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Configuring Rf Interface Support

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partial UDR</td>
<td>Final UDR</td>
<td>C-C on PS-Information Level</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Idled Out</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Specific Unit Limit</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Max Number of Changes in Charging</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>

N/A  Management Intervention  N/A  N/A  N/A  N/A  N/A  N/A  Management intervention will close the PDN session from P-GW.
### Configuring RF Interface Support

**Cisco ASR 5x00 Serving Gateway Administration Guide**

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim</td>
<td>-</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PartiaL UDR</td>
<td>Final UDR</td>
<td>C-C on PDN Information Level</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C-C on PDN Level</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC on PDN Information Level</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC on TDV Level</td>
<td>N/A</td>
</tr>
</tbody>
</table>

This is included here to indicate that an ACR[Interim] due to AII timer will contain one or more populated TDVs for a/all bearer/s, but Change-Condition AVP will NOT be populated.

---

**Configuring P-CSCF/S-CSCF RF Interface Support**

To configure P-CSCF/S-CSCF RF interface support, use the following configuration:

```plaintext
configure
c
context vpn
d
  aaa group default
d
    diameter authentication dictionary aaa-custom8
d
    diameter accounting dictionary aaa-custom2
d
    diameter accounting endpoint <endpoint_name>
d
    diameter accounting server <server_name> priority <priority>
exit
d
    diameter endpoint <endpoint_name>

    origin realm <realm_name>

    use-proxy
```
Enabling Charging for SIP Methods

To enable the charging for all Session Initiation Protocol (SIP) methods in CSCF, use the following configuration:

```
configure
  context vpn
    cscf service pcscf
    charging
end
```

**Important:** Please note that charging is disabled by default.

To enable the charging for all SIP methods except REGISTER, use the following configuration:

```
configure
  context vpn
    cscf service pcscf
    charging
    exclude register
end
```

To enable the charging only for INVITE SIP method, use the following configuration:

```
configure
  context vpn
    cscf service pcscf
    no charging
    exclude invite
```
Configuring S-GW Rf Interface Support

To configure S-GW Rf interface support, use the following configuration:

```
configure
  context <context_name>
    sgw-service <service_name>
      associate accounting-policy <policy_name>
    exit
  exit
  policy accounting <policy_name>
    accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change } action { interim | stop-start }
    accounting-keys qci
    accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
    cc profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets | uplink octets } | total octets | uplink octets | downlink octets } | serving-nodes num | tariff { time1 min hrs | time2 min hrs...time4 min hrs | volume { downlink octets | uplink octets } | total octets | uplink octets | downlink octets } }
    max-containers { containers | fill-buffer }
  exit
end
```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting policies/modes/event triggers, refer to the Accounting Policy Configuration Mode Commands chapter in the Command Line Interface Reference.
- For an S-GW session, the containers will be cached when the event trigger is one of the following:
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
- Similarly, if the event trigger is one of the following, the containers will be released:
- VOLUME_LIMIT
- TIME_LIMIT
- PLMN_CHANGE
- TIMEZONE_CHANGE

Table 19. S-GW and CCF Behavior for Change-Condition in ACR[Stop] and ACR[Interim] for LTE

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partia l UDR</td>
<td>Final UDR</td>
<td>C-C on PS-Information Level</td>
</tr>
<tr>
<td>Stop</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>Normal Release</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>Normal Release</td>
<td>YES NO NO N/A</td>
<td>Normal Release for the specific bearer that is released</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES NO YES</td>
<td>Abnormal Release</td>
<td>Abnormal Release for all bearers</td>
<td>Abnormal Release</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>QoS-Change</td>
<td>YES</td>
<td>NO</td>
<td>N/A</td>
<td>QoS-Change - added to TDV for the bearer that is affected by this trigger.</td>
<td>[The container for this change condition will be cached by the S-GW and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or AII trigger (Interim) trigger. For APN-AMBR change, containers (TDVs) for all existing non-GBR bearers will be cached.]</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Volume Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Volume Limit for all bearers Volume Limit for all bearers Volume Limit</td>
</tr>
</tbody>
</table>

Interim Volume Limit

On a per PDN Session basis for per PDN accounting. On a per PDN per QCI basis for the per PDN per QCI accounting. The Volume Limit is configured as part of the Charging profile and the Charging Characteristic AVP will carry the charging profile identifier that is passed from HSS to S-GW via MME. The charging profile value can be configured in the HSS on a per APN basis.
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partia l UDR</td>
<td>Final UDR</td>
<td>C-C on PS-Information Level</td>
</tr>
<tr>
<td>Interim</td>
<td>Time Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Time Limit for all bearers</td>
</tr>
<tr>
<td>N/A</td>
<td>Serving Node Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Serving Node PLMN Change</td>
<td>YES</td>
<td>NO</td>
<td>Serving Node PLMN Change for bearer</td>
<td>PLMN change noticed at the S-GW, without S-GW relocation. eNB/MME may change and belong to a new PLMN (rural operator) or eNB may change with no MME/S-GW relocation; however eNB belongs to new serving network. This Change Condition is required as S-GW could support a MME owned by a rural operator. With S-GW relocation, the old S-GW terminates the Diameter charging session &amp; the new S-GW starts a Diameter charging session (S-GW-Change AVP included).</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).</td>
<td>User Location Change</td>
<td>YES NO NO</td>
<td>N/A</td>
<td>N/A</td>
<td>ULI Change - added to TDV for all bearers.</td>
</tr>
<tr>
<td>N/A</td>
<td>RAT Change</td>
<td>YES YES NO</td>
<td>RAT Change</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Interim</td>
<td>UE Timezone Change</td>
<td>YES YES NO</td>
<td>UE Timezone Change</td>
<td>UE Timezone Change for all bearers</td>
<td>UE Timezone Change</td>
</tr>
<tr>
<td>N/A</td>
<td>Tariff Time Change</td>
<td>N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Idled Out</td>
<td>N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Specific Unit Limit</td>
<td>N/A N/A N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Max Number of Changes in Charging Conditions to change condition that occurred (QoS-Change or ULI change or Normal Bearer Termination, Abnormal Bearer Termination)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C-C on PS-Information Level</td>
<td>C-C on TDV Level</td>
<td>Max Number of Changes in Charging Conditions to change condition that occurred (QoS-Change or ULI Change)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CC on TDV Level</td>
<td>CC on PS-Information Level</td>
<td>TDV corresponds to change condition that occurred (QoS-Change or ULI Change)</td>
</tr>
</tbody>
</table>

This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. The Max Number of Changes in Charging Conditions is set at 10. Example: [1] Max Number of Changes in Charging Conditions set at S-GW = 2. [2] When Change Condition 1 takes place no ACR[Interim] is sent, but S-GW will store the container data for this change condition. (continued)
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Management Intervention</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Management intervention will close the PDN session from P-GW.</td>
</tr>
</tbody>
</table>

[3] Change Condition 2 takes place. An ACR Interim is sent. Now Max Number of Changes in Charging conditions is populated in the PS-Information and the both the TDVs for the Change condition 1 and Change Condition 2 is populated in the 2 TDVs. Please note the TDVs need to be in the order that they are created so that the Billing Mediation system is not confused with the usage data sequence. [4] CCF creates the partial record.
## ACR Message | Change-Condition Value | CCF Response to Change-Condition Value | PDN Connection level reporting (PDN Session based accounting) | EPS bearer level reporting (PDN Session per QCI accounting) | Comments
--- | --- | --- | --- | --- | ---
Interim | - | YES | NO | NO | N/A | N/A | N/A | N/A

### Gathering Statistics

This section explains how to gather Rf and related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

<table>
<thead>
<tr>
<th>Statistics/Information</th>
<th>Action to perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete statistics for Diameter Rf accounting sessions</td>
<td>show diameter aaa-statistics</td>
</tr>
</tbody>
</table>

The following is a sample output of the `show diameter aaa-statistics` command:

```
Authentication Servers Summary

Message Stats :

Total MA Requests: 0 Total MA Answers: 0
MAR - Retries: 0 MAA Timeouts: 0
MAA - Dropped: 0
Total SA Requests: 0 Total SA Answers: 0
```
SAR - Retries: 0 SAA Timeouts: 0
SAA - Dropped: 0
Total UA Requests: 0 Total UA Answers: 0
UAR - Retries: 0 UAA Timeouts: 0
UAA - Dropped: 0
Total LI Requests: 0 Total LI Answers: 0
LIR - Retries: 0 LIA Timeouts: 0
LIA - Dropped: 0
Total RT Requests: 0 Total RT Answers: 0
RTR - Rejected: 0
Total PP Requests: 0 Total PP Answers: 0
PPR - Rejected: 0
Total DE Requests: 0 Total DE Answers: 0
DEA - Accept: 0 DEA - Reject: 0
DER - Retries: 0 DEA Timeouts: 0
DEA - Dropped: 0
Total AA Requests: 0 Total AA Answers: 0
AAR - Retries: 0 AAA Timeouts: 0
AAA - Dropped: 0
ASR: 0 ASA: 0
RAR: 0 RAA: 0
STR: 0 STA: 0
STR - Retries: 0
Message Error Stats:
Diameter Protocol Errs: 0 Bad Answers: 0
Unknown Session Reqs: 0 Bad Requests: 0
Request Timeouts: 0 Parse Errors: 0
Request Retries: 0
Session Stats:
Total Sessions: 0 Freed Sessions: 0
Session Timeouts: 0 Active Sessions: 0
STR Termination Cause Stats:
Diameter Logout: 0 Service Not Provided: 0
Bad Answer: 0 Administrative: 0
Link Broken: 0 Auth Expired: 0
User Moved: 0 Session Timeout: 0
User Request: 0 Lost Carrier 0
Lost Service: 0 Idle Timeout 0
NAS Session Timeout: 0 Admin Reset 0
Admin Reboot: 0 Port Error: 0
NAS Error: 0 NAS Request: 0
NAS Reboot: 0 Port Unneeded: 0
Port Preempted: 0 Port Suspended: 0
Service Unavailable: 0 Callback: 0
User Error: 0 Host Request: 0
Accounting Servers Summary
---------------------------
Message Stats :
Total AC Requests: 0 Total AC Answers: 0
ACR-Start: 0 ACA-Start: 0
ACR-Start Retries : 0 ACA-Start Timeouts: 0
ACR-Interim: 0 ACA-Interim: 0
ACR-Interim Retries : 0 ACA-Interim Timeouts: 0
ACR-Event: 0 ACA-Event: 0
ACR-Stop : 0 ACA-Stop: 0
ACR-Stop Retries : 0 ACA-Stop Timeouts: 0
ACA-Dropped : 0
AC Message Error Stats:
Diameter Protocol Errs: 0 Bad Answers: 0
Unknown Session Reqs: 0 Bad Requests: 0
Request Timeouts: 0 Parse Errors: 0
Request Retries: 0
Appendix D
S-GW Engineering Rules

This appendix provides Serving Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5x00 for your network deployment. General and network-specific rules are located in the appendix of the System Administration Guide for the specific network type.

The following rules are covered in this appendix:

- Interface and Port Rules
- S-GW Service Rules
- S-GW Subscriber Rules
Interface and Port Rules

The assumptions and rules discussed in this section pertain to Ethernet line cards and the type of interfaces they facilitate.

Assumptions

Overall assumptions for the S5/S8 and S11 interfaces used in the LTE EPC between Serving Gateway and PDN-GW are listed below.

- GTPv2-C is the signaling protocol used on the S5/S8 and S11 interfaces. Message and IE definitions comply with 3GPP 29.274.
- S5 and S11 interfaces use IPv6 transport as defined in 29.274, section 10.
- MSISDN is assumed to be sent by MME in initial attach.
- MEI will always be retrieved by MME from UE and sent on S11 during initial attach and UE Requested PDN connectivity procedure.
- MME will always send UE time zone information.
- The default bearer does not require any TFT.
- The PCO IE in Create Session Request shall contain two DNS server IP addresses. [S5/S8]
- UE's location change reporting support is required. [S5/S8]
- The S-GW does not verify the content of the IEs which are forwarded on the S5/S8 interface from the S11 interface. The P-GW verifies the content of all the IEs received on the S5/S8 interface.

S1-U/S11 Interface Rules

The following engineering rules apply to the S1-U0/S11 interface:

- An S1-U0/S11 interface is created once the IP address of a logical interface is bound to an S-GW service.
- The logical interface(s) that will be used to facilitate the S1-U0/S11 interface(s) must be configured within an “ingress” context.
- S-GW services must be configured within an “ingress” context.
- At least one S-GW service must be bound to each interface, however, multiple S-GW services can be bound to a single interface if secondary addresses are assigned to the interface.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S1-U0/S11 interface can be limited.

S5/S8 Interface Rules

This section describes the engineering rules for the S5 interface for communications between the Mobility Access Gateway (MAG) service residing on the S-GW and the Local Mobility Anchor (LMA) service residing on the P-GW.
MAG to LMA Rules

The following engineering rules apply to the S5/S8 interface from the MAG service to the LMA service residing on the P-GW:

- An S5/S8 interface is created once the IP address of a logical interface is bound to an MAG service.
- The logical interface(s) that will be used to facilitate the S5/S8 interface(s) must be configured within the egress context.
- MAG services must be configured within the egress context.
- MAG services must be associated with an S-GW service.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S5/S8 interface can be limited.
S-GW Service 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. Only create a large number of services only if your application absolutely requires it. Please contact your local service representative for more information.

- The system maintains statistics for a maximum of 4,096 peer LMAs per MAG service.
- The total number of entries per table and per chassis is limited to 256.
- Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty troubleshooting problems, and make it difficult to understand outputs of `show` commands.
S-GW Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- A maximum of 2,048 local subscribers can be configured per context.
- Default subscriber templates may be configured on a per S-GW or MAG service.