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.

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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://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. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface

About this Guide xv

Conventions Used xv

Supported Documents and Resources xvi

Related Common Documentation xvi

Related Product Documentation xvi

Obtaining Documentation xvii

Contacting Customer Support xvii

CHAPTER 1

Serving Gateway Overview 1

Product Description 1

Platform Requirements 4

Licenses 4

Network Deployment(s) 4

Serving Gateway in the E-UTRAN/EPC Network 5

Supported Logical Network Interfaces (Reference Points) 6

S1-U Interface 6

S4 Interface 7

S5/S8 Interface 8

S11 Interface 9

S12 Interface 9

Gxc Interface 10

Gz Interface 10

Rf Interface 11

Features and Functionality - Base Software 11

3GPP Release 12 Cause-Code IE Support 12

Abnormal Bearer Termination Cause in CDR 12

ANSI T1.276 Compliance 12
Subscriber Level Trace 30
Threshold Crossing Alerts (TCA) Support 30
ULI Enhancements 31
Features and Functionality - Optional Enhanced Feature Software 32
128k eNodeB Support 32
Direct Tunnel 33
Intelligent Paging for ISR 34
Inter-Chassis Session Recovery 34
IP Security (IPSec) Encryption 35
Lawful Intercept 35
Layer 2 Traffic Management (VLANs) 35
New Call Policy for Stale Sessions 36
Overcharging Protection Support 36
R12 Load and Overload Support 37
Operation 38
Separate Paging for IMS Service Inspection 38
Session Recovery Support 38
How the Serving Gateway Works 39
GTP Serving Gateway Call/Session Procedures in an LTE-SAENetwork 39
Subscriber-initiated Attach (initial) 40
Subscriber-initiated Detach 43
Supported Standards 43
3GPP References 44
Release 12 3GPP References 44
Release 11 3GPP References 44
Release 10 3GPP References 45
Release 9 Supported Standards 45
Release 8 Supported Standards 45
3GPP2 References 46
IETF References 46
Object Management Group (OMG) Standards 47

CHAPTER 2
Serving Gateway Configuration 49
Configuring the System as a Standalone eGTP S-GW 49
Information Required 49
Configuring ACL-based Node-to-Node IP Security on the S1-U and S5 Interfaces 69
   Creating and Configuring a Crypto Access Control List 70
   Creating and Configuring an IPSec Transform Set 70
   Creating and Configuring an IKEv2 Transform Set 70
   Creating and Configuring a Crypto Map 71
Configuring R12 Load Control Support 72
Configuring R12 Overload Control Support 73
Configuring S4 SGSN Handover Capability 73

CHAPTER 3  Monitoring the Service 75
   Monitoring System Status and Performance 75
   Configuring the S-GW to Include IMSI/IMEI in Logging Events 77
   Configuring S-GW to Include IMSI/IMEI in Event Logs 79
   Clearing Statistics and Counters 80

CHAPTER 4  Collision Handling on the P-GW/SAEGW/S-GW 81
   Feature Description 81
      Relationships to Other Features 81
   How It Works 82
      Collision Handling 82
         Example Collision Handling Scenarios 83
      Limitations 84
   Standards Compliance 84
   Configuring Collision Handling 84
      Configuring DBcmd Message Behavior 84
   Verifying the Configuration 85
   Monitoring the Collision Handling Feature 85
      Collision Handling Show Command(s) and/or Outputs 85
         show configuration 85
         show egtp-service all 85
         show egtp statistics verbose 85

CHAPTER 5  Session Tracing 87
   Session Tracing Overview 87
   Session Trace Types 89
<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iu Release with Direct Tunnel</td>
<td>119</td>
</tr>
<tr>
<td>Service Request with Direct Tunnel</td>
<td>120</td>
</tr>
<tr>
<td>Downlink Data Notification with Direct Tunnel when UE in Connected State</td>
<td>121</td>
</tr>
<tr>
<td>Downlink Data Notification with Direct Tunnel when UE in Idle State</td>
<td>122</td>
</tr>
<tr>
<td>Intra SGSN Routing Area Update without SGW Change</td>
<td>124</td>
</tr>
<tr>
<td>Routing Area Update with S-GW Change</td>
<td>127</td>
</tr>
<tr>
<td>Intra SRNS with S-GW Change</td>
<td>130</td>
</tr>
<tr>
<td>Intra SRNS without S-GW Change</td>
<td>132</td>
</tr>
<tr>
<td>New SRNS with S-GW Change and Direct Data Transfer</td>
<td>133</td>
</tr>
<tr>
<td>New SRNS with S-GW Change and Indirect Data Transfer</td>
<td>135</td>
</tr>
<tr>
<td>Old SRNS with Direct Data Transfer</td>
<td>137</td>
</tr>
<tr>
<td>Old SRNS with Indirect Data Transfer</td>
<td>138</td>
</tr>
<tr>
<td>Network Initiated Secondary PDP Context Activation</td>
<td>140</td>
</tr>
<tr>
<td>PGW Init Modification when UE is Idle</td>
<td>140</td>
</tr>
<tr>
<td>Limitations</td>
<td>141</td>
</tr>
<tr>
<td>Standards Compliance</td>
<td>142</td>
</tr>
<tr>
<td>Configuring Support for Direct Tunnel</td>
<td>142</td>
</tr>
<tr>
<td>Configuring Direct Tunnel on an S4-SGSN</td>
<td>142</td>
</tr>
<tr>
<td>Enabling Setup of GTP-U Direct Tunnel</td>
<td>142</td>
</tr>
<tr>
<td>Enabling Direct Tunnel to RNCs</td>
<td>143</td>
</tr>
<tr>
<td>Restricting Direct Tunnels</td>
<td>144</td>
</tr>
<tr>
<td>Verifying the Call-Control Profile Configuration</td>
<td>144</td>
</tr>
<tr>
<td>Verifying the RNC Configuration</td>
<td>144</td>
</tr>
<tr>
<td>Configuring S12 Direct Tunnel Support on the S-GW</td>
<td>145</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting Direct Tunnel</td>
<td>145</td>
</tr>
<tr>
<td>show subscribers sgsn-only</td>
<td>145</td>
</tr>
<tr>
<td>show gmm-sm statistics sm-only</td>
<td>146</td>
</tr>
<tr>
<td>Direct Tunnel Bulk Statistics</td>
<td>146</td>
</tr>
</tbody>
</table>

### Chapter 7

**3GPP R12 GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW**

- Feature Description 147
  - Relationships to Other Features 148
  - How It Works 148
  - Creating and Configuring a 3GPP R12 GTP-C Load Control Profile 149
  - Configuration Overview 149
Creating the GTPP R12 Load Control Profile 149
Configuring the 3GPP R12 Load Control Profile Weightage Settings 149
Configuring the 3GPP R12 Load Control Profile Inclusion Frequency 150
Configuring the 3GPP R12 Load Control Threshold 151
Configuring 3GPP R12 Load Control Information Handling 151
Configuring 3GPP R12 Load Control Information Publishing 151
Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service 152
Verifying the 3GPP R12 Load Control Configuration 152
Saving the Configuration 153
Creating and Configuring a 3GPP R12 GTP-C Overload Control Profile 153
Configuration Overview 154
Creating the GTPP R12 Overload Control Profile 154
Configuring 3GPP R12 Overload Control Weightage Settings 154
Configuring the 3GPP R12 Overload Control Inclusion Frequency 155
Configuring the 3GPP R12 Overload Control Validity Period 156
Configuring 3GPP R12 Overload Control Tolerance Limits 156
Configuring 3GPP R12 Overload Control Throttling Behavior 157
Configuring 3GPP R12 Overload Control Message Prioritization 157
Configuring 3GPP R12 Overload Control Self-Protection Behavior 158
Configuring 3GPP R12 Overload Control Information Handling 158
Configuring 3GPP R12 Overload Control Information Publishing 159
Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service 159
Verifying the 3GPP R12 Overload Control Configuration 160
Saving the 3GPP R12 Overload Control Configuration 160
Monitoring and Troubleshooting the 3GPP R12 GTP-C Load and Overload Control Feature 161
3GPP R12 GTP-C Load and Overload Show Commands 161
show egtpc statistics egtp-service <egtp-service name> 161
show gtpc-load-control-profile full all 161
show gtpc-load-control-profile full name <name> 161
show gtpc-overload-control-profile full all 161
show gtpc-overload-control-profile full name <name> 161
show pgw-service all 161
CHAPTER 8

Intelligent RAT Paging for ISR on the S-GW 163

Feature Description 163
Relationships to Other Features 164
How it Works 164
Intelligent RAT Paging for ISR on the S-GW 164
Licenses 164
Limitations 165
Flows 165
Configuring Intelligent RAT Paging for ISR on the S-GW 168
Configuring the Intelligent RAT Paging for ISR Feature 168
Verifying the Intelligent RAT Paging for ISR Configuration 168

CHAPTER 9

Operator Policy 171

What Operator Policy Can Do 171
A Look at Operator Policy on an SGSN 171
A Look at Operator Policy on an S-GW 172
The Operator Policy Feature in Detail 172
Call Control Profile 173
APN Profile 174
IMEI-Profile (SGSN only) 174
APN Remap Table 175
Operator Policies 175
IMSI Ranges 176
How It Works 176
Operator Policy Configuration 177
Call Control Profile Configuration 178
Configuring the Call Control Profile for an SGSN 178
Configuring the Call Control Profile for an MME or S-GW 179
APN Profile Configuration 179
IMEI Profile Configuration - SGSN only 180
APN Remap Table Configuration 180
Operator Policy Configuration 181
IMS Range Configuration 181
  Configuring IMSI Ranges on the MME or S-GW 181
  Configuring IMSI Ranges on the SGSN 182
Associating Operator Policy Components on the MME 182
Configuring Accounting Mode for S-GW 182
Verifying the Feature Configuration 183

CHAPTER 10
Overcharging Protection Support 185
  Overcharging Protection Feature Overview 185
  License 186
Configuring Overcharging Protection Feature 186
  Configuring Overcharging Support on the P-GW 186
  Configuring Overcharging Support on the S-GW 187
Monitoring and Troubleshooting 188
  P-GW Schema 188
  show apn statistics all 188
  show pgw-service all 188
  show pgw-service statistics all 188
  show sgw-service statistics name <sgw_service_name> 189
  show subscribers full 189
  show subscribers pgw-only full all 189
  show subscribers summary 189

CHAPTER 11
Rf Interface Support 191
  Introduction 191
  Offline Charging Architecture 193
    Charging Collection Function 194
    Charging Trigger Function 194
    Dynamic Routing Agent 195
  License Requirements 195
  Supported Standards 195
  Features and Terminology 195
  Offline Charging Scenarios 195
    Basic Principles 195
    Event Based Charging 197
About this Guide

This preface describes the S-GW Administration Guide, how it is organized and its document conventions. The Serving Gateway (S-GW) 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. This document provides feature descriptions, configuration procedures and monitoring and troubleshooting information.

- Conventions Used, page xv
- Supported Documents and Resources, page xvi
- Contacting Customer Support, page xvii

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

<table>
<thead>
<tr>
<th>Typeface Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as a screen display</td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td>Typeface Conventions</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Text represented as **commands** | 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. |
| Text represented as a **command variable** | 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. |
| Text represented as menu or sub-menu names | This typeface represents menus and sub-menus that you access within a software application, for example:  
  Click the **File** menu, then click **New** |

**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:

- AAA Interface Administration and Reference
- Command Line Interface Reference
- GTPP Interface Administration and Reference
- Hardware Installation Guide (hardware dependent)
- Release Change Reference
- SNMP MIB Reference
- Statistics and Counters Reference
- System Administration Guide (hardware dependent)
- Thresholding Configuration Guide

**Related Product Documentation**

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

- Product Description, page 1
- Network Deployment(s), page 4
- Features and Functionality - Base Software, page 11
- Features and Functionality - Optional Enhanced Feature Software, page 32
- How the Serving Gateway Works, page 39
- Supported Standards, page 43

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.

Figure 2: S-GW in the Basic E-UTRAN/EPC and eHRPD Network

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), on page 6 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.

**Figure 4: S-GW in the E-UTRAN/EPC Network**

---

**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-Uv1). 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
- Tunneling: IPv4 or IPv6 GTPv1-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

**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

**Figure 6: Supported Protocols on the S4 Interface**

<table>
<thead>
<tr>
<th>S-GW</th>
<th>S4</th>
<th>SGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Transport</td>
<td>Transport</td>
</tr>
<tr>
<td>GTP C/U</td>
<td>GTP C/U</td>
<td>IPv4/IPv6</td>
</tr>
<tr>
<td>UDP</td>
<td>UDP</td>
<td>IPv4/IPv6</td>
</tr>
<tr>
<td>IPv4/IPv6</td>
<td>IPv4/IPv6</td>
<td>L1/L2</td>
</tr>
<tr>
<td>L1/L2</td>
<td>L1/L2</td>
<td>L1/L2</td>
</tr>
</tbody>
</table>

**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

**Figure 7: Supported Protocols on the S5/S8 Interface**

<table>
<thead>
<tr>
<th>S-GW</th>
<th>S5/S8 (GTP)</th>
<th>P-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Transport</td>
<td>Transport</td>
</tr>
<tr>
<td>GTP-CU</td>
<td>GTP-CU</td>
<td>IPv4/IPv6</td>
</tr>
<tr>
<td>UDP</td>
<td>UDP</td>
<td>IPv4/IPv6</td>
</tr>
<tr>
<td>IPv4/IPv6</td>
<td>IPv4/IPv6</td>
<td>L1/L2</td>
</tr>
<tr>
<td>L1/L2</td>
<td>L1/L2</td>
<td>L1/L2</td>
</tr>
</tbody>
</table>
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

Figure 8: Supported Protocols on the S11 Interface

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

**Figure 9: Supported Protocols on the S12 Interface**

<table>
<thead>
<tr>
<th>UTRAN RNC</th>
<th>S12</th>
<th>S-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTP-U</td>
<td>IPv6</td>
<td>IPv6</td>
</tr>
<tr>
<td>UDP</td>
<td>IPv6</td>
<td>IPv6</td>
</tr>
<tr>
<td>L1/L2</td>
<td>IPv6</td>
<td>IPv6</td>
</tr>
</tbody>
</table>

**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

**Figure 10: Supported Protocols on the Gxc Interface**

<table>
<thead>
<tr>
<th>S-GW</th>
<th>Gxc</th>
<th>PCRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter</td>
<td>Diameter</td>
<td></td>
</tr>
<tr>
<td>SCTP/TCP</td>
<td>SCTP/TCP</td>
<td></td>
</tr>
<tr>
<td>IPv4/IPv6</td>
<td>IPv4/IPv6</td>
<td></td>
</tr>
<tr>
<td>L1/L2</td>
<td>L1/L2</td>
<td></td>
</tr>
</tbody>
</table>

**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

**Figure 11: Supported Protocols on the Gz Interface**

<table>
<thead>
<tr>
<th>S-GW</th>
<th>Gz</th>
<th>OCF$</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPP</td>
<td>GTPP</td>
<td>UDP/TCP</td>
</tr>
<tr>
<td>L1/L2</td>
<td>L1/L2</td>
<td>L1/L2</td>
</tr>
</tbody>
</table>

**Rf Interface**

**Important** In StarOS 19 and later releases, the Rf interface is not supported on the S-GW.

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

**Figure 12: Supported Protocols on the Rf Interface**

**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.
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.

**3GPP Release 12 Cause-Code IE Support**

When an ERAB or a data session is dropped, an operator may need to get, beyond the ULI information, detailed RAN and/or NAS release cause codes information from the access network to be included in the S-GW and P-GW CDRs for call performance analysis, User QoE analysis and proper billing reconciliation. Also, for IMS sessions, the operator may need to get the above information available at P-CSCF.

'Per E-RABCause' is received in ERAB Release Command and ER AB Release Indication messages over S1. However, RAN and NAS causes are not forwarded to the SGW and PGW, nor provided by the PGW to PCRF.

To resolve this issue, a "RAN/NAS Release Cause" information element (IE), which indicates AS and/or NAS causes, has been added to the Session Deletion Request and Delete Bearer Command. The "RAN/NAS Release Cause" provided by the MME is transmitted transparently by the S-GW to the P-GW (if there exists signaling towards P-GW) for further propagation towards the PCRF.

For backward compatibility, the S-GW can still receive the cause code from the CC IE in the S4/S11 messages and/or receive the cause code from some customers' private extension.

**Abnormal Bearer Termination Cause in CDR**

This feature provides additional information in a S-GW/P-GW CDR for a VoLTE call drop. A dropped bearer was previously reported as a ‘abnormalrelease’ in the CDR. This feature has the S-GW / P-GW CDRs indicate the proper bearer release for all failure cases identified in the VoLTE Retainability formula. This will provide the customer with the ability to perform gateway/network wide analysis for failures in the network.

New Disconnect reasons are added for GTPC/GTPU path failure and local purge GTPU error indications.

New field abnormalTerminationCause enum 83 is added in the S-GW CDR for a specific customer dictionary.

**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 an element management system 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 an element management system, 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.

An element management system is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of an element management system 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 an element management system server.

**Important**

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

**CDR Support for Including LAPI (Signaling Priority)**

This feature is related to M2M support. 3GPP has added the LAPI (signaling priority) indication being sent in the GTP messages, to indicate that the PDN is a low priority bearer and thus can be treated accordingly. APN backoff timer support based on LAPI indication is not yet supported.

3GPP has also added a new AVP in CDR defined in TS 32.298 named "lowPriorityIndicator". If the S-GW receives the LAPI indicator in GTP, the SGW-CDR and generated will contain the LAPI indication.

The benefit of this feature is that it provides support for carrying the LAPI attribute in SGW-CDR and PGW-CDR, so that billing system can then accordingly bill for that PDN.

**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:
Collision Counter Support in the GTP Layer

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The S-GW software has been enhanced so that these collisions are now tracked by statistics and handled based on a pre-defined action for each message collision type.

If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will still see the respective collision statistics if they occur.

The output of the `show egtp statistics verbose` command has been enhanced to provide information on GTPv2 message collisions, including:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5), or PGW (S5).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type)**: The new procedure and message type.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - No Collision Detected
  - **Suspend Old**: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - **Abort Old**: Abort the original message handling and processes the new message.
  - **Reject New**: The new message is rejected, and the original (old) message is processed.
  - **Silent Drop New**: Drop the new incoming message, and the old message is processed.
  - **Parallel Hndl**: Both the original (old) and new messages are handled in parallel.
  - **Buffer New**: The new message is buffered and processed once the original (old) message processing is done.
- **Counter**: The number of times each collision type has occurred.

**Important**
The Message Collision Statistics section of the command output only appears if any of the collision statistics have a counter total that is greater than zero.

**Sample output**:

```
Message Collision Statistics
Interface Old Proc (Msg Type) New Proc (Msg Type) Action Counter
SGW(S5) NW Init Bearer Create (95) NW Init PDN Delete (99) Abort Old 1
```

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the
S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.

The action that is carried out due to this collision at eGTP-C is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the PDN Delete procedure. The Counter total of 1 indicates that this collision happened only once.

### 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 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* chapter in the System Administration Guide.

---

### Dedicated Bearer Timeout Support on the S-GW

The S-GW has been enhanced to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value. Operators now can configure a bearer inactivity timeout for GBR and non-GBR bearers for more efficient use of system resources.
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.

DSCP Ingress and Egress and DSCP Marking at the APN Profile

This feature will provide an operator with a configuration to set the DSCP value per APN profile, so different APNs can have different DSCP markings as per QOS requirements for traffic carried by the APN. In addition,
the \textit{qci-qos mapping} table is updated with the addition of a \textit{copy-outer} for copying the DSCP value coming in the encapsulation header from the S1u interface to the S5 interface and vice-versa.

**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 \textit{Configuring the GTP Echo Timer} section located in the \textit{Configuring Optional Features on the eGTP S-GW} section of the \textit{Serving Gateway Configuration} chapter.

**Event-Based Idle Second Micro-Check Point Generation for the S-GW**

Prior to StarOS release 19, micro-checkpoints were configurable only with the \textit{micro-checkpoint-periodicity} option in the \textit{timeout idle} command in APN Configuration Mode.

Now, the S-GW can be configured to send an idlesec micro-checkpoint from an Active to Standby chassis when the session state changes from active to idle or from idle to active. The micro-checkpoint carries information about the time when the session became active or idle. Upon receipt of the micro-checkpoint, the Standby chassis updates the active/idle time. This process enables the Active and Standby chassis to be synchronized with respect to when a particular session became active or idle.

Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event occurs, as opposed to sending micro-check points based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not.

To enable this functionality, use the \textit{micro-checkpoint-deemed-idle} keyword in the \textit{timeout idle} command in APN Configuration Mode.

**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 \textit{S-GW Event Reporting} chapter 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 \textit{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 \textit{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.

IMSI/IMEI Available in System Event Logs of Type Error and Critical

The S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available. If the IMSI is not available, the S-GW will make a best effort to obtain the IMEI.

Table 1: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 12225 | Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: %s, error code %d"
| 12226 | Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s"
| 12227 | Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-%d Ran out of session handles"
| 140075 | Represents error_log1 in format "[IMSI <IMSI>] %s"

| **Modified Events** | |
| 139001 | To print miscellaneous PGW error log. |
| 191006 | To print miscellaneous SAEGW error log. |
| 10034 | Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=%s(%) state=%s(%) event=%s(%)"
<p>| 10035 | Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%) event=%s(%)&quot; |</p>
<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s&quot;. For example &quot;[IMSI 112233445566778 Sessmgr-1: Request to create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td>12668</td>
<td>Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot;</td>
</tr>
<tr>
<td>12774</td>
<td>Represents pgw_purge_invalidErrMsg in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot;</td>
</tr>
<tr>
<td>12855</td>
<td>Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig recvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td>12857</td>
<td>Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig: TFT validation failed for nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>12858</td>
<td>Represents ncqos_nxrx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.&quot;</td>
</tr>
<tr>
<td>12859</td>
<td>Represents ncqos_nxrx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%u&gt;: pf_id_bitmap 0x%x and tft_opcode: %d&quot;</td>
</tr>
<tr>
<td>12860</td>
<td>Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;&quot;%s&quot;&gt;.&quot;</td>
</tr>
<tr>
<td>12861</td>
<td>Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;&quot;%s&quot;&gt;.&quot;</td>
</tr>
<tr>
<td>12862</td>
<td>Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state: &lt;%s&gt;, [event:&lt;&quot;%s&quot;&gt;]&quot;</td>
</tr>
<tr>
<td>11830</td>
<td>Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN does not support Deffered allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
<tr>
<td>11832</td>
<td>Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0x%x&gt; not found.&quot;</td>
</tr>
<tr>
<td>12960</td>
<td>Represents gtp_pdp_type_mismatch in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN %s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>11282</td>
<td>Represents pcc_intf_error_info in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents collision_error in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d&quot;</td>
</tr>
<tr>
<td>11917</td>
<td>Represents rcvd_invalid_bearer_binding_req_from_acs in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr %d: Received invalid bearer binding request from ACS.&quot;</td>
</tr>
<tr>
<td>11978</td>
<td>Represents saegw_uid_error in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11994</td>
<td>Represents unwanted_pcc_intf_setup_req error in format &quot;[IMSI &lt;IMSI&gt;] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface &quot;</td>
</tr>
<tr>
<td>140005</td>
<td>Represents ue_fsmillegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled UE event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>140006</td>
<td>Represents pdn_fsmillegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled PDN event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>140007</td>
<td>Represents epsb_fsmillegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled EPSB event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>10726</td>
<td>Represents saegwdrv_generic_error &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
</tbody>
</table>

Enable this functionality by using the `logging include-uid` command in `Global Configuration Mode`. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

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

**Important**

In StarOS v19 and later releases, the Diameter Rf offline charging interface is not supported on the S-GW.

**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 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 timezone IE from the MME, it forwards this IE towards the P-GW across the S5/S8 interface.

**MME Restoration Support**

MME restoration is a 3GPP specification-based feature designed to gracefully handle the sessions at S-GW once S-GW detects that the MME has failed or restarted. If the S-GW detects an MME failure based on a different restart counter in the Recovery IE in any GTP Signaling message or Echo Request / Response, it will terminate sessions and not maintain any PDN connections.

As a part of this feature, if a S-GW detects that a MME or S4-SGSN has restarted, instead of removing all the resources associated with the peer node, the S-GW shall maintain the PDN connection table data and MM bearer contexts for some specific S5/S8 bearer contexts eligible for network initiated service restoration, and initiate the deletion of the resources associated with all the other S5/S8 bearers.

The S5/S8 bearers eligible for network initiated service restoration are determined by the S-GW based on operator's policy, for example, based on the QCI and/or ARP and/or APN.

The benefit of this feature is that it provides support for the geo-redundant pool feature on the S4-SGSN/MME. In order to restore session when the MME receives a DDN, the S-GW triggers restoration when the serving MME is unavailable, by selecting another MME and sending DDN. This helps in faster service restoration/continuity in case of MME/S4-SGSN failures.

**MME Restoration Standards Extension**

The solution to recover from MME node failures proposed in the 3GPP standards rely on the deployment of MME pools where each pool services a coverage area. Following an MME failure, the S-GW and MSC/VLR nodes may select the same MME that used to service a UE, if it has restarted, or an alternate MME in the same pool to process Network-initiated signaling that it received in accordance with the NTSR procedures defined in 3GPP TS 23.007 Release 11.

For a failed MME, the S-GW will select an alternate MME from the associated NTSR pool in round robin fashion in each sessmgr instance.
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 LMA's. 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 the 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.

Important

Note that the S-GW does not support MABR functionality.

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 fallback 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

Important

In StarOS release 19 and later releases, Offline Charging is not supported on the S-GW.
Online Charging is not supported on the S-GW.

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.

The offline charging implementation offers built-in heartbeat 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 reactives itself and is able to begin pulling the cached charging records.

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 GTPPP 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.

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 - GTPP (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.

**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 S-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 (SDFs) 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 S-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

Important

In StarOS release 19 and later releases, Rf Diameter Accounting is not supported on the S-GW.

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 adjunct 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 correlate charging records with EPC bearers.

S-GW Collision Handling

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. The S-GW has been enhanced to process collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification (DDN) message with Create Bearer Request or Update Bearer Request.

The enhanced behavior is as follows:

1. A CBReq and MBReq ([Inter MME/Inter RAT (with or without ULI change)]) collision at the S-GW ingress interface results in the messages being handled in parallel. The CBReq will wait for a Create Bearer Response (CBRsp) from the peer. Additionally, an MBReq is sent in parallel to the P-GW.
2. An UBRreq and MBReq ([Inter MME/Inter RAT (with or without a ULI change)]) collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBRreq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBRreq procedure is resumed.
3. The Downlink Data Notification (DDN) message transaction is dis-associated from bearers. So Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

As a result of this enhancement no S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.
Viewing S-GW Collision Statistics

The output of the `show egtpc statistics verbose` command has been enhanced to provide information on GTPv2 message collisions at the S-GW ingress interface, including:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- **New Proc (Msg Type)**: The new procedure and message type.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - No Collision Detected
  - Suspend Old: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - Abort Old: Abort the original message handling and processes the new message.
  - Reject New: The new message is rejected, and the original (old) message is processed.
  - Silent Drop New: Drop the new incoming message, and the old message is processed.
  - Parallel Hndl: Both the original (old) and new messages are handled in parallel.
  - Buffer New: The new message is buffered and processed once the original (old) message processing is done.
- **Counter**: The number of times each collision type has occurred.

The `Message Collision Statistics` section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

**Important**

A session idle timer has been implemented on the S-GW to remove stale sessions in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down those sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

**Important**

The session idle timer feature will not work if the Fast Data Path feature is enabled.
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 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 (e.g. 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 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 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 a 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 an element management system.

  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*.

---

**ULI Enhancements**

VoLTE carriers need the last cell/sector updates within the IMS CDRs to assist in troubleshooting customer complaints due to dropped calls as well as LTE network analysis, performance, fraud detection, and operational maintenance. The ultimate objective is to get the last cell sector data in the IMS CDR records in addition to the ULI reporting for session establishment.

To address this issue, the S-GW now supports the following:

- RAN/NAS Cause IE within bearer context of Delete Bearer Command message.

- The S-GW ignores the ULI received as call is going down so there is no point in updating the CDR.
Support for ULI and ULI Timestamp in Delete Bearer Command message had already been added in release 17.0.
Now, when a new ULI is received in the Delete Bearer Command message, a S-GW CDR is initiated.

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.

128k eNodeB Support

128k eNodeB Support is an optional licensed feature. Contact your Cisco account or service representative for detailed information on licensing requirements.
Prior to release 19.1, the StarOS supported up to 64k eNodeBs. However, in some densely populated regions there can be more than 64k eNodeBs. Or, there could be a large number of small Cell eNodeBs directly connecting to an S-GW over the S1-U interface. There could also be P-GW and S-GW peers in the GTPU data path. With StarOS release 19.1, up to 128k eNodebs are supported. Note that 128k is a collective limit for P-GW/S-GW peers in the GTPU data path as well as S1-U peers. This enables operators to anchor a large number of such eNodeBs or small Cell eNodeBs.
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.

Figure 13: GTP-U with Direct Tunnel

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.

Important

For more information on direct tunnel support, refer to the Direct Tunnel for 4G (LTE) Networks chapter 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 provide 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 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card 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 packet processing card failure will cause a packet processing card 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 propriety 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. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:
• router identifier
• chassis priority
• chassis MAC address

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 chapter 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 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 chapter in the *System Administration Guide*.

---

## New Call Policy for Stale Sessions

Use of new call policy for stale sessions requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

If the newcall policy is set to **reject release-existing-session** and there are pre-existing sessions for the IMSI/IMEI received in Create Session Req, they will be deleted. This allows for no hung sessions on node with newcall policy reject release configured. When S-GW releases the existing call, it follows a proper release process of sending Accounting Stop, sending CCR-T to PCRF/OCS, and generating CDR(s).

---

## 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.

**Important**

This feature is supported on the P-GW, and S-GW. Overcharging Protection is supported on the SAEGW only if the SAEGW is configured for Pure P or Pure S functionality.

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.

If the S-GW supports the Overcharging Protection feature, then it will send a CSReq with the PDN Pause Support Indication flag set to 1 in an Indication IE to the P-GW.

If the PGW supports the Overcharging Protection feature then it will send a CSRsp with the PDN Pause Support Indication flag set to 1 in Indication IE and/or private extension IE to the S-GW.

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. The MBreq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBreq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.
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 charging downlink packets 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).

This feature aligns with the 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) specification.

For more information on this feature, refer to the Overcharging Protection Support chapter in this guide.

**R12 Load and Overload Support**

Use of R12 Load and Overload Support requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

GTP-C Load Control feature is an optional feature which allows a GTP control plane node to send its Load Information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of Overload control Information in order to mitigate overload situation for the overloaded node through actions taken by the peer node(s). This feature is supported over the S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control Information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes may be used to reduce and/or throttle the amount of GTP-C signaling traffic between these nodes. As such, the Overload control Information provides guidance to the receiving node to decide actions, which leads to mitigation towards the sender of the information.

In brief, load control and overload control can be described in this manner:

- **Load control** enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

- **Overload control** enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

A maximum of 64 different load and overload profiles can be configured.

---

**Important**

R12 Load and Overload Support is a license-controlled feature. Contact your Cisco representative for more information on licensing requirements.
Operation

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, ((number of active sessions per service / max session allowed for the service license) * 100).

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.

Separate Paging for IMS Service Inspection

Use of Separate Paging for IMS Service Inspection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

When some operators add an additional IMS service besides VoLTE such as RCS, they can use the same IMS bearer between the two services. In this case, separate paging is supported at the MME using an ID which can be assigned from the S-GW according to the services, where the S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from using an ID which is assigned from SGW according to the services. The S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from (for example IP, Port and so on). After the MME receives this ID from the S-GW after IMS service inspection, the MME will do classified separate paging for each of the services as usual.

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-chassiss 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* chapter 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, on page 39

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

The following topics and procedure flows are included:

- Subscriber-initiated Attach (initial), on page 40
- Subscriber-initiated Detach, on page 43
Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

**Figure 14: Subscriber-initiated Attach (initial) Call Flow**

<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>
</tbody>
</table>
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 S1-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.

2 If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.

3 The UE responds with Identity Response (IMSI).

4 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.

5 The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.

6 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.

7 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.

8 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.

9 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.

10 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.

11 The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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 15: Subscriber-initiated Detach Call Flow

Table 3: 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>
<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 signaling 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 some of the standards in the following standards categories:

- 3GPP References, on page 44
3GPP References

Release 12 3GPP References

The S-GW currently supports the following Release 12 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under 3GPP2 References.

- 3GPP TS 23.007: Restoration procedures
- 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)

Release 11 3GPP References

The S-GW currently supports the following Release 11 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under 3GPP2 References.

- 3GPP TS 23.007: Restoration procedures
- 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)
- 3GPP TS 32.423: Telecommunication management; Subscriber and equipment trace; Trace data definition and management.
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport
Release 10 3GPP References

Important

The S-GW currently supports the following Release 10 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under 3GPP2 References.

- 3GPP TS 23.007: Restoration procedures
- 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3 (Release 9)
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling 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) Tunneling Protocol for Control plane (GTPv2-C); Stage 3 (Release 8)
• 3GPP TS 29.274: Evolved GPRS Tunneling 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 Tunneling protocols, version 8.1.0
• 3GPP TS 29.281: GPRS Tunneling 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

• X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

IETF References

• RFC 768: User Datagram Protocol (STD 6).
• 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
Serving Gateway Configuration

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

Important

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.

This chapter includes the following topics:

• Configuring the System as a Standalone eGTP S-GW, page 49

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 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 4: Required Information for Local Context Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Interface Configuration</td>
<td></td>
</tr>
<tr>
<td>Interface name</td>
<td>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</td>
</tr>
<tr>
<td></td>
<td>Multiple names are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 addresses assigned to the interface.</td>
</tr>
<tr>
<td></td>
<td>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>
<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>
<tr>
<td>Remote access type(s)</td>
<td>The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.</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 5: 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>
Required Information | Description
--- | ---
**S1-U/S11 Interface Configuration (To/from eNodeB/MME)**  
**Note**  The configuration provided in this guide assumes a shared S1-U/S11 interface. These interfaces can be separated to support a different network architecture. The information below applies to both.  
Interface name | An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.  
| Multiple names are needed if multiple interfaces will be configured.  
IP address and subnet | IPv4 or IPv6 addresses assigned to the interface.  
| Multiple addresses and subnets are needed if multiple interfaces will be configured.  
Physical port number | 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.  
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**  
GTP-U service name (for S1-U/S11 interface) | 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.  
IP address | S1-U/S11 interface IPv4 or IPv6 address.  

**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**  
eGTP S1-U/S11 ingress service name | 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.
## 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 6: Required Information for S-GW Egress Context Configuration

<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>
<tr>
<td>S5/S8 Interface Configuration (To/from P-GW)</td>
<td></td>
</tr>
<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>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
<tr>
<td>GTP-U Service Configuration</td>
<td></td>
</tr>
<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>
<tr>
<td>eGTP Egress Service Configuration</td>
<td></td>
</tr>
<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.

*Figure 17: eGTP S-GW Configurable Components*

---

**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*, on page 55.

**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*, on page 57.

**Step 4**
Verify and save the configuration by following the instruction in the *Verifying and Saving the Configuration*, on page 58.
Initial Configuration

Step 1  Set local system management parameters by applying the example configuration in the Modifying the Local Context, on page 55.

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, on page 55.

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, on page 56.

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, on page 56.

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, on page 57.

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, on page 57.

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 tnelnetd
    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
```
Creating an eGTP Ingress Service

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

```
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.

```
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:

```text
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:

```text
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, on page 57.

Step 2
Configure the S-GW service by applying the example configuration in the Configuring the S-GW Service, on page 58.

Step 3
Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring an IP Route, on page 58.

---

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:

```text
configure
  context <sgw_ingress_context_name>
    gtpu 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>
```
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.

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**

```bash
configure
c    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:

**Figure 18: Failure and Recovery Scenario: Example 1**
• The multiplier (x2) is system-coded and cannot be configured.

**GTP-U**

```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:

*Figure 19: Failure and Recovery Scenario: Example 2*

- 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**

```plaintext
configure
c   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>
e
```

**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:

*Figure 20: Failure and Recovery Scenario: Example 3*

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

**GTP-U**

```
configure
context <context_name>
gtpu-service <gtpu_service_name>
echo-interval <seconds> dynamic smooth-factor <multiplier>
echo-retransmission-timeout <seconds>
```
**max-retransmissions <num>**

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:

*Figure 21: Failure and Recovery Scenario: Example 4*

- 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:

```
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
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:

Important

In StarOS release 19 and later releases, Diameter Offline Accounting is not supported on the S-GW.

```
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>
      precedence <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:

```plaintext
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:

```plaintext
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
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.

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 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 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
context <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
context <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
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.
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:

```plaintext
configure
case <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:

```plaintext
configure
case <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
case <sgw_context_name>
```
ikev2-ikesa transform-set <ikev2_transform-set_name>
  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 <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:

```plaintext
configure
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>
exit
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 R12 Load Control Support

Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

Use the following example to configure this feature:

```plaintext
configure
gtpc-load-control-profile profile_name
  inclusion-frequency advertisement-interval interval_in_seconds
  weightage system-cpu-utilization percentage
  system-memory-utilization percentage
license-session-utilization percentage
end
configure
context context_name
  sgw-service sgw_service_name
    associate gtpc-load-control-profile profile_name
end
```

Notes:
• The inclusion-frequency parameter determines how often the Load control information element is sent to the peer(s).

• The total of the three weightage parameters should not exceed 100.

• The associate command is used to associate the Load Control Profile with an existing S-GW service.

## Configuring R12 Overload Control Support

Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its GTP-C peers to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signalling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Use the following example to configure this feature.

```bash
configure
gtpc-overload-control-profile profile_name
  inclusion-frequency advertisement-interval interval_in_seconds
  weightage system-cpu-utilization percentage system-memory-utilization percentage
  license-session-utilization percentage
  throttling-behavior emergency-events exclude
  tolerance threshold report-reduction-metric percentage self-protection-limit percentage
  validity-period seconds
end
```

configure
```
context context_name
sgw-service sgw_service_name
associate gtpc-overload-control-profile profile_name
end
```

Notes:

• The inclusion-frequency parameter determines how often the Overload control information element is sent to the peer(s).

• The total of the three weightage parameters should not exceed 100.

• validity-period configures how long the overload control information is valid. Valid entries are from 1 to 3600 seconds. The default is 600 seconds.

• The associate command is used to associate the Overload Control Profile with an existing S-GW service.

## Configuring S4 SGSN Handover Capability

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

Use the following example to configure this feature:

```bash
configure
  context <ingress_context_name> -noconfirm
  interface <s4_interface_name>
    ip address <ipv4_address_primary>
    ip address <ipv4_address_secondary>
end
```
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 ipv6 address command.
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, page 75
- Clearing Statistics and Counters, page 80

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 7: System Status and Performance Monitoring Commands

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Congestion-Control Information</td>
<td></td>
</tr>
<tr>
<td>View Congestion-Control Statistics</td>
<td>show congestion-control statistics { a11mgr</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>View Subscriber Information</td>
<td></td>
</tr>
<tr>
<td>View session resource status</td>
<td>show resources session</td>
</tr>
<tr>
<td>Display Subscriber Configuration Information</td>
<td></td>
</tr>
<tr>
<td>To do this:</td>
<td>Enter this command:</td>
</tr>
<tr>
<td>------------</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>View Subscribers Currently Accessing the System</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>View Statistics for Subscribers using S-GW Services on the System</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>View Statistics for Subscribers using MAG Services on the System</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>View Session Subsystem and Task Information</td>
<td></td>
</tr>
<tr>
<td>Display Session Subsystem and Task Statistics</td>
<td></td>
</tr>
<tr>
<td><strong>Important</strong> Refer to the StarOS Tasks appendix in the System Administration Guide 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>
<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>View Session Recovery Information</td>
<td></td>
</tr>
<tr>
<td>View session recovery status</td>
<td><code>show session recovery status [ verbose ]</code></td>
</tr>
<tr>
<td>View Session Disconnect Reasons</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>View S-GW Service Information</td>
<td></td>
</tr>
<tr>
<td>View S-GW service statistics</td>
<td><code>show sgw-service statistics all</code></td>
</tr>
</tbody>
</table>
### Configuring the S-GW to Include IMSI/IMEI in Logging Events

The S-GW can be configured to provide the IMSI/IMEI in the event log details for the following system event logs of type error and critical, if available. If the IMSI is not available, the S-GW will make a best effort to obtain the IMEI.

### Table 8: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

<table>
<thead>
<tr>
<th>Event Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Events</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 12225       | Represents misc_error3 in format 
"[IMSI <IMSI>] Misc Error3: s, error code d" |
| 12226       | Represents recover_call_from_crr_failed1 error in format 
"[IMSI <IMSI>] Sessmgr-d Recover call from CRR failed for callid:0x reason=s" |
| 12227       | Represents aaa_create_session_failed_no_more_sessions1 error in format 
"[IMSI <IMSI>] Sessmgr-d Ran out of session handles" |
| 140075      | Represents error_log1 in format 
"[IMSI <IMSI>]s" |
<p>| <strong>Modified Events</strong>                                 |                                                                            |</p>
<table>
<thead>
<tr>
<th>Event Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>139001</td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td>191006</td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td>10034</td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=s(d) state=s(d) event=s(d)&quot;</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=s(d) event=s(d)&quot;</td>
</tr>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-d: Request to s bearer rejected. Reason: s&quot;. For example &quot;[IMSI 1122334455666778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress&quot;</td>
</tr>
<tr>
<td>12668</td>
<td>Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code d&quot;</td>
</tr>
<tr>
<td>12774</td>
<td>Represents pgw_purge_invalid_err in format &quot;[IMSI &lt;IMSI&gt;] Local s TEID [lu] Collision: Clp Connect Time: lu, Old Clp Callid: d, Old Clp Connect Time: lu s&quot;</td>
</tr>
<tr>
<td>12855</td>
<td>Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rvd in invalid bcm mode.&quot;</td>
</tr>
<tr>
<td>12857</td>
<td>Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;u&gt;.&quot;</td>
</tr>
<tr>
<td>12858</td>
<td>Represents ncqos_nrxx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;u&gt;.&quot;</td>
</tr>
<tr>
<td>12859</td>
<td>Represents ncqos_nrxx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;u&gt;:pf_id_bitmap 0xx and tft_opcode: d&quot;</td>
</tr>
<tr>
<td>12860</td>
<td>Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;u&gt; rejected, due to &lt;s&gt;.&quot;</td>
</tr>
<tr>
<td>12861</td>
<td>Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;u&gt;, due to &lt;s&gt;.&quot;</td>
</tr>
<tr>
<td>12862</td>
<td>Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state:&lt;s&gt;,[event:&lt;s&gt;]&quot;</td>
</tr>
<tr>
<td>11830</td>
<td>Represents ggsn_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call.&quot;</td>
</tr>
<tr>
<td>Event Log</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>11832</td>
<td>Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0xx&gt; not found.&quot;</td>
</tr>
<tr>
<td>12960</td>
<td>Represents gtp_pdp_type_mismatch in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>11282</td>
<td>Represents pcc_intf_error_info in format &quot;[IMSI &lt;IMSI&gt;] s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents collision_error in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code d&quot;</td>
</tr>
<tr>
<td>11917</td>
<td>Represents rcvd_invalid_bearer_binding_req_from_acs in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr d: Received invalid bearer binding request from ACS.&quot;</td>
</tr>
<tr>
<td>11978</td>
<td>Represents saegw_uid_error in format &quot;[IMSI &lt;IMSI&gt;] s&quot;</td>
</tr>
<tr>
<td>11994</td>
<td>Represents unwanted_pcc_intf_setup_req_error in format &quot;[IMSI &lt;IMSI&gt;] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface &quot;</td>
</tr>
<tr>
<td>140005</td>
<td>Represents ue_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled UE event &lt;s&gt; in state &lt;s&gt;&quot;</td>
</tr>
<tr>
<td>140006</td>
<td>Represents pdn_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled PDN event &lt;s&gt; in state &lt;s&gt;&quot;</td>
</tr>
<tr>
<td>140007</td>
<td>Represents epsb_fsm_illegal_event in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled EPSB event &lt;s&gt; in state &lt;s&gt;&quot;</td>
</tr>
<tr>
<td>10726</td>
<td>Represents saegwdrv_generic_error &quot;[IMSI &lt;IMSI&gt;] s&quot;</td>
</tr>
</tbody>
</table>

### Configuring S-GW to Include IMSI/IMEI in Event Logs

The **include-ueid** keyword has been added to the **logging** command in Global Configuration Mode. When enabled, the previously mentioned system events of type error and critical will provide the IMSI/IMEI in the logging details, if available.

Use the following example to enable/disable the **logging include-ueid** functionality.

```plaintext
configure
    logging include-ueid
    no logging include-ueid
end
```

**Notes:**
• **no** disables the inclusion of the IMSI/IMEI in system event logs of type error and critical

• To determine if **logging include-ueid** is enabled on the S-GW, use the **show configuration** command in Exec Mode. This command will indicate one of the following:
  * logging include-ueid (when enabled)
  * no logging include-ueid (when disabled)

### 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.
Feature Description

GTPv2 message collisions occur in the network when a node is expecting a particular procedure message from a peer node but instead receives a different procedure message from the peer. GTP procedure collisions are quite common in the network; especially with dynamic Policy and Charging Control, the chances of collisions happening in the network are very high.

These collisions are tracked by statistics and processed based on a pre-defined action for each message collision type. These statistics assist operators in debugging network issues.

Important

If the SAEGW is configured as a pure P-GW or a pure S-GW, operators will see the respective collision statistics if they occur.

Relationships to Other Features

- This feature is a part of the base software license for the P-GW/SAEGW/S-GW. No additional license is required.
- A P-GW, S-GW, or SAEGW service must be configured to view GTPv2 collision statistics.
How It Works

Collision Handling

As GTPv2 message collisions occur, they are processed by the P-GW, SAEGW, and S-GW. They are also tracked by statistics and with information on how the collision was handled.

Specifically, the output of the `show egtpc statistics verbose` command has been enhanced to provide information on GTPv2 message collision tracking and handling at the S-GW and P-GW ingress interfaces. The information available includes:

- **Interface**: The interface on which the collision occurred: SGW (S4/S11), SGW (S5), and P-GW (S8).
- **Old Proc (Msg Type)**: Indicates the ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure. Note that the Old Proc are per 3GPP TS 23.401.
- **New Proc (Msg Type)**: The new procedure and message type. Note that the New Proc are per 3GPP TS 23.401.
- **Action**: The pre-defined action taken to handle the collision. The action can be one of:
  - No Collision Detected
  - Suspend Old: Suspend processing of the original (old) message, process the new message, then resume old message handling.
  - Abort Old: Abort the original message handling and processes the new message.
  - Reject New: Reject the new message, and process the original (old) message.
  - Silent Drop New: Drop the new incoming message, and the process the old message.
  - Parallel Hndl: Handle both the original (old) and new messages in parallel.
  - Buffer New: Buffer the new message and process it once the original (old) message has been processed.
  - Counter: The number of times each collision type has occurred.

The `Message Collision Statistics` section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.

**Sample output:**

```
Message Collision Statistics
Interface    Old Proc (Msg Type)    New Proc (Msg Type)    Action    Counter
SGW(S5)      NW Init Bearer Create (95) NW Init PDN Delete (99) Abort Old 1
```

In this instance, the output states that at the S-GW egress interface (S5) a Bearer creation procedure is going on due to a CREATE BEARER REQUEST(95) message from the P-GW. Before its response comes to the S-GW from the MME, a new procedure PDN Delete is triggered due to a DELETE BEARER REQUEST(99) message from the P-GW.
The action that is carried out due to this collision at the eGTP-C layer is to abort (Abort Old) the Bearer Creation procedure and carry on normally with the Initiate PDN Delete procedure. The Counter total of 1 indicates that this collision happened once.

**Example Collision Handling Scenarios**

This section describes several collision handling scenarios for the S-GW and P-GW.

The S-GW processes additional collisions at the S-GW ingress interface for:

1. Create Bearer Request or Update Bearer Request messages with Inter-MME/Inter-RAT Modify Bearer Request messages (with and without a ULI change).
2. Downlink Data Notification (DDN) message with Create Bearer Request or Update Bearer Request.

The S-GW behavior to handle these collision scenarios are as follows:

1. A CBReq and MBReq [(Inter MME/Inter RAT (with or without ULI change)] collision at the S-GW ingress interface results in the messages being handled in parallel. The CBReq will wait for a Create Bearer Response (CBRsp) from the peer. Additionally, an MBReq is sent in parallel to the P-GW.
2. An UBReq and MBReq [(Inter MME/Inter RAT (with or without a ULI change)] collision at the SGW ingress interface is handled with a suspend and resume procedure. The UBReq would be suspended and the MBReq would be processed. Once the MBRsp is sent to the peer from the SGW ingress interface, the UBReq procedure is resumed.
3. Create Bearer Request (CBR) or Update Bearer Request (UBR) with Downlink Data Notification (DDN) messages are handled parallel.

As a result, no S-GW initiated Cause Code message 110 (Temporarily rejected due to handover procedure in progress) will be seen as a part of such collisions. Collisions will be handled in parallel.

The following GTP-C example collision handling scenarios may also be seen on the P-GW:

**DBCmd/MBreq Collision Handling**

The P-GW enables operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW.

There are three CLI-controlled options to handle the collision between the DBcmd and MBReq messages:

- Queue the DBcmd message when the MBreq message is pending. The advantage of this option is that the DBcmd message is not lost for most of the collisions. It will remain on the P-GW until the MBRsp is sent out.
- Drop the DBcmd message when the MBreq message is pending. Note that with this option the S-GW must retry the DBcmd.
- Use pre-StarOS 19.0 behavior: abort the MBreq message and handle the DBcmd message. The advantage of this option is that it provides backward compatibility if the operator wants to retain pre-StarOS 19.0 functionality.

The CLI command collision handling provides more flexibility in configuring the handling of the DBcmd message and MBReq message collision scenario. Also refer to Configuring DBcmd Message Behavior, on page 84 in this document for instructions on how to configure the behavior for this collision handling scenario.

**MBReq/CBreq Parallel Processing; Handling CBRsp**

The P-GW/S-GW has handles the following example collision scenario:
The node queues the CBRsp message and feeds the CBRsp message to the P-GW/S-GW session manager when the MBRsp is sent out. As a result, operators will see no retransmission of CBRsp messages from the MME.

**Handling UBRsp when Transaction is Suspended:**
The P-GW/S-GW handles the following example collision scenario:
When the P-GW/S-GW receives an UBRsp message, then the P-GW/S-GW handles the UBRsp message for the suspended transaction. As a result, The UBRsp message will be buffered until the MBRsp message is sent out.

**Limitations**
There are no known limitations to the collision handling feature on the P-GW/SAEGW/S-GW.

**Standards Compliance**
Specifications and standards do not specify any hard rules for collision handling cases.

**Configuring Collision Handling**
Operators can use the Command Line Interface (CLI) to configure the behavior of the P-GW for handling the following GTPv2 message collision:

- DBcmd Message when the MBreq Message for the Default Bearer is pending at the P-GW

| Important | Configuration via the CLI is not required for all other P-GW and S-GW collision handling scenarios. |

**Configuring DBcmd Message Behavior**
Use the following example to configure the collision handling behavior for the Delete Bearer command message when the Modify Bearer Request message for the Default Bearer is pending at the P-GW.

```bash
configure
  context context_name
    egtp-service egtp_service_name
      collision-handling dbcmd-over-mbreq { drop | queue }
      { default | no } collision-handling dbcmd-over-mbreq
end
```

Notes:

- **drop**: Drop the DBcmd message when the MBreq message is pending.
- **queue**: Queue the DBcmd message when the MBreq message is pending.
- The default behavior is to abort the MBReq message and handle the DBcmd message.
Verifying the Configuration

To verify the DBcmd Message when the MBreq Message for the Default Bearer is pending at the P-GW configuration, use the following command in Exec Mode:

```
show egtpc service all
```

Collision handling: DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort MBreq and handle Dbcmd>

Monitoring the Collision Handling Feature

This section describes how to monitor the collision handling feature.

Collision Handling Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the collision handling on the P-GW/SAEGW/S-GW feature.

**show configuration**

The output of this command indicates if collision handling for the DBcmd message when the MBreq message is pending is enabled or disabled.

- collision-handling dbcmd-over-mbreq queue
- no collision-handling dbcmd-over-mbreq queue

**show egtp-service all**

The output of this command indicates how the P-GW is configured to handle the DBcmd Message when the MBreq Message for the Default Bearer is pending at the P-GW.

- Collision handling:
  - DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort MBreq and handle Dbcmd>

**show egtp statistics verbose**

The output of this command has been enhanced to provide detailed information for all supported GTPv2 message collisions at the P-GW/S-GW ingress interface, including:

- The interface on which the collision occurred.
- The ongoing procedure at eGTP-C when a new message arrived at the interface which caused the collision. The Msg Type in brackets specifies which message triggered this ongoing procedure.
- The new procedure and message type.
• The pre-defined action taken to handle the collision.
• The number of times each collision type has occurred.

---

**Important**

The *Message Collision Statistics* section of the command output appears only if any of the collision statistics have a counter total that is greater than zero.
CHAPTER 5

Session Tracing

This chapter provides information on subscriber session trace functionality that allows an operator to trace subscriber activity at various points in the network and at various level of detail. Subscriber session tracing is supported on the following UMTS/EPC GW network elements:

- GGSN
- P-GW
- SAEGW
- S-GW

Important

For detailed information for session tracing on the MME, refer to the MME Administration Guide.

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 includes a feature description, configuration procedures, monitoring commands, and a session tracing file example.

- Session Tracing Overview, page 87
- Configuring Session Trace Functionality, page 91
- Monitoring the Session Trace Functionality, page 102
- Supported SAEGW Session Trace Configurations, page 103
- Session Trace File Example, page 107

Session Tracing Overview

Session Trace capability enables an operator to trace subscriber activity at various points in the network and at various levels of detail. The trace can be subscriber initiated (that is, signaling based) or management
initiated from the CLI (Command Line Interface) and can be propagated throughout the access cloud via the various signaling interfaces available to the UMTS/EPC network element.

Essentially, 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 User Equipment (UE) connects to the access network.

All monitored activity is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a File Transfer Protocol (FTP) or secure FTP (sFTP) connection.

---

**Important**

Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

As can be seen in the following illustration, of the three Network Elements (NEs) shown, one NE is actively tracing data on one or more interfaces. All data collected is stored as files in an XML format and then transferred to the collection entity using (S)FTP or FTP. Note that IPv4 or IPv6 connectivity is required between the NE and the TCE in order to transfer the files.

*Figure 22: Session Tracing Architecture*
Session Trace Types

There are three types of session trace functions available.

- **Management Trace**: The operator sends an activation request via the CLI directly to the UMTS/EPC network element where the trace is to be initiated. The network element establishes the trace session and waits for a configured trigger event to start actively tracing. When management-initiated trace activations are executed at the network element, they are never propagated to other NEs whether or not it is involved in the actual recording of the call.

- **Random Trace**: Enables or disables the subscriber session trace functionality based on a random trace on the UMTS/EPC network element. The trace control and configuration parameters are configured directly in the specified network element through the **random trace** CLI command. There is no propagation of trace parameters in random based trace activation. This NE shall not propagate the received data to any other NEs whether or not it is involved in the actual recording of the call. If enabled, the subscriber selection will be based on random logic all instances of session on the specified UMTS/EPC network element.

- **Signaling Trace**: With a signaling based activation, the trace session is indicated to the UMTS/EPC network element 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). Signaling based activations are always propagated to neighboring NEs even if the current NE does not participate in the trace (either they not enabled by configuration or not present in the configured trace parameters).

---

**Important**

Note that the maximum number of unique International Mobile Subscriber Identification (IMSI) numbers or International Mobile Equipment Identification (IMEI) numbers cannot exceed 32; however, each NE can trace all 32 unique IMSI/IMEIs.

**Caution**

Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

---

**Session Trace 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, an (S)FTP connection to the Trace Collection Entity (TCE) is established if one does not already exist. The NE will store up to 2 MB of XML data on its local disk to allow for the (S)FTP connection to be established and the files to be pushed to or pulled from the TCE.

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

Data Collection

Data collection is done inline by each of the NEs. In order to reduce the overhead on a per-control packet basis, a copy of the entire packet is made and stored into an internal database (DB) of packets.

The local internal path for the trace database is /hd-raid/trace.

This storage is done regardless of the trace depth. After xx bytes (or xx messages) have been stored or a configurable number of seconds have elapsed, all cached data is encoded in the standard XML format and written out to a file to be forwarded to/pulled from the TCE. If there is no TCE active, the UMTS/EPC network element will continue to cache data and create trace files as long as there is space available before stopping the trace recording session. Once the connection to the TCE becomes active, all cached data will be sent immediately to the TCE.

Data Forwarding

When a session is activated, the IP address of the TCE is supplied in the session activation request. Upon activation and if the push mode is used, a check is made to see if there is already an (S)FTP connection to the TCE. If so, it is used for all traffic associated with this trace session. If not, an (S)FTP connection is made to the TCE using the supplied IP address. Data is buffered locally and trace files generated until the connection is established. Once the connection is established, all previously created trace files are sent to the TCE. Note that the (S)FTP connection is established to the TCE at session activation regardless of whether or not a trace recording session has been triggered. The (S)FTP connection is maintained until the trace session is deactivated.

Note the following:

• If a default TCE IP Address is supplied when the trace capability is configured, a default (S)FTP connection is made to the remote TCE.
• The TCE can be reachable either via IPv4 or IPv6 addressing. The supplied TCE address indicates the version.
• If the push mode is not used, the files are stored on the local hard drive (/hd-raid/trace) and must be pulled off by the TCE using FTP or SFTP.

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added for the Session Trace feature:
Configuring Session Trace Functionality

Configuring Session Trace on the UMTS/EPC network element consists of the following:

1. **Enabling Session Tracing**, on page 91
2. **Configuring a Session Trace Template for the Management Trace Function**, on page 93
3. **Configuring a Management Session Trace**, on page 96
4. **Configuring a Signaling Session Trace**, on page 98
5. **Configuring a Random Trace**, on page 99

The trace files can be stored locally, or pushed to a Trace Collection Entity (TCE) specified in the various trace commands.

---

**Important**

Not all combinations of Session Trace configuration types are allowed on the SAEGW. For details on the supported session trace configuration types, refer to **Supported SAEGW Session Trace Configurations**, on page 103 in this document.

---

### Enabling Session Tracing

Session Tracing functionality must first be enabled before a specific management, random, or signaling session trace can be configured.

The following commands enable or disable the subscriber session trace functionality based on a specified subscriber device or ID on one or all instances of a session on a specified UMTS/EPC network element.

Use the following example to enable session tracing on the UMTS/EPC network element:

```
cfg
  config
    session trace network-element { all | ggsn | hnb | mme | pgw | saegw | sgw } [ file-type <a-type | b-type> ] [ tce-mode none | transport ftp | sftp ] username [ encrypted password | password ] path directory_path collection timer ctimer_value
  end
```

**Notes:**

- **session trace network-element**: Enables Session Tracing functionality on the specified network element. To enable session tracing for all supported network elements, enter **all**.
• file-type { a-type | b-type }: Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. Note that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs. The default is a-type.

• tce-mode : Specifies that trace files are stored locally and must be pulled by the TCE (none) or trace files are pushed to the TCE (push). The default is none.

• transport : Specifies the method by which the trace files are pushed to the TCE (either ftp or sftp.) The default is sftp.

• username: Must be specified if the tce-mode is push.

• password: Must be specified if the tce-mode is push.

• encrypted: Specifies that the password used to push files to the TCE server will be encrypted.

• password: Specifies the password to use to push files to the TCE server. The user name can be from 1 to 31 alphanumeric characters.

• collection-timer: Specifies the amount of time, in seconds, to wait from initial activation/data collection before data is reported to TCE. The default is 10 seconds.

• retry-timer: Specifies the amount of time, in seconds, to wait before retrying a file transfer if the previous transfer failed. The default is 60 seconds.

Example:
```
session trace network-element saegw tce-mode push transport sftp path /SessionTrace username root encrypted password 5c4a38dc2ff61f72 collection-timer 5
```

Verifying that Session Tracing is Enabled

Use the following example to verify that session tracing functionality is enabled on the UMTS/EPC network element:
```
show session trace statistics
```
The output indicates for which NEs session tracing is enabled, and also indicates the configured trace type, where applicable. For example:
```
Network element status:
MME: Enabled Cell-Trace: Disabled
S-GW: Enabled
SAEGW Enabled
PGW: Trace-Type: None
SGW: Trace-Type: None
```

Disabling Session Trace Functionality

Use the following example to disable session tracing functionality:
```
config
no session trace network-element { all | ggsn | hnbgw | mme | pgw | saegw | sgw }
end
```
Configuring a Session Trace Template for the Management Trace Function

Operators must create a template for a management trace in Global Configuration Mode. Management traces executed in Exec mode will use the template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

Note that to activate subscriber session traces for specific IMSI/IMEI, the operator will use the Exec mode `session trace subscriber` command specifying a pre-configured template and the IMSI/IMEI, trace reference, and TCE address.

Use the following example to configure a template for use with the `session trace subscriber` command:

```bash
config
  template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name template_name
```

Once this command is entered, the user is placed in `Session Trace Template Configuration Mode`. In this mode, the operator selects the interfaces to be traced for the selected network element.

**Important**

The options available in `Session Trace Template Configuration Mode` are dependent on the network element selected in the previous command.

For the GGSN, MME, P-GW and S-GW, enter the following command in `Session Trace Template Configuration Mode`:

```bash
interface interface_name
end
```

For the SAEGW, enter the following command in `Session Trace Template Configuration Mode`:

```bash
{ func-pgw | func-sgw } interface interface_name
end
```

- **Notes**: The available UMTS/EPC network elements provide various interface options for the session trace template.

**GGSN**

Available `ggsn` interfaces include:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

**HNBGW**
Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the iucs interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the iups interface between the HNB-GW and the SGSN.

**MME**

Available **mme** interfaces include:

- **all**: Specifies that all MME interfaces are to be traced.
- **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s13**: Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.
- **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

**P-GW**

Available **pgw** interfaces are:

- **all**: Specifies that all available P-GW interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.

- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

**SAEGW**

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

- **Available **func-pgw** interface options are:**
  - **all**: Specifies that all available **func-pgw** interfaces are to be traced.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
  - **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
  - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

- **Available **func-sgw** interface options are:**
  - **all**: Specifies that all available **func-sgw** interfaces are to be traced.
  - **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
* **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

**S-GW**

The available **sgw** interfaces are:

- **all**: Specifies that all available S-GW interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

### Verifying the Session Trace Template Configuration

To verify the session trace configuration, enter the following command in Exec Mode:

```
show session trace template network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } all
```

The output provides the template name, the NE type, and all interfaces configured for tracing.

### Disabling the Session Trace Template Configuration

Use the following example to disable the session trace template configuration:

```
no template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw }
```

### Disabling the Session Trace Template Configuration per Network Element and Subscriber

To disable the session trace template per network element and subscriber:

```
no session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name
```

### Configuring a Management Session Trace

Session tracing functionality must be enabled before a management trace can be configured. Refer to Enabling Session Tracing, on page 91 for the procedure.

To configure a management session trace on the UMTS/EPC network element from Exec Mode:

```
session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name
```

**Notes:**
• **template-name**: Specifies the name of the session trace template to use for this session trace. Session
  trace templates are configured in *Global Configuration Mode* using the `template-session-trace` command.
  Management traces executed in Exec mode will use the specified template.

• **imsi id**: Specifies the International Mobile Subscriber Identification Number for the subscriber.

• **imei id**: Specifies the International Mobile Equipment Identification number for the subscriber.

• **trace-ref**: Specifies the Trace Reference for this subscriber management trace. It must be composed of
  the Mobile Country Code (MCC) + the Mobile Network Code (MNC) + a 3 byte octet string Trace ID.
  Example: 31001212349.

• **collection-entity**: Specifies the IP address of the Trace Collection Entity (TCE) to which the trace file
  generated will be sent. The IP address must be in IPv4 format.

**Example:**

This following is a complete example showing the configuration of a subscriber management trace for all
S-GW and P-GW interfaces. It consists of enabling session tracing on the SAEGW, creating the session trace
template for all S-GW and P-GW interfaces, and then executing the subscriber management trace for a specific
IMSI using the template.

```config
  config
    session trace network-element saegw
  end
  config
    template-session-trace network-element saegw template-name saegw_all
       func-pgw interface all
       func-sgw interface all
  end
  session trace subscriber network-element saegw template-name saegw_all imsi 123456789012345
  trace-ref 123456789012 collection-entity 1.1.1.1
```

**Verifying the Management Trace Configuration**

To verify that the management trace configuration for the subscriber is enabled, enter the `show session trace
statistics` command from Exec Mode. Verify that the correct NE(s) show their Network element status as
*Enabled*. For example:

```
SAEGW Enabled
  Trace-Type: M
PGW: Trace-Type: M
SGW: Trace-Type: M
```

Use the following example to verify that specific parameters have been activated for the subscriber management
trace:

```sh
show session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace-ref
```

The output fields show the NE Type and the Trace Type configured for each network element. Below is
sample output for an SAEGW management trace configuration:

```
NE Type: SAEGW
  Trace-Type: M
PGW:
  Trace-Type: M
SGW:
```

```
Traced Interfaces:
PGW: <P-GW interfaces configured for the trace.>
SGW: <S-GW interfaces configured for the trace.>
```
Disabling the Management Trace Configuration

To disable the management trace configuration from Exec Mode:

```bash
no session trace subscriber network element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace ref
```

Configuring a Signaling Session Trace

Session trace functionality must be enabled before a signaling session trace can be configured. Refer to Enabling Session Tracing, on page 91 for the procedure.

To configure a signaling session trace:

```bash
session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw | func-pgw | func-sgw | sgw }
```

Notes:

- **func-pgw**: Enables tracing of the P-GW signaling under the SAEGW
- **func-sgw**: Enables tracing of the S-GW signaling under the SAEGW
- If neither **func-sgw** or **func-pgw** is specified, then the signaling trace will be performed for all P-GW and S-GW interfaces of the SAEGW.
- **collection-entity**: Specifies the IPv4 or IPv6 address of the Trace Collection Entity (TCE) to which the trace files are sent.

Example:

This example configures a signaling session trace for all S-GW and P-GW interfaces under an SAEGW:

```bash
session trace signaling network-element saegw
```

Verifying the Signaling Session Trace Configuration

To verify the signaling session trace configuration:

```bash
show session trace statistics
```

Look for the following fields to verify the signaling trace configuration. For example:

```
Network element status:

SAEGW Enabled

  PGW: Trace-Type: S
  SGW: Trace-Type: S
```

Disabling the Signaling Session Trace

To deactivate signaling trace on the SAEGW:

```bash
no session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw | func-pgw | func-sgw | sgw }
```
Configuring a Random Trace

Session trace functionality first must be enabled on the UMTS/EPC network element before a random trace can be configured. Refer to Enabling Session Tracing, on page 91 in this chapter for the procedure.

The following command enables or disables the subscriber session trace functionality based on a random trace on the UMTS/EPC network element. If enabled, the subscriber selection will be based on random logic for all instances of session on a specified network element.

To configure a random session trace:

```
session trace random range network-element { ggsn | hnbgw | pgw | saegw | sgw [ func-pgw | func-sgw ] } interface [ all | interface ] collection-entity ipv4_address
```

Notes:

- **session trace random range**: Enables a random trace for a specified number of subscribers. Valid entries are from 1 to 1000 subscribers.
- `{ ggsn | hnbgw | pgw | saegw | sgw [ func-pgw | func-sgw ] }`: Specifies that the random trace is enabled for the selected network element.
- **func-pgw**: Enables random tracing of the P-GW interfaces under the SAEGW.
- **func-sgw**: Enables random tracing of the S-GW interfaces under the SAEGW.
- If neither **func-pgw** or **func-sgw** are specified, random tracing will occur for both the P-GW and S-GW.
- **interface**: Specifies the network interfaces for the random trace. Interfaces available depend on the network element type selected.

**GGSN**

Available **ggsn** interfaces are:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

**HNBGW**

Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the **iucs** interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the iups interface between the HNB-GW and the SGSN.

**P-GW**

Available P-GW interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

**SAEGW**

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

Available SAEGW **func-pgw interface** options are:

- **all**: Specifies that all **func-pgw** interfaces configured under an SAEGW are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
• **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.

• **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.

• **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

• **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.

Available SAEGW **func-sgw** interfaces are:

• **all**: Specifies that all available **func-sgw** interfaces under an SAEGW are to be traced.

• **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.

• **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.

• **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.

• **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.

• **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

**S-GW**: Available **sgw** interfaces are:

• **all**: Specifies that all interfaces are to be traced.

• **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.

• **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.

• **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.

• **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.

• **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

• **collection-entity** specifies the IPv4 address of the Trace Collection Entity (TCE)

**Example:**

To enable random tracing on a range of 40 SAEGW subscribers on all S-GW interfaces and the s5 interface of the P-GW in the SAEGW, enter the following sample command:

```
session trace random 40 network-element saegw func-pgw interface s5 func-sgw interface all collection-entity 1.1.1.1
```
Verifying the Random Trace Configuration

To verify the random session trace configuration:

**show session trace statistics**

Look for the fields that verify that Random Session Trace has been enabled for the network element. For example:

```
Network element status:
...
SAEGW Enabled
PGW: Trace-Type: R
SGW: Trace-Type: R Configured-Random: 40
```

Disabling the Random Trace for a Specific Network Element

To disable random session tracing for a specific network element:

**no session trace random network-element { ggsn | hnbgw | pgw | saegw | sgw [ func-pgw | func-sgw ] }**

Monitoring the Session Trace Functionality

This section provides information on commands you can use to monitor the session trace functionality

**show session trace statistics**

This command provides high-level statistics on the current use of the session trace functionality, including:

- Number of current trace sessions
- Number of total trace sessions
- Total sessions activated
- Number of activation failures
- Number of sessions triggered
- Total messages traced
- Number of current TCE connections
- Total number of TCE connections
- Total number of files uploaded to all TCEs

**show session trace subscriber network-element trace-ref**

This command shows detailed information about a specific trace, based on the trace-ref value of the session and network element type. It includes activation time, IMSI, start time, number of trace messages, and total number of files created. It also lists the interfaces that this session trace is configured to trace.

**show session trace trace-summary**

This command provides the trace-ref value of all session traces, broken down by network element type.
show session trace tce-summary
This command provides the IP address and index information for all configured TCEs.

show session trace tce-address
This command provides detailed information about a specific TCE, including IP address, start time, and total number of files uploaded.

Supported SAEGW Session Trace Configurations

Different tracing configurations are supported on the SAEGW. The different combinations of session tracing types depend on Call Type, Trace Type, and whether the operator would like to configure a Func-SGW and/or a Func-PGW trace.

Note the following:
- M = Management
- R = Random
- S = Signaling

Table 9: Supported Session Trace Configurations on the SAEGW

<table>
<thead>
<tr>
<th>Func-S-GW Trace Config</th>
<th>Func-P-GW Trace Config</th>
<th>Call Type</th>
<th>S-GW Trace?</th>
<th>P-GW Trace?</th>
<th>Output</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>M</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td>When M traces are enabled for Func-SGW, Func-PGW and call type Collapsed both S-GW control messages (gtpv2) and P-GW control messages shall be traced in 1 SAEGW trace file.</td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>S</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
</tbody>
</table>
### Supported SAEGW Session Trace Configurations

<table>
<thead>
<tr>
<th>Func-S-GW Trace Config</th>
<th>Func-P-GW Trace Config</th>
<th>Call Type</th>
<th>S-GW Trace?</th>
<th>P-GW Trace?</th>
<th>Output</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>M+S</td>
<td>M+S</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>2 SAEGW trace files generated</td>
<td>When M+S traces are enabled for Func-S-GW, Func-P-GW and call type collapsed both -SGW control messages (gtpv2) and P-GW control messages shall be traced in 2 SAEGW trace files. One Trace file due to Management and other due to Signaling. Both files have the same contents.</td>
</tr>
<tr>
<td>M+R</td>
<td>M+R</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>R</td>
<td>Collapsed</td>
<td>No</td>
<td>No</td>
<td>None</td>
<td>Not a valid trace configuration</td>
</tr>
<tr>
<td>R</td>
<td>S</td>
<td>Collapsed</td>
<td>No</td>
<td>No</td>
<td>None</td>
<td>Not a valid trace configuration</td>
</tr>
<tr>
<td>M</td>
<td>R</td>
<td>Collapsed</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>M</td>
<td>Collapsed</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>S</td>
<td>Collapsed</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>M</td>
<td>Collapsed</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M+S</td>
<td>M</td>
<td>Collapsed</td>
<td>Yes</td>
<td>No</td>
<td>2 SAEGW trace files generated</td>
<td>P-GW Trace is not generated</td>
</tr>
<tr>
<td>M</td>
<td>M+S</td>
<td>Collapsed</td>
<td>No</td>
<td>Yes</td>
<td>2 SAEGW trace files generated, but S-GW trace not generated</td>
<td>S-GW Trace is not generated</td>
</tr>
</tbody>
</table>
### Supported SAEGW Session Trace Configurations

<table>
<thead>
<tr>
<th>Func-S-GW Trace Config</th>
<th>Func-P-GW Trace Config</th>
<th>Call Type</th>
<th>S-GW Trace?</th>
<th>P-GW Trace?</th>
<th>Output</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>M+S</td>
<td>S</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>2 SAEGW trace files generated</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>M+S</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>2 SAEGW trace files generated</td>
<td></td>
</tr>
<tr>
<td>M+R</td>
<td>M</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>M+R</td>
<td>Collapsed</td>
<td>Yes</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M+R</td>
<td>R</td>
<td>Collapsed</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>M+R</td>
<td>Collapsed</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>n/a</td>
<td>Pure S</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td>Config for func-P-GW is not applicable for Pure S calls</td>
</tr>
<tr>
<td>S</td>
<td>n/a</td>
<td>Pure S</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>n/a</td>
<td>Pure S</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>M+S</td>
<td>n/a</td>
<td>Pure S</td>
<td>Yes</td>
<td>No</td>
<td>2 SAEGW trace files generated</td>
<td></td>
</tr>
<tr>
<td>M+R</td>
<td>n/a</td>
<td>Pure S</td>
<td>Yes</td>
<td>No</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>R+S</td>
<td>n/a</td>
<td>Pure S</td>
<td>No</td>
<td>No</td>
<td>None</td>
<td>Not a valid trace configuration.</td>
</tr>
<tr>
<td>n/a</td>
<td>M</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>S</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>R</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
</tbody>
</table>
### Supported SAEGW Session Trace Configurations

<table>
<thead>
<tr>
<th>Func-S-GW Trace Config</th>
<th>Func-P-GW Trace Config</th>
<th>Call Type</th>
<th>S-GW Trace?</th>
<th>P-GW Trace?</th>
<th>Output</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>M+S</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>2 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>M+R</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>1 SAEGW trace file generated</td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>R+S</td>
<td>Pure P</td>
<td>No</td>
<td>Yes</td>
<td>None</td>
<td>Not a valid trace configuration</td>
</tr>
</tbody>
</table>
Session Trace File Example

This section provides an example of a signaling trace file.

**Figure 23: Signaling Trace File Example (1 of 3)**

```
<<<OUTBOUND  10:04:53:997 EventId:141005(3)
[MME-S1l]GTPv2C Tx PDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x000004D3, Message type: GTP_CTRL_SESSION_ACTIVATION (0x47)
Sequence Number: 0x000401 (1025)
GTP HEADER
  Version number: 2
  TEID flag: Present
  Piggybacking flag: Not present
  Message Length: 0x003A (58)
INFORMATION ELEMENTS
  IMSI:
    Type: 1 Length: 8 Inst: 0
    Value: 123456789012345
    hex: 0100 0800 2143 6587 0921 4385
  Trace Info:
    Type: 96 Length: 34 Inst: 0
    Value:
      MCC: 123
      MNC: 056
      Trace Id: 03039

  Triggering Event: 1/0: Event shall be traced / not traced.
  MSC Server:
    SS: 0
    HANDOVERS: 0
    LU/IMSI ATT/DEN: 0
    MO & MT SMS: 0
    MO & MT CALLS: 0
  MGW:
    CONTEXT: 0
  SGSN:
    MEKS CONTEXT: 0
    RAU/GPRS ATT/DEN: 0
    MO & MT SMS: 0
    PDP CONTEXT: 0
  GGSN:
    MEKS CONTEXT: 0
    PDP CONTEXT: 0
  MME:
    HANDOVERS: 1
    BEARER ACT/MOD/DEL: 1
    UE INIT PDN DISC: 1
    INIT ATT/TAU/DEN: 1
    SERVICE REQUEST: 1
    UE INIT PDN CON REQ: 1
```

**Figure 24: Signaling Trace File Example (2 of 3)**
Session Trace File Example

PGW:

BEARER ACT/MOD/DEL: 1
PDN CONN TERMINATE: 1
PDN CONN CREATE: 1

SGW:

BEARER ACT/MOD/DEL: 0
PDN CONN TERMINATE: 0
PDN CONN CREATE: 0

List of NE Types: 1/0: Trace Session activated/ not activated.

SGW: 0
MME: 1
BMSC: 0
RNC: 0
GGSN: 0
SGSN: 0
MGW: 0
MSC-S: 0
E-NODEB: 1
PDN-GW: 1

Trace Depth:
Value: 5 [MAXIMUM w/o Vendor Specific Extension]

List of Interfaces: 1/0: Interface will be traced/ not traced.

SGS Server:
CAP: 0
MAP-F: 0
MAP-E: 0
MAP-B: 0
MAP-G: 0
MC: 0
IU: 0
A: 0
MAP-C: 0
MAP-D: 0

MGW:
IU-UP: 0
Nd-UP: 0
MC: 0

GGSN:
GE: 0
GS: 0
MAP-GF: 0
MAP-GD: 0
MAP-GR: 0
GR: 0
IU: 0
GB: 0

GGSN:
QMB: 0
GI: 0
GN: 0

Figure 25: Signaling Trace File Example (3 of 3)
Session Tracing

Session Trace File Example

RNC:
  UU: 0
  IUB: 0
  IUR: 0
  IU: 0

BSC:
  GM: 0

MME:
  S11: 1
  S10: 1
  S6A: 1
  S3: 1
  S1-MME: 1

SGW:
  GXC: 0
  S11: 0
  S8B: 0
  S5: 0
  S4: 0

PDN-GW:
  SGi: 0
  S8B: 1
  GX: 1
  S6B: 0
  S5: 1
  S2C: 0
  S2B: 0
  S2A: 0

ENODEB:
  UU: 0
  X2: 1
  S1-MME: 1

TCE IP Addr:
  IPV4 Addr: 1.1.1.1

Hex: 0000 2200 2163 5400 3039 0000 0000 0000
  003F 7040 0305 0000 0000 0000 0000 1F00
  6803 0101 0101

S-GW Administration Guide, StarOS Release 19

109
Direct Tunnel for 4G (LTE) Networks

This chapter briefly describes support for direct tunnel (DT) functionality over an S12 interface for a 4G (LTE) network to optimize packet data traffic.

Cisco LTE devices (per 3GPP TS 23.401 v8.3.0) supporting direct tunnel include:

- Serving GPRS Support Node (S4-SGSN)
- 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 following sections are included in this chapter:

- Direct Tunnel for 4G Networks - Feature Description, page 111
- How It Works, page 114
- Configuring Support for Direct Tunnel, page 142
- Monitoring and Troubleshooting Direct Tunnel, page 145

Direct Tunnel for 4G Networks - Feature Description

The amount of user plane data will increase significantly during the next few years because of High Speed Packet Access (HSPA) and IP Multimedia Subsystem technologies. Direct tunneling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates. Direct Tunnel (DT) offers a solution that optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.
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.

Establishment of a direct tunnel is controlled by the SGSN; for 4G networks this requires an S4 license-enabled SGSN setup and configured as an S4-SGSN.

Once a direct tunnel is established, the S4-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 PDP context activation.

Figure 26: GTP-U Direct Tunneling

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 S4-SGSN/S-GW to handle the user plane processing.
A direct tunnel is achieved upon PDP context activation when the S4-SGSN establishes a user plane tunnel (GTP-U tunnel) directly between the RNC and the S-GW over an S12 interface, using a Create Bearer Response or Modify Bearer Request towards the S-GW.

**Figure 27: Direct Tunneling - LTE Network, S12 Interface**

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.

S4-SGSN supports establishment of a GTP-U direct tunnel between an RNC and the S-GW under the scenarios listed below:

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without S-GW change
- Intra SGSN Routing Area Update with S-GW change
- Intra SGSN SRNS relocation without S-GW change
- Intra SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation without S-GW relocation
- E-UTRAN-to-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
• UTRAN-to-E-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
• Network Initiated PDP Activation

Scenarios that vary at S4-SGSN when direct tunneling is enabled, as compared to DT on a 2G or 3G SGSN using the Gn interface, include:
• RAB Release
• Iu Release
• Error Indication from RNC
• Downlink Data Notification from S-GW
• Downlink Data Error Indication from S-GW
• MS Initiated PDP Modification
• P-GW Initiated PDP Modification while the UE is IDLE
• HLR/HSS Initiated PDP Modification
• Session Recovery with Direct Tunnel

The above scenarios exhibit procedural differences in S4-SGSN when a direct tunnel is established.

How It Works

DT functionality enables direct user plane tunnel between RNC and SGW within the PS domain. With direct tunneling the S4-SGSN provides the RNC with the TEID and user plane address of the S-GW, and also provides the S-GW with the TEID and user plane address of the RNC.

The SGSN handles the control plane signaling and makes the decision when to establish the direct tunnel between RNC and S-GW, or use two tunnels for this purpose (based on configuration).
DT Establishment Logic

The following figure illustrates the logic used within the S4-SGSN/S-GW to determine if a direct tunnel will be setup.

*Figure 28: Direct Tunneling - Establishment Logic*
Establishment of Direct Tunnel

The S4-SGSN uses the S12 interface for DT.
Direct Tunnel Activation for Primary PDP Context

For the PDP Context Activation procedure this solution uses new information elements (IEs) for the GPRS Tunnelling Protocol v2 (GTPv2) as defined in TS 29.274. SGSN provides the user plane addresses for RNC and S-GW as S12U FTEIDs as illustrated in the figure below.

The sequence for establishing a direct tunnel between the RNC and S-GW during PDP activation is as follows:

- SGSN sends a Create Session Request to the S-GW with the indication flag DTF (direct tunnel flag) bit set.
- In its Create Session Response, the S-GW sends the SGSN an S12U FTEID (Fully Qualified Tunnel Endpoint Identifier).
- The SGSN forwards the S-GW S12U to the RNC during the RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends the SGSN its transport address and Tunnel Endpoint ID (TEID).
- The SGSN forwards the RNC S12 U FTEID o the S-GW via a Modify Bearer Request.

Figure 29: Primary PDP Activation with Direct Tunnel

Direct Tunnel Activation for UE Initiated Secondary PDP Context

The following is the general sequence for establishing a direct tunnel for a Secondary PDP Context Activation:

- The SGSN sends a Bearer Resource Command to the S-GW with no flags set. (S-GW already knows Direct Tunnel is enabled for primary.)
- The S-GW sends a Create Bearer Response that includes the S12U FTEID to the SGSN.
• The SGSN forwards the S-GW S12U to RNC via a RAB Assignment Request.
• In its RAB Assignment Response, the RNC sends its transport address and TEID to the SGSN.
• The SGSN forwards the S12U TEID received from the RNC to the S-GW via a Create Bearer Response.

Figure 30: Secondary PDP Activation with Direct Tunnel

RAB Release with Direct Tunnel

If the SGSN receives a RAB Release Request from the RNC for bearer contexts activated with Direct Tunnel, it sends a Release Access Bearer Request to the S-GW.

Upon receiving the Release Access Bearer Request, the S-GW removes the S12 U RNC FTEID. If any downlink data appears, the S-GW sends a Downlink Data Notification because it does not have a user plane FTEID with which to forward data.
Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming/conversational bearers upon RAB release.

**Figure 31: RAB Release Procedure with Direct Tunnel**

Operators should not use conversational or streaming class bearers in S4-SGSN.

**Iu Release with Direct Tunnel**

If the SGSN receives an Iu Release and bearers are activated with direct tunneling, it sends a Release Access Bearer Request to the S-GW.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming or conversational bearers upon Iu release.
Operators should not use conversational or streaming class bearers in S4-SGSN.

**Service Request with Direct Tunnel**

When a UE is Idle and wants to establish a data or signaling connection, it sends a Service Request for data. Alternatively a UE can also send a Service Request to the SGSN when it is paged by the SGSN.
Upon receiving a Service Request for data, the SGSN establishes RABs and sends a Modify Bearer Request to the S-GW with the 12U FTEID received from the RNC.

**Figure 33: Service Request Procedure with Direct Tunnel**

**Downlink Data Notification with Direct Tunnel when UE in Connected State**

When RABs are released (but UE retains an Iu connection with the SGSN), the SGSN notifies the S-GW to release the RNC side TEIDs via a Release Access Bearer Request.

If the S-GW receives any downlink GTPU data from the P-GW after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification message from the S-GW.
If the Downlink Data Notification is received from the S-GW, all of the missing RABs are established and a Modify Bearer Request is sent to the S-GW with the RNC S12U FTEID

**Figure 34: Downlink Data Notification with Direct Tunnel**

---

**Downlink Data Notification with Direct Tunnel when UE in Idle State**

When an Iu is released the UE goes IDLE. The SGSN informs the S-GW to release the RNC side TEIDs by sending a Release Access Bearer Request. After this point if the S-GW receives any downlink GTPU data from the P-GW, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data.

If the S-GW receives any downlink GTPU data after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification from the S-GW. If a Downlink
Data Notification is received from S-GW when the UE is idle, the SGSN pages the UE before establishing the RABs. The SGSN sends a Modify Bearer Request to the S-GW with the RNC S12U FTEID.

*Figure 35: Downlink Data Notification when UE in Idle State*
**Intra SGSN Routing Area Update without SGW Change**

For a Routing Area Update without an S-GW change with Direct Tunnel, the SGSN sends a Modify Bearer Request to the S-GW with the RNC FTEID. The SGSN will establish RABs with the target RNC only if the RABs were present with the source RNC.

*Figure 36: Routing Area Update Procedure without SGW Change*

The table below includes detailed behaviors for a Routing Area Update without S-GW change.

**Table 10: Routing Area Update without S-GW Change Behavior Table**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>No</td>
<td>Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. No Modify Bearer Request to S-GW</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>No</td>
<td>Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. No Modify Bearer Request to S-GW</td>
</tr>
<tr>
<td>Scenario</td>
<td>Old RNC Status</td>
<td>Old RNC RAB</td>
<td>Old RNC DT Status</td>
<td>PLMN Change</td>
<td>NEW RNC DT Status</td>
<td>S-GW Change</td>
<td>SGSN Action</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>Some RABs</td>
<td>Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>No</td>
<td>Only the present RABs are established. MBR sent to S-GW with the bearers with RABs that are be modified and the rest released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Yes</td>
<td>Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. MBR is sent with only PLMN change. Bearer Context will not carry any TEID.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Yes</td>
<td>Supported</td>
<td>No</td>
<td>Same as above.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>No</td>
<td>Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. Modify Bearer Request to S-GW with DTF set and no user FTEID.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>No</td>
<td>Supported</td>
<td>No</td>
<td>Same as above.</td>
</tr>
</tbody>
</table>
### Establishment of Direct Tunnel

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB Status</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>Some RABs</td>
<td>Not Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>No</td>
<td>Only the present RABs are established. MBR sent to S-GW with the bearers with RABs to be modified and the rest to be released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID. Modify Bearer.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>Yes</td>
<td>Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. MBR is sent with only PLMN change. SGSN will page / Service req / establish RABs when a downlink data notification is received.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>Yes</td>
<td>Supported</td>
<td>No</td>
<td>Same as above.</td>
</tr>
</tbody>
</table>

**Intra RAU: New RNC does not support Direct Tunnel. No SGW relocation**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB Status</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>Not Supported</td>
<td>No</td>
<td>No RAB establishment with new RNC. SGSN sends Modify Bearer Request to S-GW with S4U TEID. If there is change in PLMN ID, then new PLMN ID will be carried.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>No Supported</td>
<td>No</td>
<td>Same as above.</td>
</tr>
</tbody>
</table>
Routing Area Update with S-GW Change

In a Routing Area Update with an S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. In its Create Session Response, the S-GW sends an S12U FTEID which is forwarded to the RNC via a RAB Assignment Request.

The SGSN sends the RNC FTEID received in the RAB Assignment Response to the S-GW in a Modify Bearer Request. There are many scenarios to consider during Intra SGSN RAU.

**Figure 37: Routing Area Update Procedure with SGW Change**

The table below includes detailed behaviors for a Routing Area Update with S-GW change.
### Table 11: Routing Area Update with S-GW Change Behavior Table

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intra RAU: Both RNCs support Direct Tunnel. SGW relocation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Send CSR request to new S-GW with DTF flag but no S4U/S12U FTEID. S-GW will send its S12U TEID that SGSN stores as part of DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN will get DDN and establish RABs and send MBR.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Same as above.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>Some RABs</td>
<td>Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Send CSR request to new S-GW with DTF flag but no S4U/S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC. MBR will be initiated only with those RABs that are present rest of bearers to be removed.</td>
</tr>
<tr>
<td><strong>Intra RAU: Old RNC does not support Direct Tunnel. SGW relocation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scenario</td>
<td>Old RNC Status</td>
<td>Old RNC RAB</td>
<td>Old RNC DT Status</td>
<td>PLMN Change</td>
<td>NEW RNC DT Status</td>
<td>S-GW Change</td>
<td>SGSN Action</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Send CSR request to new S-GW with DTF flag but no S4U/S12 UFTEID. S-GW sends its S12U TEID that SGSN stores as part of our DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN gets DDN and establishes RABs and sends MBR.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Not Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Same as above.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>Some RABs</td>
<td>Not Supported</td>
<td>Do not care</td>
<td>Supported</td>
<td>Yes</td>
<td>Send CSR request to new S-GW with DTF flag but no S4U/S12 UFTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC and MBR will be initiated only with those RABs that are present and the rest as bearers to be removed.</td>
</tr>
</tbody>
</table>

Intra RAU: New RNC does not support Direct Tunnel. SGW relocation

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra RAU</td>
<td>Not Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>Not Supported</td>
<td>Yes</td>
<td>CSR request without DTF flag and with S4U FTEID.</td>
</tr>
</tbody>
</table>
### Intra SRNS with S-GW Change

In Intra SRNS (Serving Radio Network Subsystem) with S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. The Create Session Response from the new S-GW contains the SGW S12U FTEID which the SGSN forwards to the Target RNC in a Relocation Request.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Old RNC Status</th>
<th>Old RNC RAB</th>
<th>Old RNC DT Status</th>
<th>PLMN Change</th>
<th>NEW RNC DT Status</th>
<th>S-GW Change</th>
<th>SGSN Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>No RAB</td>
<td>Supported</td>
<td>Do not care</td>
<td>Not Supported</td>
<td>Yes</td>
<td>CSR request without DTF flag and with S4U FTEID.</td>
</tr>
<tr>
<td>Intra RAU</td>
<td>Present</td>
<td>Some rABs</td>
<td>Supported</td>
<td>Do not care</td>
<td>Not Supported</td>
<td>Yes</td>
<td>CSR request without DTF flag and with S4U FTEID. No deactivation of PDPs.</td>
</tr>
</tbody>
</table>
The SGSN sends the RNC S12U FTEID to the new S-GW in a Modify Bearer Request.

**Figure 38: Intra SRNS with S-GW Change**

<table>
<thead>
<tr>
<th>SRNC</th>
<th>TRNC</th>
<th>SGSN</th>
<th>Old S-GW</th>
<th>New S-GW</th>
<th>P-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table below includes detailed behaviors for intra SRNS scenarios.
Intra SRNS without S-GW Change

In Intra SRNS without S-GW change, a Relocation Request is sent with SGW S12 U FTEID. The RNC S12 U FTEID received is forwarded to the S-GW in a Modify Bearer Request.

**Figure 39: Intra SRNS without S-GW Change**

<table>
<thead>
<tr>
<th>SRNC</th>
<th>TRNC</th>
<th>SGSN</th>
<th>Old S-GW</th>
<th>New S-GW</th>
<th>P-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table below includes detailed behaviors for intra SRNS scenarios.

**Table 12: Intra SRNS Behaviors**

<table>
<thead>
<tr>
<th>Old RNC DT Status</th>
<th>New RNC DT Status</th>
<th>S-GW Relocation</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Supported</td>
<td>No</td>
<td>Relocation Request to Target RNC is sent with S-GW S12 U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.</td>
</tr>
<tr>
<td>Supported</td>
<td>Not Supported</td>
<td>No</td>
<td>Relocation Request to Target RNC is sent with SGSN S4 U FTEID. Modify Bearer Request to S-GW is sent with SGSN S4 U FTEID</td>
</tr>
<tr>
<td>Old RNC DT Status</td>
<td>New RNC DT Status</td>
<td>S-GW Relocation</td>
<td>Behavior</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Not Supported</td>
<td>Supported</td>
<td>No</td>
<td>Relocation Request to Target RNC is sent with S-GW S12U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.</td>
</tr>
<tr>
<td>Not Supported</td>
<td>Supported</td>
<td>Yes</td>
<td>Create Session Request to new S-GW is sent with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response SGSN internally treats that as an S12U FTEID and continues the relocation. Relocation Request to Target RNC is sent with S12 U FTEID received in Create Session Response. Modify Bearer Request to new S-GW is sent with RNC S12U FTEID.</td>
</tr>
<tr>
<td>Supported</td>
<td>Not Supported</td>
<td>Yes</td>
<td>Create Session Request to new SGW is sent with S4 U FTEID. Relocation Request to Target RNC is sent with SGSN U FTEID. Modify Bearer Request is sent with SGSN S4U FTEID.</td>
</tr>
<tr>
<td>Supported</td>
<td>Supported</td>
<td>Yes</td>
<td>SGSN sends a Create Session Request to new SGW with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response, SGSN will internally treat that as S12U FTEID and continue the relocation. Relocation Request to the Target RNC is sent with the S12 U FTEID received in the Create Session Response. Modify Bearer Request to new S-GW is sent with RNC U FTEID.</td>
</tr>
</tbody>
</table>

**New SRNS with S-GW Change and Direct Data Transfer**

The new SGSN sends a Create Session Request with DTF flag set and no user plane FTEID to the new S-GW. The new SGSN sends the SGW S12U FTEID received in the Create Session Response in Relocation Request...
to the Target RNC. The new SGSN sends the RNC S12U FTEID received in a Relocation Request Ack to the new S-GW in a Modify Bearer Request.

**Figure 40: New SRNS with S-GW Change with Data Transfer**

The table below includes detailed behaviors for New SRNS scenarios.
New SRNS with S-GW Change and Indirect Data Transfer

Indirect Data Transfer (IDFT) during a new SGSN SRNS happens during E-UTRAN-to-UTRAN connected mode IRAT handover. See the figure below for a detailed call flow.

Figure 41: New SRNS with S-GW Change and Indirect Data Transfer

The table below includes detailed behaviors for New SRNS scenarios.
Table 13: New SRNS Behaviors

<table>
<thead>
<tr>
<th>Target RNC DT Status</th>
<th>Direct Forwarding</th>
<th>S-GW Relocation</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Relocation Request with S12U FTEID received in Forward Relocation Request. SGSN includes RNC U FTEID in Forward Relocation Response. RNC U FTEID is also sent in ModifyBearer Request with DTF flag set.</td>
</tr>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>Relocation Request with S12U FTEID received in Forward Relocation Request. In Forward Relocation Response RNC U FTEID is included. And in ModifyBearer Request RNC U FTEID is sent and DTF flag is set.</td>
</tr>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. Create Indirect Data Forwarding Tunnel Request is sent with RNC FTEID received in Relocation Request Acknowledge. In Forward Relocation Response SGW DL U FTEID received in Create IDFT response is sent. Modify Bearer Request is send with DTF set and RNC U FTEID.</td>
</tr>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. In Forward Relocation Response RNC FTEID is sent and Modify Bearer Request is sent with DTF flag set and RNC U FTEID.</td>
</tr>
</tbody>
</table>
Old SRNS with Direct Data Transfer

This scenario includes SRNS relocation between two SGSNs and hence IDFT is not applicable. Data will be forwarded between the source and target RNCs directly. Forward Relocation Request is sent with S12U FTEID.

Figure 42: Old SRNS with Direct Data Transfer

The table below includes detailed behaviors for Old SRNS.
Old SRNS with Indirect Data Transfer

Indirect Data Transfer (IDFT) during Old SGSN SRNS happens during UTRAN-to-E-UTRAN connected mode IRAT handover. A Forward Relocation Request is sent with SGW S12U FTEID.

Figure 43: Old SRNS with Indirect Data Transfer
Table 14: Old SRNS Behaviors

<table>
<thead>
<tr>
<th>Source RNC DT Status</th>
<th>Direct Forwarding</th>
<th>S-GW Relocation</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Forward Relocation Request is send with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then a Create Indirect Data Forwarding Tunnel Request is sent with User plane FTEID received in the Forward Relocation Response. This will be the eNB user plane FTEID. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.</td>
</tr>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC user plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.</td>
</tr>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Forward Relocation Request is sent with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then Create Indirect Data Forwarding Tunnel Request is sent with eNB User plane FTEID received in the Forward Relocation Response. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.</td>
</tr>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC use plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.</td>
</tr>
</tbody>
</table>
Network Initiated Secondary PDP Context Activation

The S-GW sends a Create Bearer Request for Network Initiated Secondary PDP Context Activation with the SGW S12U FTEID. This FTEID is sent in a RAB Assignment Request to the RNC. The RNC S12U FTEID received in the RAB Assignment Response is sent to the S-GW in a Create Bearer Response.

Figure 44: Network Initiated Secondary PDP Context Activation 5

PGW Init Modification when UE is Idle

If UE is in IDLE state and PGW Init Modification is received, the SGSN sends the first MBR. Upon getting PGW Init Modification in Idle State, the SGSN queues the PGW Init Modification and feeds a Downlink Data
Notification internally. This sets up all RABs (using old QoS) and sends a Modify Bearer Request. When the Downlink Data Procedure is completed, the queued PGW Init Modification is processed.

*Figure 45: PGW Init Modification when UE in Idle State*

**Limitations**

During an intra RAU, intra SRNS or Service Request triggered by RAB establishment, if a few RABs fail the Modify Bearer Request the SGSN will mark those RABs as bearers to be removed. Under current specifications, it is not possible to send a Modify Bearer Request with a few bearers having S12U U-FTEIDs and a few bearers not having U-FTEIDs.
There is an ongoing CR at 3GPP to allow such Modify Bearer Requests and the S-GW should send DDN when it gets downlink data for the bearers that did not have U-FTEIDs. If this CR is approved, the SGSN will support (in a future release) sending a partial set of bearers with S12U FTEID and some bearers without any U-FTEID.

Standards Compliance

The Direct Tunnel complies with the following standards:

- 3GPP TS 23.060 version 10 sec 9.2.2 General Packet Radio Service (GPRS) Service description
- 3GPP TS 29.274 v10.5.0 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

Configuring Support for Direct Tunnel

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.

By default, direct tunnel support is

- disallowed on the SGSN/S-GW
- allowed on the GGSN/P-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 operator policy named default. 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 the purpose and uses of operator policies, refer to the section Operator Policy.

Configuring Direct Tunnel on an S4-SGSN

Configuration of a GTP-U direct tunnel (DT) requires enabling DT both in a call control profile and for the RNC.

Important

Direct tunneling must be enabled at both endpoints to allow direct tunneling for the MS/UE.

Enabling Setup of GTP-U Direct Tunnel

The SGSN determines whether a direct tunnel can be setup and by default the SGSN does not support direct tunnel. The following configuration enables a GTP-U DT in a call control profile:

```
config
call-control-profile policy_name
```
direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
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.

• Beginning with Release 19.3.5, to-ggsn and to-sgw options have been added to the direct-tunnel command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  • Use the keyword attempt-when-permitted without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  • Use the keyword attempt-when-permitted with the to-ggsn keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  • Use the keyword attempt-when-permitted with the to-sgw keyword filter to enable only the S4's S12 interface between the RNC and the SGW.

• To remove the direct tunnel settings from the configuration, use the following command: direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]

• Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel to 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, DT functionality is enabled for all RNCs.

The following configuration sequence enables DT to a specific RNC that had been previously disabled for direct tunneling:

```
config context ctxt_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.
Restricting Direct Tunnels

The following configuration scenario prohibits the S4-SGSN to setup direct tunneling over the S12 interface during Inter SGSN RAUs:

```
config
call-control-profile profile_name
    rau-inter avoid-s12-direct-tunnel
end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
context context_name
    iups-service service_name
        rnc id rnc_id
            direct-tunnel not-permitted-by-rnc
end
```

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 = ccpprofile1

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

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 S-GW over the S11 interfaces. The S-GW responds with its 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
  exit
context  egress_context_name  -noconfirm
  gtpu-service  s12_gtpu_egress_service_name
    bind ipv4-address  s12_interface_ip_address
  exit
  egtp-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.

Monitoring and Troubleshooting Direct Tunnel

```
show subscribers sgsn-only
```

The output of this command indicates whether Direct Tunnel has been established.

```
show subscribers sgsn-only full all

Username: 123456789012345
Access Type: sgsn-pdp-type-ipv4  Network Type: IP
Access Tech: WCDMA UTRAN
```

Direct Tunnel for 4G (LTE) Networks
show gmm-sm statistics sm-only

The output of this command indicates the number of total active PDP contexts with direct tunnels.

**Show gmm-sm statistics sm-only**

Activate PDP Contexts:

<table>
<thead>
<tr>
<th>Context Type</th>
<th>Total Actv PDP Ctx:</th>
<th>3G-Actv Pdp Ctx:</th>
<th>2G-Avtv Pdp Ctx:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Gn Interface</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4 Interface</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Actv Pdp Ctx:</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Direct Tunnel Bulk Statistics**

Currently there are no bulk statistics available to monitor the number of PDP contexts with Direct Tunnel. Bulk statistics under the EGTPC schema are applicable for both Direct Tunnel and Idle Mode Signalling Reduction (ISR) [3G and 2G]. The following statistics track the release access bearer request and response messages which are sent by the SGSN to the S-GW upon Iu or RAB release when either a direct tunnel or ISR is active:

- `tun-sent-relacbearreq`
- `tun-sent-retransrelacbearreq`
- `tun-recv-relacbearresp`
- `tun-recv-relacbearrespsDiscard`
- `tun-recv-relacbearrespaccept`
- `tun-recv-relacbearrespdenied`

The following bulk stats under EGTPC schema track Downlink Data Notification (DDN) Ack and failure messages between the S-GW and the SGSN when either direct tunnel or ISR is active:

- `tun-recv-dlinknotif`
- `tun-recv-dlinknotifDiscard`
- `tun-recv-dlinknotifNorsp`
- `tun-recv-retransdlinknotif`
- `tun-sent-dlinknotifackaccept`
- `tun-sent-dlinknotifackdenied`
- `tun-sent-dlinkdatafail`

For complete descriptions of these variables, see the EGTPC Schema Statistics chapter in the *Statistics and Counters Reference.*
3GPP R12 GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW

This chapter describes the 3GPP Release 12 GTP-C Load and Overload Control feature on the P-GW, SAEGW, and S-GW.

- Feature Description, page 147
- How It Works, page 148
- Creating and Configuring a 3GPP R12 GTP-C Load Control Profile, page 149
- Creating and Configuring a 3GPP R12 GTP-C Overload Control Profile, page 153
- Monitoring and Troubleshooting the 3GPP R12 GTP-C Load and Overload Control Feature, page 161

Feature Description

This section describes the 3GPP R12 GTP-C Load and Overload Control feature.

Important Use of the 3GPP R12 Load and Overload Control feature requires that a valid license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

The 3GPP R12 GTP-C Load and Overload Control feature is a licensed, optional feature which allows a GTP control plane node to send its load information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load information reflects the operating status of the resources of the originating GTP control plane node.

Nodes using GTP control plane signaling may support communication of overload control information in order to mitigate overload situations for the overloaded node through actions taken by the peer node(s). This feature is supported over the S4, S11, S5 and S8 interfaces via the GTPv2 control plane protocol.

A GTP-C node is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). Overload control information reflects an indication of when the originating node has reached such a situation. This information, when transmitted between GTP-C nodes, may be used to reduce and/or throttle the amount of GTP-C signaling.
traffic between these nodes. As such, the overload control information provides guidance to the receiving node to decide upon the correct actions, which leads to mitigation towards the sender of the information.

To summarize, load control and overload control can be described in this manner:

- **Load Control**: Load control enables a GTP-C entity (for example, an P-GW/SAEGW/S-GW) to send its load information to a GTP-C peer (for example, an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

- **Overload Control**: Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

### Relationships to Other Features

Note the following before configuring the GTPP R12 GTP-C Load and Overload Control feature:

- One of the following services must be configured on the node before GTP-C Load and Overload Control can be configured.
  - P-GW
  - SAEGW
  - S-GW

- Once configured, the GTP-C Load and Overload Control profiles must be associated with a P-GW, SAEGW, or S-GW service to function properly in the network.

### How It Works

The node periodically fetches various parameters (for example, License-Session-Utilization, System-CPU-Utilization, and System-Memory-Utilization), which are required for Node level load control information. The node then calculates the load/overload control information itself either based on the weighted factor provided by the user or using the default weighted factor.

Node level load control information is calculated every 30 seconds. The resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level.

For each configured service, load control information can be different. This can be achieved by providing a weightage to the number of active session counts per service license, for example, \( \left( \frac{\text{number of active sessions per service}}{\text{max session allowed for the service license}} \right) \times 100 \).

The node's resource manager calculates the system-CPU-utilization and System-Memory-Utilization at a systems level by averaging CPU and Memory usage for all cards and which might be different from that calculated at the individual card level.
Creating and Configuring a 3GPP R12 GTP-C Load Control Profile

This section describes how to create and configure a 3GPP R12 GTP-C load control profile.

Configuration Overview

Creating and configuring a 3GPP R12 GTP-C load control profile consists of the following procedures:

1. Create a load control profile. Refer to Creating the GTPP R12 Load Control Profile, on page 149.
2. Configure the load control weightage settings. Refer to Configuring the 3GPP R12 Load Control Profile Weightage Settings, on page 149.
3. Configure the load control inclusion frequency. Refer to Configuring the 3GPP R12 Load Control Profile Inclusion Frequency, on page 150.
4. P-GW Only. Configure the load control threshold. Refer to Configuring the 3GPP R12 Load Control Threshold, on page 151.
5. Configure load control information handling. Refer to Configuring 3GPP R12 Load Control Information Handling, on page 151.
7. Associate the load control profile with a P-GW, SAEGW, or S-GW service. Refer to Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service., on page 152.
8. Verify the configuration settings. Refer to Verifying the 3GPP R12 Load Control Configuration, on page 152.
9. Save the configuration. Refer to Saving the Configuration, on page 153.

Creating the GTPP R12 Load Control Profile

Use the following example to create a load control profile on the P-GW/SAEGW/S-GW:

```
config
gtp-load-control-profile  profile_name
end
```

Notes:

- The profile name must be an alphanumeric string from 1 to 64 characters in length.
- Once you have created the load control profile, you will enter \textit{GTP-C Load Control Profile Configuration Mode}.

Configuring the 3GPP R12 Load Control Profile Weightage Settings

This section describes how to set weightage percentages for system CPU, memory, and license session utilization as part of a GTP-C load control profile configuration. These settings constitute the basic load control...
profile for this network element. These parameters allow the P-GW/S-GW/SAEGW to send its load information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedures for the P-GW and S-GW. Load information reflects the operating status of the resources of the originating GTP control plane node.

Use the following example to configure the load control profile weightage settings on the P-GW/SAEGW/S-GW:

```config
gtpc-load-control-profile profile_name
weightage system-cpu-utilization percentage system-memory-utilization percentage
license-session-utilization percentage
end
```

**Notes:**

- **system-cpu-utilization percentage**: Configures system CPU utilization weightage as a percentage of 100.
  
  *percentage* must be an integer from 0 to 100. The default is 40.

- **system-memory-utilization percentage**: Configures system memory utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.

- **license-session-utilization percentage**: Configures license session utilization weightage as a percentage of 100. *percentage* must be an integer from 0 to 100. The default is 30.

---

**Important**

All parameters must be specified. The total of all three parameter settings should equal, but not exceed, 100.

---

**Configuring the 3GPP R12 Load Control Profile Inclusion Frequency**

This section describes how to set the parameters that determine the inclusion frequency of the Load Control Information Element (LCI) for a GTP-C Load Control Profile configuration. The LCI is a 3GPP-specific Information Element that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send this information to the node's peers.

Use the following example to configure the load control profile inclusion frequency on the P-GW/SAEGW/S-GW:

```config
gtpc-load-control-profile profile_name
inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor } end
```

**Notes:**

- **inclusion frequency**: Configures parameters to determine the inclusion frequency of the LCI.

- **advertisement-interval interval_in_seconds**: Configures advertisement-interval for the LCI in seconds. This specifies how often load control information should be sent to the peers. If configured to 0, the node will send load control information in each and every outgoing message to the peers. *interval_in_seconds* must be an integer from 0 to 3600. The default is 300.

- **change-factor change_factor**: Configures the change factor for the load control profile. If the load control change factor changes by the configured factor, whether it is an increase or decrease in load, the
load control information is sent to the peers. This information is only sent to the peers when the load factor changes by the factor configured. change_factor must be an integer from 1 to 20. The default is 5.

Configuring the 3GPP R12 Load Control Threshold

This section describes how to configure the minimum threshold value above which P-GW-provided load control information should be utilized for calculating the P-GW effective weight during initial node selection. Use the following example to configure Load Control Profile threshold on the P-GW.

```
config
gtpc-load-control-profile profile_name
threshold time_in_seconds
end
```

Notes:
- The default threshold value is 50.

Configuring 3GPP R12 Load Control Information Handling

The handling of load control information for the home or visited PLMN can be enabled/disabled via this procedure. Use the following example to enable/disable load control profile information handling on the SAEGW/S-GW/P-GW.

```
config
gtpc-load-control-profile profile_name
load-control-handling { home | visited }
no load-control-handling { home | visited }
end
```

Notes:
- no disables load-control-handling for the specified option.

Configuring 3GPP R12 Load Control Information Publishing

The publishing of load control information can be enabled/disabled for the home or visited PLMN. Use the following example to enable/disable load control profile information publishing on the P-GW/SAEGW/S-GW.

```
config
gtpc-load-control-profile profile_name
load-control-publishing { home | visited }
no load-control-publishing { home | visited }
end
```

Notes:
- no disables load control profile information publishing for the specified option.
Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service.

Once the 3GPP R12 GTP-C load control profile is created, it must be associated with an existing P-GW, SAEGW, or S-GW service.

Use the following examples to associate the GTP-C load control profile with an existing P-GW, SAEGW, or S-GW service.

**P-GW Service Association:**

```
configure
  context context_name
    pgw-service pgw_service_name
      associate gtpc-load-control-profile profile_name
      no associate gtpc-load-control-profile
  end
end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

**S-GW Service Association:**

```
configure
  context context_name
    sgw-service sgw_service_name
      associate gtpc-load-control-profile profile_name
      no associate gtpc-load-control-profile
  end
end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

**SAEGW Service Association:**

```
configure
  context context_name
    sgw-service sgw_service_name
      associate gtpc-load-control-profile profile_name
      exit
    pgw-service pgw_service_name
      associate gtpc-load-control-profile profile_name
      exit
  saegw-service saegw_service_name
    associate sgw-service sgw_service_name
    associate pgw-service pgw_service_name
    exit
```

Verifying the 3GPP R12 Load Control Configuration

Use the following command to view the load control profile configuration settings:

```
show gtpc-overload-control-profile full name load_control_profile_name
```

The output of this command provides the configuration settings of all load control parameters, including:
- Weightage
- Inclusion Frequency
- Load control information handling
- Load control information publishing
- Load threshold

**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*.

**Creating and Configuring a 3GPP R12 GTP-C Overload Control Profile**

This section describes how to create and configure a 3GPP R12 GTP-C overload control profile on the P-GW/SAEGW/S-GW.
Configuration Overview

**Step 1** Create the GTP-C overload control profile. Refer to Creating the GTPP R12 Overload Control Profile, on page 154.

**Step 2** Configure the weightage settings. Refer to Configuring 3GPP R12 Overload Control Weightage Settings, on page 154.

**Step 3** Configure the inclusion frequency. Refer to Configuring the 3GPP R12 Overload Control Inclusion Frequency, on page 155.

**Step 4** Configure the validity period. Refer to Configuring the 3GPP R12 Overload Control Validity Period, on page 156.

**Step 5** Configure the tolerance settings. Refer to Configuring 3GPP R12 Overload Control Tolerance Limits, on page 156.

**Step 6** Configure the throttling behavior for the node. Refer to Configuring 3GPP R12 Overload Control Throttling Behavior, on page 157.

**Step 7** Configure the message prioritization. Refer to Configuring 3GPP R12 Overload Control Message Prioritization, on page 157.

**Step 8** Configure self-protection behavior for the node. Refer to Configuring 3GPP R12 Overload Control Self-Protection Behavior, on page 158.

**Step 9** Configure overload control information handling. Refer to Configuring 3GPP R12 Overload Control Information Handling, on page 158.

**Step 10** Configure overload control information publishing. Refer to Configuring 3GPP R12 Overload Control Information Publishing, on page 159.

**Step 11** Associate the overload control configuration with an existing P-GW/SAEGW/S-GW service. Refer to Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service, on page 159.

**Step 12** Verify the overload control configuration. Refer to Verifying the 3GPP R12 Overload Control Configuration, on page 160.

**Step 13** Save the configuration. Refer to Saving the 3GPP R12 Overload Control Configuration, on page 160.

Creating the GTPP R12 Overload Control Profile

Use the following example to create the GTP-C Overload Control Profile:

```bash
configure
gtpc-overload-control-profile profile_name
no gtpc-overload-control-profile profile_name
end
```

Notes:

- **no**: Removes specified GTP-C Overload Control profile.
- **profile_name** must be an alphanumeric string from 1 to 64 characters in length.

Configuring 3GPP R12 Overload Control Weightage Settings

This section describes how to configure GTP-C Overload Control weightage parameters. These parameters constitute the basic settings for this GTP-C Overload Control Profile. Communication of these parameters
indicate to peers when this network element is becoming or being overloaded. When this occurs, the NE will be able to instruct its peers to gracefully reduce its incoming signaling load by instructing the peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Use the following example to configure the GTP-C Overload Control Weightage settings on the P-GW/SAEGW/S-GW.

```config
configure gtpc-overload-control-profile profile_name
  weightage system-cpu-utilization percentage
  system-memory-utilization percentage
  license-session-utilization percentage
  default weightage
end
```

Notes:

- Total weightage for all parameters should be 100.
- `system-cpu-utilization percentage`: Configures system cpu utilization weightage as a percentage of 100. `percentage` must be an integer from 0 to 100. The default is 40.
- `system-memory-utilization percentage`: Configures system memory utilization weightage as a percentage of 100. `percentage` must be an integer from 0 to 100. The default is 30.
- `license-session利用率 percentage`: Configures license session utilization weightage as a percentage of 100. `percentage` must be an integer from 0 to 100. The default is 30.

### Configuring the 3GPP R12 Overload Control Inclusion Frequency

This section describes how to set the parameters that determine the inclusion frequency of the Overload Control Information Element (OCI) for a GTP-C Load Control Profile configuration. The OCI is a 3GPP-specific IE that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send this information to the peers.

Use the following example to configure the overload control profile inclusion frequency on the P-GW/SAEGW/S-GW.

```config
configure gtpc-overload-control-profile profile_name
  inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor }
  default inclusion-frequency { advertisement-interval | change-factor }
end
```

Notes:

- `inclusion frequency`: Configures parameters to decide inclusion frequency of the OCI information element.
- `advertisement-interval interval_in_seconds`: Configures the advertisement-interval for overload control in seconds. Specifies how often overload control information should be sent to the peers. If configured to 0, the node will send overload control information in each and every outgoing message to the peers. `interval_in_seconds` must be an integer from 0 to 3600. The default is 300.
- `change-factor change_factor`: P-GW only. Configures the change factor for overload control. If the overload control factor changes by a configured factor, whether by an increase or decrease, the overload control information should be sent to the peers. This information is only sent to the peers when the
overload factor changes by the factor configured. \texttt{change\_factor} must be an integer from 1 to 20. The default is 5.

## Configuring the 3GPP R12 Overload Control Validity Period

This section describes how to configure the overload control validity period. The validity period is the length of time during which the overload condition specified by the overload control information element is to be considered as valid, unless overridden by subsequent new overload control information.

Use the following example to configure the GTP-C Overload Control validity period on the P-GW/SAEGW/S-GW.

```plaintext
configure
gtpc-overload-control-profile profile_name
  validity-period seconds
  default validity-period
end
```

Notes:

- \texttt{validity-period \texttt{seconds}}: Configures the validity of overload control information. \texttt{seconds} must be an integer from 1 to 3600. The default is 600 seconds.

## Configuring 3GPP R12 Overload Control Tolerance Limits

Use this example to configure GTP-C Overload Control Tolerance limits.

```plaintext
configure
gtpc-overload-control-profile profile_name
  tolerance { initial-reduction-metric percentage | threshold report-reduction-metric percentage }
  self-protection-limit percentage
  default tolerance { initial-reduction-metric | threshold }
end
```

Notes:

- \texttt{initial-reduction-metric \texttt{percentage}}: Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit. When reaching the configured minimum threshold, this parameter specifies how much the node wants the peers to reduce incoming traffic. \texttt{percentage} must be an integer from 1 to 100. The default is 10.

- \texttt{threshold report-reduction-metric \texttt{percentage}}: Configures the minimum overload tolerance threshold for advertising overload reduction metric to the peer. When the minimum threshold is reached, the node will report this information to peers. When the maximum limit is reached, the node will go into self-protection mode. \texttt{percentage} must be an integer from 1 to 100. The default is 80.

- The \texttt{threshold report-reduction-metric} should always be lower than the \texttt{self-protection-limit}.

- \texttt{self-protection-limit \texttt{percentage}}: Configures the maximum overload tolerance threshold after which node will move to self protection mode. When the maximum limit is reached, the node will start rejecting all incoming messages, except for delete messages. The node will not initiate any new messages to the peers. This is to mitigate the overload condition. \texttt{percentage} must be an integer from 1 to 100. The default is 95.
Configuring 3GPP R12 Overload Control Throttling Behavior

Use this command to configure throttling behavior based on peer's overload reduction-metric by excluding some or all emergency events and/or messages with configured EARP. Message throttling applies only to initial messages. Triggered request or response messages should not be throttled since that would result in the retransmission of the corresponding request message by the sender.

If throttling-behavior is configured, the profile can be associated with an S-GW or P-GW service. If a P-GW specific keyword is configured, and the profile is associated with an S-GW service, the S-GW will ignore the P-GW specific configuration. Only the parameters specific to S-GW or P-GW will be utilized.

Use this example to configure GTP-C overload control throttling behavior on the P-GW/SAEGW/S-GW.

```
configure
gtpc-overload-control-profile profile_name
  throttling-behavior { earp [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 ] exclude } | emergency-events exclude }
  no throttling-behavior [ earp [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 ] exclude | emergency-events exclude ]
end
```

Notes:
- **throttling-behavior**: Configures throttling behavior based on peer's overload reduction-metric.
- **earp**: Excludes the specified messages with configured earp from throttling due to peer's overload-reduction metric. If a bearer with configured EARP is created or updated, it will be excluded from throttling.
- *****: Indicates that more than one of the keywords can be entered within a single command.
- **emergency-events exclude**: P-GW Only. Excludes all emergency events from throttling due to the peer's overload reduction-metric. While reducing messages towards the peer based on the overload information received from the peer, the P-GW will exclude events sent for emergency sessions.

Configuring 3GPP R12 Overload Control Message Prioritization

In the R12 GTP-C Load Overload control feature, it is possible to apply message throttling, (when a peer indicates it is overloaded), based on message priority. To apply message prioritization it is necessary to configure the percentage of two groups of messages that each node (P-GW or ePDG) is expected to generate. The operator can define the expected number of messages as a percentage for each message group.

Use the following example to configure message prioritization.

```
configure
gtpc-overload-control-profile profile_name
  message-prioritization group1 percentage group2 percentage
  no message-prioritization
  default message-prioritization
end
```

Notes:
- **group1** specifies the message priority percentage for the following messages:
  - Update Bearer Request message for default bearer generated from P-GW ingress
• Update Bearer Request message for dedicated bearer generated from P-GW ingress
• Handoff Create Session Request message generated from ePDG egress.

• **group2** specifies the message priority percentage for the following messages:
  
  • Create Bearer Request message for default bearer generated from P-GW ingress
  • PDN connection requested Create Session Request message from ePDG egress

• The total percentage for the message groups should equal 100.
• **group1** messages will have the highest priority (1) and are dropped last. **group2** messages will have the lowest priority (2) and are dropped first.
• **default** returns the group message priority settings to their default value. The default for each group is 50.
• The default behavior for this command is enabled. To disable the command use the **no** option.

## Configuring 3GPP R12 Overload Control Self-Protection Behavior

This functionality enables the operator to configure APN names and EARP priority level values for self-protection mode so that incoming request messages for emergency packet data node (PDN) connections and/or configured EARP priority values are not rejected even if the system is under self-protection mode.

Use this example to configure GTP-C overload control self-protection behavior.

```plaintext
configure
gtpc-overload-control-profile profile_name
  self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude } }
  no self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude } }
end
```

Notes:

• **apn** configures up to three APN names to be allowed under self-protection behavior.
• **earp** configures up to three EARP priority level values so that incoming request messages for the configured evolved ARP priority values are not rejected even if the system is under self-protection mode.
• **no** disables the specified options.

## Configuring 3GPP R12 Overload Control Information Handling

Use this command to enable/disable the handling of overload control information for the home or visited PLMN.

```plaintext
configure
gtpc-load-control-profile profile_name
  overload-control-handling { home | visited }
  no overload-control-handling { home | visited }
  default overload-control-handling
end
```
Notes:

- **home**: Enables the handling of load control information for the home PLMN.
- **visited**: enables the handling of load control information for the visited PLMN.
- **default**: Returns load control handling to its default behavior (enabled).

### Configuring 3GPP R12 Overload Control Information Publishing

Enables or disables the publishing of load control information towards the home or visited PLMN.

```bash
configure
gtpc-overload-control-profile profile_name
   overload-control-publishing { home | visited }
   no overload-control-publishing { home | visited }
   default overload-control-publishing
end
```

Notes:

- **home**: Enables the publishing of load control information towards the home PLMN.
- **visited**: Enables the publishing of load control information towards the visited PLMN.
- **default**: Returns load control handling to its default behavior (enabled).

### Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service

Once the 3GPP R12 overload control profile has been configured, it must be associated with an existing P-GW, SAEGW, or S-GW service.

Use the following examples to associate the overload control configuration to an existing service.

#### P-GW Service Association:

```bash
configure
   context context_name
      pgw-service pgw_service_name
         associate gtpc-overload-control-profile profile_name
      no associate gtpc-overload-control-profile
end
```

Notes:

- **no** disables the service association for the GTP-C Load Control Profile.

#### S-GW Service Association:

```bash
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-overload-control-profile profile_name
      no associate gtpc-overload-control-profile
end
```

Notes:
Verifying the 3GPP R12 Overload Control Configuration

- `no` disables the service association for the GTP-C Load Control Profile.

### SAEGW Service Association:

```plaintext
configure
  context context_name
    sgw-service sgw_service_name
      associate gtpc-overload-control-profile profile_name
      exit
    pgw-service pgw_service_name
      associate gtpc-overload-control-profile profile_name
      exit
  saegw-service saegw_service_name
    associate sgw-service sgw_service_name
    associate pgw-service pgw_service_name
  exit
```

**Verifying the 3GPP R12 Overload Control Configuration**

Use the following command to view the overload control configuration settings.

```
show gtpc-overload-control-profile full name overload_control_profile_name
```

The output of this command provides all overload control profile configuration settings, including:

- Weightage
- Tolerance
- Inclusion Frequency
- Validity Period
- Throttling Profile
- Self-Protection Behavior
- Overload control information Handling
- Overload control information Publishing
- Message Prioritization

**Saving the 3GPP R12 Overload Control 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**.
Monitoring and Troubleshooting the 3GPP R12 GTP-C Load and Overload Control Feature

This section provides information to assist operators in monitoring the 3GPP R12 GTP-C Load and Overload Control feature.

3GPP R12 GTP-C Load and Overload Show Commands

This section provides information regarding show commands in support of the 3GPP R12 Load and Overload Control feature.

show egtpc statistics egtp-service <egtp-service name>
The output of this command provides detailed granular statistics for 3GPP R12 load and overload control profile statistics that have been transmitted (TX) and received (RX). Statistics are provided on a per egtp-service basis.

show gtpc-load-control-profile full all
The output of this command provides all configuration settings for all 3GPP R12 load control profiles configured on the node. Use this command to determine if the load control profile is configured as intended.

show gtpc-load-control-profile full name <name>
Use this command to view all configuration settings for the specified 3GPP R12 load control profile.

show gtpc-overload-control-profile full all
The output of this command provides all configuration settings for all 3GPP R12 overload control profiles configured on the node. Use this command to determine if the overload control profile is configured as intended.

show gtpc-overload-control full name <name>
The output of this command provides all configuration settings for all 3GPP R12 Overload Control Profiles configured on the node. Use this command to determine if the Overload Control Profile is configured as intended.

show pgw-service all
Use this command to obtain the names of all 3GPP R12 load control and 3GPP R12 overload control profiles configured on the P-GW.
**show sgw-service all**

Use this command to obtain the names of all 3GPP R12 Load Control and Overload Control profiles configured on the S-GW.

**eGTP-C Bulk Statistics**

The following statistics are included in the eGTP-C Schema in support of the 3GPP R12 Load and Overload Control feature:

- load-overload-own-lci
- load-overload-own-oci
- load-overload-num-msg-throttled
- load-overload-num-ovrload-cond-reached

For descriptions of these variables, see "eGTP Schema Statistics" in the *Statistics and Counters Reference*. 

---

S-GW Administration Guide, StarOS Release 19
CHAPTER 8

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, page 163
- How it Works, page 164
- Configuring Intelligent RAT Paging for ISR on the S-GW, page 168

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

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 (CLI).

Licenses

Intelligent RAT Paging for ISR is a licensed-controlled 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.

*Figure 46: Intelligent RAT Paging for ISR: Sequential Paging Procedure*
### Table 15: 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>
Figure 47: Intelligent RAT Paging for ISR: Parallel Paging Procedure

Table 16: Intelligent RAT Paging for ISR: Parallel Paging Procedure 1

<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
  end

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
...
```
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, page 171
- The Operator Policy Feature in Detail, page 172
- How It Works, page 176
- Operator Policy Configuration, page 177
- Verifying the Feature Configuration, page 183

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)
• 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 ccp.
  • 15 - maximum number of supported equivalent PLMNs for 3G per ccp.
• 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 48: 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**

After creating or modifying the S4-SGSN's configuration, you must save the configuration and reboot the node for the change(s) to take effect.

---

**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.

**Note**
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
```
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.

```bash
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.

```configure
  configure
  imei-profile profile_name
    ggsn-address 211.211.123.3
    direct-tunnel not-permitted-by-ggsn (SGSN only)
    associate apn-remap-table remap1
  end
```

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
  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
end
```

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
```

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.

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 homers1
      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 10

Overcharging Protection Support

This chapter describes the Overcharging Protection Support feature and explains how it is configured. 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 P-GW Administration Guide, the S-GW Administration Guide, or the SAEGW Administration Guide before using the procedures in this chapter.

This chapter includes the following sections:

- Overcharging Protection Feature Overview, page 185
- License, page 186
- Configuring Overcharging Protection Feature, page 186
- Monitoring and Troubleshooting, page 188

Overcharging Protection Feature Overview

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.

Important

This feature is supported on the P-GW, and S-GW. Overcharging Protection is supported on the SAEGW only if the SAEGW is configured for Pure P or Pure S functionality.

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.

If the S-GW supports the Overcharging Protection feature, then it will send a CSReq with the PDN Pause Support Indication flag set to 1 in an Indication IE to the P-GW.
If the P-GW supports the Overcharging Protection feature then it will send a CSRsp with the PDN Pause Support Indication flag set to 1 in Indication IE and/or private extension IE to the S-GW.

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. The MBReq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.

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 charging downlink packets 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).

This feature aligns with the 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) specification.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.</td>
</tr>
</tbody>
</table>

License

Overcharging Protection is a license enabled feature and a new license key has been introduced for Overcharging Protection for P-GW functionality.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact your Cisco account representative for information on how to obtain a license.</td>
</tr>
</tbody>
</table>

Configuring Overcharging Protection Feature

This section describes how to configure overcharging protection support on the P-GW and S-GW.

Configuring Overcharging Support on the P-GW

This command enables overcharge protection for APNs controlled by this APN profile and configures overcharging protection by temporarily not charging during loss of radio coverage. Each overcharging protection option is a standalone configuration and it does not override the previous option set, if any. Use this command to specify P-GW to pause charging on abnormal-s1-release, DDN failure notification, or if the number of packets or bytes dropped exceeds the configured limit.
This configuration sequence is valid for the P-GW only.

```
close
    apn-profile apn_profile_name
    overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit drop_limit_value { packets | bytes } }
    [ remove ] overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit }
end
```

Notes:

- **remove**: Removes the specified configuration.

- **abnormal-s1-release**:  
  (for future use) If overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if Abnormal Release of Radio Link signal occurs from MME.

- **ddn-failure**:  
  If overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

- **drop-limit drop_limit_value { packets | bytes }**  
  Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.

  * **packets**: Configures drop-limit in packets.
  * **bytes**: Configures drop-limit in bytes.

---

### Configuring Overcharging Support on the S-GW

The following configuration is required for overcharging support on the S-GW:

```
close
    context context_name
    egtp-service service_name
    gtpc private-extension overcharge-protection
end
```

Notes:

- Enabling this command indicates that the S-GW has to interact with a release 15 P-GW for the overcharging protection feature which does not support 3GPP TS 29.274 Release 12 – 3GPP Evolved Packet System (EPS): Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3.

- When the **gtpc private-extension overcharge-protection** command is configured, the S-GW includes a Private Extension in the Create Session Request (CSReq) and Modify Bearer Request (MBReq) messages.

- Whenever a P-GW receives a CSReq with an Indication IE with the PDN Pause Support Indication flag set to 1, it responds only with an Indication IE.
When a CSReq does not have an Indication IE with the PDN Pause Support Indication flag set to 1, but the P-GW supports Overcharging Protection, then it responds with both an Indication and Private Extension IE.

### Monitoring and Troubleshooting

#### P-GW Schema

The following bulk statistics have been added to the P-GW schema for Overcharging Protection:

For descriptions of these variables, see the *Statistics and Counters Reference* guide.

- sessstat-ovrchrgprtctn-uplkpktdrop
- sessstat-ovrchrgprtctn-uplkbytedrop
- sessstat-ovrchrgprtctn-dnlkpktdrop
- sessstat-ovrchrgprtctn-dnlkbytedrop

#### show apn statistics all

The following counters display overcharging protection stats for this APN:

- UL Ovrchr Prtctn byte drop
- UL Ovrchr Prtctn pkt drop
- DL Ovrchr Prtctn byte drop
- DL Ovrchr Prtctn pkt drop

#### show pgw-service all

The following field display configuration information for Overcharging Protection on this P-GW service:

- EGTP Overcharge Protection

#### show pgw-service statistics all

The following counters display Overcharging Protection for this P-GW node:

- Drops Due To Overcharge Protection
  - Packets
  - Bytes
**show sgw-service statistics name <sgw_service_name>**

The output of this command shows the total number of PDNs where charging was paused:

- PDNs Total:
  - Paused Charging: <Total number of PDNs where charging was paused>

**show subscribers full**

The following counters display Overcharging Protection for all subscribers:

- in packet dropped overcharge protection
- in bytes dropped overcharge protection
- out packet dropped overcharge protection
- out bytes dropped overcharge protection

---

**Important**

When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own.; separate debug stats have been added for P-GW.

**show subscribers pgw-only full all**

The following field and counters display Overcharging Protection:

- Bearer State
  - in packet dropped overcharge protection
  - in bytes dropped overcharge protection
  - out packet dropped overcharge protection
  - out bytes dropped overcharge protection

**show subscribers summary**

The following counters display overcharging protection for all subscribers:

- in bytes dropped ovrchrgPtn
- in packet dropped ovrchrgPtn
- out bytes dropped ovrchrgPtn
• out packet dropped ovrchrgPtn

**Important**

When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own; separate debug stats have been added for P-GW.
Chapter 11

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)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)

Important In StarOS version 19 and later releases, the Rf interface is not supported on the 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 includes the following topics:

- Introduction, page 191
- Features and Terminology, page 195
- How it Works, page 201
- Configuring Rf Interface Support, page 203

Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/eHRPD 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, 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 49: Charging Architecture
The following figure shows the Rf interface between CTF and CDF.

*Figure 50: 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.
**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 CTF to the CCF.

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 (Release9)

**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 17: 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 18: 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>
<tr>
<td></td>
<td>ISUP:ANM (applicable for the MGCF)</td>
</tr>
<tr>
<td>ACR [Interim]</td>
<td>SIP 200 OK acknowledging a SIP</td>
</tr>
<tr>
<td></td>
<td>RE-INVITE or SIP UPDATE [e.g. change in media components]</td>
</tr>
<tr>
<td></td>
<td>Expiration of AVP [Acct-Interim-Interval]</td>
</tr>
<tr>
<td></td>
<td>SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE</td>
</tr>
<tr>
<td>ACR [Stop]</td>
<td>SIP BYE message (both normal and abnormal session termination cases)</td>
</tr>
<tr>
<td></td>
<td>ISUP:REL (applicable for the MGCF)</td>
</tr>
</tbody>
</table>
### Diameter Message Table

<table>
<thead>
<tr>
<th>Diameter Message</th>
<th>Triggering SIP Method/ISUP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR [Event]</td>
<td>SIP 200 OK acknowledging non-session related SIP messages, which are:</td>
</tr>
<tr>
<td></td>
<td>• SIP NOTIFY</td>
</tr>
<tr>
<td></td>
<td>• SIP MESSAGE</td>
</tr>
<tr>
<td></td>
<td>• SIP REGISTER</td>
</tr>
<tr>
<td></td>
<td>• SIP SUBSCRIBE</td>
</tr>
<tr>
<td></td>
<td>• SIP PUBLISH</td>
</tr>
<tr>
<td></td>
<td>SIP 200 OK acknowledging an initial SIP INVITE</td>
</tr>
<tr>
<td></td>
<td>SIP 202 Accepted acknowledging a SIP REFER or any other method</td>
</tr>
<tr>
<td></td>
<td>SIP Final Response 2xx (except SIP 200 OK)</td>
</tr>
<tr>
<td></td>
<td>SIP Final/Redirection Response 3xx</td>
</tr>
<tr>
<td></td>
<td>SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up</td>
</tr>
<tr>
<td></td>
<td>SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure</td>
</tr>
<tr>
<td></td>
<td>SIP CANCEL, indicating abortion of a SIP session set-up</td>
</tr>
</tbody>
</table>

### 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 19: Diameter Rf Messages**

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Source</th>
<th>Destination</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting-Request</td>
<td>CTF</td>
<td>CDF</td>
<td>ACR</td>
</tr>
<tr>
<td>Accounting-Answer</td>
<td>CDF</td>
<td>CTF</td>
<td>ACA</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 and identity 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 expired 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". Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI command "trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } }" the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions. If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

Releases prior to 16.0, whenever the volume/time-limit event triggers are generated, ACR-Interims were sent out immediately. In 16.0 and later releases, CLI configuration options are provided in policy accounting configuration to control the various Rf messages (ACRs) triggered for sync on this feature.

This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

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.

In 17.0 and later releases, a common timer based approach is implemented for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing. Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.
Cessation of Rf Records When UE is IDLE

Releases prior to 16.0, when the UE was identified to be in IDLE state and not sending any data, the P-GW generated Rf records. During this scenario, the generated Rf records did not include Service Data Containers (SDCs).

In 16.0 and later releases, the Rf records are not generated in this scenario. New CLI configuration command "session idle-mode suppress-interim" is provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and no data is transferred.

That is, this CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

For more information on the command, 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.

**Figure 51: Rf Call Flow for Event Based Charging**

**Table 20: 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>
</tbody>
</table>
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).

The CDF receives the relevant service charging parameters and processes accounting request.

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.

The following figure and table explain the simple Rf call flow for session based charging.

**Figure 52: Rf Call Flow 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>The CDF receives the relevant service charging parameters and processes accounting request.</td>
</tr>
<tr>
<td>3</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>
### 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 Enabling Rf Interface in Active Charging Service, on page 204.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN / P-GW Rf Interface Support, on page 204
In StarOS versions 19 and later, the Rf interface is not supported on the S-GW.

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:

```
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:

```
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 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 Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 22: 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>Stop</td>
<td>Normal Release</td>
<td>YES NO YES</td>
<td>Normal Release</td>
<td>When PDN/IP session is closed, C-C in both level will have Normal Release.</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</td>
<td>N/A</td>
<td>Normal Release</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES NO YES</td>
<td>Abnormal Release</td>
<td>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 All trigger (Interim) trigger.</td>
</tr>
</tbody>
</table>

S-GW Administration Guide, StarOS Release 19
<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>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>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>Interim</td>
<td>Time Limit</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>Serving Node Change</td>
<td>YES</td>
<td>NO</td>
<td>NO</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>NO</td>
</tr>
<tr>
<td>Interim</td>
<td>RAT Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

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></td>
<td></td>
<td>Addition of Container</td>
<td>Partial FDR</td>
<td>Final FDR</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>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 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>
</tbody>
</table>

Flow Idled out. 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.

Volume Limit reached for a specific flow. 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.
<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>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>
<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>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>YES</td>
<td>NO</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>
</tbody>
</table>

This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. Max Change Condition is applicable for QoS-Change, Service-Idled Out, ULI change, Flow Normal Release, Flow Abnormal Release, Service Data Volume Limit, Service Data Time Limit, AII Timer ACR Interim and Service Node Change CC only. The Max Number of Changes in Charging Conditions is set at 10. Example assuming 1 flow in the PDN Session: [1] Max Number of Changes in Charging Conditions set at P-GW/GGSN = 2. [2] Change Condition 1 takes place. No ACR Interim is sent. P-GW/GGSN stores the SDC. [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 2 Service-Data-Containers (1 for each change condition) are
### Configuring P-CSCF/S-CSCF Rf Interface Support

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

```bash
configure
context vpn
  aaa group default
diameter authentication dictionary aaa-custom8
diameter accounting dictionary aaa-custom2
diameter accounting endpoint <endpoint_name>
diameter accounting server <server_name> priority <priority>
exit
diameter endpoint <endpoint_name>
  origin realm <realm_name>
  use-proxy
  origin host <host_name> address <ip_address>
  peer <peer_name> address <ip_address>
exit
end
```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference.*
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><code>show diameter aaa-statistics</code></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              NAS Unneeded: 0
Port Preempted: 0          Port Suspended: 0
Service Unavailable: 0     Callback: 0
```
<table>
<thead>
<tr>
<th>User Error:</th>
<th>0</th>
<th>Host Request:</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accounting Servers Summary</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Message Stats:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total AC Requests:</td>
<td>0</td>
<td>Total AC Answers:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Start:</td>
<td>0</td>
<td>ACA-Start:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Start Retries:</td>
<td>0</td>
<td>ACA-Start Timeouts:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Interim:</td>
<td>0</td>
<td>ACA-Interim:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Interim Retries:</td>
<td>0</td>
<td>ACA-Interim Timeouts:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Event:</td>
<td>0</td>
<td>ACA-Event:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Stop:</td>
<td>0</td>
<td>ACA-Stop:</td>
<td>0</td>
</tr>
<tr>
<td>ACR-Stop Retries:</td>
<td>0</td>
<td>ACA-Stop Timeouts:</td>
<td>0</td>
</tr>
<tr>
<td>ACA-Dropped:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AC Message Error Stats:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diameter Protocol Errs:</td>
<td>0</td>
<td>Bad Answers:</td>
<td>0</td>
</tr>
<tr>
<td>Unknown Session Reqs:</td>
<td>0</td>
<td>Bad Requests:</td>
<td>0</td>
</tr>
<tr>
<td>Request Timeouts:</td>
<td>0</td>
<td>Parse Errors:</td>
<td>0</td>
</tr>
<tr>
<td>Request Retries:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
S-GW Event Reporting

This chapter describes the record content and trigger mechanisms for S-GW event reporting. When enabled the S-GW writes 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.

This chapter includes the following topics:

- Event Record Triggers, page 217
- Event Record Elements, page 218
- Active-to-Idle Transitions, page 220
- 3GPP 29.274 Cause Codes, page 220

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 23: S-GW Event Record Elements

<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>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>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>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 (0-40000000000)</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>
</tbody>
</table>
Active-to-Idle Transitions

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

Table 24: Subscriber-initiated Attach (initial) Call Flow Description

<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

Table 25: 3GPP 29.274 Cause Codes

<table>
<thead>
<tr>
<th>Cause Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</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>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</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 next peer</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>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>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</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>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</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>

**Sub-Causes**

- NO_INFORMATION
- ABORTED_BY_SESSION_DELETION
- NO_RESPONSE_FROM_MME
- INTERNALLY_TRIGGERED
- BEARERS_IN_MULTIPLE_PDN_CONNECTIONS
- EXPECTED_BEARERS_MISSING_IN_MESSAGE
- UNEXPECTED_BEARERS_PRESENT_IN_MESSAGE
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:

- Interface and Port Rules, page 225
- S-GW Service Rules, page 226
- S-GW Subscriber Rules, page 227

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-U/S11 interface:

• An S1-U/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.
Large numbers of services greatly increase the complexity of management and may impact overall system performance. Only create a large number of services only be configured 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.