SAE-GW Administration Guide, StarOS Release 17
Last Updated October 15, 2015
## CONTENTS

**About this Guide**........................................................................................................... xvii  
Conventions Used............................................................................................................. xviii  
Supported Documents and Resources........................................................................... xix  
Related Common Documentation .................................................................................... xix  
Related Product Documentation ...................................................................................... xix  
Obtaining Documentation ................................................................................................ xx  
Contacting Customer Support........................................................................................... xx

**SAE Gateway Overview** ............................................................................................... 21  
SAEGW Product Description ............................................................................................ 22  
Platform Requirements .................................................................................................... 23  
Licenses .......................................................................................................................... 23  
S-GW Product Description .............................................................................................. 24  
Platform Requirements .................................................................................................... 26  
Licenses .......................................................................................................................... 26  
P-GW Product Description .............................................................................................. 27  
Platform Requirements .................................................................................................... 29  
Licenses .......................................................................................................................... 29  
S-GW Network Deployment(s) .......................................................................................... 30  
Serving Gateway in the E-UTRAN/EPC Network ............................................................. 30  
Supported Logical Network Interfaces (Reference Points) ............................................. 31  
P-GW Network Deployment(s) .......................................................................................... 36  
PDN Gateway in the E-UTRAN/EPC Network ................................................................. 36  
Supported Logical Network Interfaces (Reference Points) ............................................. 37  
PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity ............................. 42  
Supported Logical Network Interfaces (Reference Points) ............................................. 43  
S-GW Features and Functionality - Base Software ............................................................ 48  
Abnormal Bearer Termination Cause in CDR ................................................................ 49  
ANSI T1.276 Compliance ............................................................................................... 49  
APN-level Traffic Policing ............................................................................................... 49  
Bulk Statistics Support .................................................................................................... 50  
CDR Support for Including LAPI (Signaling Priority) .................................................... 50  
Circuit Switched Fall Back (CSFB) Support .................................................................... 51  
Closed Subscriber Group Support ................................................................................... 51  
Dedicated Bearer Timeout Support on the S-GW ............................................................. 51  
Downlink Delay Notification ............................................................................................ 51  
Value Handling ............................................................................................................... 52  
Throttling ....................................................................................................................... 52  
EPS Bearer ID and ARP Support ..................................................................................... 52  
DSCP Ingress and Egress and DSCP Marking at the APN Profile ................................... 52  
Dynamic GTP Echo Timer ............................................................................................... 52  
Event Reporting .............................................................................................................. 53  
Idle-mode Signaling Reduction Support .......................................................................... 53  
IMSI/IMEI Available in System Event Logs of Type Error and Critical ........................... 53  
IP Access Control Lists ................................................................................................... 55  
IPv6 Capabilities ............................................................................................................ 56
GW Features a MPLS EXP Marking of User Plane Traffic
Management System Overview
MME Restoration Support
Multiple PDN Support
Node Functionality GTP Echo
Online/Offline Charging
  Online: Gy Reference Interface
  Offline: Gz Reference Interface
  Offline: Rf Reference Interface
Operator Policy Support
Peer GTP Node Profile Configuration Support
P-GW Restart Notification Support
QoS Bearer Management
Rf Diameter Accounting
S-GW Session Idle Timer
Subscriber Level Trace
Threshold Crossing Alerts (TCA) Support
P-GW Features and Functionality - Base Software
  3GPP R9 Volume Charging Over Gx
  AAA Server Groups
  ANSI T1.276 Compliance.
  APN Support
  Assume Positive for Gy-based Quota Tracking
  Bit Rate Mapping Across Gx and GTP-based Interfaces
  Bulk Statistics Support
  Congestion Control
  Default and Dedicated EPC Bearers
  DHCP Support
  DHCPv6 Support
  Direct Tunnel Support
  DNS Support for IPv4/IPv6 PDP Contexts
  Domain Based Flow Definitions
  DSCP Marking
    GTP-U on per APN Basis
  Dynamic GTP Echo Timer
  Dynamic Policy Charging Control (Gx Reference Interface)
  Enhanced Charging Service (ECS)
    Content Analysis Support
    Content Service Steering
    Support for Multiple Detail Record Types
    Diameter Credit Control Application
    Accept TCP Connections from DCCA Server
    Gy Interface Support
  Framed-Route Attribute Support
  Gn/Gp Handoff Support
  IMS Emergency Bearer Handling
  IP Access Control Lists
  IP Address Hold Timers
  IPv6 Capabilities
  Local Break-Out
  Management System Overview
  MPLS EXP Marking of User Plane Traffic
  Mobile IP Registration Revocation
How This Configuration Works

eGTP S-GW Configuration
  Initial Configuration
  eGTP Configuration
  Verifying and Saving the Configuration

Configuring Optional Features on the eGTP S-GW
  Configuring the GTP Echo Timer
    Default GTP Echo Timer Configuration
    Dynamic GTP Echo Timer Configuration

Configuring GTTPP Offline Accounting on the S-GW

Configuring Diameter Offline Accounting on the S-GW

Configuring APN-level Traffic Policing on the S-GW

Configuring X.509 Certificate-based Peer Authentication

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

Configuring ACL-based Node-to-Node IP Security on the S1-U and S5 Interfaces
  Creating and Configuring a Crypto Access Control List

Configuring Diameter-based Node-to-Node IP Security on the S1-U and S5 Interfaces
  Creating and Configuring an IPSec Transform Set

Creating and Configuring an IKEv2 Transform Set

Creating and Configuring a Crypto Map

Configuring S4 SGSN Handover Capability

Configuring an eGTP P-GW Service
  Information Required
    Required P-GW Context Configuration Information
    Required PDN Context Configuration Information
    Required AAA Context Configuration Information
    How This Configuration Works

eGTP P-GW Configuration
  Initial Configuration
  P-GW Service Configuration
  P-GW PDN Context Configuration
  Active Charging Service Configuration

Policy Configuration
  Verifying and Saving the Configuration

DHCP Service Configuration
  DHCP Service Creation
  DHCP Server Parameter Configuration

DHCP Service Configuration Verification

DHCPv6 Service Configuration
  DHCPv6 Service Creation
  DHCPv6 Server Parameter Configuration

DHCPv6 Client Parameter Configuration
  DHCPv6 Profile Configuration

Associate DHCPv6 Configuration

DHCPv6 Service Configuration Verification

Configuring Optional Features on the P-GW
  Configuring ACL-based Node-to-Node IP Security on the S5 Interface
  Creating and Configuring a Crypto Access Control List
  Creating and Configuring an IPSec Transform Set
  Creating and Configuring an IKEv2 Transform Set
  Creating and Configuring a Crypto Map
Session Tracing on the SAEGW ................................................................. 229
  Session Tracing Overview .................................................................. 230
  Session Trace Types ......................................................................... 231
  Session Trace Activation .................................................................... 231
  Session Trace Deactivation ............................................................... 231
  Data Collection .................................................................................. 232
  Data Forwarding ................................................................................ 232
  Supported Standards ......................................................................... 232

Configuring Session Trace on the SAEGW ......................................... 233
  Enabling Session Tracing on the SAEGW ......................................... 233
    Verifying that Session Tracing is Enabled ....................................... 234
  Configuring a Session Trace Template for the SAEGW ................. 234
    Verifying the Session Trace Template Configuration .................. 236
  Configuring a Management Session Trace on the SAEGW .......... 236
    Verifying the Management Trace Configuration .......................... 236
  Configuring a Signaling Session Trace on the SAEGW ............... 237
    Verifying the Signaling Session Trace Configuration ................. 238
  Configuring a Random Trace on the SAEGW ................................. 239
    Verifying the Random Trace Configuration .................................. 240
  Monitoring the Session Trace Functionality .................................... 241
  Supported SAEGW Session Trace Configurations .......................... 242
  Session Trace File Example ............................................................... 245

Monitoring the Service ........................................................................ 249
  Monitoring System Status and Performance .................................. 250
  Clearing Statistics and Counters ...................................................... 254

CoA, RADIUS DM, and Session Redirection (Hotlining) .................... 255
  RADIUS Change of Authorization and Disconnect Message .......... 256
    CoA Overview ............................................................................. 256
  DM Overview .................................................................................. 256
  License Requirements ...................................................................... 256
  Enabling CoA and DM ................................................................. 256
    Enabling CoA and DM ............................................................... 257
    CoA and DM Attributes ............................................................. 257
    CoA and DM Error-Cause Attribute ......................................... 258
    Viewing CoA and DM Statistics ................................................ 259
  Session Redirection (Hotlining) ...................................................... 262
    Overview ..................................................................................... 262
Contents

License Requirements .......................................................... 262
Operation .............................................................................. 262
ACL Rule .............................................................................. 262
Redirecting Subscriber Sessions ............................................ 262
Session Limits On Redirection ................................................ 263
Stopping Redirection ............................................................ 263
Handling IP Fragments .......................................................... 263
Recovery .............................................................................. 263
AAA Accounting ..................................................................... 263
Viewing the Redirected Session Entries for a Subscriber ............. 263

Direct Tunnel ........................................................................ 269
Direct Tunnel Feature Overview ............................................. 270
Direct Tunnel Configuration ................................................... 274
Configuring Direct Tunnel Support on the SGSN ..................... 274
Enabling Setup of GTP-U Direct Tunnels ................................. 275
Enabling Direct Tunnel per APN ............................................ 275
Enabling Direct Tunnel per IMEI ........................................... 276
Enabling Direct Tunnel to Specific RNCs ................................. 276
Verifying the SGSN Direct Tunnel Configuration ..................... 277
Configuring S12 Direct Tunnel Support on the S-GW ............... 279

GRE Protocol Interface ......................................................... 281
Introduction .......................................................................... 282
Supported Standards ............................................................. 283
Supported Networks and Platforms ....................................... 284
Licenses .............................................................................. 285
Services and Application on GRE Interface ............................. 286
How GRE Interface Support Works ....................................... 287
Ingress Packet Processing on GRE Interface ............................ 287
Egress Packet Processing on GRE Interface ............................. 289
GRE Interface Configuration .................................................. 290
Virtual Routing And Forwarding (VRF) Configuration ............... 290
GRE Tunnel Interface Configuration ....................................... 291
Enabling OSPF for VRF ....................................................... 292
Associating IP Pool and AAA Group with VRF ....................... 292
Associating APN with VRF ................................................. 293
Static Route Configuration ...................................................... 293
Verifying Your Configuration ................................................ 294

Gx Interface Support ................................................................ 297
Rel. 6 Gx Interface ............................................................... 298
Introduction .......................................................................... 298
Supported Networks and Platforms ....................................... 298
License Requirements ........................................................... 299
Supported Standards ............................................................. 299
How it Works ......................................................................... 299
Configuring Rel. 6 Gx Interface ............................................. 301
Configuring IMS Authorization Service at Context Level ........ 301
Verifying IMS Authorization Service Configuration ............... 303
Applying IMS Authorization Service to an APN ..................... 303
Verifying Subscriber Configuration ....................................... 304
Rel. 7 Gx Interface ............................................................... 305
Introduction .......................................................................... 305
Supported Networks and Platforms ....................................... 307
Contents

License Requirements .......................................................... 307
Supported Standards ............................................................ 307
Terminology and Definitions .................................................. 307
  Policy Control ................................................................. 307
  Charging Control ............................................................ 311
  Policy and Charging Control (PCC) Rules ............................. 312
  PCC Procedures over Gx Reference Point ............................... 314
  Volume Reporting Over Gx ............................................... 316
How Rel. 7 Gx Works ............................................................ 320
Configuring Rel. 7 Gx Interface ............................................. 323
  Configuring IMS Authorization Service at Context Level .......... 323
  Applying IMS Authorization Service to an APN ..................... 326
  Configuring Volume Reporting over Gx ............................... 327
Gathering Statistics ............................................................ 327
Rel. 8 Gx Interface .............................................................. 329
HA/PDSN Rel. 8 Gx Interface Support .................................... 329
  Introduction ...................................................................... 329
  Terminology and Definitions ............................................. 331
  How it Works ..................................................................... 337
  Configuring HA/PDSN Rel. 8 Gx Interface Support ................. 340
  Gathering Statistics .......................................................... 342
P-GW Rel. 8 Gx Interface Support ........................................... 343
  Introduction ...................................................................... 343
  Terminology and Definitions ............................................. 344
Rel. 9 Gx Interface .............................................................. 349
P-GW Rel. 9 Gx Interface Support ........................................... 349
  Introduction ...................................................................... 349
  Terminology and Definitions ............................................. 349
Rel. 10 Gx Interface .............................................................. 355
P-GW Rel. 10 Gx Interface Support ........................................... 355
  Introduction ...................................................................... 355
  Terminology and Definitions ............................................. 355
Supported Gx Features ........................................................... 363
Assume Positive for Gx ......................................................... 363
  Default Policy on CCR-I Failure ....................................... 364
  Gx Back off Functionality .................................................. 365
  Support for Volume Reporting in Local Policy ...................... 365
  Support for Session Recovery and Session Synchronization .... 365
  Configuring Gx Assume Positive Feature .............................. 366
Time Reporting Over Gx ........................................................ 369
  License Requirements ....................................................... 369
  Feature Overview ............................................................. 369
  Usage Monitoring ............................................................. 370
  Usage Reporting ............................................................... 371
  Configuring Time Reporting over Gx .................................... 371
Support for Multiple Active and Standby Gx Interfaces to PCRF .... 372
  Configuring Diameter Peer Selection at Diabase in Failure Scenarios 373
Support for Multiple CCR-U on Gx Interface ......................... 373
  Configuring Gateway Node to Support Back-to-Back CCR-U ... 374
Support for 'RAN/NAS Cause’ IE on Gx Interface .................... 375
  Configuring Supported Feature 'Netloc-RAN-NAS-Cause’ ........ 375
Support ADC Rules over Gx Interface .................................... 376
  Limitations ...................................................................... 376
  Configuring ADC Rules over Gx ........................................ 377
Contents

Gy Interface Support ..............................................................................................................379
    Introduction ..........................................................................................................................380
    License Requirements ..........................................................................................................381
    Supported Standards ...........................................................................................................381
Features and Terminology ......................................................................................................382
    Charging Scenarios .............................................................................................................382
    Session Charging with Reservation ..................................................................................382
    Basic Operations ................................................................................................................382
    Re-authorization ................................................................................................................383
    Threshold based Re-authorization Triggers .........................................................................383
    Termination Action ..............................................................................................................383
Diameter Base Protocol ..........................................................................................................383
Diameter Credit Control Application ....................................................................................384
    Quota Behavior ..................................................................................................................385
    Supported AVPs ................................................................................................................396
    Unsupported AVPs ..............................................................................................................399
PLMN and Time Zone Reporting .............................................................................................405
    Interworking between Session-based Gy and Event-based Gy .............................................406
OCS Unreachable Failure Handling Feature ........................................................................406
Backpressure Handling ..........................................................................................................408
Gy Backpressure Enhancement ..............................................................................................408
CC based Selective Gy Session Control ................................................................................409
    Feature Description ..........................................................................................................409
    Configuring CC based Selective Gy Session Control ........................................................410
    Monitoring and Troubleshooting the Selective Gy Session Control Feature ......................411
Configuring Gy Interface Support ........................................................................................412
    Configuring GGSN / P-GW / IPSG Gy Interface Support ..................................................412
    Configuring HA / PDSN Gy Interface Support ..................................................................413
    Configuring PLMN and Time Zone Reporting ..................................................................415
    Configuring Server Unreachable Feature ..........................................................................417
    Gathering Statistics ..........................................................................................................417
ICAP Interface Support ........................................................................................................419
    ICAP Interface Support Overview ....................................................................................420
    Failure Action on Retransmitted Packets ..........................................................................421
    Supported Networks and Platforms ..................................................................................422
    License Requirements .......................................................................................................422
Configuring ICAP Interface Support ...................................................................................423
    Creating ICAP Server Group and Address Binding ..........................................................423
    Configuring ICAP Server and Other Parameters ..............................................................424
    Configuring ECS Rulebase for ICAP Server Group ..........................................................424
    Configuring Charging Action for ICAP Server Group ......................................................425
    Verifying the ICAP Server Group Configuration ...............................................................425
L2TP Access Concentrator .....................................................................................................427
    Applicable Products and Relevant Sections .....................................................................428
    Supported LAC Service Configurations for PDSN Simple IP ............................................429
    Attribute-based Tunneling ................................................................................................429
    How The Attribute-based L2TP Configuration Works ......................................................430
    Configuring Attribute-based L2TP Support for PDSN Simple IP .....................................430
    PDSN Service-based Compulsory Tunneling ....................................................................431
    How PDSN Service-based Compulsory Tunneling Works ..............................................431
    Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP .........................432
    Supported LAC Service Configurations for the GGSN and P-GW .................................434
Contents

Transparent IP PDP Context Processing with L2TP Support ........................................ 435
Non-transparent IP PDP Context Processing with L2TP Support ................................. 436
PPP PDP Context Processing with L2TP Support .......................................................... 437
Configuring the GGSN or P-GW to Support L2TP ....................................................... 438
Supported LAC Service Configuration for Mobile IP ..................................................... 439
How The Attribute-based L2TP Configuration for MIP Works .................................... 439
Configuring Attribute-based L2TP Support for HA Mobile IP ...................................... 440
Configuring Subscriber Profiles for L2TP Support ....................................................... 442
RADIUS and Subscriber Profile Attributes Used ......................................................... 442
RADIUS Tagging Support .............................................................................................. 443
Configuring Local Subscriber Profile for L2TP Support .............................................. 443
Configuring Local Subscriber ....................................................................................... 444
Verifying the L2TP Configuration .................................................................................. 444
Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes .... 445

Configuring LAC Services .............................................................................................. 446
Configuring LAC Service .............................................................................................. 446
Configuring LNS Peer .................................................................................................... 447
Verifying the LAC Service Configuration ..................................................................... 447
Modifying PDSN Services for L2TP Support ................................................................. 449
Modifying PDSN Service .............................................................................................. 449
Verifying the PDSN Service for L2TP Support ............................................................. 450
Modifying APN Templates to Support L2TP ................................................................. 451
Assigning LNS Peer Address in APN Template ............................................................ 451
Configuring Outbound Authentication .......................................................................... 452
Verifying the APN Configuration ................................................................................... 452

Mobile IP Registration Revocation ............................................................................ 453
Overview ....................................................................................................................... 454
Configuring Registration Revocation .......................................................................... 455
Configuring FA Services .............................................................................................. 455
Configuring HA Services .............................................................................................. 455

Multi-Protocol Label Switching (MPLS) Support ....................................................... 459
Overview ....................................................................................................................... 460
Chassis as MPLS-CE Connecting to PE ....................................................................... 460
Chassis as MPLS-CE Connected to ASBR .................................................................. 461
Engineering Rules .......................................................................................................... 461
Supported Standards ...................................................................................................... 462
Supported Networks and Platforms ............................................................................. 463
Licenses ......................................................................................................................... 464
Benefits .......................................................................................................................... 465
Configuring BGP/MPLS VPN with Static Labels .......................................................... 466
Create VRF with Route-distinguisher and Route-target .............................................. 466
Set Neighbors and Enable VPNv4 Route Exchange ..................................................... 467
Configure Address Family and Redistributed Connected Routes ............................... 467
Configure IP Pools with MPLS Labels ......................................................................... 468
Bind DHCP Service for Corporate Servers ................................................................. 468
Bind AAA Group for Corporate Servers ..................................................................... 468

Configuring BGP/MPLS VPN with Dynamic Labels ..................................................... 470
Create VRF with Route-distinguisher and Route-target .............................................. 470
Set Neighbors and Enable VPNv4 Route Exchange ..................................................... 471
Configure Address Family and Redistributed Connected Routes ............................... 471
Configure IP Pools with MPLS Labels ......................................................................... 472
Bind DHCP Service for Corporate Servers ................................................................. 472
Bind AAA Group for Corporate Servers ..................................................................... 473
Network Mobility (NEMO) ................................................................. 475

Operator Policy .................................................................................. 487

Proxy-Mobile IP .................................................................................. 503
Routing Behind the Mobile Station on an APN ........................................581
 Feature Description ................................................................. 582
 How It Works ................................................................................. 583
 Configuring Routing Behind the Mobile Station ......................... 583
 Configuration Overview .............................................................. 584
 Creating an APN Profile ............................................................... 584
 Enabling Routing Behind the Mobile Station ............................. 585
 Verifying the Routing Behind the Mobile Station ....................... 585
 Monitoring and Troubleshooting the Routing Behind the Mobile Station .................................................................................. 592
 How it Works ................................................................................. 592
 show apn name <apn_name> ..................................................... 592

S-GW Event Reporting ..................................................................593
 Event Record Triggers .................................................................. 594
 Event Record Elements .............................................................. 595
 Active-to-Idle Transitions ............................................................ 597
 3GPP 29.274 Cause Codes ......................................................... 598

S-GW Restoration Support ......................................................... 601
 Feature Description ................................................................. 602
 Relationships to Other Features .................................................. 602
 How it Works ................................................................................. 603
 Changes at P-GW ................................................................. 603
 Changes at the E-GTPC .............................................................. 603
 Changes at the MME and SGSN ................................................ 603
 Demux Failure Detection ............................................................ 603
 Standards Compliance ............................................................... 604
 Configuring S-GW Restoration Support .................................... 605
 Sample Configuration ............................................................... 605
 Verifying the S-GW Configuration ............................................. 605
 Monitoring and Troubleshooting S-GW Restoration Support ...... 607
 S-GW Show Commands ............................................................ 607
 show ims-authorization policy-control statistics ...................... 607
 show pgw-service statistics all ................................................. 607
 show subscribers pgw-only full all ........................................... 607

Traffic Policing and Shaping ...................................................... 609
 Overview ................................................................................. 610
 Traffic Policing ................................................................. 610
 Traffic Shaping ................................................................. 610
 Traffic Policing Configuration .................................................. 611
 Configuring Subscribers for Traffic Policing ............................. 611
 Configuring APN for Traffic Policing in 3GPP Networks ............ 612
 Traffic Shaping Configuration .................................................. 614
 Configuring Subscribers for Traffic Shaping ............................. 614
 Configuring APN for Traffic Shaping in 3GPP Networks ............ 615
 RADIUS Attributes ................................................................. 617
 Traffic Policing for CDMA Subscribers .................................... 617
 Traffic Policing for UMTS Subscribers .................................... 618

S-GW Engineering Rules ......................................................... 621
 Interface and Port Rules ............................................................ 622
 Assumptions ............................................................................. 622
 S1-U/S11 Interface Rules ........................................................... 622

SAE-GW Administration Guide, StarOS Release 17
Contents

S5/S8 Interface Rules ........................................................................................................... 622
MAG to LMA Rules .............................................................................................................. 623
S-GW Service Rules ............................................................................................................ 624
S-GW Subscriber Rules ....................................................................................................... 625

P-GW Engineering Rules .................................................................................................... 627

Interface and Port Rules ..................................................................................................... 628
S2a Interface Rules ............................................................................................................. 628
LMA to MAG ....................................................................................................................... 628
S5/S8 Interface Rules (GTP)............................................................................................... 628
P-GW Context and Service Rules ...................................................................................... 629
P-GW Subscriber Rules ...................................................................................................... 630
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

The following tables describe the conventions used throughout this documentation.

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

**Typeface Conventions**

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

Related Common Documentation

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

The following common documents are available:

- 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:

- GGSN Administration Guide
- HSGW Administration Guide
- IPSec Reference
- IPSG Administration Guide
- MME Administration Guide
- PDSN Administration Guide
- P-GW Administration Guide
- SAEGW Administration Guide
- SGSN Administration Guide

Obtaining Documentation

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

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

Use the information in this section to contact customer support.

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

The Cisco® ASR 5x00 provides wireless carriers with a flexible solution that functions as a System Architecture Evolution (SAE) Gateway with Packet Data Network (PDN) Gateway (P-GW) and Serving Gateway (S-GW) functions in LTE-SAE (3GPP2 Long Term Evolution-System Architecture Evolution) wireless data networks.

This overview provides general information about the SAEGW including:

- SAEGW Product Description
- S-GW Product Description
- P-GW Product Description
- S-GW Network Deployment(s)
- P-GW Network Deployment(s)
- S-GW Features and Functionality - Base Software
- P-GW Features and Functionality - Base Software
- P-GW Features and Functionality - Inline Service Support
- S-GW Features and Functionality - Optional Enhanced Feature Software
- P-GW Features and Functionality - Optional Enhanced Feature Software
- How the Serving Gateway Works
- How the PDN Gateway Works
- S-GW Supported Standards
- P-GW Supported Standards
SAEGW Product Description

The SAEGW node is a combination of S-GW and P-GW nodes. SAEGW operates as a service on ASR5x00 and requires existing S-GW and P-GW services to be configured and mentioned inside SAEGW service configuration. Existing standalone S-GW and P-GW services (when part of an SAEGW umbrella service) will work in tandem to present a single SAEGW node as a black-box view.

The SAEGW supports all of the interfaces that the standalone S-GW and P-GW products support, namely:

- **S11/S4** – GTPv2 based control interface towards MME/S4-SGSN
- **S1U/S12/S4U** – GTPv1 based data interface towards eNodeB/RNC/S4-SGSN
- **S5/S8** – GTPv2 based control interface between S-GW and P-GW
- **Gi** – Data interface towards packet data network
- **Gx** – Diameter based interface between P-GW and PCRF
- **S6b** – Diameter based interface between P-GW and HSS
- **Rf** – Diameter based offline charging interface between P-GW/S-GW and charging data function
- **Gy** – GTPP based online charging interface between P-GW and online charging system
- **Gz** – GTPP based offline charging interface between P-GW/S-GW and charging gateway function

Mode of operation is described as the functionality performed by SAEGW for a call. Granularity for mode of operation is per-PDN. The SAEGW service supports the following three modes of operation:

- **S+P Collapsed**: When a UE is using S-GW part of SAEGW and a PDN connection is terminating within the P-GW part of SAEGW.
- **Pure-S**: When a UE is using S-GW part of SAEGW and a PDN connection is terminating at an external P-GW not part of SAEGW.
- **Pure-P**: When a UE is using an external S-GW not part of SAEGW and a PDN connection is terminating within P-GW part of SAEGW.

**Important**: For a given UE with multiple PDNs, SAEGW will be able to support S+P mode for some PDNs while Pure-S mode for others.

**Important**: SAEGW supports change of operation-mode in life of a PDN. For example, a PDN initially doing S+P mode may change to doing Pure-P if S-GW gets relocated to external S-GW that is not part of SAEGW. Similarly, a PDN doing Pure-P mode may change to S+P mode if S-GW relocated so that new S-GW is part of SAEGW service.

An optimized SAEGW provides the following benefits:

- **Higher Capacity**
  A UE with one PDN connection that passes through standalone S-GW and P-GW services consumes two license units because both S-GW and P-GW services account for it separately. SAEGW as a single node consumes only one license unit for the same, thus increasing the capacity. Contact your Cisco account representative for detailed information on product licensing.

- **Cohesive Configuration**
  Configuration and management of SAEGW as a node is easier to follow than starting standalone S-GW and P-GW services.
Platform Requirements

The SAEGW 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 SAEGW 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.
S-GW Product Description

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

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

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

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

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

Licenses

The S-GW is a licensed Cisco product covered by the SAEGW license when part of an SAEGW umbrella service. 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.
P-GW Product Description

The P-GW is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening.

Figure 3 P-GW in the Basic E-UTRAN/EPC Network
Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

P-GW functions include:

- Mobility anchor for mobility between 3GPP access systems and non-3GPP access systems. This is sometimes referred to as the SAE Anchor function.
- Policy enforcement (gating and rate enforcement)
- Per-user based packet filtering (deep packet inspection)
- Charging support
- Lawful Interception
- UE IP address allocation
- Packet screening
- Transport level packet marking in the downlink;
- Downlink rate enforcement based on Aggregate Maximum Bit Rate (AMBR)

The following are additional P-GW functions when supporting non-3GPP access (eHRPD):

- P-GW includes the function of a Local Mobility Anchor (LMA) according to draft-ietf-netlmm-proxy-mip6, if PMIP-based S5 or S8 is used.
- The P-GW includes the function of a DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal, if S2c is used.
Platform Requirements

The P-GW service runs on a Cisco® ASR 5x00 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 P-GW is a licensed Cisco product covered by the SAEGW license when part of an SAEGW umbrella service. 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.
S-GW Network Deployment(s)

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

Serving Gateway in the E-UTRAN/EPC Network

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

Figure 5. Supported S-GW Interfaces in the E-UTRAN/EPC Network

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

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

**S1-U Interface**

This reference point provides bearer channel tunneling between the eNodeB and the S-GW. It also supports eNodeB path switching during handovers. The S-GW provides the local mobility anchor point for inter-eNodeB handovers. It provides inter-eNodeB path switching during handovers when the X2 handover interface between base stations cannot be used. The S1-U interface uses GPRS tunneling protocol for user plane (GTP-U1). 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

### S5/S8 Interface

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

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

### S11 Interface

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

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

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

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

**Gxc Interface**

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

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

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

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

---

**Rf Interface**

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

**Supported protocols:**
- Transport Layer: TCP or SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet
P-GW Network Deployment(s)

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

PDN Gateway in the E-UTRAN/EPC Network

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

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

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

**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 and TS 23.402. 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:
SAE Gateway Overview

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

S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers.

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AA) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and
secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

StarOS Release 17 and onwards, P-GW supports receiving AVP “Restoration-Priority-Indicator” from AAA server over the S6b interface to distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections. KPIs are also provided based on the AVP value.

**Important:** The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

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

### SGi Interface

This reference point provides connectivity between the P-GW and a packet data network (3GPP TS 23.401). This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

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

### Gx Interface
This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

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

For more information on the Gx interface, refer to *Dynamic Policy Charging Control (Gx Reference Interface)* in the *P-GW Features and Functionality - Base Software* section of this chapter.

**Gy Interface**

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

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

For more information on the Gy interface and online accounting, refer to *Gy Interface Support* in the *P-GW Features and Functionality - Base Software* section of this chapter.

**Gz Interface**

The Gz reference interface enables offline accounting functions on the P-GW. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

**Supported protocols:**
Gn/Gp Interface

This reference point provides tunneling and management between the P-GW and the SGSN during handovers between the EPS and 3GPP 2G and/or 3G networks (3GPP TS 29.060). For more information on the Gn/Gp interface, refer to Gn/Gp Handoff Support in the P-GW Features and Functionality - Base Software section of this chapter.

Supported protocols:
- Transport Layer: UDP, TCP
- Tunneling: GTP: GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

Rf Interface

The Rf interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

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

P-GW Network Deployment(s)

- Diameter
- SCTP
- IPv4/IPv6
- L1/L2

P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity

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

Figure 9. P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity

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

The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

**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: IPv4 or IPv6 GTP-C (signaling channel) and GTP-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet
S2a Interface

This reference point supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the PDN Gateway. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

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

S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF
This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers.

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the CLI.

Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

**Important:** The S6b interface can be disabled via the CLI in the event of a long-term AAA outage.

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

**SGi Interface**

This reference point provides connectivity between the P-GW and a packet data network. This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

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

This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

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

For more information on the Gx interface, refer to Dynamic Policy Charging Control (Gx Reference Interface) in the P-GW Features and Functionality - Base Software section of this chapter.

Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

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

For more information on Rf accounting, refer to the section in the P-GW Features and Functionality - Base Software section of this chapter.

Gy Interface
The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

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

For more information on the Gy interface and online accounting, refer to Gy Interface Support in the P-GW Features and Functionality - Base Software section of this chapter.
S-GW Features and Functionality - Base Software

**Important:** The SAEGW supports all of these features if an S-GW service is assigned to the SAEGW service.

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

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

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

- Abnormal Bearer Termination Cause in CDR
- ANSI T1.276 Compliance
- APN-level Traffic Policing
- Bulk Statistics Support
- CDR Support for Including LAPI (Signaling Priority)
- Circuit Switched Fall Back (CSFB) Support
- Closed Subscriber Group Support
- Dedicated Bearer Timeout Support on the S-GW
- Downlink Delay Notification
- DSCP Ingress and Egress and DSCP Marking at the APN Profile
- Dynamic GTP Echo Timer
- Event Reporting
- Idle-mode Signaling Reduction Support
- IP Access Control Lists
- IPv6 Capabilities
- LIPA Support
- Location Reporting
- Management System Overview
- MME Restoration Support
- Multiple PDN Support
- Node Functionality GTP Echo
- Online/Offline Charging
- Operator Policy Support
- Peer GTP Node Profile Configuration Support
SAE Gateway Overview

- P-GW Restart Notification Support
- QoS Bearer Management
- Rf Diameter Accounting
- S-GW Session Idle Timer
- Subscriber Level Trace
- Threshold Crossing Alerts (TCA) Support

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 (EMS), 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 EMS is capable of further processing the statistics data through XML parsing, archiving, and graphing. The Bulk Statistics Server component of an EMS 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 EMS 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 LAPI indication.

This benefit of this feature is that it provides support for carrying then 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:

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

Dedicated Bearer Timeout Support on the S-GW

The SAE-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 provides operators 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 `qci-qos mapping` table is updated with the addition of a `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.
Event Reporting

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

The S-GW Event Reporting 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 session-event-module command in the Context Configuration mode allows an operator to set the method and destination for transferring event files, as well as the format and handling characteristics of event files. For a detailed description of this command, refer to the Command Line Interface Reference.

Idle-mode Signaling Reduction Support

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

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

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

The GGSN/P-GW/SAEGW/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.

**Important:** Note that the GGSN/P-GW/SAEGW/S-GW will make a best effort attempt to include the IMSI/IMEI in system event logs of type error and critical. However, there still may be cases where the IMSI is not seen which are not mentioned in the following table.

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Events</td>
<td></td>
</tr>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format “[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d”</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format “[IMSI &lt;IMSI&gt;] Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s”</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format “[IMSI &lt;IMSI&gt;] Sessmgr-%d Ran out of session handles”</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format “[IMSI &lt;IMSI&gt;]%s”</td>
</tr>
<tr>
<td>Modified Events</td>
<td></td>
</tr>
<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 “[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)”</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format “[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)”</td>
</tr>
<tr>
<td>12382</td>
<td>Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format “[IMSI &lt;IMSI&gt;] Sessmgr-%d: Request to %s bearer rejected. Reason: %s”. For example “[IMSI 11223445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress”</td>
</tr>
<tr>
<td>12668</td>
<td>Represents fsm_event_error in format “[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d”</td>
</tr>
<tr>
<td>12774</td>
<td>Represents pgw_purge_invalid_err in format “[IMSI &lt;IMSI&gt;] Local%te %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s”</td>
</tr>
<tr>
<td>12855</td>
<td>Represents ncqos_nrspca_trig_err in format “[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcmmode”</td>
</tr>
<tr>
<td>12857</td>
<td>Represents ncqos_nrupc_tft_err in format “[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%u&gt;.”</td>
</tr>
<tr>
<td>12858</td>
<td>Represents ncqos_nrxx_trig_already in format “[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.”</td>
</tr>
<tr>
<td>12859</td>
<td>Represents ncqos_nrxx_tft_check_fail in format “[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”</td>
</tr>
<tr>
<td>12860</td>
<td>Represents ncqos_sec_rej in format “[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;%s&gt;.”</td>
</tr>
<tr>
<td>12861</td>
<td>Represents ncqos_upc_rej in format “[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;%s&gt;.”</td>
</tr>
<tr>
<td>12862</td>
<td>Represents ggsn_subsession_invalid_state in format “[IMSI &lt;IMSI&gt;] GGSN subsession invalid state: &lt;%s&gt;, [event: &lt;%s&gt;]”</td>
</tr>
<tr>
<td>11830</td>
<td>Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format “[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn’t support Deferred allocation for IPv4v6, dropping the call.”</td>
</tr>
<tr>
<td>11832</td>
<td>Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format “[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.”</td>
</tr>
<tr>
<td>11834</td>
<td>Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format “[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC &lt;0x%x&gt; not found.”</td>
</tr>
</tbody>
</table>
### IP Access Control Lists

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

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

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

**Important:** The S-GW supports interface-based ACLs only. For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.
IPv6 Capabilities

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

The S-GW platform offers the following IPv6 capabilities:

**IPv6 Connections to Attached Elements**

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

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

**Routing and Miscellaneous Features**

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

LIPA Support

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

In order to support millions of LIPA GTPC peers, S-GW memory management has been enhanced with regards to GTPv2 procedures and as well as to support the maintenance of statistics per peer node.

Establishment of LIPA PDN follows a normal call flow similar to that of a normal PDN as per 23.401; the specification does not distinguish between a LGW and a PGW call. As a result, the S-GW supports a new configuration option to detect a LIPA peer. As a fallback mechanism, heuristic detection of LIPA peer based on data flow characteristics of a LIPA call is also supported.

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

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

Location Reporting

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

ULI data reported in GTPv2 messages includes:

- **TAI-ID:** Tracking Area Identity
- **MCC:** Mobile Country Code, **MNC:** 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.

Management System Overview

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

Cisco's O+M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

- Using the Command Line Interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the console port on the SPIO card via an RS-232 serial connection
- Using an EMS application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (such as, Microsoft Internet Explorer v6.0 and above or others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG’s) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.
**Important:** P-GW management functionality is enabled by default for console-based access.

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

**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 a 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.

**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 (PMIPv6) tunnel for all user sessions toward the Local Mobility Anchor (LMA) function of the P-GW.

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

**Important:** Up to 11 multiple PDN connections are supported.

### Node Functionality GTP Echo

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

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

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

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

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

### Online/Offline Charging

The Cisco EPC platforms support offline charging interactions with external OCS and CGF/CDF servers. To provide subscriber level accounting, the Cisco EPC platform supports integrated Charging Transfer Function (CTF) and Charging Data Function (CDF) / Charging Gateway Function (CGF). Each gateway uses Charging-IDs to distinguish between default and dedicated bearers within subscriber sessions.

The ASR 5x00 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it also possible to enable file compression using protocols such as GZIP.

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

### Online: Gy Reference Interface

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

**Offline: Gz Reference Interface**

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

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

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

**Offline: Rf Reference Interface**

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

**Operator Policy Support**

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

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

A default operator policy can be configured and applied to all subscribers that do not match any of the per-PLMN or IMSI range policies.
The S-GW uses operator policy to set the Accounting Mode - 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.

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

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

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

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

**Policing:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (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.

**Rf Diameter Accounting**

Provides the framework for offline charging in a packet switched domain. The gateway support nodes use the Rf interface to convey session related, bearer related or service specific charging records to the CGF and billing domain for enabling charging plans.

The Rf reference interface enables offline accounting functions on the HSGW in accordance with 3GPP Release 8 specifications. In an LTE application the same reference interface is also supported on the S-GW and P-GW platforms. The Cisco gateways use the Charging Trigger Function (CTF) to transfer offline accounting records via a Diameter interface to an 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 Session Idle Timer**

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 Gx. The trace can be initiated using multiple methods:

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

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

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

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

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

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

As subscriber level trace is a CPU intensive activity the maximum number of concurrently monitored trace sessions per Cisco P-GW or S-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.
Threshold Crossing Alerts (TCA) Support

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

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

The following thresholding models are supported by the system:

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

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and clear) of each of the monitored values.
  
  Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
  
  Logs are supported in both the Alert and the Alarm models.

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

---
P-GW Features and Functionality - Base Software

**Important:** The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

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

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

This section describes the following features:

- 3GPP R9 Volume Charging Over Gx
- AAA Server Groups
- ANSI T1.276 Compliance
- APN Support
- Assume Positive for Gy-based Quota Tracking
- Bit Rate Mapping Across Gx and GTP-based Interfaces
- Bulk Statistics Support
- Congestion Control
- Default and Dedicated EPC Bearers
- DHCP Support
- DHCPv6 Support
- Direct Tunnel Support
- DNS Support for IPv4/IPv6 PDP Contexts
- Domain Based Flow Definitions
- DSCP Marking
- Dynamic GTP Echo Timer
- Dynamic Policy Charging Control (Gx Reference Interface)
- Enhanced Charging Service (ECS)
- GnGp Handoff Support
- IMS Emergency Bearer Handling
- IP Access Control Lists
- IP Address Hold Timers
- IPv6 Capabilities
- Local Break-Out
- Management System Overview
- Mobile IP Registration Revocation
- MPLS EXP Marking of User Plane Traffic
- MTU Size PCO
- Multiple PDN Support
- Node Functionality GTP Echo
- Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover
- Online/Offline Charging
- P-CSCF Recovery
- Peer GTP Node Profile Configuration Support
- PMIPv6 Heartbeat
- Proxy Mobile IPv6 (S2a)
- QoS Bearer Management
- RADIUS Support
- SGW Restoration Support
- Source IP Address Validation
- SRVCC PS-to-CS Handover Indication Support
- Subscriber Level Trace
- Threshold Crossing Alerts (TCA) Support
- UE Time Zone Reporting
- Virtual APN Support

3GPP R9 Volume Charging Over Gx

Also known as accumulated usage tracking over Gx, this 3GPP R9 enhancement provides a subset of the volume and charging control functions defined in TS 29.212 based on usage quotas between a P-GW and PCRF. The quotas can be assigned to the default bearer or any of the dedicated bearers for the PDN connection.

This feature enables volume reporting over Gx, which entails usage monitoring and reporting of the accumulated usage of network resources on an IP-CAN session or service data flow basis. PCRF subscribes to the usage monitoring at session level or at flow level by providing the necessary information to PCEF. PCEF in turn reports the usage to the PCRF when the conditions are met. Based on the total network usage in real-time, the PCRF will have the information to enforce dynamic policy decisions.

When usage monitoring is enabled, the PCEF can monitor the usage volume for the IP-CAN session, or applicable service data flows, and report accumulated usage to the PCRF based on any of the following conditions:

- When a usage threshold is reached,
- When all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated,
• When usage monitoring is explicitly disabled by the PCRF,
• When an IP CAN session is terminated or,
• When requested by the PCRF.

Accumulated volume reporting can be measured by total volume, the uplink volume, or the downlink volume as requested by the PCRF. When receiving the reported usage from the PCEF, the PCRF deducts the value of the usage report from the total allowed usage for that IP-CAN session, usage monitoring key, or both as applicable.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis.

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 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 Support

The P-GW's Access Point Name (APN) support offers several benefits:

• Extensive parameter configuration flexibility for the APN.
• Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
• Virtual APNs to allow differentiated services within a single APN.

In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW. In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

• **Accounting**: RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
**Authentication**: Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.

**Enhanced Charging**: Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).

**IP**: Method for IP address allocation (e.g., local allocation by P-GW, Mobile IP, DHCP, etc.). IP address ranges, with or without overlapping ranges across APNs.

**Tunneling**: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the P-GW independently from the APN.

**QoS**: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the P-GW, the subscriber may be authenticated/authorized with an AAA server. The P-GW allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the P-GW during subscriber authentication/authorization.

---

**Assume Positive for Gy-based Quota Tracking**

In the current implementation, the PCEF uses a Diameter based Gy interface to interact with the OCS and obtain quota for each subscriber's data session. Now, the PCEF can retry the OCS after a configured amount of quota has been utilized or after a configured amount of time. The quota value would be part of the dcca-service configuration, and would apply to all subscribers using this dcca-service. The temporary quota will be specified in volume (MB) and/or time (minutes) to allow for enforcement of both quota tracking mechanisms, individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the PCEF shall retry the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS. In the event that the OCS services have not been restored, the PCEF should reallocate the configured amount of quota and time assigned to the user. The PCEF should report all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the PCEF shall report quota used during all allocation intervals.

When the Gy interface is unavailable, the P-GW shall enter “assume positive” mode. Unique treatment is provided to each subscriber type. Each functional application shall be assigned unique temporary quota volume amounts and time periods based on a command-level AVP from the PCRF on the Gx interface. In addition, a configurable option has been added to disable assume positive functionality for a subscriber group identified by a command-level AVP sent on the Gx interface by the PCRF.

---

**Bit Rate Mapping Across Gx and GTP-based Interfaces**

This feature provides for more consistent behavior and ensures correct bandwidth is allocated for bearers.

Bit rate granularity provided by different interfaces was not aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

With this feature, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up.
This feature (rounding up the bitrate in kbps) will be enabled by default. However, a CLI command under P-GW service, \texttt{[ no ] egtp bitrates-rounded-down-kbps}, controls the behavior of rounding-up. The CLI command enables/disables the old behavior of rounding down. By default, this CLI command is configured to use rounded-up bitrate values. Depending on how the CLI is configured, either rounded-up (Ceil) or rounded-down bitrate value will be sent on GTP interface towards the Access side. If the CLI command is enabled, then it will result in the old behavior. In addition, \texttt{show subscribers pgw-only full all} shows the APN-AMBR in terms of bps. Previously, \texttt{show subscribers pgw-only full all} used to show in terms of kbps.

CR - C4-132189 - is defined for TS 29.274 for GTP conversion by P-GW.

**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 (EMS), 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 list of supported schemas for P-GW:

- **APN**: Provides Access PointName statistics
- **APN Expansion**: Provides more granular GTP-C statistics on a per-APN and per-QCI level
- **Card**: Provides card-level statistics
- **Context**: Provides context service statistics
- **Diameter-acct**: Provides Diameter Accounting statistics
- **Diameter-auth**: Provides Diameter Authentication statistics
- **ECS**: Provides Enhanced Charging Service statistics
- **EGTPC**: Provides Evolved GPRS Tunneling Protocol - Control message statistics
- **FA**: Provides FA service statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP**: Provides GPRS Tunneling Protocol - Prime message statistics
- **GTPU**: Provides GPRS Tunneling Protocol - User message statistics
- **HA**: Provides HA service statistics
- **IMSA**: Provides IMS Authorization service statistics
- **IP Pool**: Provides IP pool statistics
- **LMA**: Provides Local Mobility Anchor service statistics
- **P-GW**: Provides P-GW node-level service statistics
- **Port**: Provides port-level statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **System**: Provides system-level statistics
The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the 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 only for headers and footers), and/or the time that the file was generated.

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

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

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

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

### Congestion Control

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

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

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation 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.
Default and Dedicated EPC Bearers

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.

In the StarOS 9.0 release, the Cisco EPC core platforms support one or more EPS bearers (default plus dedicated). An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in the case of a GTP-based S5/S8 interface, and between a UE and HSGW (HRPD Serving Gateway) in case of a PMIP-based S2a interface. In networks where GTP is used as the S5/S8 protocol, the EPS bearer constitutes a concatenation of a radio bearer, S1-U bearer and an S5/S8 bearer anchored on the P-GW. In cases where PMIPv6 is used the EPS bearer is concatenated between the UE and HSGW with IP connectivity between the HSGW and P-GW.

Note: This release supports only GTP-based S5/S8 and PMIPv6 S2a capabilities with no commercial support for PMIPv6 S5/S8.

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and P-GW in the GTP-based S5/S8 design, and between a UE and HSGW in the PMIPv6 S2a approach. If different QoS scheduling priorities are required between Service Data Flows, they should be assigned to separate EPS bearers. Packet filters are signalled in the NAS procedures and associated with a unique packet filter identifier on a per-PDN connection basis.

One EPS bearer is established when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. A PDN connection represents a traffic flow aggregate between a mobile access terminal and an external Packet Data Network (PDN) such as an IMS network, a walled garden application cloud or a back-end enterprise network. Any additional EPS bearer that is established to the same PDN is referred to as a dedicated bearer. The EPS core elements assign a separate bearer ID for each established EPS bearer. At a given time a UE may have multiple PDN connections on one or more P-GWs.

DHCP Support

The P-GW supports dynamic IP address assignment to subscriber IP PDN contexts using the Dynamic Host Control Protocol (DHCP), as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

The method by which IP addresses are assigned to a PDN context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. Dynamically assigned IP addresses for subscriber PDN contexts can be assigned through the use of DHCP.

The P-GW acts as a DHCP server toward the UE and a DHCP client toward the external DHCP server. The DHCP server function and DHCP client function on the P-GW are completely independent of each other; one can exist without the other.

DHCP supports both IPv4 and IPv6 addresses.

The P-GW does not support DHCP-relay.
Deferred IPv4 Address Allocation

Apart from obtaining IP addresses during initial access signalling, a UE can indicate via PCO options that it prefers to obtain IP address and related configuration via DHCP after default bearer has been established. This is also known as Deferred Address Allocation.

IPv4 addresses are becoming an increasingly scarce resource. Since 4G networks like LTE are always on, scarce resources such as IPv4 addresses cannot/should not be monopolized by UEs when they are in an ECM-IDLE state.

PDN-type IPv4v6 allows a dual stack implementing. The P-GW allocates an IPv6 address only by default for an IPv4v6 PDN type. The UE defers the allocation of IPv4 addresses based upon its needs, and relinquishes any IPv4 addresses to the global pool once it is done. The P-GW may employ any IPv4 address scheme (local pool or external DHCP server) when providing an IPv4 address on demand.

DHCPv6 Support

The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables the DHCP servers to pass the configuration parameters, such as IPv6 network addresses to IPv6 nodes. It offers the capability of allocating the reusable network addresses and additional configuration functionality automatically.

The DHCPv6 support does not just feature the address allocation, but also fulfills the requirements of Network Layer IP parameters. Apart from these canonical usage modes, DHCPv6’s Prefix-Delegation (DHCP-PD) has also been standardized by 3GPP (Rel 10) for “network-behind-ue” scenarios. P-GW manages IPv6 prefix life-cycle just like it manages IPv4 addresses, thus it is responsible for allocation, renew, and release of these prefixes during the lifetime of a call. IPv6 prefixes may be obtained from either local-pool, AAA (RADIUS/DIAMETER) or external DHCPv6 servers. Stateless DHCPv6 procedures are used to supply higher layer IP parameters to the end host.

DHCPv6 support for P-GW covers the following requirements:

- RFC 3633, prefix delegation and Stateless services (primarily via the INFORMATION-REQUEST) mechanism
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC 4039, Rapid Commit Support

**Important:** For more information on DHCPv6 service configuration, refer to the DHCPv6 Configuration section of the PDN Gateway Configuration chapter.

Direct Tunnel Support

When Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality.

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel “switching” latency from the user plane. An additional advantage of direct tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The direct tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typically makes the decision to establish direct tunnel at PDP Context Activation. A direct tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request toward the GGSN).
A major consequence of deploying direct tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced as part of direct tunnel deployment. The Cisco GGSN and SGSN offer massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once direct tunnel is deployed.

**DNS Support for IPv4/IPv6 PDP Contexts**

This feature adds functionality in P-GW for PDN type IPv4v6. in StarOS Release 15.0. Previously, if an MS requested an IPv4 DNS address, P-GW did not send the IPv4 DNS address.

MS may request for DNS server IPv4 or IPv6 addresses using the Protocol Configurations Options IE (as a container or as part of IPCP protocol configuration request) in PDP Context Activation procedure for PDP Type IPv4, IPv6, or IPv4v6. In that case, the P-GW may return the IP address of one or more DNS servers in the PCO IE in the PDP Context Activation Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008.

For PDP Type IPv4v6, if MS requested DNS server IPv4 address, it did not return an IPv4 address. Support is now added to respond with address requested by MS.

AAA server may also provide DNS Server IP Address in Access-Accept Auth Response. In such cases, AAA provided DNS server IPs takes priority over the one configured under APN.

When DNS server address is requested in PCO configuration, the following preference would be followed:

1. DNS values received from RADIUS Server.
2. DNS values locally configured with APN.
3. DNS values configured at context level with ip name-servers CLI.

**Domain Based Flow Definitions**

This solution provides improved flexibility and granularity in obtaining geographically correct exact IP entries of the servers by snooping DNS responses.

Currently, it is possible to configure L7 rules to filter based on domain (m.google.com). Sometimes multiple servers may serve a domain, each with its own IP address. Using an IP-rule instead of an http rule will result in multiple IP-rules; one IP-rule for each server “behind” the domain, and it might get cumbersome to maintain a list of IP addresses for domain-based filters.

In this solution, you can create rules defining specifying hostnames (domain names) and parts of hostnames (domain names). Upon the definition of the hostnames/domain names or parts of them, the P-GW will monitor all the DNS responses sent towards the UE and will snoop only the DNS response, which has q-name or a-name as specified in the rules, and identify all the IP addresses resulted from the DNS responses. DNS snooping will be done on live traffic for every subscriber.

**DSCP Marking**

Provides support for more granular configuration of DSCP marking.

For Interactive Traffic class, the P-GW supports per-gateway service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The following matrix may be used to determine the DiffServ markings used based on the configured traffic class and Allocation/Retention Priority:
### Table 2. Default DSCP Value Matrix

<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>2</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>

In addition, the P-GW allows configuration of diameter packets and GTP-C/GTP-U echo with DSCP values.

### GTP-U on per APN Basis

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.

The S-GW/P-GW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

Previously, DSCP marking table was configured on P-GW service level. As part of this requirement, CLI was added to associate the qos-qci-mapping table in APN.

---

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

In order to be backward compatible with older configurations, if a DSCP marking table is associated with P-GW service and not with the APN, then the one in P-GW service will be used. If table is associated in both P-GW service and APN, then the one on APN will take precedence.

### 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.

### Dynamic Policy Charging Control (Gx Reference Interface)

Dynamic policy and charging control provides a primary building block toward the realization of IMS multimedia applications. In contrast to statically provisioned architectures, the dynamic policy framework provides a centralized service control layer with global awareness of all access-side network elements. The centralized policy decision elements simplify the process of provisioning global policies to multiple access gateways. Dynamic policy is especially useful in an Always-On deployment model as the usage paradigm transitions from a short lived to a lengthier online
session in which the volume of data consumed can be extensive. Under these conditions dynamic policy management enables dynamic just in-time resource allocation to more efficiently protect the capacity and resources of the network.

Dynamic Policy Control represents the ability to dynamically authorize and control services and application flows between a Policy Charging Enforcement Function (PCEF) on the P-GW and the PCRF. Policy control enables a centralized and decoupled service control architecture to regulate the way in which services are provisioned and allocated at the bearer resource layer.

The StarOS 9.0 release included enhancements to conform with 3GPP TS 29.212 and 29.230 functions. The Gx reference interface uses Diameter transport and IPv6 addressing. The subscriber is identified to the PCRF at session establishment using IMSI based NAI’s within the Subscription-ID AVP. Additionally the IMEI within the Equipment-Info AVP is used to identify the subscriber access terminal to the policy server. The Gx reference interface supports the following capabilities:

- Authorize the bearer establishment for a packet flow
- Dynamic L3/L4 transfer of service data flow filters within PCC rules for selection and policy enforcement of downlink/uplink IP CAN bearers
- Support static pre-provisioned L7 rulebase name attribute as trigger for activating Inline Services such as Peer-to-Peer Detection
- Authorize the modification of a service data flow
- Revoke the authorization of a packet flow
- Provision PCC rules for service data flows mapped to default or dedicated EPS bearers
- Support P-GW initiated event triggers based on change of access network gateway or IP CAN
- Provide the ability to set or modify APN-AMBR for a default EPS bearer
- Create or modify QoS service priority by including QCI values in PCC rules transmitted from PCRF to PCEF functions

Enhanced Charging Service (ECS)

The Enhanced Charging Service provides an integrated in-line service for inspecting subscriber data packets and generating detail records to enable billing based on usage and traffic patterns. Other features include:

- Content Analysis Support
- Content Service Steering
- Support for Multiple Detail Record Types
- Diameter Credit Control Application
- Accept TCP Connections from DCCA Server
- Gy Interface Support

The Enhanced Charging Service (ECS) is an in-line service feature that is integrated within the system. ECS enhances the mobile carrier’s ability to provide flexible, differentiated, and detailed billing to subscribers by using Layer 3 through Layer 7 deep packet inspection with the ability to integrate with back-end billing mediation systems.

ECS interacts with active mediation systems to provide full real-time prepaid and active charging capabilities. Here the active mediation system provides the rating and charging function for different applications.

In addition, ECS also includes extensive record generation capabilities for post-paid charging with in-depth understanding of the user session. Refer to the Support for Multiple Detail Record Types section for more information.
The major components include:

- **Service Steering**: Directs subscriber traffic into the ECS subsystem. Service Steering is used to direct selective subscriber traffic flows via an Access Control List (ACL). It is used for other redirection applications as well for both internal and external services and servers.

- **Protocol Analyzer**: The software stack responsible for analyzing the individual protocol fields and states during packet inspection. It performs two types of packet inspection:
  - **Shallow Packet Inspection**: inspection of the layer 3 (IP header) and layer 4 (e.g. UDP or TCP header) information.
  - **Deep Packet Inspection**: inspection of layer 7 and 7+ information. Deep packet inspection functionality includes:
    - Detection of URI (Uniform Resource Identifier) information at level 7 (e.g., HTTP, WTP, RTSP Uniform Resource Locators (URLs)).
    - Identification of true destination in the case of terminating proxies, where shallow packet inspection would only reveal the destination IP address / port number of a terminating proxy.
    - De-encapsulation of upper layer protocol headers, such as MMS-over-WTP, WSP-over-UDP, and IP-over GPRS.
    - Verification that traffic actually conforms to the protocol the layer 4 port number suggests.

- **Rule Definitions**: User-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true. Expressions may contain a number of operator types (string, =, >, etc.) based on the data type of the operand. Each Ruledef configuration is consisting of multiple expressions applicable to any of the fields or states supported by the respective analyzers.

- **Rule Bases**: a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. It is possible to define a rule definition with different actions.

**Mediation and Charging Methods**

To provide maximum flexibility when integrating with billing mediation systems, ECS supports a full range of charging and authorization interfaces.

- **Pre-paid**: In a pre-paid environment, the subscribers pay for service prior to use. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or call ends. The pre-paid accounting server is responsible for authorizing network nodes (GGSNs) to grant access to the user, as well as grant quotas for either time connected or volume used. It is up to the network node to track the quota use, and when these use quotas run low, the network node sends a request to the pre-paid server for more quota.

  If the user has not used up the purchased credit, the server grants quota and if no credit is available to the subscriber the call will be disconnected. ECS and DCCA manage this functionality by providing the ability to setup quotas for different services.

  Pre-paid quota in ECS is implemented using DIAMETER Credit Control Application (DCCA). DCCA supports the implementation of real-time credit control for a variety of services, such as networks access, messaging services, and download services.

  In addition to being a general solution for real-time cost and credit control, DCCA includes these features:
    - **Real-time Rate Service Information** - DCCA can verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
    - **Support for Multiple Services** - DCCA supports the usage of multiple services within one subscriber session. Multiple Service support includes; 1) ability to identify and process the service or group of services that are subject to different cost structures 2) independent credit control of multiple services in a single credit control sub-session.
Sae Gateway Overview

P-GW Features and Functionality - Base Software

Refer to the Diameter Credit Control Application section for more information.

- **Post-paid**: In a post-paid environment, the subscribers pay after use of the service. A AAA server is responsible for authorizing network nodes (GGSNs) to grant access to the user and a CDR system generates G-CDRs/eG-CDRs/EDRs/UDRs or Comma Separated Values (CSVs) for billing information on pre-defined intervals of volume or per time.

**Important**: Support for the Enhanced Charging Service requires a service license; the ECS license is included in the P-GW session use license. For more information on ECS, refer to the Enhanced Charging Service Administration Guide.

### Content Analysis Support

The Enhanced Charging Service is capable of performing content analysis on packets of many different protocols at different layers of the OSI model.

The ECS content analyzers are able to inspect and maintain state across various protocols at all layers of the OSI stack. ECS system supports, inspects, and analyzes the following protocols:

- IP
- TCP
- UDP
- DNS
- FTP
- TFTP
- SMTP
- POP3
- HTTP
- ICMP
- WAP: WTP and WSP
- Real-Time Streaming: RTP and RTSP
- MMS
- SIP and SDP
- **File analysis**: examination of downloaded file characteristics (e.g. file size, chunks transferred, etc.) from file transfer protocols such as HTTP and FTP.

Traffic analyzers in enhanced charging subsystem are based on configured rules. Rules used for Traffic analysis analyze packet flows and form usage records. Usage records are created per content type and forwarded to a pre-paid server or to a mediation/billing system. A traffic analyzer performs shallow (Layer 3 and Layer 4) and deep (above Layer 4) packet inspection of the IP packet flows.

The Traffic Analyzer function is able to do a shallow (layer 3 and layer 4) and deep (above layer 4) packet inspection of IP Packet Flows.

It is able to correlate all layer 3 packets (and bytes) with higher layer trigger criteria (e.g. URL detected in a HTTP header) and it is also perform stateful packet inspection to complex protocols like FTP, RTSP, SIP that dynamically open ports for the data path and by this way, user plane payload is differentiated into “categories”.

SAE-GW Administration Guide, StarOS Release 17
The Traffic Analyzer works on the application level as well and performs event based charging without the interference of the service platforms.

**Important:** This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the Enhanced Charging Service Administration Guide.

### Content Service Steering

Content Service Steering (CSS) directs selective subscriber traffic into the ECS subsystem (In-line services internal to the system) based on the content of the data presented by mobile subscribers.

CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of “rules” (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and applies to a subscriber through either a subscriber profile or an APN profile in the destination context.

**Important:** For more information on CSS, refer to the Content Service Steering chapter of the System Administration Guide.

**Important:** For more information on ACLs, refer to the IP Access Control Lists chapter of the System Administration Guide.

### Support for Multiple Detail Record Types

To meet the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the Enhanced Charging Service (ECS) provides the following type of usage records:

- **Event Detail Records (EDRs)**
- **Usage Detail Records (UDRs)**

ECS provides for the generation of charging data files, which can be periodically retrieved from the system and used as input to a billing mediation system for post-processing. These files are provided in a standard format, so that the impact on the existing billing/mediation system is minimal and at the same time, these records contain all the information required for billing based on the content.

GTPP accounting in ECS allows the collection of counters for different types of data traffic into detail records. The following types of detail records are supported:

- **Event Detail Records (EDRs):** An alternative to standard G-CDRs when the information provided by the G-CDRs is not sufficient to do the content billing. EDRs are generated according to explicit action statements in rule commands that are user-configurable. The EDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.

- **User Detail Records (UDRs):** Contain accounting information related to a specific mobile subscriber. The fields to be reported in them are user-configurable and are generated on any trigger of time threshold, volume threshold, handoffs, and call termination. The UDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.
Important: This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the Enhanced Charging Service Administration Guide.

Diameter Credit Control Application

Provides a pre-paid billing mechanism for real-time cost and credit control based on the following standards:

- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005

The Diameter Credit Control Application (DCCA) is used to implement real-time credit-control for a variety of end user services such as network access, Session Initiation Protocol (SIP) services, messaging services, download services etc.

Used in conjunction with ECS, the DCCA interface uses a mechanism to allow the user to be informed of the charges to be levied for a requested service. In addition, there are services such as gaming and advertising that may credit as well as debit from a user account.

DCCA also supports the following:

- **Real-time Rate Service Information**: The ability to verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services**: The usage of multiple services within one subscriber session is supported. Multiple Service support includes:
  - The ability to identify and process the service or group of services that are subject to different cost structures.
  - Independent credit control of multiple services in a single credit control sub-session.

Important: This functionality is available for use with the Enhanced Charging Service, which requires a session-use license. For more information on ECS, refer to the Enhanced Charging Service Administration Guide.

Accept TCP Connections from DCCA Server

This feature allows for peer Diameter Credit Control Application servers to initiate a connection the NGME.

This feature allows peer diameter nodes to connect to the NGME on TCP port 3868 when the diameter server is incapable of receiving diameter incoming diameter requests.

Important: For more information on Diameter support, if you are using StarOS 12.3 or an earlier release, refer to the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

Gy Interface Support

The Gy interface enables the wireless operator to implement a standardized interface for real-time content based charging with differentiated rates for time based and volume based charging.

As it is based on a quota mechanism, the Gy interface enables the wireless operator to spare expensive Prepaid System resources.
As it enables time-, volume-, and event-based charging models, the Gy interface flexibly enables the operator to implement charging models tailored to their service strategies.

The Gy interface provides a standardized Diameter interface for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation.

It provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an “online” or “prepaid” style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

Gy is a Diameter interface. As such, it is implemented atop, and inherits features from, the Diameter Base Protocol. The system supports the applicable Base network and application features, including directly connected, relayed or proxied DCCA servers using TLS or plaintext TCP.

In the simplest possible installation, the system exchanges Gy Diameter messages over Diameter TCP links between itself and one “prepay” server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

The Cisco implementation is based on the following standards:

- RFC 4006 generic DCCA, including:
  - CCR Initial, Update, and Final signaling
  - ASR and RAR asynchronous DCCA server messages
  - Time, Total-Octets, and Service-Specific-Units quota management
  - Multiple independent quotas using Multiple-Services-Credit-Control
  - Rating-Group for quota-to-traffic association
  - CC-Failure-Handling and CC-Session-Failover features
  - Final-Unit-Action TERMINATE behavior
  - Tariff-Time-Change feature.
- 3GPP TS 32.299 online mode “Gy” DCCA, including:
  - Final-Unit-Action REDIRECT behavior
  - Quota-Holding-Time: This defines a user traffic idle time, on a per-category basis, after which the usage is returned and no new quota is explicitly requested
  - Quota-Thresholds: These AVPs define a low value watermark at which new quota will be sought before the quota is entirely gone; the intent is to limit interruption of user traffic. These AVPs exist for all quota flavors, for example “Time-Quota-Threshold”.
  - Trigger-Type: This AVP defines a set of events which will induce a re-authentication of the current session and its quota categories.

Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the P-GW authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet.
Framed-Route attribute also specifies the subnet routing information to be installed in the P-GW for the “mobile router.” If the P-GW receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session. For more information, see Routing Behind the Mobile Station on an APN chapter.

Gn/Gp Handoff Support

Integrated support of this feature requires that a valid session use license key be installed for both P-GW and GGSN. Contact your local Sales or Support representative for information on how to obtain a license.

In LTE deployments, smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. P-GW supports handovers as user equipment (UE) moves across different access technologies. Cisco’s P-GW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs, which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. These Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and P-GW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the P-GW works as an IP anchor for the EPC.

Important: To support the seamless handover of a session between GGSN and P-GW, the two independent services must be co-located on the same node and configured within the same context for optimum interoperation.

Important: For more information on Gn/GP handoffs, refer to Gn/Gp GGSN/SGSN (GERAN/UTRAN) in the Supported Logical Network Interfaces (Reference Points) section in this chapter.

IMS Emergency Bearer Handling

With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Signaling either happens on the default emergency bearer, or signaling and RTP media flow over separate dedicated emergency bearers. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions). Receiving emergency services in limited service state does not require a subscription.

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only
MSI required, authentication optional

All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.

- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

**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, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

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

**Important:** For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the System Administration Guide.

**IP Address Hold Timers**

Also known as address quarantining, this subscriber-level CLI introduces an address hold timer to temporarily buffer a previously assigned IP address from an IP address pool to prevent it from being recycled and reassigned to a new subscriber session. It is especially useful during inter-RAT handovers that sometimes lead to temporary loss of the mobile data session.

This feature provides a higher quality user experience for location-based services where the remote host server needs to reach the mobile device.

**Important:** Currently, the P-GW only supports an address hold timer with IPv4 addresses.

**IPv6 Capabilities**

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

The P-GW offers the following IPv6 capabilities:
Native IPv6 and IPv6 transport
- Support for any combination of IPv4, IPv6 or dual stack IPv4/IPv6 address assignment from dynamic or static address pools on the P-GW.
- Support for native IPv6 transport and service addresses on PMIPv6 S2a interface. Note that transport on GTP S5/S8 connections in this release is IPv4 based.
- Support for IPv6 transport for outbound traffic over the SGi reference interface to external Packet Data Networks.

IPv6 Connections to Attached Elements
IPv6 transport and interfaces are supported on all of the following connections:
- Diameter Gx policy signaling interface
- Diameter Gy online charging reference interface
- S6b authentication interface to external 3GPP AAA server
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

Routing and Miscellaneous Features
- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (e.g. ECS)

Local Break-Out
Provides a standards-based procedure to enable LTE operators to generate additional revenues by accepting traffic from visited subscribers based on roaming agreements with other mobile operators.

Local Breakout is a policy-based forwarding function that plays an important role in inter-provider roaming between LTE service provider networks. Local Breakout is determined by the SLAs for handling roaming calls between visited and home networks. In some cases, it is more beneficial to locally breakout a roaming call on a foreign network to the visited P-W rather than incur the additional transport costs to backhaul the traffic to the Home network.

If two mobile operators have roaming agreement in place, Local Break-Out enables the visited user to attach to the V-PLMN network and be anchored by the local P-GW in the visited network. The roaming architecture relies on the HSS in the home network and also introduces the concept of the S9 policy signaling interface between the H-PCRF in the H-PLMN and the V-PCRF in the V-PLMN. When the user attaches to the EUTRAN cell and MME (Mobility Management Entity) in the visited network, the requested APN name in the S6a NAS signaling is used by the HSS in the H-PLMN to select the local S-GW (Serving Gateway) and P-GWs in the visited EPC network.

Management System Overview
The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (EMS) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems - giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.
Cisco's O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

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

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.
**Important:** P-GW management functionality is enabled by default for console-based access.

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

**MPLS EXP Marking of User Plane Traffic**

Similar to 802.1p marking, MPLS EXP bit marking is supported for Enterprise APN’s that use MPLS tunneling on the SGi interface on the P-GW. The QoS marking used in the LTE/EPC network (QCI per EPS bearer) is mapped to the 802.1p and MPLS EXP bit marking between the P-GW and L2/EPC switch and MPLS/PE routers (this is applicable to the upstream direction, from the P-GW to the Network). MPLS EXP marking related configuration is available as part of the QCI-QOS configuration table. MPLS EXP marking is selected based on QCI of the bearer to which that packet belongs.

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

Mobile IP registration revocation functionality provides the following benefits:

- Timely release of Mobile IP resources at the HSGW and/or P-GW
- Accurate accounting
- Timely notification to mobile node of change in service

Registration Revocation is a general mechanism whereby either the P-GW or the HSGW providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HSGW by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of HSGW sessions (sessions that could not be recovered)

**Important:** Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the P-GW can initiate the revocation for Proxy-MIP calls.

MTU Size PCO

UEs usually use a hardcoded MTU size for IP communication. If this hardcoded value is not in sync with the network supported value, it can lead to unnecessary fragmentation of packets sent by the UE. Thus, in order to avoid unnecessary fragmentation, this feature helps in using the network-provided MTU size instead of the hardcoded MTU in UE.

3GPP defined a new PCO option in Release 10 specifications for the network to be able to provide an IPv4 MTU size to the UE. P-GW supports an option to configure a IPv4 Link MTU size in the APN profile.

If the UE requests IPv4 Link MTU size in the PCO options during Initial Attach or PDN connectivity request, the P-GW will provide the preconfigured value based on the APN.

If the MTU size configuration on APN is changed, the new MTU size will take effect only for new PDN connections and initial attaches. P-GW will not update for the existing PDN connections.

If UE does not request IPv4 Link MTU size, P-GW will not include the IPv4 Link MTU size.

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 off-deck content services.

The 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 tunnel for all user sessions toward the 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 & dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.
Important: Up to 11 multiple PDN connections are supported.

Node Functionality GTP Echo

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

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

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

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

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

Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover

This feature enables a seamless inter-technology roaming capability in support of dual mode e-HRPD/e-UTRAN access terminals.

The non-optimized inter-technology mobility procedure is rooted at the P-GW as the mobility anchor point for supporting handovers for dual radio technology e-HRPD/E-UTRAN access terminals. To support this type of call handover, the P-GW supports handoffs between the GTP-based S5/S8 (GTPv2-C / GTPv1-U) and PMIPv6 S2a tunneled connections. It also provisions IPv4, IPv6, or dual stack IPv4/IPv6 PDN connections from a common address pool and preserves IP addresses assigned to the UE during inter-technology handover. In the current release, the native LTE (GTP-based) P-GW service address is IPv4-based, while the e-HRPD (PMIP) address is an IPv6 service address.

During the initial network attachment for each APN that the UE connects to, the HSS returns the FQDN of the P-GW for the APN. The MME uses DNS to resolve the P-GW address. When the PDN connection is established in the P-GW, the P-GW updates the HSS with the IP address of the P-GW on PDN establishment through the S6b authentication process. When the mobile user roams to the e-HRPD network, the HSS returns the IP address of the P-GW in the P-GW Identifier through the STa interface and the call ends up in the same P-GW. The P-GW is also responsible for initiating the session termination on the serving access connection after the call handover to the target network.

During the handover procedure, all dedicated EPS bearers must be re-established. On LTE handovers to a target e-HRPD access network, the dedicated bearers are initiated by the mobile access terminal. In contrast, on handovers in the opposite direction from e-HRPD to LTE access networks, the dedicated bearers are network initiated through Gx policy interactions with the PCRF server.

Finally, in order to support the inter-technology handovers, the P-GW uses common interfaces and Diameter endpoint addresses for the various reference points:

- S6b: Non-3GPP authentication
- Gx: QoS Policy and Charging
- Rf: Offline Charging
All three types of sessions are maintained during call handovers. The bearer binding will be performed by the HSGW during e-HRPD access and by the P-GW during LTE access. Thus, the Bearer Binding Event Reporting (BBERF) function needs to migrate between the P-GW and the HSGW during the handover. The HSGW establishes a Gxa session during e-HRPD access for bearer binding and releases the session during LTE access. The HSGW also maintains a limited context during the e-HRPD <>LTE handover to reduce latency in the event of a quick handover from the LTE RAN back to the e-HRPD network.

**Important:** For more information on handoff interfaces, refer to the Supported Logical Network Interfaces (Reference Points) section in this chapter.

### Online/Offline Charging

The Cisco EPC platform offers support for online and offline charging interactions with external OCS and CGF/CDF servers.

#### Online Charging

**Gy/Ro Reference Interfaces**


Online charging is a process whereby charging information for network resource usage must be obtained by the network in order for resource usage to occur. This authorization is granted by the Online Charging System (OCS) upon request from the network. The P-GW uses a charging characteristics profile to determine whether to activate or deactivate online charging. Establishment, modification or termination of EPS bearers is generally used as the event trigger on the PCRF to activate online charging PCC rules on the P-GW.

When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource usage authorization that may be limited in its scope (e.g. volume of data or duration based). The OCS assigns quotas for rating groups and instructs the P-GW whether to continue or terminate service data flows or IP CAN bearers.

The following Online Charging models and functions are supported:

- Time based charging
- Volume based charging
- Volume and time based charging
- Final Unit Indication and termination or redirection of service data flows when quota is consumed
- Reauthorization triggers to rearm quotas for one or more rating groups using multi-service credit control (MSCC) instances
- Event based charging
- Billing cycle bandwidth rate limiting: Charging policy is enforced through interactions between the PDN GW and Online Charging Server. The charging enforcement point periodically conveys accounting information for subscriber sessions to the OCS and it is debited against the threshold that is established for the charging policy. Subscribers can be assigned a max usage for their tier (gold, silver, bronze for example), the usage can be tracked over a month, week, day, or peak time within a day. When the subscriber exceeds the usage limit, bandwidth is either restricted for a specific time period, or dropped depending on their tier of service.
- Fair usage controls
Offline Charging

**Ga/Gz Reference Interfaces**

The Cisco P-GW supports 3GPP-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 pre-release 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 and P-GWs support integrated Charging Transfer Functions (CTF) and Charging Data Functions (CDF). Each gateway uses Charging-ID's to distinguish between default and dedicated bearers within subscriber sessions. The Ga/Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP/S-FTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to FTP/S-FTP charging records between the CDF and CGF server. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc. The ASR 5x00 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it also possible to enable file compression using protocols such as GZIP. The Offline Charging implementation offers built-in heartbeat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighbor CGF within the configurable polling interval, they will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct OCS servers (See Online Charging description above).

**Rf Reference Interface**

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

**P-CSCF Recovery**

Supports spec-based mechanism to support P-CSCF discovery for GTP-based S2b interface for WiFi integration. This is needed for Voice over WiFi service.

The P-GW can store the P-CSCF FQDN received during the initial registration with the AAA. Upon receiving the P-CSCF restoration flag from the MME/S-GW, the P-GW performs a new DNS query using the existing P-CSCF FQDN to provide the updated list of three P-CSCF IP addresses using PCO.

**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 P-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 P-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.

**PMIPv6 Heartbeat**

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The core functional entities Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) set up tunnels dynamically to manage mobility for a mobile node.

Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

PMIP heartbeats from the HSGW to the P-GW are supported per RFC 5847. Refer to the `heartbeat` command in the LMA Service mode or MAG Service mode respectively to enable this heartbeat and configure the heartbeat variables.

**Proxy Mobile IPv6 (S2a)**

Provides a mobility management protocol to enable a single LTE-EPC core network to provide the call anchor point for user sessions as the subscriber roams between native EUTRAN and non-native e-HRPD access networks.

S2a represents the trusted non-3GPP interface between the LTE-EPC core network and the evolved HRPD network anchored on the HSGW. In the e-HRPD network, network-based mobility provides mobility for IPv6 nodes without host involvement. Proxy Mobile IPv6 extends Mobile IPv6 signaling messages and reuses the HA function (now known as LMA) on the P-GW. This approach does not require the mobile node to be involved in the exchange of signaling messages between itself and the Home Agent. A proxy mobility agent (e.g. MAG function on HSGW) in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network.

The S2a interface uses IPv6 for both control and data. During the PDN connection establishment procedures the P-GW allocates the IPv6 Home Network Prefix (HNP) via Proxy Mobile IPv6 signaling to the HSGW. The HSGW returns the HNP in router advertisement or based on a router solicitation request from the UE. PDN connection release events can be triggered by either the UE, the HSGW or the P-GW.

In Proxy Mobile IPv6 applications the HSGW (MAG function) and P-GW (LMA function) maintain a single shared tunnel and separate GRE keys are allocated in the PMIP Binding Update and Acknowledgement messages to distinguish between individual subscriber sessions. If the Proxy Mobile IP signaling contains Protocol Configuration Options (PCOs) it can also be used to transfer P-CSCF or DNS server addresses.

**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 PDN 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 (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). The Cisco EPC gateways also support the ability to map the QCI values to DiffServ code points in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.

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

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

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

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

**Policing:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (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.
The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority**: Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.

- **Routing Algorithm**: Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in the following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named “default”. This default server group is available to all subscribers in that context through the realm (domain) without any configuration.

- It provides a facility to create “user defined” RADIUS server groups, as many as 399 (excluding “default” server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator’s network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the P-GW supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.

**Important**: For more information on RADIUS AAA configuration, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

**S-GW Restoration Support**

S-GW Restoration helps in handling the S-GW failure in the EPC network in a graceful manner. It allows affected PDNs due to S-GW failure to be restored by selecting another S-GW to serve the affected PDNs, thus avoiding unnecessary flooding of signaling for PDN cleanup.
S-GW Restoration is based on 3GPP Release 11. It requires enhancements at P-GW for maintaining the sessions in case path failure is detected or when S-GW restart is detected via recovery IE on GTP-C signaling. P-GW shall ensure that any dropped packets in this scenario are not charged and P-GW shall reject any bearer addition/modification request received for the PDN connection maintained after the S-GW failure detection, till the time that PDN is restored again.

**Important:** If the S-GW Restoration feature is configured and enabled for a PGW that is associated with an SAEGW service, the feature supports Pure-P calls only.

Once the session has been restored by the MME (i.e., P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW), P-GW shall resume forwarding any received downlink data and start charging them.

When subscriber is in S-GW restoration phase, all RARs (except for Session Termination) will be rejected by PCEF. P-GW will reject all internal updates which can trigger CCR-U towards PCRF. P-GW shall trigger a CCR U with AN-GW-Change for the PDNs that are restored if the S-GW has changed on restoration.

**Important:** Only MME/S4-SGSN triggered S-GW restoration procedure will be supported. S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

MME/S4-SGSN is locally configured to know that P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at P-GW, it shall support it for all S-GWs/MMEs.

For more details on this feature, refer to the *S-GW Restoration Support* chapter in this guide.

**Source IP Address Validation**

Insures integrity between the attached subscriber terminal and the PDN GW by mitigating the potential for unwanted spoofing or man-in-the-middle attacks.

The P-GW includes local IPv4/IPv6 address pools for assigning IP addresses to UEs on a per-PDN basis. The P-GW defends its provisioned address bindings by insuring that traffic is received from the host address that it has awareness of. In the event that traffic is received from a non-authorized host, the P-GW includes the ability to block the non-authorized traffic. The P-GW uses the IPv4 source address to verify the sender and the IPv6 source prefix in the case of IPv6.

**SRVCC PS-to-CS Handover Indication Support**

This feature helps in notifying the PCRF about the exact reason for PCC rule deactivation on Voice bearer deletion. This exact cause will help PCRF to then take further action appropriately.

This feature ensures complete compliance for SRVCC, including support for PS-to-CS handover indication when voice bearers are released. The support for SRVCC feature was first added in StarOS Release 12.2.

SRVCC service for LTE comes into the picture when a single radio User Equipment (UE) accessing IMS-anchored voice call services switches from the LTE network to the Circuit Switched domain while it is able to transmit or receive on only one of these access networks at a given time. This removes the need for a UE to have multiple Radio Access Technology (RAT) capability.

After handing over the PS sessions to the target, the source MME shall remove the voice bearers by deactivating the voice bearer(s) towards S-GW/P-GW and setting the VB (Voice Bearer) flag of Bearer Flags IE in the Delete Bearer Command message (TS 29.274 v9.5.0).
If the IP-CAN bearer termination is caused by the PS to CS handover, the PCEF may report related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER (TS 29.212 v10.2.0 and TS 23.203 v10.3.0).

Support for new AVP PS-to-CS-Session-Continuity (added in 3GPP Release 11) inside Charging Rule Install, which indicates if the bearer is selected for PS to CS continuity, is not added.

**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 P-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S5/S8, S2a, SGi, and Gx. The trace can be initiated using multiple methods:

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

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

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the 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 a 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:

- S5/S8: Create Session Request
- S5/S8: Modify Bearer Request
- S5/S8: Trace Session Activation (New message defined in TS 32.422)

**Performance Goals:** As subscriber level trace is a CPU intensive activity the max number of concurrently monitored trace sessions per Cisco P-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

3GPP tracing was enhanced in StarOS Release 15.0 to increase the number of simultaneous traces to 1000. The generated trace files are forwarded to external trace collection entity at regular intervals through (S)FTP if “push” mode is enabled. If the push mode is not used, the files are stored on the local hard drive and must be pulled off by the TCE using FTP or SFTP.
The number of session trace files generated would be limited by the total available hard disk capacity.

3GPP Tracing to Intercept Random Subscriber

Previously, a subscriber identifier like IMSI was required in order to enable trace. Sometimes operators want to enable a trace without knowing the subscriber ID. For example, an operator may want to monitor the next “n” number of calls, or monitor subscribers in a particular IMSI range.

3GPP tracing was enhanced in StarOS Release 15.0 to intercept random subscribers with this feature. The current session trace feature is either signaling or management based, which is very specific to a particular subscriber. The requirement is to trace random subscribers which are not explicitly linked or identified by IMSI in GTP messages or configured through CLI.

The random subscribers could be in an IMSI range, context activation in particular time intervals, etc.

The session trace is activated on demand for a limited period of time for specific analysis purposes. The maximum limit would restrict the number of random subscriber tracing. Random session trace will be given priority over signalling and management-based session trace.

Threshold Crossing Alerts (TCA) Support

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

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

The following thresholding models are supported by the system:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

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

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

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. 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 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*.

**UE Time Zone Reporting**

This feature enables time-based charging for specialized service tariffs, such as super off-peak billing plans. Time Zone of the UE is associated with UE location (Tracking Area/Routing Area). The UE Time Zone Information Element is an attribute the MME tracks on a Tracking Area List basis and propagates over S11 and S5/S8 signalling to the P-GW. Time zone reporting can be included in billing records or conveyed in Gx/Gy signaling to external PCRF and OCS servers.

**Virtual APN Support**

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNS. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address
P-GW Features and Functionality - Inline Service Support

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

**Important:** The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

This section describes the following features:

- Content Filtering
- Header Enrichment: Header Insertion and Encryption
- Mobile Video Gateway
- Network Address Translation (NAT)
- Peer-to-Peer Detection
- Personal Stateful Firewall

### Content Filtering

The Cisco P-GW offers two variants of network-controlled content filtering / parental control services. Each approach leverages the native DPI capabilities of the platform to detect and filter events of interest from mobile subscribers based on HTTP URL or WAP/MMS URI requests:

- **Integrated Content Filtering:** A turnkey solution featuring a policy enforcement point and category-based rating database on the Cisco P-GW. An offboard AAA or PCRF provides the per-subscriber content filtering information as subscriber sessions are established. The content filtering service uses DPI to extract URLs or URIs in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.

- **Content Filtering ICAP Interface:** This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5x00 platform to extract events of interest. However in this case, the extracted requests are transferred via the Integrated Content Adaptation Protocol (ICAP) with subscriber identification information to the external ACF server which provides the category rating database and content decision functions.

### Integrated Adult Content Filter

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The integrated solution enables a single policy decision and enforcement point thereby streamlining the number of signaling interactions with external AAA/Policy Manager servers. When used in parallel with other services such as Enhanced Content Charging (ECS) it increases billing accuracy of charging records by insuring that mobile subscribers are only charged for visited sites they are allowed to access.

The Integrated Adult Content Filter is a subscriber-aware inline service provisioned on an ASR 5x00 running P-GW services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active P-GW sessions on the system.
Content Filtering policy enforcement is the process of deciding if a subscriber should be able to receive some content. Typical options are to allow, block, or replace/redirect the content based on the rating of the content and the policy defined for that content and subscriber. The policy definition is transferred in an authentication response from a AAA server or Diameter policy message via the Gx reference interface from an adjunct PCRF. The policy is applied to subscribers through rulebase or APN/Subscriber configuration. The policy determines the action to be taken on the content request on the basis of its category. A maximum of one policy can be associated with a rulebase.

ICAP Interface

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The Content Filtering ICAP solution is appropriate for operators with existing installations of Active Content Filtering servers in their networks.

The Enhanced Charging Service (ECS) for the P-GW provides a streamlined Internet Content Adaptation Protocol (ICAP) interface to leverage the Deep Packet Inspection (DPI) to enable external Application Servers to provide their services without performing the DPI functionality and without being inserted in the data flow. The ICAP interface may be attractive to mobile operators that prefer to use an external Active Content Filtering (ACF) Platform. If a subscriber initiates a WAP (WAP 1.x or WAP 2.0) or Web session, the subsequent GET/POST request is detected by the deep packet inspection function. The URL of the GET/POST request is extracted by the local DPI engine on the ASR 5x00 platform and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the Application Server (AS). The AS checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked or redirected by answering the GET/POST message. Depending upon the response received from the ACF server, the P-GW either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

Header Enrichment: Header Insertion and Encryption

Header enrichment provides a value-added capability for mobile operators to monetize subscriber intelligence to include subscriber-specific information in the HTTP requests to application servers. Extension header fields (x-header) are the fields that can be added to headers of a protocol for a specific purpose. The enriched header allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. Unrecognized fields should be ignored by the recipient and must be forwarded by transparent proxies.

Extension headers can be supported in HTTP/WSP GET and POST request packets. The Enhanced Charging Service (ECS) for the P-GW offers APN-based configuration and rules to insert x-headers in HTTP/WSP GET and POST request packets. The charging action associated with the rules will contain the list of x-headers to be inserted in the packets. Protocols supported are HTTP, WAP 1.0 and WAP 2.0 GET, and POST messages.

Important: For more information on ECS, see the Enhanced Charging Service Administration Guide.

The data passed in the inserted HTTP header attributes is used by end application servers (also known as Upsell Servers) to identify subscribers and session information. These servers provide information customized to that specific subscriber.

The Cisco P-GW can include the following information in the http header:

- User-customizable, arbitrary text string
- Subscriber's MSISDN (the RADIUS calling-station-id, in clear text)
- Subscriber's IMSI
- Subscriber's IP address
- S-GW IP address (in clear text)

X-Header encryption enhances the header enrichment feature by increasing the number of fields that can be supported and through encryption of the fields before inserting them.

The following limitations to insertion of x-header fields in WSP headers apply:

- x-header fields are not inserted in IP fragmented packets before StarOS v14.0.
- In case of concatenated request, x-header fields are only inserted in first GET or POST request (if rule matches for the same). X-header fields are not inserted in the second or later GET/POST requests in the concatenated requests. For example, if there is ACK+GET in packet, x-header is inserted in the GET packet. However, if GET1+GET2 is present in the packet and rule matches for GET2 and not GET1 x-header is still inserted in GET2. In case of GET+POST also, x-header is not inserted in POST.
- In case of CO, x-header fields are not inserted if the WTP packets are received out of order (even after proper reordering).
- If route to MMS is present, x-headers are not inserted.
- x-headers are not inserted in WSP POST packet when header is segmented. This is because POST contains header length field which needs to be modified after addition of x-headers. In segmented WSP headers, header length field may be present in one packet and header may complete in another packet.

Mobile Video Gateway

The Cisco ASR 5x00 chassis provides mobile operators with a flexible solution that functions as a Mobile Video Gateway in 2.5G, 3G, and 4G wireless data networks.

The Cisco Mobile Video Gateway consists of new software for the ASR 5x00. The Mobile Video Gateway is the central component of the Cisco Mobile Videoscape. It employs a number of video optimization techniques that enable mobile operators to enhance the video experience for their subscribers while optimizing the performance of video content transmission through the mobile network.

The Mobile Video Gateway features and functions include:

- DPI (Deep Packet Inspection) to identify subscriber requests for video vs. non-video content
- Transparent video re-addressing to the Cisco CAE (Content Adaptation Engine) for retrieval of optimized video content
- CAE load balancing of HTTP video requests among the CAEs in the server cluster
- Video optimization policy control for tiered subscriber services
- Video white-listing, which excludes certain video clips from video optimization
- Video pacing for “just in time” video downloading
- TCP link monitoring
- Dynamic inline transrating
- Dynamically-enabled TCP proxy
- Traffic performance optimization
- N+1 redundancy support
- SNMP traps and alarms (threshold crossing alerts)
Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One

Important: For more information on NAT, refer to the Network Address Translation Administration Guide.

NAT64 Support

This feature helps facilitate the co-existence and gradual transition to IPv6 addressing scheme in the networks. Use of NAT64 requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises will continue to build and roll out IPv6 networks. However, because of the broad scale IPv4 deployment, it is not practical that the world changes to IPv6 overnight. There is need to protect the IPv4 investment combined with the need to expand and grow the network will force IPv4 and IPv6 networks to co-exist together for a considerable period of time and keep end-user experience seamless.

The preferred approaches are to run dual stacks (both IPv4 and IPv6) on the end hosts, dual stack routing protocols, and dual stack friendly applications. If all of the above is available, then the end hosts will communicate natively using IPv6 or IPv4 (using NAT). Tunneling through the IPv4 or IPv6 is the next preferred method to achieve communication wherever possible. When all these options fail, translation is recommended.

Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice- versa. The system supports a Stateful NAT64 translator based on IETF Behave WG drafts whose framework is described in draft-ietf-behave-v6v4-
Peer-to-Peer Detection

Allows operators to identify P2P traffic in the network and applying appropriate controlling functions to ensure fair distribution of bandwidth to all subscribers.

Peer-to-Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node can function as a client, a server, or both—a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.

Detecting peer-to-peer protocols requires recognizing, in real time, some uniquely identifying characteristic of the protocols. Typical packet classification only requires information uniquely typed in the packet header of packets of the stream(s) running the particular protocol to be identified. In fact, many peer-to-peer protocols can be detected by simple packet header inspection. However, some P2P protocols are different, preventing detection in the traditional manner. This is designed into some P2P protocols to purposely avoid detection. The creators of these protocols purposely do not publish specifications. A small class of P2P protocols is stealthier and more challenging to detect. For some protocols no set of fixed markers can be identified with confidence as unique to the protocol.

Operators care about P2P traffic because of the behavior of some P2P applications (for example, Bittorrent, Skype, and eDonkey). Most P2P applications can hog the network bandwidth such that 20% P2P users can generate as much as traffic generated by the rest 80% non-P2P users. This can result into a situation where non-P2P users may not get enough network bandwidth for their legitimate use because of excess usage of bandwidth by the P2P users. Network operators need to have dynamic network bandwidth/traffic management functions in place to ensure fair distributions of the network bandwidth among all the users. And this would include identifying P2P traffic in the network and applying appropriate controlling functions to the same (for example, content-based premium billing, QoS modifications, and other similar treatments).

Cisco’s P2P detection technology makes use of innovative and highly accurate protocol behavioral detection techniques.

**Important:** For more information on peer-to-peer detection, refer to the Application Detection and Control Administration Guide.

Personal Stateful Firewall

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.

In stateless inspection, the firewall inspects a packet to determine the 5-tuple—source and destination IP addresses and ports, and protocol—information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer/layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state. For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgement numbers of the packets traversing the connection, TCP packet flags, etc. is
maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded.

The Enhanced Charging Service (ECS)/Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the Enhanced Charging Service Administration Guide.

**Important:** For more information on Personal Stateful Firewall, refer to the Personal Stateful Firewall Administration Guide.
S-GW Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the S-GW service.

**Important:** The SAEGW supports all of these features if an S-GW service is assigned to the SAEGW service.

Each of the following features require the purchase of an additional license to implement the functionality with the S-GW service.

This section describes the following features:

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

**Always-On Licensing**

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

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

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

**Direct Tunnel**

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

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

For more information on Direct Tunnel configuration, refer to the Direct Tunnel Configuration 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 provides industry-leading carrier-class redundancy. The system protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

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

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

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

Interchassis Communication

Chassis configured to support ICSR communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. 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
- SPIO 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 Cisco StarOS IP Security (IPSec) Reference.

Lawful Intercept

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

Layer 2 Traffic Management (VLANs)

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

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

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

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-chassis session recovery (ICSR) for S-GW sessions.

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

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

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

Important: For more information on session recovery support, refer to the Session Recovery chapter in the System Administration Guide.
P-GW Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the P-GW service.

**Important:** The SAEGW supports all of these features if a P-GW service is assigned to the SAEGW service.

Each of the following features requires the purchase of an additional license to implement the functionality with the P-GW service.

**Important:** 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*.

This section describes the following features:

- AAA and Prefix Delegation DHCP Correlation
- Always-On Licensing
- Cause IE Enhancement for Delete Bearer Request
- Dynamic RADIUS Extensions (Change of Authorization)
- GRE Protocol Interface Support
- GTP Throttling
- Inter-Chassis Session Recovery
- IP Security (IPSec) Encryption
- L2TP LAC Support
- Lawful Intercept
- Layer 2 Traffic Management (VLANs)
- Local Policy Decision Engine
- MPLS Forwarding with LDP
- NEMO Service Supported
- Network Provided Location Information for IMS
- Session Recovery Support
- Smartphone Tethering Detection Support
- Traffic Policing
- UBR Suppression Feature
- User Location Information Reporting
AAA and Prefix Delegation DHCP Correlation

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Currently at the DHCP server, DHCPv6 does not provide any mechanism to correlate allocated IPv6 (/64) prefix to a particular subscriber. This feature correlates the default prefix allocated from AAA server with the delegated prefix allocated from external DHCPv6 server during the PDN connection setup.

Options are available in DHCP Client Profile Configuration Mode to enable P-GW to send USER_CLASS_OPTION in DHCPv6 messages to external DHCPv6 server during delegated prefix setup.

Always-On Licensing

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

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

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

Cause IE Enhancement for Delete Bearer Request

Use of Cause IE Enhancement for Delete Bearer Request requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The cause value in the Delete Bearer Request previously had been limited. The behavior impacted by this feature is:

- Delete Bearer Request/Delete PDP Context due to idle-timer/session-timer expiration
- Delete Bearer Request due to bearer inactivity of default bearer
- Delete PDP Context due to bearer inactivity of the last PDP context of PDN connection
- Delete Bearer Request/Delete PDP Context triggered by clear subscriber CLI command

Configuration now is available to set cause values and cause inclusion in the following scenarios:

- CLI-based trigger to disconnect
- per APN when P-GW initiated disconnection for above mentioned timer expiry

Important: This feature allows operator to override existing behavior. Such overridden behavior may not be compliant with standards.

Dynamic RADIUS Extensions (Change of Authorization)

Use of Dynamic RADIUS Extensions (CoA and PoD) requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.
Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization**: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.

- **Disconnect Message**: The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.

**GRE Protocol Interface Support**

Use of GRE Interface Tunneling requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW supports GRE generic tunnel interfaces in accordance with RFC 2784, Generic Routing Encapsulation (GRE). The GRE protocol allows mobile users to connect to their enterprise networks through GRE tunnels.

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSec offers, for example).

GRE tunneling consists of three main components:

- **Passenger protocol**: protocol being encapsulated. For example: CLNS, IPv4 and IPv6.

- **Carrier protocol**: protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.

- **Transport protocol**: protocol used to carry the encapsulated protocol. The main transport protocol is IP.
GTP Throttling

Use of GTP and Diameter Interface Throttling requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

This feature will help control the rate of incoming/outgoing messages on P-GW/GGSN. This will help in ensuring P-GW/GGSN doesn’t get overwhelmed by the GTP control plane messages. In addition, it will help in ensuring the P-GW/GGSN will not overwhelm the peer GTP-C peer with GTP Control plane messages.

This feature requires shaping/policing of GTP (v1 and v2) control messages over Gn/Gp and S5/S8 interfaces. Feature will cover overload protection of P-GW/GGSN nodes and other external nodes with which it communicates. Throttling would be done only for session level control messages. Path management messages would not be rate limited at all.

External node overload can happen in a scenario where P-GW/GGSN generates signaling requests at a higher rate than other nodes can handle. If the incoming message rate is higher than the configured message rate, extra messages will get silently dropped. Also the actual call setup rate can be lower than the msg-rate configured, which could be due to delays in setting up the session due to many reasons like slow peer nodes or overloaded sm. Also the drops done as part of this throttling are silent drops, hence if path failure is configured for non-echo messages, path failure can be observed.

For protecting external nodes from getting overloaded from P-GW/GGSN control signaling, a framework will be used to handle shaping/policing of outbound control messages to external interfaces.

Inter-Chassis Session Recovery

Use of Interchassis Session Recovery requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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

The system provides several levels of system redundancy:

- Under normal N+1 PSC/PSC2 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 PSC/PSC2 failure will cause a PSC switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the MME Inter-Chassis Session Recovery 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 reactivation storms.

The Interchassis Session Recovery feature 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 Interchassis Session Recovery 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
- SPIO 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 the *System Administration Guide*.

### IP Security (IPSec) Encryption

Use of Network Domain Security requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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 P-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.

### L2TP LAC Support

Use of L2TP LAC requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name...
and password, and use IPCP to request an address. To support PPP negotiation between the P-GW and the corporation, an L2TP tunnel must be setup in the P-GW running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the P-GW and benefits from dynamic resource allocation and distributed message and data processing.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware or software issues. Tunnel state is preserved by copying the information across processor cards.

Lawful Intercept

The feature use license for Lawful Intercept on the P-GW is included in the P-GW session use license.

The Cisco Lawful Intercept feature is supported on the P-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)

Use of Layer 2 Traffic Management requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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.

Local Policy Decision Engine

Use of the Local Policy Decision Engine requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The Local Policy Engine is an event-driven rules engine that offers Gx-like QoS and policy controls to enable user or application entitlements. As the name suggests, it is designed to provide a subset of a PCRF in cases where an operator elects not to use a PCRF or scenarios where connections to an external PCRF are disrupted. Local policies are used to control different aspects of a session like QoS, data usage, subscription profiles, and server usage by means of locally defined policies. A maximum of 1,024 local policies can be provisioned on a P-GW system.

Local policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Potential uses cases for the Local Policy Decision Engine include:

- Disaster recovery data backup solution in the event of a loss of PCRF in a mobile core network.
- Dedicated bearer establishment for emergency voice calls.
- Network-initiated bearer establishment on LTE to non-3GPP inter-domain handovers.
MPLS Forwarding with LDP

Use of MPLS requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF, and therefore it is not a routing protocol.

MPLS generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR), which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

In order to support the increasing number of corporate APNs, which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least the following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, the MPLS backbone automatically negotiates routes using the labels binded with the IP packets. Cisco P-GW as an LSR learns the default route from the connected provider edge (PE), while the PE populates its routing table with the routes provided by the P-GW.

NEMO Service Supported

Use of NEMO requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW may be configured to enable or disable Network Mobility (NEMO) service.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

NEMO Support in GGSN

Use of Dynamic Network Mobile Routing (NEMO) for GGSN requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

This feature now supports standards-based NEMO feature on GGSN, which allows operators to support Enterprise VPN service with the advantage of faster deployment and flexible bandwidth arrangement for customers.

NEMO (NEtwork MObility) provides wireless connectivity between enterprise core network and remote sites over 3G/4G network. The wireless connection can be used as either primary link or backup link. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Enterprise VPN service is one of the main use case for this feature. Fast deployment and flexible bandwidth arrangement for customers are some of the advantages of this service. Customers include banks, financial institutions, multi-sited enterprises, city public safety departments, transportation fleet, etc.
NEMO support in P-GW was added in earlier StarOS releases. In release 15.0, support was added for GGSN as well so that NEMO can be supported for subscribers roaming out on 3G (UMTS/GERAN) networks.

Network Provided Location Information for IMS

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

This feature enables the P-GW to provide the required access network information to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP as requested by the PCRF. The P-GW will also provide the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

During bearer deactivation or UE detach procedure, the P-GW will provide the access network information to the PCRF within the 3GPP-User-Location-Info AVP and information on when the UE was last known to be in that location within User-Location-Info-Time AVP. If the PCRF requested User location info as part of the Required-Access-Info AVP and it is not available in the P-GW, then the P-GW will provide the serving PLMN identifier within the 3GPP-SGSN-MCC-MNC AVP.

Previously, the P-GW notified ULI/MS-TimeZone/PLMN-ID to ECS/IMSA/PCRF only when their value changed. With this feature, the P-GW receives NetLoc indication in the rules sent by ECS regardless of whether the values changed and it sends this to the ECS/IMSA/PCRF. If the P-GW receives NetLoc as ‘1’, then it will inform MS-Timezone. If the P-GW receives NetLoc as ‘0’, then it will inform ULI and ULI Timestamp. If ULI is not available in that case, then the PLMN-ID is sent. If NetLoc indication is received for an update, then the P-GW will indicate this information to the access side in the UBReq using the RetLoc Indication flag.

This is required for VoLTE and aids in charging and LI functionality in IMS domain. This feature allows EPC core to support an efficient way of reporting ULI and Time-Zone information of the subscriber to the IMS core network.

Session Recovery Support

The feature use license for Session Recovery on the P-GW is included in the P-GW session use license.

Session recovery 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 Release 9.0 adds the ability to support stateful intra-chassis session recovery for P-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 PSC/PSC2 during the upgrade process.

**Important:** For more information on session recovery support, refer to the Session Recovery chapter in the System Administration Guide.
Smartphone Tethering Detection Support

Use of Smartphone Tethering Detection requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

On the P-GW, using the inline heuristic detection mechanism, it is now possible to detect and differentiate between the traffic from the mobile device and a tethered device connected to the mobile device.

Traffic Policing

Use of Per-Subscriber Traffic Policing requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Traffic policing allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers. Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APNs of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR)**: The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR)**: The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- **Burst-size**: The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber’s “bucket”. Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop**: The offending packet is discarded.
- **Transmit**: The offending packet is passed.
- **Lower the IP Precedence**: The packet’s ToS bit is set to “0”, thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet’s ToS bit was already set to “0”, this action is equivalent to “Transmit”.

UBR Suppression Feature

The Update Bearer Request (UBR) Suppression feature is a license controlled feature. Please contact your Cisco account or service representative for more information.

As the bit rate is expressed in bps on Gx and kbps on GTP, the P-GW does a round-off to convert a Gx request into a GTP request. When the P-GW receives RAR from PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in Kbps) is already set for the bearer. The UBR suppression feature enables the P-GW to suppress such a UBR where there is no update for any of the bearer parameters.
A new CLI command, `suppress-ubr no-bitrate-change`, has been added to the P-GW Service Configuration Mode to enable UBR suppression. Once the CLI is configured, P-GW suppresses the UBR if the bit rate is the same after the round-off.

When UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

To summarize, if the license is enabled and the CLI command is configured for UBR suppression, then UBR is suppressed if bit rates in kbps are the same after round-off and all other parameters, such as QCI, ARP, and TFT, that might trigger UBR are also unchanged.

**User Location Information Reporting**

Use of User Location Information (ULI) Reporting requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

ULI Reporting allows the eNodeB to report the location of a UE to the MME, when requested by a P-GW.

The following procedures are used over the S1-MME interface to initiate and stop location reporting between the MME and eNodeB:

- **Location Reporting Control**: The purpose of Location Reporting Control procedure is to allow the MME to request that the eNodeB report where the UE is currently located. This procedure uses UE-associated signaling.

- **Location Report Failure Indication**: The Location Report Failure Indication procedure is initiated by an eNodeB in order to inform the MME that a Location Reporting Control procedure has failed. This procedure uses UE-associated signaling.

- **Location Report**: The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signaling.

The start/stop trigger for location reporting for a UE is reported to the MME by the S-GW over the S11 interface. The Change Reporting Action (CRA) Information Element (IE) is used for this purpose. The MME updates the location to the S-GW using the User Location Information (ULI) IE.

The following S11 messages are used to transfer CRA and ULI information between the MME and S-GW:

- **Create Session Request**: The ULI IE is included for E-UTRAN Initial Attach and UE-requested PDN Connectivity procedures. It includes ECGI and TAI. The MME includes the ULI IE for TAU/ X2-Handover procedure if the P-GW has requested location information change reporting and the MME support location information change reporting. The S-GW includes the ULI IE on S5/S8 exchanges if it receives the ULI from the MME. If the MME supports change reporting, it sets the corresponding indication flag in the Create Session Request message.

- **Create Session Response**: The CRA IE in the Create Session Response message can be populated by the S-GW to indicate the type of reporting required.

- **Create Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.

- **Modify Bearer Request**: The MME includes the ULI IE for TAU/Handover procedures and UE-initiated Service Request procedures if the P-GW has requested location information change reporting and the MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.

- **Modify Bearer Response**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Delete Session Request**: The MME includes the ULI IE for the Detach procedure if the P-GW has requested location information change reporting and MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.

- **Update Bearer Request**: The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.

- **Change Notification Request**: If no existing procedure is running for a UE, a Change Notification Request is sent upon receipt of an S1-AP location report message. If an existing procedure is running, one of the following messages reports the ULI:
  - Create Session Request
  - Create Bearer Response
  - Modify Bearer Request
  - Update Bearer Response
  - Delete Bearer Response
  - Delete Session Request

If an existing Change Notification Request is pending, it is aborted and a new one is sent.

---

**Important**: Information on configuring User Location Information (ULI) Reporting support is located in the Configuring Optional Features on the MME section of the Mobility Management Entity Configuration chapter in the Mobility Management Entity Administration Guide.
How the Serving Gateway Works

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

The S-GW supports the following network flows:

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

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

The following topics and procedure flows are included:

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

 Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.
### Figure 14. Subscriber-initiated Attach (initial) Call Flow

#### Table 3. Subscriber-initiated Attach (initial) Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2</td>
<td>The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an MME selection function. The eNodeB forwards the Attach Request message to the new MME contained in a SI-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.</td>
</tr>
<tr>
<td>3</td>
<td>If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.</td>
</tr>
<tr>
<td>4</td>
<td>The UE responds with Identity Response (IMSI).</td>
</tr>
<tr>
<td>5</td>
<td>If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.</td>
</tr>
<tr>
<td>6</td>
<td>The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.</td>
</tr>
<tr>
<td>7</td>
<td>The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the EPS subscribed QoS profile for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.</td>
</tr>
<tr>
<td>8</td>
<td>The MME selects an S-GW using the Serving GW selection function and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause PDN GW selection function. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.</td>
</tr>
<tr>
<td>9</td>
<td>The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.</td>
</tr>
<tr>
<td>10</td>
<td>If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.</td>
</tr>
<tr>
<td>11</td>
<td>The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.</td>
</tr>
<tr>
<td>12</td>
<td>The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.</td>
</tr>
<tr>
<td>13</td>
<td>The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.</td>
</tr>
<tr>
<td>14</td>
<td>The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.</td>
</tr>
<tr>
<td>15</td>
<td>The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.</td>
</tr>
</tbody>
</table>
How the Serving Gateway Works

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 tunnelled 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>
<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>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</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 signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.</td>
</tr>
</tbody>
</table>
How the PDN Gateway Works

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

The P-GW supports the following network flows:

- PMIPv6 PDN Gateway CallSession Procedures in an eHRPD Network
- GTP PDN Gateway CallSession Procedures in an LTE-SAENetwork

PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network

The following topics and procedure flows are included:

- Initial Attach with IPv6IPv4 Access
- PMIPv6 Lifetime Extension without Handover
- PDN Connection Release Initiated by UE
- PDN Connection Release Initiated by HSGW
- PDN Connection Release Initiated by P-GW

Initial Attach with IPv6/IPv4 Access

This section describes the procedure of initial attach and session establishment for a subscriber (UE).
Table 5. Initial Attach with IPv6/IPv4 Access Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The subscriber (UE) attaches to the eHRPD network.</td>
</tr>
<tr>
<td>2a</td>
<td>The eAN/PCF sends an A11 RRQ to the HSGW. The eAN/PCF includes the true IMSI of the UE in the A11 RRQ.</td>
</tr>
<tr>
<td>2b</td>
<td>The HSGW establishes A10s and respond back to the eAN/PCF with an A11 RRP.</td>
</tr>
<tr>
<td>3a</td>
<td>The UE performs LCP negotiation with the HSGW over the established main A10.</td>
</tr>
</tbody>
</table>
### How the PDN Gateway Works

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3b</td>
<td>The UE performs EAP over PPP.</td>
</tr>
<tr>
<td>3c</td>
<td>EAP authentication is completed between the UE and the 3GPP AAA. During this transaction, the HSGW receives the subscriber profile from the AAA server.</td>
</tr>
<tr>
<td>4a</td>
<td>After receiving the subscriber profile, the HSGW sends the QoS profile in A11 Session Update Message to the eAN/PCF.</td>
</tr>
<tr>
<td>4b</td>
<td>The eAN/PCF responds with an A11 Session Update Acknowledgement (SUA).</td>
</tr>
<tr>
<td>5a</td>
<td>The UE initiates a PDN connection by sending a PPP-VSNCP-Conf-Req message to the HSGW. The message includes the PDNID of the PDN, APN, PDN-Type=IPv6/[IPv4], PDSN-Address and, optionally, PCO options the UE is expecting from the network.</td>
</tr>
<tr>
<td>5b</td>
<td>The HSGW sends a PBU to the P-GW.</td>
</tr>
<tr>
<td>5c</td>
<td>The P-GW processes the PBU from the HSGW, assigns an HNP for the connection and responds back to the HSGW with PBA.</td>
</tr>
<tr>
<td>5d</td>
<td>The HSGW responds to the VSNCP Conf Req with a VSNCP Conf Ack.</td>
</tr>
<tr>
<td>5e</td>
<td>The HSGW sends a PPP-VSNCP-Conf-Req to the UE to complete PPP VSNCP negotiation.</td>
</tr>
<tr>
<td>5f</td>
<td>The UE completes VSNCP negotiation by returning a PPP-VSNCP-Conf-Ack.</td>
</tr>
<tr>
<td>6</td>
<td>The UE optionally sends a Router Solicitation (RS) message.</td>
</tr>
<tr>
<td>7</td>
<td>The HSGW sends a Router Advertisement (RA) message with the assigned Prefix.</td>
</tr>
</tbody>
</table>

### PMIPv6 Lifetime Extension without Handover

This section describes the procedure of a session registration lifetime extension by the P-GW without the occurrence of a handover.
Figure 17. PMIPv6 Lifetime Extension (without handover) Call Flow

Table 6. PMIPv6 Lifetime Extension (without handover) Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE is attached to the EPC and has a PDN connection with the P-GW where PDNID=x and an APN with assigned HNP.</td>
</tr>
<tr>
<td>2</td>
<td>The HSGW MAG service registration lifetime nears expiration and triggers a renewal request for the LMA.</td>
</tr>
<tr>
<td>3</td>
<td>The MAG service sends a Proxy Binding Update (PBU) to the P-GW LMA service with the following attributes: Lifetime, MNID, APN, ATT=HRPD, HNP.</td>
</tr>
<tr>
<td>4</td>
<td>The P-GW LMA service updates the Binding Cache Entry (BCE) with the new granted lifetime.</td>
</tr>
<tr>
<td>5</td>
<td>The P-GW responds with a Proxy Binding Acknowledgement (PBA) with the following attributes: Lifetime, MNID, APN.</td>
</tr>
</tbody>
</table>

PDN Connection Release Initiated by UE

This section describes the procedure of a session release by the UE.
**How the PDN Gateway Works**

**Figure 18. PDN Connection Release by the UE Call Flow**

![Diagram of PDN connection release by the UE call flow]

**Table 7. PDN Connection Release by the UE Call Flow Description**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.</td>
</tr>
<tr>
<td>2</td>
<td>The UE decides to disconnect from the PDN and sends a PPP VSNCP-Term-Req with PDNID=x.</td>
</tr>
<tr>
<td>3</td>
<td>The HSGW starts disconnecting the PDN connection and sends a PPP-VSNCP-Term-Ack to the UE (also with PDNID=x).</td>
</tr>
<tr>
<td>4</td>
<td>The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, ATT=HRPD, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.</td>
</tr>
<tr>
<td>5</td>
<td>The P-GW looks up the Binding Cache Entry (BCE) based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).</td>
</tr>
<tr>
<td>6</td>
<td>The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.</td>
</tr>
</tbody>
</table>

**PDN Connection Release Initiated by HSGW**

This section describes the procedure of a session release by the HSGW.
Table 8. PDN Connection Release by the HSGW Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.</td>
</tr>
<tr>
<td>2</td>
<td>The HSGW MAG service triggers a disconnect of the PDN connection for PDNID=x.</td>
</tr>
<tr>
<td>3</td>
<td>The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.</td>
</tr>
<tr>
<td>4</td>
<td>The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).</td>
</tr>
<tr>
<td>5</td>
<td>The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.</td>
</tr>
<tr>
<td>6</td>
<td>The P-GW looks up the BCE based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).</td>
</tr>
<tr>
<td>7</td>
<td>The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.</td>
</tr>
</tbody>
</table>

**PDN Connection Release Initiated by P-GW**

This section describes the procedure of a session release by the P-GW.
Figure 20. PDN Connection Release by the P-GW Call Flow

Table 9. PDN Connection Release by the P-GW Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.</td>
</tr>
<tr>
<td>2</td>
<td>A PGW trigger causes a disconnect of the PDN connection for PDNID=x and the PGW sends a Binding Revocation Indication (BRI) message to the HSGW with the following attributes: MNID, APN, HNP.</td>
</tr>
<tr>
<td>3</td>
<td>The HSGW responds to the BRI message with a Binding Revocation Acknowledgement (BRA) message with the same attributes (MNID, APN, HNP).</td>
</tr>
<tr>
<td>4</td>
<td>The HSGW MAG service triggers a disconnect of the UE PDN connection for PDNID=x.</td>
</tr>
<tr>
<td>5</td>
<td>The HSGW sends a PPP VSNCMP-Term-Req with PDNID=x to the UE.</td>
</tr>
<tr>
<td>6</td>
<td>The UE acknowledges the receipt of the request with a VSNCMP-Term-Ack (PDNID=x).</td>
</tr>
<tr>
<td>7</td>
<td>The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.</td>
</tr>
</tbody>
</table>

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

The following topics and procedure flows are included:
- Subscriber-initiated Attach (initial)
- Subscriber-initiated Detach

**Subscriber-initiated Attach (initial)**

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

**Figure 21. Subscriber-initiated Attach (initial) Call Flow**

**Table 10. Subscriber-initiated Attach (initial) Call Flow Description**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.</td>
</tr>
<tr>
<td>2</td>
<td>The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an “MME selection function”. The eNodeB forwards the Attach Request message to the new MME contained in a SI-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.</td>
</tr>
<tr>
<td>3</td>
<td>If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.</td>
</tr>
<tr>
<td>4</td>
<td>The UE responds with Identity Response (IMSI).</td>
</tr>
<tr>
<td>5</td>
<td>If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.</td>
</tr>
<tr>
<td>6</td>
<td>The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.</td>
</tr>
<tr>
<td>7</td>
<td>The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.</td>
</tr>
<tr>
<td>8</td>
<td>The MME selects an S-GW using “Serving GW selection function” and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause “PDN GW selection function”. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.</td>
</tr>
<tr>
<td>9</td>
<td>The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.</td>
</tr>
<tr>
<td>10</td>
<td>If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.</td>
</tr>
<tr>
<td>11</td>
<td>The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.</td>
</tr>
<tr>
<td>12</td>
<td>The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.</td>
</tr>
<tr>
<td>13</td>
<td>The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</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 tunnelled 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.

![Subscriber-initiated Detach Call Flow](image-url)
### How the PDN Gateway Works

Table 11. 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 DeleteBearerRequest (TEID) message to the S-GW.</td>
</tr>
<tr>
<td>3</td>
<td>The S-GW sends a DeleteBearerRequest (TEID) message to the P-GW.</td>
</tr>
<tr>
<td>4</td>
<td>The P-GW acknowledges with a DeleteBearerResponse (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 DeleteBearerResponse (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 DetachAccept message to the UE.</td>
</tr>
<tr>
<td>8</td>
<td>The MME releases the S1-MME signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.</td>
</tr>
</tbody>
</table>
S-GW Supported Standards

The S-GW service complies with the following standards.

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

3GPP References

Release 11 3GPP References

**Important:** 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) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling 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) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
Release 9 Supported Standards

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

Release 8 Supported Standards

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

3GPP2 References
- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

IETF References
- 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
P-GW Supported Standards

The P-GW service complies with the following standards.

- Release 12 3GPP References
- Release 11 3GPP References
- Release 10 3GPP References
- Release 9 3GPP References
- Release 8 3GPP References
- 3GPP2 References
- IETF References
- Object Management Group (OMG) Standards

Release 12 3GPP References

Important: The P-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 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

Release 11 3GPP References

Important: The P-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 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 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 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

Release 10 3GPP References

**Important:** The P-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 23.203: Policy and charging control architecture; Stage 2
- 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 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)

Release 9 3GPP References

**Important:** The P-GW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under 3GPP2 References.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 22.115: Service aspects; Charging and billing
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.207: End-to-end Quality of Service (QoS) concept and architecture
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2
- 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 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230: Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 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 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols; Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging application

Release 8 3GPP References

---

**Important:** The P-GW currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under 3GPP2 References.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
**SAE Gateway Overview**

**P-GW Supported Standards**

- 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 23.869: Support for Internet Protocol (IP) based IP Multimedia Subsystem (IMS) Emergency calls over General Packet Radio Service (GPRS) and Evolved Packet Service (EPS)
- 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 27.060: Mobile Station (MS) supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.210: Charging rule provisioning over Gx interface
- 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 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 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 36.300. EUTRA and EUTRAN; Overall description Stage 2
- 3GPP TS 36.412. EUTRAN S1 signaling transport
- 3GPP TS 36.413. EUTRAN S1 Application Protocol (S1AP)

**3GPP2 References**

- X.S0057-0 v3.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

**IETF References**

- RFC 791: Internet Protocol (STD 5).
- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2473: Generic Packet Tunneling in IPv6 Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3162: RADIUS and IPv6
- RFC 3266: Support for IPv6 in Session Description Protocol (SDP)
- RFC 3588: Diameter Base Protocol
- RFC 3589: Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3775: Mobility Support in IPv6
- RFC 4004: Diameter Mobile IPv4 Application
- RFC 4005: Diameter Network Access Server Application
- 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 5149: Service Selection for Mobile IPv6
- RFC 5213: Proxy Mobile IPv6
- RFC 5447: Diameter Mobile IPv6: Support for NAS to Diameter Server Interaction
- RFC 5555: Mobile IPv6 Support for Dual Stack Hosts and Routers
- RFC 5844: IPv4 Support for Proxy Mobile IPv6
- RFC 5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5846: Binding Revocation for IPv6 Mobility
- Internet-Draft (draft-ietf-dime-qos-attributes-07): QoS Attributes for Diameter
- Internet-Draft (draft-ietf-mip6-nemo-v4traversal-06.txt): Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-02.txt) IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress
- Internet-Draft (draft-meghana-netlmm-pmipv6-mipv4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking
Object Management Group (OMG) Standards

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

This chapter provides configuration information for the SAE Gateway (SAEGW).

**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 SAEGW product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

- Configuring an SAEGW Service
- Configuring an eGTP S-GW Service
- Configuring Optional Features on the eGTP S-GW
- Configuring an eGTP P-GW Service
- Configuring Optional Features on the P-GW
Configuring an SAEGW Service

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

- Information Required
- SAEGW Configuration

Information Required

The following sections describe the minimum amount of information required to configure and make the SAEGW operational on the network. To make the process more efficient, it is recommended that this information be 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 SAEGW 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 SAEGW.

<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. 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. 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 SAEGW Context Configuration Information

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

Table 13.  Required Information for SAEGW Context Configuration

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

SAEGW Service Configuration

<table>
<thead>
<tr>
<th>SAEGW service name</th>
<th>An identification string from 1 to 63 characters (alpha and/or numeric) by which the SAEGW service will be recognized by the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-GW service name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the S-GW service will be recognized by the system.</td>
</tr>
<tr>
<td>P-GW service name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system.</td>
</tr>
</tbody>
</table>

SAEGW Configuration

**Step 1**  Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

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

**Step 3**  Configure the system to perform as an SAEGW and associate an eGTP S-GW service and eGTP P-GW service by applying the example configurations presented in the **SAEGW Service Configuration** section.

**Step 4**  Verify and save the configuration by following the steps found in the **Verifying and Saving the Configuration** section.

Initial Configuration

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

**Step 2**  Create the context where the SAEGW, S-GW, and P-GW services will reside by applying the example configuration in the **Creating and Configuring an SAEGW Context** section.

**Step 3**  Configure an eGTP S-GW service by applying the example configurations found in the **Configuring an eGTP S-GW Service** section of this chapter.

**Step 4**  Configure an eGTP P-GW service by applying the example configurations found in the **Configuring an eGTP P-GW Service** section of this chapter.
Modifying the Local Context

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

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

Notes:
- Service names must be unique across all contexts within a chassis.

Creating and Configuring an SAEGW Context

Use the following example to create the context where the SAEGW, S-GW, and P-GW services will reside:

```
configure
  context <saegw_context_name>
end
```
SAEGW Service Configuration

Step 1  Configure the SAEGW service by applying the example configuration in the Configuring the SAEGW Service section.

Configuring the SAEGW Service

Use the following example to configure the SAEGW service:

```plaintext
configure
  context <saegw_context_name>
    saegw-service <saegw_service_name> -noconfirm
    associate sgw-service <sgw_service_name>
    associate pgw-service <pgw_service_name>
  end
```

Notes:

- The SAEGW, S-GW, and P-GW services must all reside within the same SAEGW context.
- Service names must be unique across all contexts within a chassis.

Verifying and Saving the Configuration

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.
Configuring an eGTP S-GW Service

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

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

Information Required

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

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

Required 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>
<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>
<tr>
<td>S1-U/S11 Interface Configuration (To/from eNodeB/MME)</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>Gateway IP address</td>
<td>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
</tbody>
</table>
### Required Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GTP-U Service Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>GTP-U service name (for S1-U/S11 interface)</td>
<td>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.</td>
</tr>
<tr>
<td>IP address</td>
<td>S1-U/S11 interface IPv4 or IPv6 address.</td>
</tr>
<tr>
<td><strong>S-GW Service Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>S-GW service name</td>
<td>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.</td>
</tr>
<tr>
<td><strong>eGTP Ingress Service Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>eGTP S1-U/S11 ingress service name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP S1-U/S11 ingress service is recognized by the system.</td>
</tr>
</tbody>
</table>

### Required S-GW Egress Context Configuration Information

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

**Table 15. 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>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
</tbody>
</table>

### GTP-U Service Configuration

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

**Figure 23.** eGTP S-GW Call Processing Using a Single Ingress and Egress Context

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 an eGTP S-GW, review the following graphic and subsequent steps.

**Step 1**
Set system configuration parameters such as activating PSCs by applying the example configurations found in the System Administration Guide.

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

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

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

Step 1  Create an ingress context where the S-GW and eGTP ingress service will reside by applying the example configuration in the Creating an S-GW Ingress Context section.

Step 2  Create an eGTP ingress service within the newly created ingress context by applying the example configuration in the Creating an eGTP Ingress Service section.

Step 3  Create an S-GW egress context where the eGTP egress services will reside by applying the example configuration in the Creating an S-GW Egress Context section.

Step 4  Create an eGTP egress service within the newly created egress context by applying the example configuration in the Creating an eGTP Egress Service section.

Step 5  Create a S-GW service within the newly created ingress context by applying the example configuration in the Creating an S-GW Service section.

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 <saegw_context_name> -noconfirm
    subscriber default
    exit
  interface <s1u-s11_interface_name>
    ip address <ipv4_address_primary>
    ip address <ipv4_address_secondary>
    exit
  ip route 0.0.0.0 0.0.0.0 <next_hop_address> <sgw_interface_name>
  exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s1u-s11_interface_name> <saegw_context_name>
end
```

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

Service names must be unique across all contexts within a chassis.

### Creating an eGTP Ingress Service

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

```bash
configure
context <saegw_context_name>
  egtp-service <egtp_ingress_service_name> -noconfirm
end
```

Notes:
- Service names must be unique across all contexts within a chassis.

### 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.

```bash
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
```

```bash
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.
- Service names must be unique across all contexts within a chassis.
Creating an eGTP Egress Service

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

```plaintext
configure

countext <egress_context_name>

egtp-service <egt_ep_egress_service_name> -noconfirm

end
```

Notes:
- Service names must be unique across all contexts within a chassis.

Creating an S-GW Service

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

```plaintext
configure

countext <saegw_context_name>

sgw-service <sgw_service_name> -noconfirm

end
```

Notes:
- Service names must be unique across all contexts within a chassis.

eGTP Configuration

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

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

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

**Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings**

Use the following configuration example to set the system to perform as an eGTP S-GW and configure the GTP-U and eGTP services:

```plaintext
configure

countext <saegw_context_name>

gtpp 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 <slu-sll_interface_ip_address>
exit
exit
context <sgw_egress_context_name>

gtpu-service <gtpu_egress_service_name>
    bind ipv4-address <s5s8_interface_ip_address>
exit
egtp-service <egtp_egress_service_name>
    interface-type interface-sgw-egress
    validation-mode default
    associate gtpu-service <gtpu_egress_service_name>
    gtpc bind address <s5s8_interface_ip_address>
end

Notes:
- The bind command in the GTP-U ingress and egress service configuration can also be specified as an IPv6 address using the ipv6-address command.
- Service names must be unique across all contexts within a chassis.

**Configuring the S-GW Service**

Use the following example to configure the S-GW service:

```bash
configure

case <saegw_context_name>

    sgw-service <sgw_service_name> -noconfirm
```
associate ingress egtp-service \(<\text{egtp\_ingress\_service\_name}\> \\
associate egress-proto gtp egress-context \(<\text{egress\_context\_name}\> \\
qci-qos-mapping \(<\text{map\_name}\> \\
end

Notes:
- Service names must be unique across all contexts within a chassis.

Configuring an IP Route

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

```
configure 

context \(<\text{egress\_context\_name}\>

ip route \(<\text{pgw\_ip\_addr/mask}\> \,<\text{sgw\_next\_hop\_addr}\> \,<\text{sgw\_intrfc\_name}\>
end
```

Notes:
- Service names must be unique across all contexts within a chassis.

Verifying and Saving the Configuration

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command \texttt{save configuration}. For additional information on how to verify and save configuration files, refer to the \textit{System Administration Guide} and the \textit{Command Line Interface Reference}. 
Configuring Optional Features on the eGTP S-GW

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

The following optional configurations are provided in this section:

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

Configuring the GTP Echo Timer

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

Default GTP Echo Timer Configuration

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

**eGTP-C**

```
configure

configure

context <context_name>

egtp-service <egtp_service_name>

gtpc echo-interval <seconds>

gtpc echo-retransmission-timeout <seconds>

gtpc max-retransmissions <num>

end
```

Notes:
- This configuration can be used in either the ingress context supporting the S1-U and/or S11 interfaces with the eNodeB and MME respectively; and the egress context supporting the S5/S8 interface with the P-GW.
• Service names must be unique across all contexts within a chassis.

• The following diagram describes a failure and recovery scenario using default settings of the three `gtpc` commands in the example above:

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

**GTP-U**

```plaintext
configure

configure

context <context_name>

gtpu-service <gtpu_service_name>

echo-interval <seconds>

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.

- Service names must be unique across all contexts within a chassis.

- The following diagram describes a failure and recovery scenario using default settings of the three GTP-U commands in the example above:

  ![Diagram](image)

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

**Dynamic GTP Echo Timer Configuration**

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

**eGTP-C**

```
configure
```
configure

context <context_name>

egtp-service <egtp_service_name>

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

gtpc echo-retransmission-timeout <seconds>

gtpc max-retransmissions <num>

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.

- Service names must be unique across all contexts within a chassis.

- The following diagram describes a failure and recovery scenario using default settings of the three gtpc commands in the example above and an example round trip timer (RTT) of six seconds:
• The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

GTP-U

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

Notes:

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

Configuring GTPP Offline Accounting on the S-GW

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

```bash
configure
    gtpp single-source
    context <saegw_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 <saegw_context_name> gtpp group default
associate accounting-policy <gz_policy_name>
exit
exit
context <saegw_context_name>
interface <gz_interface_name>
ip address <address>
exit
exit
port ethernet <slot_number/port_number>
no shutdown
bind interface <gz_interface_name> <saegw_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.
- Service names must be unique across all contexts within a chassis.

## Configuring Diameter Offline Accounting on the S-GW

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

configure

operator-policy name <policy_name>
associate call-control-profile <call_cntrl_profile_name>
exit
call-control-profile <call_cntrl_profile_name>
accounting mode radius-diameter
exit
lte-policy
subscriber-map <map_name>
    precedence <number> match-criteria all operator-policy-name <policy_name>
    exit
exit
context <saegw_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 <saegw_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> <saegw_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.

- Service names must be unique across all contexts within a chassis.

### 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:

```bash
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`.
- Service names must be unique across all contexts within a chassis.

Configuring X.509 Certificate-based Peer Authentication

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

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

The following configuration example enables X.509 certificate-based peer authentication on the S-GW. In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure

certificate name <cert_name> pem url <cert_pem_url> private-key pem url <private_key_url>

ca-certificate name <ca_cert_name> pem url <ca_cert_url>

end
```

Notes:
- The `certificate name` and `ca-certificate list` 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:

```plaintext
configure

context <saegw_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

disable
```

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.
- Service names must be unique across all contexts within a chassis.

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

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

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

The following configuration examples are included in this section:

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

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

```plaintext
configure
c  ontex <saegw_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.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```plaintext
configure
c  ontex <saegw_context_name>
   ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
```
Notes:

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

- The \texttt{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 \texttt{hmac} command configures the Encapsulating Security Payload (ESP) integrity algorithm. The \texttt{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 \texttt{lifetime} command configures the time the security key is allowed to exist, in seconds.

- The \texttt{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 \texttt{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.

- Service names must be unique across all contexts within a chassis.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```bash
configure

   context <saegw_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

end
```

Notes:

- The \texttt{ikev2-ikesa transform-set list} command specifies up to six IKEv2 transform sets.

- The \texttt{ipsec transform-set list} command specifies up to four IPSec transform sets.

- Service names must be unique across all contexts within a chassis.
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

c ontext <saegw_context_name>

gtpu-service <gtpu_ingress_service_name>

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

  exit

egtp-service <egtp_ingress_service_name>

  interface-type interface-sgw-ingress

  associate gtpu-service <gtpu_ingress_service_name>

  gtpc bind address <s1u_interface_ip_address>

  exit

  exit

c  ontext <sgw_egress_context_name>

  gtpu-service <gtpu_egress_service_name>

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

  exit

egtp-service <egtp_egress_service_name>

  interface-type interface-sgw-egress

  associate gtpu-service <gtpu_egress_service_name>

  gtpc bind address <s5_interface_ip_address>

  exit

  exit

c  ontext <saegw_context_name>

  sgw-service <sgw_service_name> -noconfirm

  egtp-service ingress service <egtp_ingress_service_name>

  egtp-service egress context <sgw_egress_context_name>
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.
- Service names must be unique across all contexts within a chassis.

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

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

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

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

### Creating and Configuring a Crypto Access Control List

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

```bash
configure

context <saegw_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
  context <saegw_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.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```plaintext
configure
  context <saegw_context_name>
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
```
Notes:

- The encryption algorithm, \texttt{aes-cbc-128}, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The \texttt{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 \texttt{hmac} command configures the Encapsulating Security Payload (ESP) integrity algorithm. The \texttt{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 \texttt{lifetime} command configures the time the security key is allowed to exist, in seconds.
- The \texttt{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 \texttt{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.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring a Crypto Map

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

```plaintext
configure

cryptomap crypto_map_name ikev2-ipv4
    match address <acl_name>
    peer <ipv4_address>
    authentication local pre-shared-key key <text>
    authentication remote pre-shared-key key <text>
    ikev2-ikesa transform-set list <name1> ... <name6>
    payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> ... <name4>
    exit
exit
interface <sl-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> <saegw_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.
- Service names must be unique across all contexts within a chassis.

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

```
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
  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.
- Service names must be unique across all contexts within a chassis.

Configuring S4 SGSN Handover Capability

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

Use the following example to configure this feature:

```
configure
   context <saegw_context_name> -noconfirm
      interface <s4_interface_name>
         ip address <ipv4_address_primary>
         ip address <ipv4_address_secondary>
      exit
   exit
port ethernet <slot_number/port_number>
   no shutdown
   bind interface <s4_interface_name> <saegw_context_name>
   exit
context <saegw_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.
- Service names must be unique across all contexts within a chassis.
Configuring an eGTP P-GW Service

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

- Information Required
- How This Configuration Works
- eGTP P-GW Configuration
- DHCP Service Configuration
- DHCPv6 Service Configuration

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be 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 P-GW in the network. Information on these parameters can be found in the appropriate sections of the Command Line Interface Reference.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

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

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

<table>
<thead>
<tr>
<th>Interface name</th>
<th>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
</tbody>
</table>
### Required Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.</td>
</tr>
<tr>
<td>IP address</td>
<td>S5/S8 interface IPv4 address.</td>
</tr>
<tr>
<td>P-GW Service Configuration</td>
<td></td>
</tr>
<tr>
<td>P-GW service name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.</td>
</tr>
<tr>
<td>PLMN ID</td>
<td>MCC number: The mobile country code (MCC) portion of the PLMN’s identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN’s identifier (a 2 or 3 digit integer value between 00 and 999).</td>
</tr>
<tr>
<td>eGTP Service Configuration</td>
<td></td>
</tr>
<tr>
<td>eGTP Service Name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP service will be recognized by the system.</td>
</tr>
</tbody>
</table>

### Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

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

### IP Address Pool Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address pool name and range</td>
<td>An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.</td>
</tr>
<tr>
<td>Required Information</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 address pool name and range</td>
<td>An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.</td>
</tr>
</tbody>
</table>

**Access Control List Configuration**

<table>
<thead>
<tr>
<th>IPv4 access list name</th>
<th>An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 access list name</td>
<td>An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.</td>
</tr>
</tbody>
</table>

**Deny/permit type**

- any
- by host IP address
- by IP packets
- by source ICMP packets
- by source IP address masking
- by TCP/UDP packets

**Readdress or redirect type**

- readdress server
- redirect context
- redirect css delivery-sequence
- redirect css service
- redirect nexthop

**SGi Interface Configuration (To/from IPv4 PDN)**

<table>
<thead>
<tr>
<th>Interface name</th>
<th>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet</td>
<td>IPv4 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>
</tbody>
</table>

**SGi Interface Configuration (To/from IPv6 PDN)**
### Required Information

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
</tr>
<tr>
<td>IP address and subnet</td>
</tr>
<tr>
<td>Physical port number</td>
</tr>
<tr>
<td>Gateway IP address</td>
</tr>
</tbody>
</table>

### Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gx Interface Configuration (to PCRF)</td>
</tr>
<tr>
<td>Gx Diameter Endpoint Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
</tr>
<tr>
<td>IP address and subnet</td>
</tr>
<tr>
<td>Physical port number</td>
</tr>
<tr>
<td>Gateway IP address</td>
</tr>
<tr>
<td>End point name</td>
</tr>
<tr>
<td>Origin realm name</td>
</tr>
<tr>
<td>Origin host name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<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>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<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>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
<tr>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.</td>
</tr>
<tr>
<td>An identification string between 1 and 127 characters. The realm is the Diameter identity. The originator’s realm is present in all Diameter messages and is typically the company or service name.</td>
</tr>
<tr>
<td>An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.</td>
</tr>
</tbody>
</table>
# Configuring an eGTP P-GW Service

## SAE Gateway Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin host address</td>
<td>The IP address of the Gx interface.</td>
</tr>
<tr>
<td>Peer name</td>
<td>The Gx endpoint name described above.</td>
</tr>
<tr>
<td>Peer realm name</td>
<td>The Gx origin realm name described above.</td>
</tr>
<tr>
<td>Peer address and port number</td>
<td>The IP address and port number of the PCRF.</td>
</tr>
<tr>
<td>Route-entry peer</td>
<td>The Gx endpoint name described above.</td>
</tr>
</tbody>
</table>

### Gy Interface Configuration (to on-line charging server)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
</tbody>
</table>

### Gy Diameter Endpoint Configuration

<table>
<thead>
<tr>
<th>End point name</th>
<th>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin realm name</td>
<td>An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator’s realm is present in all Diameter messages and is typically the company or service name.</td>
</tr>
<tr>
<td>Origin host name</td>
<td>An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.</td>
</tr>
<tr>
<td>Origin host address</td>
<td>The IP address of the Gy interface.</td>
</tr>
<tr>
<td>Peer name</td>
<td>The Gy endpoint name described above.</td>
</tr>
<tr>
<td>Peer realm name</td>
<td>The Gy origin realm name described above.</td>
</tr>
<tr>
<td>Peer address and port number</td>
<td>The IP address and port number of the OCS.</td>
</tr>
<tr>
<td>Route-entry peer</td>
<td>The Gy endpoint name described above.</td>
</tr>
</tbody>
</table>

### Gz Interface Configuration (to off-line charging server)

| 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. |

---

184
<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet</td>
<td>IPv4 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>
</tbody>
</table>

**Rf Interface Configuration (to off-line charging server)**

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the interface(s) to a specific network.</td>
</tr>
</tbody>
</table>

**Rf Diameter Endpoint Configuration**

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End point name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.</td>
</tr>
<tr>
<td>Origin realm name</td>
<td>An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator’s realm is present in all Diameter messages and is typically the company or service name.</td>
</tr>
<tr>
<td>Origin host name</td>
<td>An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.</td>
</tr>
<tr>
<td>Origin host address</td>
<td>The IP address of the Rf interface.</td>
</tr>
<tr>
<td>Peer name</td>
<td>The Rf endpoint name described above.</td>
</tr>
<tr>
<td>Peer realm name</td>
<td>The Rf origin realm name described above.</td>
</tr>
<tr>
<td>Peer address and port number</td>
<td>The IP address and port number of the OFCS.</td>
</tr>
<tr>
<td>Route-entry peer</td>
<td>The Rf endpoint name described above.</td>
</tr>
</tbody>
</table>
How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.

1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality 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. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.
eGTP P-GW Configuration

To configure the system to perform as an eGTP P-GW:

**Step 1**
Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

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

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

**Step 4**
Configure the PDN context by applying the example configuration in the *P-GW PDN Context Configuration* section.

**Step 5**
Enable and configure the active charging service for Gx interface support by applying the example configuration in the *Active Charging Service Configuration* section.

**Step 6**
Create a AAA context and configure parameters for policy by applying the example configuration in the *Policy Configuration* section.

**Step 7**
Verify and save the configuration by following the steps found in the *Verifying and Saving the Configuration* section.
Initial Configuration

Step 1 Create the context where the eGTP service will reside by applying the example configuration in the Creating and Configuring an eGTP P-GW Context section.

Step 2 Create and configure APNs in the P-GW context by applying the example configuration in the Creating and Configuring APNs in the P-GW Context section.

Step 3 Create and configure AAA server groups in the P-GW context by applying the example configuration in the Creating and Configuring AAA Groups in the P-GW Context section.

Step 4 Create an eGTP service within the newly created context by applying the example configuration in the Creating and Configuring an eGTP Service section.

Step 5 Create and configure a GTP-U service within the P-GW context by applying the example configuration in the Creating and Configuring a GTP-U Service section.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in the Creating a P-GW PDN Context section.

Creating and Configuring an eGTP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv4 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```bash
configure
gtpp single-source
category saegw_context_name -noconfirm
interface s5s8_interface_name
    ip address ipv4_address
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
```
SAE Gateway Configuration

Configuring an eGTP P-GW Service

```
exit
policy accounting <rf_policy_name> -noconfirm
accounting-level {level_type}
accounting-event-trigger interim-timeout action stop-start
operator-string <string>
cc profile <index> interval <seconds>
exit
exit
subscriber default
exit
port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <saegw_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.
- The S5/S8 (P-GW to S-GW) interface IP address can also be specified as an IPv6 address using the `ipv6 address` command.
- Set the accounting policy for the Rf (off-line charging) interface. The 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.
- Set the GTPP group setting for Gz accounting.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure

    context <saegw_context_name> -noconfirm
    apn <name>
        accounting-mode radius-diameter
        associate accounting-policy <rf_policy_name>
```
ims-auth-service <gx_ims_service_name>

aaa group <rf-radius_group_name>

dns primary <ipv4_address>

dns secondary <ipv4_address>

ip access-group <name> in

ip access-group <name> out

mediation-device context-name <saegw_context_name>

ip context-name <pdn_context_name>

ipv6 access-group <name> in

ipv6 access-group <name> out

active-charging rulebase <name>

end

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The associate accounting-policy command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in the Creating and Configuring an eGTP P-GW Context section above.
- Service names must be unique across all contexts within a chassis.

Use the following configuration to create an APN that includes Gz interface parameters:

```
configure

context <saegw_context_name> -noconfirm

apn <name>

    bearer-control-mode mixed

    selection-mode sent-by-ms

    accounting-mode gtpp

    gtpp group default accounting-context <aaa_context_name>

    ims-auth-service <gx_ims_service_name>

    ip access-group <name> in

    ip access-group <name> out

    ip context-name <pdn_context_name>
```
active-charging rulebase <gz_rulebase_name>
end

Notes:
- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The accounting-mode GTPP and GTPP group commands configure this APN for Gz accounting.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

configure
context <saegw_context_name> -noconfirm
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
aaa group default
radius attribute nas-ip-address address <ipv4_address>
radius accounting interim interval <seconds>
diameter authentication dictionary <name>
diameter accounting dictionary <name>
diameter accounting endpoint <rf_cfg_name>
diameter accounting server <rf_cfg_name> priority <num>

Notes:
- Service names must be unique across all contexts within a chassis.

Creating and Configuring an eGTP Service

Use the following configuration example to create the eGTP service:

```
configure

context <saegw_context_name>

egtp-service <egtp_service_name> -noconfirm

    interface-type interface-pgw-ingress
    validation mode default
    associate gtpu-service <gtpu_service_name>
    gtpc bind address <s5s8_interface_address>

end
```

Notes:
- Co-locating a GGSN service on the same ASR 5x00 requires that the `gtpc bind address` command uses the same IP address the GGSN service is bound to.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring a GTP-U Service

Use the following configuration example to create the GTP-U service:

```
configure

context <saegw_context_name>

gtpu-service <gtpu_service_name> -noconfirm

    bind ipv4-address <s5s8_interface_address>

end
```

Notes:
- The `bind` command can also be specified as an IPv6 address using the `ipv6-address` command.
- Service names must be unique across all contexts within a chassis.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure

context <pdn_context_name> -noconfirm
```
interface <sgi_ipv4_interface_name>
  ip address <ipv4_address>
interface <sgi_ipv6_interface_name>
  ipv6 address <address>
end

Notes:
- Service names must be unique across all contexts within a chassis.

P-GW Service Configuration

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service section.

Step 2 Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring a Static IP Route section.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
  context <saegw_context_name>
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id>
      associate egtp-service <egtp_service_name>
      associate qci-qos-mapping <name>
  end
```

Notes:
- QCI-QoS mapping configurations are created in the AAA context. Refer to the Configuring QCI-QoS Mapping section for more information.
- Co-locating a GGSN service on the same ASR 5x00 requires the configuration of the associate ggsn-service name command within the P-GW service.
- Service names must be unique across all contexts within a chassis.

Configuring a Static IP Route

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

```
configure
```
context <saegw_context_name>
  ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>
end

Notes:
- Service names must be unique across all contexts within a chassis.

**P-GW PDN Context Configuration**

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```
configure
  context <pdn_context_name> -noconfirm
  interface <sgi_ipv4_interface_name>
    ip address <ipv4_address>
    exit
  interface <sgi_ipv6_interface_name>
    ip address <ipv6_address>
    exit
  ip pool <name> range <start_address end_address> public <priority>
  ipv6 pool <name> range <start_address end_address> public <priority>
  subscriber default
    exit
  ip access-list <name>
    redirect css service <name> any
    permit any
    exit
  ipv6 access-list <name>
    redirect css service <name> any
    permit any
    exit
  aaa group default
```
exit
exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <sgi_ipv4_interface_name> <pdn_context_name>
exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <sgi_ipv6_interface_name> <pdn_context_name>
end

Notes:
  • Service names must be unique across all contexts within a chassis.

Active Charging Service Configuration

Use the following example to enable and configure active charging:

configure
  require active-charging optimized-mode
active-charging service <name>
  ruledef <name>
    <rule_definition>
      .
      .
    <rule_definition>
  exit
ruledef default
  ip any-match = TRUE
  exit
ruledef icmp-pkts
  icmp any-match = TRUE
exit
ruledef qci3
   icmp any-match = TRUE
exit
ruledef static
   icmp any-match = TRUE
exit
charging-action <name>
   <action>
      .
      .
   <action>
exit
charging-action icmp
   billing-action egcdr
exit
charging-action qci3
   content-id <id>
   billing-action egcdr
   qos-class-identifier <id>
   allocation-retention-priority <priority>
   tft-packet-filter qci3
exit
charging-action static
   service-identifier <id>
   billing-action egcdr
   qos-class-identifier <id>
   allocation-retention-priority <priority>
   tft-packet-filter qci3
exit

packet-filter <packet_filter_name>

ip remote address = { ipv4/ipv6_address | ipv4/ipv6_address/mask }

ip remote-port { = port_number | range start_port_number to end_port_number }

exit

rulebase default

exit

rulebase <name>

<rule_base>

... 

<rule_base>

exit

rulebase <gx_rulebase_name>

dynamic-rule order first-if-tied 

egcdr tariff minute <minute> hour <hour>(optional)

billing-records egcdr

action priority 5 dynamic-only ruledef qci3 charging-action qci3

action priority 100 ruledef static charging-action static

action priority 500 ruledef default charging-action icmp

action priority 570 ruledef icmp-pkts charging-action icmp

egcdr threshold interval <interval>

egcdr threshold volume total <bytes>

end

Notes:

- A rule base is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Charging actions define the action to take when a rule definition is matched.
• Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.

• The billing-action egcdr command in the charging-action qci13,icmp, and static examples is required for Gz accounting.

• The Gz rulebase example supports the Gz interface for off-line charging. The billing-records egcdr command is required for Gz accounting. All other commands are optional.

• Service names must be unique across all contexts within a chassis.

**Important:** If an uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

**Policy Configuration**

**Step 1** Configure the policy and accounting interfaces by applying the example configuration in the Creating and Configuring the AAA Context section.

**Step 2** Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping section.

**Creating and Configuring the AAA Context**

Use the following example to create and configure a AAA context including diameter support and policy control, and bind Ethernet ports to interfaces supporting traffic between this context and a PCRF, an OCS, and an OFCS:

```
configure

context <aaa_context_name> -noconfirm

interface <gx_interface_name>
ipv6 address <address>
exit

interface <gy_interface_name>
ipv6 address <address>
exit

interface <gz_interface_name>
ip address <ipv4_address>
exit

interface <rf_interface_name>
ip address <ipv4_address>
exit
```
subscriber default

exit

ims-auth-service <gx_ims_service_name>

p-cscf discovery table <#> algorithm round-robin
p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_addr>

policy-control

diameter origin endpoint <gx_cfg_name>

diameter dictionary <name>

diameter host-select table <#> algorithm round-robin

diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

exit

exit


diameter endpoint <gx_cfg_name>

origin realm <realm_name>

origin host <name> address <aaa_ctx_ipv6_address>

peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>

route-entry peer <gx_cfg_name>

exit


diameter endpoint <gy_cfg_name>

origin realm <realm_name>

origin host <name> address <gy_ipv6_address>

connection retry-timeout <seconds>

peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>

route-entry peer <gy_cfg_name>

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
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gx_interface_name> <aaa_context_name>
exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gy_interface_name> <aaa_context_name>
exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gz_interface_name> <aaa_context_name>
exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <rf_interface_name> <aaa_context_name>
end

Notes:
- The p-cscf table command under ims-auth-service can also specify an IPv4 address to the PCRF.
- The Gx interface IP address can also be specified as an IPv4 address using the ip address command.
- The Gy interface IP address can also be specified as an IPv4 address using the ip address command.
- The Rf interface IP address can also be specified as an IPv6 address using the ipv6 address command.
- Service names must be unique across all contexts within a chassis.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

configure
  qci-qos-mapping <name>
Verifying and Saving the Configuration

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using the following method, as configured within an APN:

**DHCP-proxy**: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

There are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.

**Important**: This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer to the DHCP Service Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and P-GW service as described in eGTP P-GW Configuration section of this chapter.

To configure the DHCP service:

**Step 1**  
Create the DHCP service in system context and bind it by applying the example configuration in the DHCP Service Creation section.

**Step 2**  
Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the DHCP Server Parameter Configuration section.

```plaintext
qci 1 user-datagram dscp-marking <hex>
qci 3 user-datagram dscp-marking <hex>
qci 9 user-datagram dscp-marking <hex>
exit
```

Notes:

- The SAEGW does not support non-standard QCI values. QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203; the SAEGW supports these standard values.
- The above configuration only shows one keyword example. Refer to the QCI-QOS Mapping Configuration Mode Commands chapter in the Command Line Interface Reference for more information on the `qci` command and other supported keywords.
Step 3  Verify your DHCP Service configuration by following the steps in the *DHCP Service Configuration Verification* section.

Step 4  Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

**DHCP Service Creation**

Use the following example to create the DHCP service to support DHCP-based address assignment:

```plaintext
configure
    context <dest_ctxt_name>
    dhcp-service <dhcp_svc_name>
        bind address <ip_address> [nexthop-forwarding-address <nexthop_ip_address> [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]]]
    end
```

**Notes:**

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword `nexthop-forwarding-address <nexthop_ip_address> [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]]` applies DHCP over MPLS traffic.
- Service names must be unique across all contexts within a chassis.

**DHCP Server Parameter Configuration**

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

```plaintext
configure
    context <dest_ctxt_name>
    dhcp-service <dhcp_svc_name>
        dhcp server <ip_address> [priority <priority>
        dhcp server selection-algorithm {first-server | round-robin}]
        lease-duration min <minimum_dur> max <max_dur>
        dhcp deadtime <max_time>
        dhcp detect-dead-server consecutive-failures <max_number>
        max-retransmissions <max_number>
        retransmission-timeout <dur_sec>
    end
```
Notes:

- Multiple DHCP can be configured by entering `dhcp server` command multiple times. A maximum of 20 DHCP servers can be configured.
- The `dhcp detect-dead-server` command and `max-retransmissions` command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with `max-retransmissions` command.
- Service names must be unique across all contexts within a chassis.

**DHCP Service Configuration Verification**

**Step 1**  Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

```
show dhcp service all
```

This command produces an output similar to that displayed below where DHCP name is `dhcpl`:

```
Service name: dhcpl
Context: isp
Bind: Done
Local IP Address: 150.150.150.150
Next Hop Address: 192.179.91.3
MPLS-label:
    Input: 5000
Output: 1566 1899
Service Status: Started
Retransmission Timeout: 3000 (milli-secs)
Max Retransmissions: 2
Lease Time: 600 (secs)
Minimum Lease Duration: 600 (secs)
Maximum Lease Duration: 86400 (secs)
DHCP Dead Time: 120 (secs)
DHCP Dead consecutive Failure: 5
DHCP T1 Threshold Timer: 50
DHCP T2 Threshold Timer: 88
DHCP Client Identifier: Not Used
```
DHCP Algorithm: Round Robin

DHCP Servers configured:

Address: 150.150.150.150  Priority: 1

DHCP server rapid-commit: disabled

DHCP client rapid-commit: disabled

DHCP chaddr validation: enabled

Step 2 Verify the DHCP service status by entering the following command in Exec Mode:

show dhcp service status

DHCPv6 Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) for IPv6 to enable the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCPv6 configuration is done within an APN.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and APN as described in P-GW PDN Context Configuration section of this chapter.

To configure the DHCPv6 service:

Step 1 Create the DHCPv6 service in system context and bind it by applying the example configuration in the DHCPv6 Service Creation section.

Step 2 Configure the DHCPv6 server and other configurable values for Renew Time, Rebind Time, Preferred Lifetime, and Valid Lifetime by applying the example configuration in the DHCPv6 Server Parameter Configuration section.

Step 3 Configure the DHCPv6 client and other configurable values for Maximum Retransmissions, Server Dead Tries, and Server Resurrect Time by applying the example configuration in the DHCPv6 Client Parameter Configuration section.

Step 4 Configure the DHCPv6 profile by applying the example configuration in the DHCPv6 Profile Configuration section.

Step 5 Associate the DHCPv6 profile configuration with the APN by applying the example configuration in the Associate DHCPv6 Configuration section.

Step 6 Verify your DHCPv6 Service configuration by following the steps in the DHCPv6 Service Configuration Verification section.

Step 7 Save your configuration as described in the Verifying and Saving Your Configuration chapter.

DHCPv6 Service Creation

Use the following example to create the DHCPv6 service to support DHCP-based address assignment:

configure
collection <dest_ctxt_name>
SAE Gateway Configuration

Configuring an eGTP P-GW Service

SAE Gateway Administration

Notes:
- To ensure proper operation, DHCPv6 functionality should be configured within a destination context.
- The Port specifies the listen port and is used to start the DHCPv6 server bound to it. It is optional and if unspecified, the default port is 547.
- Service names must be unique across all contexts within a chassis.

DHCPv6 Server Parameter Configuration

Use the following example to configure the DHCPv6 server parameters to support DHCPv6-based address assignment:

```plaintext
dhcpv6-service <dhcpv6_svc_name>

  bind address <ipv6_address> port <port>

end
```

Notes:
- Multiple DHCP can be configured by entering `dhcp server` command multiple times. A maximum of 3 DHCPv6 servers can be configured.
- `renew-time` configures the renewal time for prefixes assigned by dhcp-service. Default is 900 seconds.
- `rebind-time` configures the rebind time for prefixes assigned by dhcp-service. Default is 900 seconds.
- `preferred-lifetime` configures the preferred lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.
- `valid-lifetime` configures the valid lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.
- Service names must be unique across all contexts within a chassis.

DHCPv6 Client Parameter Configuration

Use the following example to configure the DHCPv6 client parameters to support DHCPv6-based address assignment:

```plaintext
configure

  context <dest_ctxt_name>

  dhcpv6-service <dhcpv6_svc_name>

  dhcpv6-server

  renew-time <renewal_time>

  rebind-time <rebind_time>

  preferred-lifetime <pref_lifetime>

  valid-lifetime <valid_lifetime>

end
```

Notes:
context <dest_ctxt_name>

dhcpv6-service <dhcpv6_svc_name>

dhcpv6-client

server-ipv6-address <ipv6_addr> port <port> priority <priority>

max-retransmissions <max_number>

server-dead-time <dead_time>

server-resurrect-time <revive_time>

end

Notes:

- DHCPv6 client configuration requires an IPv6 address, port, and priority. The port is used for communicating with the DHCPv6 server. If not specified, default port 547 is used. The Priority parameter defines the priority in which servers should be tried out.
- max-retransmissions configures the max retransmission that DHCPV6-CLIENT will make towards DHCPV6-SERVER. Default is 20.
- server-dead-time: PDN DHCPV6-SERVER is considered to be dead if it does not respond after given tries from client. Default is 5.
- server-resurrect-time: PDN DHCPV6-SERVER is considered alive after it has been dead for given seconds. Default is 20.
- Service names must be unique across all contexts within a chassis.

**DHCPv6 Profile Configuration**

Use the following example to configure the DHCPv6 profile:

configure

context <dest_ctxt_name>

dhcp-server-profile <server_profile>

enable rapid-commit-dhcpv6

process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority <priority>

dhcpv6-server-preference <pref_value>

enable dhcpv6-server-unicast

enable dhcpv6-server-reconf

exit

dhcp-client-profile <client_profile>
client-identifier { IMSI | MSISDN }
enable rapid-commit-dhcpv6
enable dhcp-message-spray
request dhcp-option dns-address
request dhcp-option netbios-server-address
request dhcp-option sip-server-address
end

Notes:
- **dhcp-server-profile** command creates a server profile and then enters the DHCP Server Profile configuration mode.
- **enable rapid-commit-dhcpv6** command enables rapid commit on the DHCPv6 server. By default it is disabled. This is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the UE.
- **process dhcp-option-from** command configures in what order the configuration options should be processed for a given client request. For a given client configuration, values can be obtained from either AAA, PDN-DHCP-SERVER, or LOCAL. By default, AAA is preferred over PDN-DHCP, which is preferred over LOCAL configuration.
- **dhcpv6-server-preference**: According to RFC-3315, DHCPv6-CLIENT should wait for a specified amount of time before considering responses to its queries from DHCPv6-SERVERS. If a server responds with a preference value of 255, DHCPv6-CLIENT need not wait any longer. Default value is 0 and it may have any configured integer between 1 and 255.
- **enable dhcpv6-server-unicast** command enables server-unicast option for DHCPv6. By default, it is disabled.
- **enable dhcpv6-server-reconf** command configures support for reconfiguration messages from the server. By default, it is disabled.
- **dhcp-client-profile** command creates a client profile and then enters the DHCP Client Profile configuration mode.
- **client identifier** command configures the client-identifier, which is sent to the external DHCP server. By default, IMSI is sent. Another available option is MSISDN.
- **enable rapid-commit-dhcpv6** command configures the rapid commit for the client. By default, rapid-commit-option is enabled for both DHCPv4 & DHCPv6.
- **enable dhcp-message-spray** command enables dhcp-client to spray a DHCP message to all configured DHCP servers in the PDN. By default this is disabled. With Rapid-Commit, there can only be one server to which this can be sent.
- **request dhcp-option** command configures DHCP options which can be requested by the dhcp-client. It supports the following options:
  - dns-address
  - netbios-server-address
  - sip-server-address
  - Service names must be unique across all contexts within a chassis.
Associate DHCPv6 Configuration

Use the following example to associate the DHCPv6 profile with an APN:

```plaintext
configure
   context <dest_ctxt_name>
   apn <apn_name>
      dhcpv6 service-name <dhcpv6_svc_name> server-profile <server_profile> client-profile <client_profile>
         dhcpv6 ip-address-pool-name <dhcpv6_ip_pool>
         dhcpv6 context-name <dest_ctxt>
   exit
```

Notes:
- Service names must be unique across all contexts within a chassis.

DHCPv6 Service Configuration Verification

Step 1  Verify that your DHCPv6 servers configured properly by entering the following command in Exec Mode:

```plaintext
show dhcpv6-service all
```

This command produces an output similar to that displayed below where DHCPv6 service name is dhcpv6-service:

<table>
<thead>
<tr>
<th>Service name: dhcpv6-service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context:</td>
</tr>
<tr>
<td>2092::192:90:92:40</td>
</tr>
<tr>
<td>Bind Address:</td>
</tr>
<tr>
<td>Bind:</td>
</tr>
<tr>
<td>Service Status:</td>
</tr>
<tr>
<td>Started</td>
</tr>
<tr>
<td>Server Dead Time:</td>
</tr>
<tr>
<td>120 (secs)</td>
</tr>
<tr>
<td>Server Dead consecutive Failure:5</td>
</tr>
<tr>
<td>Server Select Algorithm:</td>
</tr>
<tr>
<td>First Server</td>
</tr>
<tr>
<td>Server Renew Time:</td>
</tr>
<tr>
<td>400 (secs)</td>
</tr>
<tr>
<td>Server Rebind Time:</td>
</tr>
<tr>
<td>500 (secs)</td>
</tr>
<tr>
<td>Server Preferred Life Time:</td>
</tr>
<tr>
<td>600 (secs)</td>
</tr>
<tr>
<td>Server Valid Life Time:</td>
</tr>
<tr>
<td>700 (secs)</td>
</tr>
</tbody>
</table>
Max Retransmissions: 3 (secs)
Server Dead Tries: 4 (secs)
Server Resurrect Time: 10 (secs)
ipv6 Nd Flag: O_FLAG

DHCPv6 Servers configured:
Address: 2092::192:90:92:40 Priority: 1 enabled

Step 2 Verify the DHCPv6 service status by entering the following command in Exec Mode:

```
show dhcpv6 status service dhcpv6_service_name
```
Configuring Optional Features on the P-GW

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

The following optional configurations are provided in this section:

- Configuring ACL-based Node-to-Node IP Security on the S5 Interface
- Configuring APN as Emergency
- Configuring Dynamic Node-to-Node IP Security on the S5 Interface
- Configuring the GTP Echo Timer
- Configuring GTPP Offline Accounting on the P-GW
- Configuring Local QoS Policy
- Configuring X.509 Certificate-based Peer Authentication

Configuring ACL-based Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IKEv2/IPSec ACL-based node-to-node tunnel endpoint on the S5 interface.

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

The following configuration examples are included in this section:

- Creating and Configuring a Crypto Access Control List
- Creating and Configuring an IPSec Transform Set
- Creating and Configuring an IKEv2 Transform Set
- Creating and Configuring a Crypto Map

Creating and Configuring a Crypto Access Control List

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

```
configure
    context <saegw_context_name> -noconfirm
    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.
- Service names must be unique across all contexts within a chassis.

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 <saegw_context_name> -noconfirm
        ipsec transform-set <ipsec_transform-set_name>
            encryption aes-cbc-128
            group none
            hmac shal-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 `shal-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.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

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

encryption aes-cbc-128

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 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 <sec>** command configures the time the security key is allowed to exist, in seconds.
- The **prf sha1** 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.
- Service names must be unique across all contexts within a chassis.

Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map:

```
configure

crypto map <crypto_map_name> ikev2-ipv4
  match address <acl_name>
  peer <ipv4_address>
  authentication local pre-shared-key key <text>
  authentication remote pre-shared-key key <text>
  ikev2-ikesa transform-set list <name1> .. name6
  payload <name> match ipv4
```
Configuring Optional Features on the P-GW

 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> <saegw_context_name>

 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.

• Service names must be unique across all contexts within a chassis.

Configuring APN as Emergency

The configuration example in this section configures an emergency APN for VoLTE based E911 support.

In APN Configuration Mode, specify the name of the emergency APN and set the emergency inactivity timeout as follows. You may also configure the P-CSCF FQDN server name for the APN.

 configure

 context <saegw_context_name> -noconfirm
 apn <name>
   emergency-apn
   timeout emergency-inactivity <seconds>
 p-cscf fqdn <fqdn>

 end
Notes:

- By default, an APN is assumed to be non-emergency.
- The `timeout emergency-inactivity` command specifies the timeout duration, in seconds, to check inactivity on the emergency session. `<seconds>` must be an integer value from 1 through 3600.
- By default, emergency inactivity timeout is disabled (0).
- The `p-cscf fqdn` command configures the P-CSCF FQDN server name for the APN. `<fqdn>` must be a string from 1 to 256 characters in length.
- P-CSCF FQDN has more significance than CLI-configured P-CSCF IPv4 and IPv6 addresses.
- Service names must be unique across all contexts within a chassis.

## Configuring Dynamic Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IPSec/IKEv2 dynamic node-to-node tunnel endpoint on the S5 interface.

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

The following configuration examples are included in this section:

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

### Creating and Configuring an IPSec Transform Set

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

```
configure

context <saegw_context_name> -noconfirm

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.

- Service names must be unique across all contexts within a chassis.

### Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure

context <saegw_context_name> -noconfirm

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.

- Service names must be unique across all contexts within a chassis.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```bash
configure
cryptotemplate <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.
- Service names must be unique across all contexts within a chassis.

Binding the S5 IP Address to the Crypto Template

The following example configures the binding of the S5 interface to the crypto template:

```bash
configure
gtpu-service <gtpu_ingress_service_name>
bind ipv4-address <s5_interface_ip_address> crypto-template <sgw_s5_crypto_template>
exit
egtp-service <egtp_ingress_service_name>
interface-type interface-pgw-ingress
```
associate gtpu-service <gtpu_ingress_service_name>
gtpc bind ipv4-address <s5_interface_ip_address>
exit
pgw-service <pgw_service_name> -noconfirm
plmn id mcc <id> mnc <id> primary
associate egtp-service <egtp_ingress_service_name>
end

Notes:
- The bind command in the GTP-U and eGTP service configuration can also be specified as an IPv6 address using the ipv6-address command.
- Service names must be unique across all contexts within a chassis.

Configuring the GTP Echo Timer

The GTP echo timer on the ASR5x00 P-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

configure

configure

context <context_name>

egtp-service <egtp_service_name>

gtpc echo-interval <seconds>
gtpc echo-retransmission-timeout <seconds>
gtpc max-retransmissions <num>
end

Notes:
- The following diagram describes a failure and recovery scenario using default settings of the three gtpc commands in the example above:
- The multiplier (x2) is system-coded and cannot be configured.
- Service names must be unique across all contexts within a chassis.

**GTP-U**

```bash
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
      end
end
```
Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three GTP-U commands in the example above:

  - The multiplier (x2) is system-coded and cannot be configured.
  - Service names must be unique across all contexts within a chassis.

### Dynamic GTP Echo Timer Configuration

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

**eGTP-C**

```bash
cfg

configure

configure

context <context_name>

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

- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.
• Service names must be unique across all contexts within a chassis.

**GTP-U**

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

**Notes:**

• The following diagram describes a failure and recovery scenario using default settings of the three `gtpc` commands in the example above and an example round trip timer (RTT) of six seconds:
- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.
- Service names must be unique across all contexts within a chassis.

Configuring GTPP Offline Accounting on the P-GW

By default the P-GW service supports GTPP accounting. To provide GTPP offline charging, configure the P-GW with the example parameters below:

```
configure
gtpp single-source
```
context <saegw_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

   exit

context <saegw_context_name>

   apn apn

   associate accounting-policy <gz_policy_name>

   exit

interface <gz_interface_name>

   ip address <address>

   exit
exit

port ethernet <slot_number/port_number>

no shutdown

bind interface <gz_interface_name> <saegw_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.
- Service names must be unique across all contexts within a chassis.

### Configuring Local QoS Policy

The configuration examples in this section create a local QoS policy. A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

**Important:** Local QoS Policy is a licensed feature and requires the purchase of the Local Policy Decision Engine feature license to enable it.

The following configuration examples are included in this section:

- Creating and Configuring a Local QoS Policy
- Binding a Local QoS Policy
- Verifying Local QoS Policy

#### Creating and Configuring a Local QoS Policy

The following configuration example enables a local QoS policy on the P-GW:

```
configure

local-policy-service <name> -noconfirm

ruledef <ruledef_name> -noconfirm

  condition priority <priority> <variable> match <string_value>
```
condition priority <priority> <variable> match <int_value>
condition priority <priority> <variable> nomatch <regex>
exit
actiondef <actiondef_name> -noconfirm
action priority <priority> <action_name> <arguments>
action priority <priority> <action_name> <arguments>
exit
actiondef <actiondef_name> -noconfirm
action priority <priority> <action_name> <arguments>
action priority <priority> <action_name> <arguments>
exit
actiondef <actiondef_name> -noconfirm
action priority <priority> <action_name> <arguments>
action priority <priority> <action_name> <arguments>
exit
eventbase <eventbase_name> -noconfirm
rule priority <priority> event <list_of_events> ruledef <ruledef_name> actiondef <actiondef_name>
end

Notes:

- A maximum of 16 local QoS policy services are supported.
- A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.
- The `condition` command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.
- A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons.
- The `action` command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.
- Currently, only one eventbase is supported and must be named “default”.
- The `rule` command can be entered multiple times to configure multiple rules for an eventbase.
- A maximum of 256 rules are suggested in an eventbase for performance reasons.
- Rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of `continue` is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.
- Service names must be unique across all contexts within a chassis.

**Binding a Local QoS Policy**
Option 1: The following configuration example binds the previously configured local QoS policy:

```plaintext
configure
    context <saegw_context_name> -noconfirm
        apn <name>
            ims-auth-service <local-policy-service name>
        end
end
```

Notes:
- A maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- Useful in case of emergency calls; PCRF is not involved.
- Service names must be unique across all contexts within a chassis.

Option 2: The following configuration example may also be used to bind the previously configured local QoS policy or a failure handling template:

```plaintext
configure
    context <saegw_context_name> -noconfirm
        ims-auth-service <auth_svc_name>
            policy-control
                associate failure-handling-template <template_name>
                associate local-policy-service <service_name>
        end
end
```

Notes:
- Only one failure handling template can be associated with the IMS authorization service. The failure handling template should be configured prior to issuing this command.
- The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template, refer to the Diameter Failure Handling Template Configuration Mode Commands chapter in the Command Line Interface Reference.
- You must select “local-fallback” in the failure handling template to support fallback to local policy.
- To support fallback to local policy in case of failure at PCRF, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.
- Service names must be unique across all contexts within a chassis.

Verifying Local QoS Policy
The following configuration example verifies if local QoS service is enforced:

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

Notes:
- Please take extreme caution not to use logging feature in console port and in production nodes.

### 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 P-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 P-GW.

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

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

Notes:
- The `certificate name` and `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.
- Service names must be unique across all contexts within a chassis.

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 <saegw_context_name> -noconfirm
crypto template <crypto_template_name> ikev2-dynamic
certificate name <cert_name>
ca-cert-name list <ca_cert_name>
```
authentication local certificate

authentication remote certificate

end

Notes:

- A maximum of 16 certificates and 16 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.

- Service names must be unique across all contexts within a chassis.
Chapter 3
Session Tracing on the SAEGW

This chapter describes Session Tracing functionality on the Serving Architecture Evolution Gateway (SAEGW), and includes configuration procedures, monitoring commands, and session tracing file examples.

- Session Tracing Overview
- Configuring Session Trace on the SAEGW
- Monitoring the Session Trace Functionality
- Supported Session Trace Configurations
- Session Trace File Example
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 SAEGW.

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 SAEGW is actively tracing data on one or more interfaces. All data collected are stored as files in an XML format and then transferred to the collection entity using (s)FTP. Note that IPv4 or IPv6 connectivity is required between the NE and the TCE in order to transfer the files.

Figure 25. 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 SAEGW where the trace is to be initiated. The SAEGW establishes the trace session and waits for a configured trigger event to start actively tracing. When management-initiated trace activations are executed at the SAEGW, 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 SAEGW. The trace control and configuration parameters are configured directly in the specified SAEGW 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/EPS network element.

- **Signaling Trace**: With a signaling based activation, the trace session is indicated to the SAEGW 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 not enabled by configuration or not present in the configured trace parameters).

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

**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.

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, a (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 concludes until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

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 a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (s)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.
Data Collection

Data collection is done in-line 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 SAEGW 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 a (s)FTP connection to the TCE. If so, it is used for all traffic associated with this trace session. If not, a (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 sFTP 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:

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

Configuring Session Trace on the SAEGW consists of the following:

- Enable session tracing on the SAEGW
- Configuring a Management Session Trace on the SAEGW
- Configuring a Signaling Session Trace on the SAEGW
- Configuring a Random Session Trace on the SAEGW

The various types of trace functions can be used in combinations to provide operators with the comprehensive trace information needed. These 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 configurations are allowed. For details on the supported session trace configuration types, refer to the Supported Session Trace Configurations section in this document.

Enabling Session Tracing on the SAEGW

Session Tracing functionality first must be enabled on the SAEGW before a specific Management, Random or Signaling session tracing type 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 instance of session on a specified UMTS/EPS network element.

To enable session tracing on the SAEGW:

```
config

    session trace network-element saegw [ file-type <a-type | b-type> ] tce-mode none | push transport ftp | sftp username username encrypted password password path directory_path collection timer ctimer_value

end
```

Notes:

- `session trace network-element saegw` enables Session Tracing functionality on the SAEGW.
- `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. It should be noted 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
```

To disable session tracing functionality on the SAEGW:

```
config
  no session trace network-element saegw
```

**Verifying that Session Tracing is Enabled**

To verify that the session tracing functionality is enabled on the SAEGW:

```
show session trace statistics
```

Look for the following fields and status indications:

SAEGW Enabled

```
PGW: Trace-Type: None
SGW: Trace-Type: None
```

**Configuring a Session Trace Template for the SAEGW**

Operators have the option of creating a template for a management trace in configuration mode for the SAEGW. 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.

To configure a template-session-trace:

```
config
  template-session-trace network-element saegw template-name template_name
```
[ func-pgw | func-sgw ] interface interface
end

Notes:

- Available **func-pgw interface** options are:
  - `all`
  - `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`
  - `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.

To disable the session trace template configuration:

```
no template-session-trace network-element saegw
```

To disable the session trace template per NE and subscriber:
Verifying the Session Trace Template Configuration

To verify the session trace configuration:

```
show session trace template network-element saegw all
```

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

Configuring a Management Session Trace on the SAEGW

Session tracing functionality must be enabled before a management trace can be configured. Refer to the Enabling Session Tracing on the SAEGW section in this Appendix for the procedure.

To configure a management session trace on the SAEGW from Exec Mode:

```
session trace subscriber network-element saegw template-name template_name { imsi id | imei id } trace-ref trace_ref_value collection-entity ip_address
```

Where:

- `template-name` specifies the name of the `session-trace-template` to use in the trace. Management traces executed in Exec mode will use the 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.

To deactivate the management trace configuration:

```
no session trace subscriber network-element saegw trace-ref trace_ref_value
```

Example:

This example configures a subscriber management trace for all S-GW and P-GW interfaces.

```
session trace subscriber network-element saegw func-pgw func-sgw 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:

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

To verify specific parameters have been activated for the subscriber management trace:
show session trace subscriber network-element saegw trace-ref trace_ref_value

Look for the following fields to verify the management trace configuration:

NE Type: SAEGW

PGW: Trace-Type: M

SGW: Trace-Type: M

......

Traced Interfaces:

PGW:

A list of the P-GW interfaces configured for the trace appear here.

SGW:

A list of the S-GW interfaces configured for the trace appear here.

Configuring a Signaling Session Trace on the SAEGW

Session trace functionality must be enabled on the SAEGW before a signaling session trace can be configured. Refer to the Enabling Session Tracing on the SAEGW section in this Appendix for the procedure.

To configure a signaling session trace on the SAEGW:

session trace signaling network-element saegw [ func-pgw | func-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 both the P-GW and S-GW of the SAEGW.
- **collection-entity** specifies the IPv4 or IPv6 address of the Trace Collection Entity (TCE) to which the trace files are sent.
- Available **func-pgw** interfaces are:
  - all
  - 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.

- Available func-sgw interfaces are:
  - all
  - 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.

**Example:**
This example configures a signaling session trace for all S-GW and P-GW interfaces.

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

To deactivate signaling trace on the SAEGW:

```
no session trace signaling network-element saegw
```

**Verifying the Signaling Session Trace Configuration**

To verify the signaling session trace configuration on the SAEGW:

```
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
```
Configuring a Random Trace on the SAEGW

Session trace functionality first must be enabled on the SAEGW before a random trace can be configured. Refer to the Enabling Session Tracing on the SAEGW section in this Appendix for the procedure.

Enables or disables the subscriber session trace functionality based on the random trace on the SAEGW. If enabled, the subscriber selection will be based on random logic for all instances of session on a specified UMTS/EPS network element.

To configure a random session trace on the SAEGW:

```
session trace random range network-element saegw [ 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.
- `saegw` specifies that the random trace is enabled for the SAEGW.
- `func-pgw` enables random tracing of the P-GW under the SAEGW.
- `func-sgw` enables random tracing of the S-GW 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. `all` specifies all interfaces. Alternatively, one of the following interfaces from `func-pgw` or `func-sgw` can be specified:
  - Available `func-pgw interface` options are:
    - `all`
    - `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.
Session Tracing on the SAEGW

- **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 func-sgw interfaces are:**
  
  - **all**
  
  - **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.
  
  - **collection-entity** specifies the IPv4 address of the Trace Collection Entity (TCE)

**Example:**

Enable the random tracing on the 40 saegw subscriber on all S-GW interfaces and the s5 interface of the P-GW in the SAEGW.

```
session trace random 40 network-element saegw func-pgw interface s5 func-sgw interface all collection-entity 1.1.1.1
```

To disable random session tracing on the SAEGW:

```
no session trace random network-element saegw
```

**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 SAEGW. For example:

```
Network element status:
...
SAEGW Enabled

PGW: Trace-Type: R

SGW: Trace-Type: R Configured-Random: 40
```
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 track.

**show session trace trace-summary**

This command provides the trace-ref value of all session traces, broken down my 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 19. 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>
<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 S-GW 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 Signalling. 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>Func-S-GW Trace Config</td>
<td>Func-P-GW Trace Config</td>
<td>Call Type</td>
<td>S-GW Trace?</td>
<td>P-GW Trace?</td>
<td>Output</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------</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>
<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+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+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>
<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>Func-S-GW Trace Config</td>
<td>Func-P-GW Trace Config</td>
<td>Call Type</td>
<td>S-GW Trace?</td>
<td>P-GW Trace?</td>
<td>Output</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------</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 26. Signaling Trace File Example (1 of 3)

<<<OUTBOUND 10:04:53:997 Eventid:141005(3)
[MME-S11]GTPv2C Tx FDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x00000453, Message type: EGTP_TRACE_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 43F5

Trace Info:
  Type: 96 Length: 34 Inst: 0
  Value:
    MCC: 123
    MNC: 456
    Trace Id: 03039

  Triggering Event: 1/0: Event shall be traced / not traced.
  MSC Server:
    SS: 0
    HANDOVERS: 0
    LU/IMSI ATT/DET: 0
    MO & MT SMS: 0
    MO & MT CALLS: 0

  MGW:
    CONTEXT: 0

  SGSN:
    MBMS CONTEXT: 0
    RAU/GRS ATT/DET: 0
    MO & MT SMS: 0
    PDP CONTEXT: 0

  GGSN:
    MBMS CONTEXT: 0
    PDP CONTEXT: 0

  MME:
    HANDOVERS: 1
    BEARER ACT/MOD/DET: 1
    UE INIT PDN DISC: 1
    INIT ATT/TAU/DET: 1
    SERVICE REQUEST: 1
    UE INIT PDN CON REQ: 1

335925
Figure 27. Signaling Trace File Example (2 of 3)

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
  ENODEB: 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.
  MSC 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
    Nb-UP: 0
    MC: 0

  SGSN:
    GE: 0
    GS: 0
    MAP-GF: 0
    MAP-GD: 0
    MAP-GR: 0
    GN: 0
    IU: 0
    GB: 0

  GGSN:
    GMB: 0
    GI: 0
    GN: 0
Figure 28. Signaling Trace File Example (3 of 3)

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

BMSC:
    GMB: 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: 6000 2200 2163 5400 3039 0000 0000 0000
    003F 7040 0305 0000 0000 0000 0000 1F00
    6803 0101 0101
Chapter 4
Monitoring the Service

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

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

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

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

Table 20. System Status and Performance Monitoring Commands

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Congestion-Control Information</strong></td>
<td></td>
</tr>
<tr>
<td>View Congestion-Control Statistics</td>
<td>show congestion-control statistics {allmgr</td>
</tr>
<tr>
<td><strong>View GTP Information</strong></td>
<td></td>
</tr>
<tr>
<td>View eGTP-C service statistics for a specific service</td>
<td>show egtpc statistics egtpc-service name</td>
</tr>
<tr>
<td>View eGTP-C service information for a specific service</td>
<td>show egtpc-service name</td>
</tr>
<tr>
<td>View GTP-U service statistics for all GTP-U data traffic on the system</td>
<td>show gtpu statistics</td>
</tr>
<tr>
<td>View eGTP-U service information for a specific service</td>
<td>show gtpu-service name</td>
</tr>
<tr>
<td><strong>View Infrastructure-DNS Queries</strong></td>
<td></td>
</tr>
<tr>
<td>Verify Infrastructure-DNS queries to resolve P-CSCF FQDN</td>
<td>dns-client query client-name client_name query-type AAAA query-name &lt;p-cscf.com&gt;</td>
</tr>
<tr>
<td><strong>View IP Information</strong></td>
<td></td>
</tr>
<tr>
<td>Display BGP Neighbors</td>
<td>context egress_pgw_context_name show ip bgp summary</td>
</tr>
<tr>
<td>Verify BGP neighbors on egress P-GW context</td>
<td>show ip bgp summary</td>
</tr>
<tr>
<td>Verify BGP neighbors on ingress P-GW context</td>
<td>context ingress_pgw_context_name show ip bgp summary</td>
</tr>
<tr>
<td><strong>Display IP Connectivity State</strong></td>
<td></td>
</tr>
<tr>
<td>Verify IP connectivity to the diameter servers for various components/interfaces, all peers should be in OPEN or WAIT_DWR state</td>
<td>show diameter peers full all</td>
</tr>
<tr>
<td><strong>Display IP Interface Status</strong></td>
<td></td>
</tr>
<tr>
<td>Verify IP interfaces are up on each context</td>
<td>show ip interface summary show ipv6 interface summary</td>
</tr>
<tr>
<td><strong>Display IP Pool Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Verify IPv4 pools have been created and are available</td>
<td>context egress_pgw_context_name show ip pool summary</td>
</tr>
<tr>
<td>Verify IPv6 pools have been created and are available</td>
<td>context egress_pgw_context_name show ipv6 pool summary</td>
</tr>
</tbody>
</table>
## Monitoring the Service

### To do this: Enter this command:

<table>
<thead>
<tr>
<th>View SAEGW Service Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View SAEGW service statistics</td>
<td><code>show saegw-service statistics all</code></td>
</tr>
<tr>
<td>Verify SAEGW services</td>
<td>`context saegw_context_name show saegw-service all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View S-GW Service Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View S-GW service statistics</td>
<td><code>show sgw-service statistics all</code></td>
</tr>
<tr>
<td>Verify S-GW services</td>
<td>`show sgw-service all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View P-GW Service Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View P-GW service statistics</td>
<td><code>show pgw-service statistics all</code></td>
</tr>
<tr>
<td>Verify P-GW services</td>
<td>`show pgw-service all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View LMA Service Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View LMA service statistics</td>
<td><code>show lma-service statistics lma-service service_name</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View QoS/QCI Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View QoS Class Index to QoS mapping tables</td>
<td><code>show qci-qos-mapping table all</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View RF Accounting Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm the PGW is sending Rf accounting records:</td>
<td>`show diameter accounting servers</td>
</tr>
<tr>
<td>- Verify “Message sent” is non-zero</td>
<td></td>
</tr>
<tr>
<td>- Verify active charging sessions are present</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Session Subsystem and Task Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Session Subsystem and Task Statistics</td>
<td></td>
</tr>
</tbody>
</table>

### Important: Refer to the *System Software Task and Subsystem Descriptions* appendix in the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.

| View AAA Manager statistics | `show session subsystem facility aaamgr all` |
| View AAA Proxy statistics  | `show session subsystem facility aaaproxy all` |
| View LMA Manager statistics | `show session subsystem facility hamgr all` |
| View MAG Manager statistics | `show session subsystem facility magmgr all` |
| View Session Manager statistics | `show session subsystem facility sessmgr all` |

<table>
<thead>
<tr>
<th>View Session Disconnect Reasons</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View session disconnect reasons with verbose output</td>
<td><code>show session disconnect-reasons</code></td>
</tr>
</tbody>
</table>
### Monitoring the Service

#### Monitoring System Status and Performance

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

#### View Subscriber Information

<table>
<thead>
<tr>
<th>Display NAT Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View the private IP assigned to the NAT user, along with any other public IPs assigned</td>
<td><code>show subscriber full username user_name</code></td>
</tr>
<tr>
<td>View NAT realms assigned to this user</td>
<td>`show subscriber full username user_name</td>
</tr>
<tr>
<td>View active charging flows for a specific NAT IP address</td>
<td><code>show active-charging flows full nat required nat-ip ip_address</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Display Session Resource Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View session resource status</td>
<td><code>show resources session</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Statistics for Subscribers using SAEGW Services on the System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View statistics for subscribers using any SAEGW service on the system</td>
<td><code>show subscribers saegw-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 saegw-service service_name</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Statistics for Subscribers using S-GW Services on the System</th>
<th></th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Statistics for Subscribers using P-GW Services on the System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View statistics for subscribers using any P-GW service on the system</td>
<td><code>show subscribers pgw-only full</code></td>
</tr>
<tr>
<td>View statistics for subscribers using a specific P-GW interface</td>
<td><code>show subscribers pgw-address ip_address</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Statistics for Subscribers using MAG Services on the System</th>
<th></th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Statistics for Subscribers using LMA Services on the System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>View statistics for subscribers using a specific LMA service on the system</td>
<td><code>show subscribers lma-service service_name</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Display Subscriber Configuration Information</th>
<th></th>
</tr>
</thead>
<tbody>
<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>To do this:</td>
<td>Enter this command:</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</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><code>show subscribers all</code></td>
</tr>
<tr>
<td>View a listing of subscribers currently accessing the system</td>
<td><code>show subscribers all</code></td>
</tr>
<tr>
<td>Display UE Attach Status</td>
<td><code>show subscriber pgw-only imsi ue_imsi</code></td>
</tr>
<tr>
<td>Confirm that a UE has attached:</td>
<td>`show active-charging sessions all</td>
</tr>
<tr>
<td>Displays IMSI with one entry for each bearer per APN connection</td>
<td><code>show egtpc peers</code></td>
</tr>
<tr>
<td>Verify active charging sessions are present</td>
<td><code>show egtpc statistics</code></td>
</tr>
<tr>
<td>Verify peers are active. Peers should correspond to S-GW EGTP addresses</td>
<td><code>show gtpu statistics</code></td>
</tr>
<tr>
<td>Verify “Create Session Request” and “Create Session Response” categories are incrementing</td>
<td><code>show lma-service session username user_name</code></td>
</tr>
<tr>
<td>Verify “Total Data Stats:” are incrementing</td>
<td><code>show lma-service statistics</code></td>
</tr>
<tr>
<td>eHRPD:</td>
<td></td>
</tr>
<tr>
<td>Verify lma-sessions are present</td>
<td></td>
</tr>
<tr>
<td>Verify “Binding Updates Received:” categories are incrementing</td>
<td></td>
</tr>
</tbody>
</table>
Clearing Statistics and Counters

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

Statistics and counters can be cleared using the CLI `clear` command. Refer to the Command Line Reference for detailed information on using this command.
Chapter 5
CoA, RADIUS DM, and Session Redirection (Hotlining)

This chapter describes Change of Authorization (CoA), Disconnect Message (DM), and Session Redirect (Hotlining) support in the system. RADIUS attributes, Access Control Lists (ACLs) and filters that are used to implement these features are discussed. 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 this Administration Guide, before using the procedures in this chapter.

Important: Not all functions, commands, and keywords/variables are available or supported for all network function or services. This depends on the platform type and the installed license(s).
RADIUS Change of Authorization and Disconnect Message

This section describes how the system implements CoA and DM RADIUS messages and how to configure the system to use and respond to CoA and DM messages.

CoA Overview

The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session. The filter-id attribute (attribute ID 11) contains the name of an Access Control List (ACL). For detailed information on configuring ACLs, refer to the IP Access Control Lists chapter in the System Administration Guide.

If the system successfully executes a CoA request, a CoA-ACK message is sent back to the RADIUS server and the data filter is applied to the subscriber session. Otherwise, a CoA-NAK message is sent with an error-cause attribute without making any changes to the subscriber session.

**Important:** Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

DM Overview

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

License Requirements

The RADIUS Change of Authorization (CoA) and Disconnect Message (DM) are licensed Cisco features. 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.

Enabling CoA and DM

To enable RADIUS Change of Authorization and Disconnect Message:

**Step 1** Enable the system to listen for and respond to CoA and DM messages from the RADIUS server as described in the Enabling CoA and DM section.

**Step 2** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.
Step 3 View CoA and DM message statistics as described in the Viewing CoA and DM Statistics section.

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. Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

Enabling CoA and DM

Use the following example to enable the system to listen for and respond to CoA and DM messages from the RADIUS server:

```
configure

context <context_name>

radius change-authorize-nas-ip <ipv4/ipv6_address>

end
```

Notes:
- `<context_name>` must be the name of the AAA context where you want to enable CoA and DM.
- For more information on configuring the AAA context, if you are using StarOS 12.3 or an earlier release, refer to the Configuring Context-Level AAA Functionality section of the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.
- A number of optional keywords and variables are available for the `radius change-authorize-nas-ip` command. For more information regarding this command please refer to the Command Line Interface Reference.

CoA and DM Attributes

For CoA and DM messages to be accepted and acted upon, the system and subscriber session to be affected must be identified correctly.

To identify the system, use any one of the following attributes:
- NAS-IP-Address: NAS IP address if present in the CoA/DM request should match with the NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the subscriber session.

To identify the subscriber session, use any one of the following attributes.
- If 3GPP2 service is configured the following attribute is used for correlation identifier:
  - 3GPP2-Correlation-ID: The values should exactly match the 3GPP2-correlation-id of the subscriber session. This is one of the preferred methods of subscriber session identification.
- If 3GPP service is configured the following attributes are used for different identifiers:
  - 3GPP-IMSI: International Mobile Subscriber Identification (IMSI) number should be validated and matched with the specified IMSI for specific PDP context.
- 3GPP-NSAPI: Network Service Access Point Identifier (NSAPI) should match to the NSAPI specified for specific PDP context.
- User-Name: The value should exactly match the subscriber name of the session. This is one of the preferred methods of subscriber session identification.
- Framed-IP-Address: The values should exactly match the framed IP address of the session.
- Calling-station-id: The value should match the Mobile Station ID.

To specify the ACL to apply to the subscriber session, use the following attribute:
- Filter-ID: CoA only. This must be the name of an existing Access Control List. If this is present in a CoA request, the specified ACL is immediately applied to the specified subscriber session. The Context Configuration mode command, `radius attribute filter-id direction`, controls in which direction filters are applied.

The following attributes are also supported:
- Event-Timestamp: This attribute is a timestamp of when the event being logged occurred.
- If 3GPP2 service is configured following additional attributes are supported:
  - 3GPP2-Discard-Reason: This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from the Home Radius server to the PDSN.
  - 3GPP2-Session-Termination-Capability: When CoA and DM are enabled by issuing the radius change-authorize-nas-ip command, this attribute is included in a RADIUS Access-request message to the Home Radius server and contains the value 3 to indicate that the system supports both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute is also included in the RADIUS Access-Accept message and contains the preferred resource management mechanism by the home network, which is used for the session and may include values 1 through 3.

**CoA and DM Error-Cause Attribute**

The Error-Cause attribute is used to convey the results of requests to the system. This attribute is present when a CoA or DM NAK or ACK message is sent back to the RADIUS server.

The value classes of error causes are as follows:
- 0-199, 300-399 reserved
- 200-299 - successful completion
- 400-499 - errors in RADIUS server
- 500-599 - errors in NAS/Proxy

The following error cause is sent in ACK messages upon successful completion of a CoA or DM request:
- 201 - Residual Session Context Removed

The following error causes are sent in NAK messages when a CoA or DM request fails:
- 401 - Unsupported Attribute
- 402 - Missing Attribute
- 403 - NAS Identification Mismatch
- 404 - Invalid Request
- 405 - Unsupported Service
- 406 - Unsupported Extension
- 501 - Administratively Prohibited
- 503 - Session Context Not Found
- 504 - Session Context Not Removable
- 506 - Resources Unavailable

**Viewing CoA and DM Statistics**

View CoA and DM message statistics by entering the following command:

`show session subsystem facility aaamgr`

The following is a sample output of this command.

```
1 AAA Managers

807 Total aaa requests 0 Current aaa requests
379 Total aaa auth requests 0 Current aaa auth requests
0 Total aaa auth probes 0 Current aaa auth probes
0 Total aaa auth keepalive 0 Current aaa auth keepalive
426 Total aaa acct requests 0 Current aaa acct requests
0 Total aaa acct keepalive 0 Current aaa acct keepalive
379 Total aaa auth success 0 Total aaa auth failure
0 Total aaa auth purged 0 Total aaa auth cancelled
0 Total auth keepalive success 0 Total auth keepalive failure
0 Total auth keepalive purged
0 Total aaa auth DMU challenged
367 Total radius auth requests 0 Current radius auth requests
2 Total radius auth requests retried
0 Total radius auth responses dropped
0 Total local auth requests 0 Current local auth requests
12 Total pseudo auth requests 0 Current pseudo auth requests
0 Total null-username auth requests (rejected)
0 Total aaa acct completed 0 Total aaa acct purged
0 Total acct keepalive success 0 Total acct keepalive timeout
```
0 Total acct keepalive purged
0 Total aaa acct cancelled
426 Total radius acct requests
0 Total radius acct requests retried
0 Total radius acct responses dropped
0 Total gtpp acct requests
0 Total gtpp acct cancelled
0 Total null acct requests
0 Total radius acct requests retried
0 Total radius acct responses dropped
0 Total gtpp acct requests
0 Total gtpp acct cancelled
0 Total null acct requests
54 Total aaa acct sessions
3 Total aaa acct archived
0 Current recovery archives
0 Current valid recovery records
2 Total aaa sockets opened
0 Total aaa requests pend socket open
0 Current aaa requests pend socket open
0 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
0 Total aaa radius coa requests
0 Total aaa radius coa acks
0 Total aaa radius coa naks
2 Total radius charg auth
0 Total radius charg auth succ
0 Total radius charg auth purg
0 Total radius charg acct
0 Total radius charg acct succ
0 Total radius charg acct cancel
357 Total gtpp charg
357 Total gtpp charg success
0 Total gtpp charg cancel
0 Total prepaid online requests
0 Total prepaid online requests
0 Total radius charg auth fail
0 Total radius charg auth cancel
0 Total radius charg acct
0 Total radius charg acct purg
0 Current gtpp charg
0 Total gtpp charg failure
0 Total gtpp charg purg
0 Current prepaid online requests
0 Current radius acct requests
0 Current gtpp acct requests
0 Current null acct requests
5 Current aaa acct sessions
0 Current aaa acct archived
0 Current valid recovery records
2 Current aaa sockets open
0 Current radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
0 Current radius charg auth
0 Current radius charg auth fail
0 Current radius charg auth cancel
0 Current radius charg acct
0 Current radius charg acct purg
0 Current gtpp charg
0 Total gtpp charg failure
0 Total gtpp charg purg
0 Current prepaid online requests
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total prepaid online success</td>
<td>0</td>
</tr>
<tr>
<td>Total prepaid online retried</td>
<td>0</td>
</tr>
<tr>
<td>Current prepaid online purged</td>
<td>0</td>
</tr>
<tr>
<td>Total aamgr purged requests</td>
<td>0</td>
</tr>
<tr>
<td>SGSN: Total db records</td>
<td>0</td>
</tr>
<tr>
<td>SGSN: Total sub db records</td>
<td>0</td>
</tr>
<tr>
<td>SGSN: Total mm records</td>
<td>0</td>
</tr>
<tr>
<td>SGSN: Total pdp records</td>
<td>0</td>
</tr>
<tr>
<td>SGSN: Total auth records</td>
<td>0</td>
</tr>
<tr>
<td>Current prepaid online failure</td>
<td>0</td>
</tr>
<tr>
<td>Total prepaid online cancelled</td>
<td>0</td>
</tr>
</tbody>
</table>
Session Redirection (Hotlining)

**Important:** Functionality described for this feature in this segment is not applicable for HNB-GW sessions.

**Overview**

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address. Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) feature.

Note that the session redirection feature is only intended to redirect a very small subset of subscribers at any given time. The data structures allocated for this feature are kept to the minimum to avoid large memory overhead in the session managers.

**License Requirements**

The Session Redirection (Hotlining) 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.

**Operation**

**ACL Rule**

An ACL rule named `readdress server` supports redirection of subscriber sessions. The ACL containing this rule must be configured in the destination context of the user. Only TCP and UDP protocol packets are supported. The ACL rule allows specifying the redirected address and an optional port. The source and destination address and ports (with respect to the traffic originating from the subscriber) may be wildcarded. If the redirected port is not specified, the traffic will be redirected to the same port as the original destination port in the datagrams. For detailed information on configuring ACLs, refer to the IP Access Control Lists chapter in the System Administration Guide. For more information on `readdress server`, refer to the ACL Configuration Mode Commands chapter of the Command Line Interface Reference.

**Redirecting Subscriber Sessions**

An ACL with the `readdress server` rule is applied to an existing subscriber session through CoA messages from the RADIUS server. The CoA message contains the 3GPP2-Correlation-ID, User-Name, Acct-Session-ID, or Framed-IP-Address attributes to identify the subscriber session. The CoA message also contains the Filter-Id attribute which specifies the name of the ACL with the `readdress server` rule. This enables applying the ACL dynamically to existing subscriber sessions. By default, the ACL is applied as both the input and output filter for the matching subscriber unless the Filter-Id in the CoA message bears the prefix `in:` or `out:`.

For information on CoA messages and how they are implemented in the system, refer to the RADIUS Change of Authorization and Disconnect Message section.
Important: Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

Session Limits On Redirection

To limit the amount of memory consumed by a session manager a limit of 2000 redirected session entries per session manager is allocated. This limit is equally shared by the set of subscribers who are currently being redirected. Whenever a redirected session entry is subject to revocation from a subscriber due to an insufficient number of available session entries, the least recently used entry is revoked.

Stopping Redirection

The redirected session entries for a subscriber remain active until a CoA message issued from the RADIUS server specifies a filter that does not contain the readdress server ACL rule. When this happens, the redirected session entries for the subscriber are deleted.

All redirected session entries are also deleted when the subscriber disconnects.

Handling IP Fragments

Since TCP/UDP port numbers are part of the redirection mechanism, fragmented IP datagrams must be reassembled before being redirected. Reassembly is particularly necessary when fragments are sent out of order. The session manager performs reassembly of datagrams and reassembly is attempted only when a datagram matches the redirect server ACL rule. To limit memory usage, only up to 10 different datagrams may be concurrently reassembled for a subscriber. Any additional requests cause the oldest datagram being reassembled to be discarded. The reassembly timeout is set to 2 seconds. In addition, the limit on the total number of fragments being reassembled by a session manager is set to 1000. If this limit is reached, the oldest datagram being reassembled in the session manager and its fragment list are discarded. These limits are not configurable.

Recovery

When a session manager dies, the ACL rules are recovered. The session redirect entries have to be re-created when the MN initiates new traffic for the session. Therefore when a crash occurs, traffic from the Internet side is not redirected to the MN.

AAA Accounting

Where destination-based accounting is implemented, traffic from the subscriber is accounted for using the original destination address and not the redirected address.

Viewing the Redirected Session Entries for a Subscriber

View the redirected session entries for a subscriber by entering the following command:

```
show subscribers debug-info { callid <id> | msid <id> | username <name> }
```

The following command displays debug information for a subscriber with the MSID 000012345:
show subscribers debug-info msid 0000012345

The following is a sample output of this command:

username: user1 callid: 01callbl msid: 0000100003
Card/Cpu: 4/2
Sessmgr Instance: 7
Primary callline:
Redundancy Status: Original Session
Checkpoints Attempts Success Last-Attempt Last-Success
Full: 27 26 15700ms 15700ms
Micro: 76 76 4200ms 4200ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
State Event
SMGR_STATE_OPEN SMGR_EVT_NEWCALL SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED SMGR_STATE_LINE_CONNECTED
SMGR_EVT_LINK_CONTROL_UP SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
Total timer expiry: 0 Total flush (tmr expiry): 0
Total no buffers: 0 Total flush (no buffers): 0
Total flush (queue full): 0 Total flush (out of range): 0
Total flush (svc change): 0 Total out-of-seq pkt drop: 0
    Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
Success: 0 In Progress: 0
Failure (timeout): 0 Failure (no buffers): 0
Failure (other reasons): 0
Redirected Session Entries:

Allowed: 2000 Current: 0
Added: 0 Deleted: 0
Revoked for use by different subscriber: 0

Peer callline:
Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success
Full: 0 0 0ms 0ms
Micro: 0 0 0ms 0ms

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

State Event
SMGR_STATE_OPEN SMGR_EVT_MAKECALL
SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION

username: user1 callid: 01callbl msid: 0000100003
Card/Cpu: 4/2
Sessmgr Instance: 7

Primary callline:
Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success
Full: 27 26 15700ms 15700ms
Micro: 76 76 4200ms 4200ms

Current state: SMGR_STATE_CONNECTED

FSM Event trace:
State Event

SMGR_STATE_OPEN SMGR_EVT_NEWCALL
SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP
SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP

Data Reorder statistics
Total timer expiry: 0 Total flush (tmr expiry): 0
Total no buffers: 0 Total flush (no buffers): 0
Total flush (queue full): 0 Total flush (out of range): 0
Total flush (svc change): 0 Total out-of-seq pkt drop: 0
Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:
Success: 0 In Progress: 0
Failure (timeout): 0 Failure (no buffers): 0
Failure (other reasons): 0

Redirected Session Entries:
Allowed: 2000 Current: 0
Added: 0 Deleted: 0
Revoked for use by different subscriber: 0

Peer callline:

Redundancy Status: Original Session

Checkpoints Attempts Success Last-Atempt Last-Success
Full: 0 0 0ms 0ms
Micro: 0 0 0ms 0ms
Current state: SMGR_STATE_CONNECTED

FSM Event trace:

State Event

SMGR_STATE_OPEN SMGR_EVT_MAKECALL
SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_ADD_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS

Data Reorder statistics

Total timer expiry: 0 Total flush (tmr expiry): 0
Total no buffers: 0 Total flush (no buffers): 0
Total flush (queue full): 0 Total flush (out of range): 0
Total flush (svc change): 0 Total out-of-seq pkt drop: 0
Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:

Success: 0 In Progress: 0
Failure (timeout): 0 Failure (no buffers): 0
Failure (other reasons): 0

Redirected Session Entries:

Allowed: 2000 Current: 0
Added: 0 Deleted: 0
Revoked for use by different subscriber: 0
Chapter 6
Direct Tunnel

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

Products supporting direct tunnel include:

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

**Important:** Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter in the System Administration Guide.

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

This chapter provides the following information:

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

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

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

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

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

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

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

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

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

The following figure illustrates the logic used within the SGSN/S-GW to determine if a direct tunnel will be setup.
Figure 30. Direct Tunneling - Establishment Logic

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

The following configurations are provided in this section:

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

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

By default, direct tunnel support is

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

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

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

Configuring Direct Tunnel Support on the SGSN

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

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

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

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

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

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

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

**Step 5** *(Optional)*
Configure the SGSN to disallow direct tunnel setup to a single GGSN that has been configured to allow it in the APN profile. This command allows the operator to restrict use of a GGSN for any reason, such as load balancing. Refer to the direct-tunnel-disabled-ggsn command in the SGTP Service Configuration Mode chapter of the Command Line Interface Reference.
Step 6  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

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

Enabling Setup of GTP-U Direct Tunnels

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

Example Configuration

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

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

Notes:

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

Enabling Direct Tunnel per APN

In each operator policy, APN profiles are configured to connect to one or more GGSNs and to control the direct tunnel access to that GGSN based on call filtering by APN. Multiple APN profiles can be configured per operator policy. By default, APN-based direct tunnel functionality is allowed so any existing direct tunnel configuration must be removed to return to default and to ensure that the setup has not been restricted.

Example Configuration

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

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

Notes:
- An APN profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the Operator Policy chapter in this guide.

- Direct tunnel is now allowed for the APN but will only setup if also allowed on the RNC.

## Enabling Direct Tunnel per IMEI

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

### Example Configuration

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

```
config

imei-profile <profile_name>

direct-tunnel check-iups-service

end
```

Notes:

- An IMEI profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the Operator Policy chapter in this guide.

- Direct tunnel is now allowed for calls within the IMEI range associated with the IMEI profile but a direct tunnel will only setup if also allowed on the RNC.

## Enabling Direct Tunnel to Specific RNCs

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

### Example Configuration

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

```
config

context <ctx_name>

iups-service <service_name>

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

end

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

Verifying the SGSN Direct Tunnel Configuration

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

Verifying the Operator Policy Configuration

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

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

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

```
[local]asr5x00# show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name : ccprofile1
  Validity : Valid
IMEI Range 99999999999990 to 99999999999995
IMEI Profile Name : imeiprofile1
  Validity : Invalid
APN NI homers1
  APN Profile Name : apnprofile1
  Validity : Valid
APN NI visitors2
  APN Profile Name : apnprofile2
  Validity : Invalid
```

Notes:
Verifying the Call-Control Profile Configuration

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

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

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

Call Control Profile Name = ccprofile1

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

Verifying the APN Profile Configuration

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

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

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

Call Control Profile Name = apnprofile1

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

Verifying the IMEI Profile Configuration

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

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

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

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

Verifying the RNC Configuration

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

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

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

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

Configuring S12 Direct Tunnel Support on the S-GW

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

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the MME over the S3 interface. The MME forwards the FTEID to the S-GW over the S11 interfaces. The S-GW responds with 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
gtpe-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 \texttt{ipv6 address} command.
Chapter 7
GRE Protocol Interface

This chapter provides information on Generic Routing Encapsulation protocol interface support in the GGSN or P-GW service node. 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.

Important: GRE protocol 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.

Important: Commands used in the configuration samples 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.

This chapter discusses following topics for GRE protocol interface support:

- Introduction
- Supported Standards
- Supported Networks and Platforms
- Services and Application on GRE Interface
- How GRE Interface Support Works
- GRE Interface Configuration
- Verifying Your Configuration
Introduction

GRE protocol functionality adds one additional protocol on Cisco’s multimedia core platforms (ASR 5000 or higher) to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiator.

It is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

Figure 31. GRE Interface Deployment Scenario
Supported Standards

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

- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2784, Generic Routing Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE
Supported Networks and Platforms

This feature supports all systems with StarOS Release 9.0 or later running GGSN and/or SGSN service for the core network services. The P-GW service supports this feature with StarOS Release 12.0 or later.
Licenses

GRE protocol 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.
Services and Application on GRE Interface

GRE interface implementation provides the following functionality with GRE protocol support.
How GRE Interface Support Works

The GRE interface provides two types of data processing; one for ingress packets and another for egress packets.

Ingress Packet Processing on GRE Interface

Figure given below provides a flow of process for incoming packets on GRE interface. Note that in case the received packet is a GRE keep-alive or a ping packet then the outer IPV4 and GRE header are not stripped off (or get reattached), but instead the packet is forwarded as is to the VPN manager or kernel respectively. In case of all other GRE tunneled packets the IPV4 and GRE header are stripped off before sending the packet for a new flow lookup.
Figure 32. Ingress Packet Processing on GRE Interface

- Start
- Lookup based on outer DA-SA and is it GRE
  - Yes: Set received tunneled packet flag
  - No: Processing of other type of packets
- Drop packet
- Does received GRE have Sequence Number, CRC or GRE Key?
  - No
  - Yes: Is it a GRE Keepalive?
    - No
    - Yes: Send packet to configured VPN mgr
      - Process the PPB:
        1. Remove the outer IPV4 header and GRE header
        2. Use the VRF number to further lookups.
      - Get Flow Record.
        (Tunnel header and VRF number)
      - Normal flow processing based on inner IP packet, in the VRF indicated by the flow record of previous successful flow record
- Send packet to configured session manager
- Lookup Successful?
  - No: Forwarding lookup in the VRF
    - Is the packet destined to our chassis?
      - No
      - Yes: If tunneled packet flag set, re-attach header and send it to kernel
    - If tunneled packet flag set, re-attach header and send it to kernel
  - Yes: End
Egress Packet Processing on GRE Interface

Figure given below provides a flow of process for outgoing packets on GRE interface:

**Figure 33. Egress Packet Processing on GRE Interface**

1. Start
2. Receive IPV4 packet with correct FLOWID
3. Do a forwarding lookup.
4. If Lookup Successful?
   - Yes: Get Forwarding Record
   - No: Proceed to next step
5. Do a Hash lookup based on SA and DA to get the Tunnel to be used
6. Does it have load balancing enabled?
   - No: Based on Flow record information, prepare the GRE header and outer IPV4 header
   - Yes: Take default route
7. Process the packet as if it was an IPV4 packet received from Session Manager
8. End
GRE Interface Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with GRE interface in GGSN or P-GW services.

**Important:** This section provides the minimum instruction set to enable the GRE Protocol Interface support functionality on a GGSN or P-GW. Commands that configure additional functions for this feature are provided in the Command Line Interface Reference.

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

To configure the system to support GRE tunnel interface:

**Step 1** Configure the virtual routing and forwarding (VRF) in a context by applying the example configurations presented in the Virtual Routing And Forwarding (VRF) Configuration section.

**Step 2** Configure the GRE tunnel interface in a context by applying the example configurations presented in the GRE Tunnel Interface Configuration section.

**Step 3** Enable OSPF for the VRF and for the given network by applying the example configurations presented in the Enabling OSPF for VRF section.

**Step 4** Associate IP pool and AAA server group with VRF by applying the example configurations presented in the Associating IP Pool and AAA Group with VRF section.

**Step 5** Associate APN with VRF through AAA server group and IP pool by applying the example configurations presented in the Associating APN with VRF section.

**Step 6** Optional. If the route to the server is not learnt from the corporate over OSPFv2, static route can be configured by applying the example configurations presented in the Static Route Configuration section.

**Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

**Step 8** Verify configuration of GRE and VRF related parameters by applying the commands provided in the Verifying Your Configuration section of this chapter.

Virtual Routing And Forwarding (VRF) Configuration

This section provides the configuration example to configure the VRF in a context:

```
configure

ccontext <vpn_context_name> -noconfirm

ip vrf <vrf_name>

ip maximum-routes <max_routes>
```
GRE Protocol Interface

GRE Interface Configuration

Notes:
- `<vpn_context_name>` is the name of the system context you want to use for VRF. For more information, refer System Administration Guide.
- A maximum of 100 VRFs in one context and up to 1024 VRFs on one chassis can be configured on system.
- `<vrf_name>` is name of the VRF which is to be associated with various interfaces.
- A maximum of 10000 routes can be configured through `ip maximum-routes <max_routes>` command.

GRE Tunnel Interface Configuration

This section provides the configuration example to configure the GRE tunnel interface and associate a VRF with GRE interface:

```
configure
  context <vpn_context_name>
    ip interface <intfc_name> tunnel
      ip vrf forwarding <vrf_name>
        ip address <internal_ip_address/mask>
        tunnel-mode gre
        source interface <non_tunn_intfc_to_corp>
        destination address <global_ip_address>
        keepalive interval <value> num-retry <retry>
    end
```

Notes:
- `<vpn_context_name>` is the name of the system context you want to use for GRE interface configuration. For more information, refer Command Line Interface Reference.
- A maximum of 511 GRE tunnels + 1 non-tunnel interface can be configured in one context. System needs at least 1 non-tunnel interface as a default.
- `<intfc_name>` is name of the IP interface which is defined as a tunnel type interface and to be used for GRE tunnel interface.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.
- `<internal_ip_address/mask>` is the network IP address with sub-net mask to be used for VRF forwarding.
- `<non_tunn_intfc_to_corp>` is the name a non-tunnel interface which is required by system as source interface and preconfigured. For more information on interface configuration refer System Administration Guide.
- `<global_ip_address>` is a globally reachable IP address to be used as a destination address.
Enabling OSPF for VRF

This section provides the configuration example to enable the OSPF for VRF to support GRE tunnel interface:

```
configure

context <vpn_context_name>

router ospf

ip vrf <vrf_name>

network <internal_ip_address/mask>

end
```

Notes:

- `<vpn_context_name>` is the name of the system context you want to use for OSPF routing. For more information, refer Routing in this guide.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.
- `<internal_ip_address/mask>` is the network IP address with sub-net mask to be used for OSPF routing.

Associating IP Pool and AAA Group with VRF

This section provides the configuration example for associating IP pool and AAA groups with VRF:

```
configure

context <vpn_context_name>

ip pool <ip_pool_name> <internal_ip_address/mask> vrf <vrf_name>

exit

aaa group <aaa_server_group>

ip vrf <vrf_name>

end
```

Notes:

- `<vpn_context_name>` is the name of the system context you want to use for IP pool and AAA server group.
- `<ip_pool_name>` is name of a preconfigured IP pool. For more information refer System Administration Guide.
- `<aaa_server_group>` is name of a preconfigured AAA server group. For more information refer AAA Interface Administration and Reference.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.
- `<internal_ip_address/mask>` is the network IP address with sub-net mask to be used for IP pool.
Associating APN with VRF

This section provides the configuration example for associating an APN with VRF through AAA group and IP pool:

```plaintext
configure
context <vpn_context_name>
apn <apn_name>
    aaa group <aaa_server_group>
    ip address pool name <ip_pool_name>
end
```

Notes:
- `<vpn_context_name>` is the name of the system context you want to use for APN configuration.
- `<ip_pool_name>` is name of a preconfigured IP pool. For more information refer System Administration Guide.
- `<aaa_server_group>` is name of a preconfigured AAA server group. For more information refer AAA Interface Administration and Reference.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.

Static Route Configuration

This section provides the optional configuration example for configuring static routes when the route to the server is not learnt from the corporate over OSPFv2:

```plaintext
configure
context <vpn_context_name>
ip route <internal_ip_address/mask> tunnel <tunnel_intfc_name> vrf <vrf_name>
end
```

Notes:
- `<vpn_context_name>` is the name of the system context you want to use for static route configuration.
- `<internal_ip_address/mask>` is the network IP address with sub-net mask to be used as static route.
- `<tunnel_intfc_name>` is name of a predefined tunnel type IP interface which is to be used for GRE tunnel interface.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.
Verifying Your Configuration

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

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

These instructions are used to verify the GRE interface configuration.

**Step 1** Verify that your interfaces are configured properly by entering the following command in Exec Mode:

```
show ip interface
```

The output of this command displays the configuration of the all interfaces configured in a context.

<table>
<thead>
<tr>
<th>Intf Name</th>
<th>Intf Type</th>
<th>Description</th>
<th>IP State</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Bcast Address</th>
<th>MTU</th>
<th>Resoln Type</th>
<th>ARP timeout</th>
<th>L3 monitor LC-port switchover</th>
<th>Number of Secondary Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo1</td>
<td>Broadcast</td>
<td></td>
<td>UP</td>
<td>1.1.1.1</td>
<td>255.255.255.0</td>
<td>1.1.1.255</td>
<td>1500</td>
<td>ARP</td>
<td>60 secs</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>foo2</td>
<td>Tunnel (GRE)</td>
<td></td>
<td>UP</td>
<td>10.1.1.1</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
<td>ARP</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Intf Name: foo3
Intf Type: Tunnel (GRE)
Description:
IP State: DOWN (<state explaining the reason of being down>)
Step 2  Verify that GRE keepalive is configured properly by entering the following command in Exec Mode:

   show ip interface gre-keepalive

The output of this command displays the configuration of the keepalive for GRE interface configured in a context.
Chapter 8
Gx Interface Support

This chapter provides information on configuring Gx interface to support policy and charging control for subscribers. The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

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 this Administration Guide.

The following topics are covered in this chapter:

- Rel. 6 Gx Interface
- Rel. 7 Gx Interface
- Rel. 8 Gx Interface
- Rel. 9 Gx Interface
- Rel. 10 Gx Interface
- Supported Gx Features
Rel. 6 Gx Interface

Rel. 6 Gx interface support is available on the Cisco ASR chassis running StarOS 8.0 and later releases for the following products:

- GGSN
- IPSG

**Important:** In 14.0 and later releases, Rel. 6 Gx interface functionality is not supported on the chassis.

This section describes the following topics:

- Introduction
- How it Works
- Configuring Rel. 6 Gx Interface

**Introduction**

In GPRS/UMTS networks, the client functionality lies with the GGSN/IPSG, therefore in the IMS authorization scenario it is also called Access Gateway (AGW).

The provisioning of charging rules that are based on the dynamic analysis of flows used for the IMS session is carried out over the Gx interface. In 3GPP, Rel. 6 the Gx is an interface between Access Gateway functioning as Traffic Plane Function (TPF) and the Charging Rule Function (CRF). It is based on the Diameter Base Protocol (DIABASE) and the Diameter Credit Control Application (DCCA) standard. The GGSN/TPF acts as the client while the CRF contains the Diameter server functionality.

The AGW is required to perform query, in reply to which the servers provision certain policy or rules that are enforced at the AGW for that particular subscriber session. The CRF analyzes the IP flow data, which in turn has been retrieved from the Session Description Protocol (SDP) data exchanged during IMS session establishment.

**Important:** In addition to standard Gx interface functionality, the Gx interface implemented here provides support of SBLP with additional AVPs in custom DPCA dictionaries. For more information on customer-specific support contact your Cisco account representative. In view of required flow bandwidth and QoS, the system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. SBLP is based on the dynamic parameters such as the media/traffic flows for data transport, network conditions and static parameters, such as subscriber configuration and category. It also provides Flow-based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage. With this additional functionality, the Cisco Systems Gateway can act as an Enhanced Policy Decision Function (E-PDF).

**Supported Networks and Platforms**

This feature is supported on all chassis with StarOS Release 8.0 or later running GGSN service for the core network services.
License Requirements

The Rel. 6 Gx 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

The Rel 6. Gx interface support is based on the following standards and request for comments (RFCs):

- 3GPP TS 29.210, Charging rule provisioning over Gx interface

<table>
<thead>
<tr>
<th>Important: Note that Charging rule provisioning over Gx interface functionality is not supported in 14.0 and later releases.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- RFC 3588, Diameter Base Protocol; September 2003</td>
</tr>
<tr>
<td>- RFC 4006, Diameter Credit-Control Application; August 2005</td>
</tr>
</tbody>
</table>

In addition to the above RFCs and standards, IMS Authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

How it Works

This section describes the IMS authorization and dynamic policy support in GPRS/UMTS networks.

The following figure and table explain the IMS authorization process between a system and IMS components that is initiated by the MN.

In the case of GGSN, the DPCA is the Gx interface to the Control and Charging Rule Function (CRF). In this context CRF will act as Enhanced Policy Decision Function (E-PDF). The CRF may reside in Proxy-Call Session Control Function (P-CSCF) or on stand-alone system.

The interface between IMSA with CRF is the Gx interface, and between Session Manager and Online Charging Service (OCS) is the Gy interface.

Note that the IMS Authorization (IMSA) service and Diameter Policy Control Application (DPCA) are part of Session Manager on the system, and separated in the following figure for illustration purpose only.
Table 21. Rel. 6 Gx IMS Authorization Call flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IMS subscriber (MN) sends request for primary PDP context activation/creation.</td>
</tr>
<tr>
<td>2</td>
<td>Session manager allocates IP address to MN.</td>
</tr>
<tr>
<td>3</td>
<td>Session manager sends IMS authorization request to IMS Authorization service (IMSA).</td>
</tr>
<tr>
<td>4</td>
<td>IMSA creates a session with the CRF on the basis of CRF configuration.</td>
</tr>
<tr>
<td>5</td>
<td>IMSA sends request to DPCA module to issue the authorization request to selected CRF.</td>
</tr>
<tr>
<td>6</td>
<td>DPCA sends a CCR-initial message to the selected CRF. This message includes the IP address allocated to MN.</td>
</tr>
<tr>
<td>7</td>
<td>CCA message sent to DPCA. If a preconfigured rule set for the PDP context is provided in CRF, it sends that charging rules to DPCA in CCA message.</td>
</tr>
<tr>
<td>8</td>
<td>DPCA module calls the callback function registered with it by IMSA.</td>
</tr>
<tr>
<td>9</td>
<td>After processing the charging rules, IMSA sends Policy Authorization Complete message to session manager.</td>
</tr>
</tbody>
</table>
### Configuring Rel. 6 Gx Interface

To configure Rel. 6 Gx interface functionality:

**Step 1** Configure the IMS Authorization Service at the context level for an IMS subscriber in GPRS/UMTS network as described in the Configuring IMS Authorization Service at Context Level section.

**Step 2** Verify your configuration, as described in the Verifying IMS Authorization Service Configuration section.

**Step 3** Configure an APN within the same context to use the IMS Authorization service for an IMS subscriber as described in the Applying IMS Authorization Service to an APN section.

**Step 4** Verify your configuration as described in the Verifying Subscriber Configuration section.

**Step 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.

### Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization Service at context level for IMS subscribers in GPRS/UMTS networks:

```plaintext
configure

context <context_name>

ims-auth-service <imsa_service_name>
```
p-cscf table { 1 | 2 } row-precedence <precedence_value> { address <ip_address> | ipv6-address <ipv6_address> }

p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus | msisdn-modulus | round-robin } ] | diameter-configured }

policy-control

diameter origin endpoint <endpoint_name>

diameter dictionary <dictionary>

failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } { diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } } [ continue | retry-and-terminate | terminate ]

diameter host-select row-precedence <precedence_value> table { 1 | 2 } host <host_name> [ realm <realm_name> ] [ secondary host <host_name> [ realm <realm_name> ] ]

end

Notes:

- `<context_name>` must be the name of the context where you want to enable IMS Authorization Service.
- `<imsa_service_name>` must be the name of the IMS Authorization Service to be configured for the Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the Command Line Interface Reference for more information on the `p-cscf table` command.

In 18 and later releases, the syntax for `p-cscf table` configuration command is:

```
p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address ipv4_address | ipv6-address ipv6_address [ ipv4-address ipv4_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } ] [ weight value ]
```

- To enable Rel. 6 Gx interface support, specific Diameter dictionary must be configured. For information on the Diameter dictionary to use, contact your Cisco account representative.
- **Optional:** To configure the quality of service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

```
qos-update-timeout <timeout_duration>
```

**Important:** This command is obsolete in release 11.0 and later releases.
• **Optional:** To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

```
signaling-flag { deny | permit }
```

```
signaling-flow permit server-address <ip_address> [ server-port { <port_number> | range <start_number> to <end_number> } ] [ description <string> ]
```

• **Optional:** To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }
```

• **Optional:** To configure the algorithm to select Diameter host table, in the Policy Control Configuration Mode, enter the following command:

```
diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }
```

### Verifying IMS Authorization Service Configuration

To verify the IMS Authorization Service configuration:

**Step 1** Change to the context where you enabled IMS Authorization Service by entering the following command:

```
context <context_name>
```

**Step 2** Verify the IMS Authorization Service’s configurations by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

### Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the Configuring IMS Authorization Service at Context Level section.

```
configure

context <context_name>

apn <apn_name>

ims-auth-service <imsa_service_name>

end
```

**Notes:**

- `<context_name>` must be the name of the context in which the IMS Authorization service was configured.
- `<imsa_service_name>` must be the name of the IMS Authorization Service configured for IMS authentication in the context.
Verifying Subscriber Configuration

Verify the IMS Authorization Service configuration for subscriber(s) by entering the following command:

```
show subscribers ims-auth-service <imsa_service_name>
```

Where `<imsa_service_name>` must be the name of the IMS Authorization Service configured for IMS authentication.
Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR chassis running StarOS 8.1 or StarOS 9.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

- Introduction
- Terminology and Definitions
- How it Works
- Configuring Rel. 7 Gx Interface
- Gathering Statistics

Introduction

For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy, and flow-based charging control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/Cisco Systems GGSN and the Policy and Charging Rules Function (PCRF).

In GPRS/UMTS networks, the client functionality lies with the GGSN, therefore in the IMS authorization scenario it is also called the Gateway. In the following figure, Gateway is the Cisco Systems GGSN, and the PCEF function is provided by Enhanced Charging Service (ECS). The Rel.7. Gx interface is implemented as a Diameter connection. The Gx messages mostly involve installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application. The following figure shows the reference points between various elements involved in the policy and charging architecture.
Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS). The following figure shows the interaction between components within the Gateway.
Supported Networks and Platforms

This feature is supported on all chassis with StarOS Release 8.1 and later running GGSN service for the core network services.

License Requirements

The Rel. 7 Gx 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

The Rel 7. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 7 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer.

Policy control comprises the following functions:

- **Binding**: Binding is the generation of an association between a Service Data Flow (SDF) and the IP CAN bearer (for GPRS a PDP context) transporting that SDF.

  The QoS demand in the PCC rule, as well as the SDF template are input for the bearer binding. The selected bearer will have the same QoS Class as the one indicated by the PCC rule.

  Depending on the type of IP-CAN and bearer control mode, bearer binding can be executed either by the PCRF, or both PCRF and PCEF.

  - For UE-only IP-CAN bearer establishment mode, the PCRF performs bearer binding. When the PCRF performs bearer binding, it indicates the bearer (PDP context) by means of Bearer ID. The Bearer ID uniquely identifies the bearer within the PDP session.
For UE/NW IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services, while the PCEF performs the binding of the PCC rules for the network-controlled services.

Prior to Release 16.0, the rule binding was getting rejected. In 16.0 and later releases, the binding of PCEF rules will be successful when BCM mode is set to UE-only for EPS IP-CAN bearer without “bearer-ID” in the PCRF messages such as RAR or CCA-U.

In the 3G to 4G handover scenario, rule binding and rule removal will be successful in UE-only mode and any filter (and related info) changes because of this modification/installation/removal will not be notified to UE as updates in UE only mode cannot be sent to UE. These rules are only considered for charging and the expectation is that the same rules are again modified in 4G (if handover is done) so that the filters (and related info) can be notified to UE.

- **Gating Control**: Gating control is the blocking or allowing of packets, belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is opened, the packets of the related IP flows are allowed to be forwarded.

- **Event Reporting**: Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF).

  - Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level.

  Note that in 11.0 and later releases, RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS. In earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.

  - The Event Reporting Function (ERF) receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response back to the PCRF. The Event Reporting Function is located in the PCEF.

  In StarOS releases prior to 14.0, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger was sent for rules irrespective of successful installation. In 14.0 and later releases, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger will be sent under the following conditions:

    - When a rule is installed successfully (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).
    - On partial failure, i.e., when two or more rules are installed and at least one of the rules were successfully installed. (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).

  On complete failure, i.e., none of the rules were installed, the event-trigger SUCCESSFULRESOURCE_ALLOCATION (22) will not be sent.

**Important**: In this release, event triggers “IP-CAN_CHANGE” and “MAX_NR_BEARERS_REACHED” are not supported.

- **QoS Control**: QoS control is the authorization and enforcement of the maximum QoS that is authorized for a SDF or an IP-CAN bearer or a QoS Class Identifier (QCI). In case of an aggregation of multiple SDFs (for
GPRS a PDP context), the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate.

- QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.
- The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the Gateway (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network-initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.
- QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorized QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF, the authorized QoS information takes effect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

**Important:** In this release, QoS Resource Reservation is not supported.

Supported Features:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Provisioning of “Authorized QoS” Per IP CAN Bearer: The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF.
- Policy Enforcement for “Authorized QoS” per IP CAN Bearer: The PCEF is responsible for enforcing the policy-based authorization, that is to ensure that the requested QoS is in-line with the “Authorized QoS” per IP CAN Bearer.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
  - Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
  - Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule. If the PCRF provides authorized QoS for both the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.

**Important:** In this release, coordination of authorized QoS scopes in mixed mode (BCM = UE_NW) is not supported.

- Provisioning of Authorized QoS Per QCI: If the PCEF performs the bearer binding, the PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. If the PCRF performs the
bearer binding the PCRF does not provision an authorized QoS per QCI. The PCRF does not provision an authorized QoS per QCI for GBR bearer QCI values.

**Important:** Only standards-based QCI values of 1 through 9 are supported. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 “Policy and charging control architecture”.

- **Policy Enforcement for Authorized QoS per QCI:** The PCEF can receive an authorized QoS per QCI for non-GBR bearer QCI values.
- **Other Features:**
  - **Bearer Control Mode Selection:** The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session modification (as a consequence of an SGSN change). It will be done using the “PCC Rule Request” procedure.
    
    If the Bearer-Control-Mode AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM. The following values are considered for each of the service types:
    
    - **GGSN:** The negotiated value between UE/SGSN/GGSN is considered.
      
      In the following scenarios UE_ONLY is chosen as the BCM:
      
      **Scenario 1:**
      
      - UE-> UE_ONLY
      - SGSN-> UE_ONLY
      - GGSN-> UE_ONLY
      - PCRF-> NO BCM
      
      **Scenario 2:**
      
      - UE-> UE_ONLY
      - SGSN-> UE_ONLY
      - GGSN-> Mixed
      - PCRF-> NO BCM
    
    - **GTP-PGW:** BCM of UE_NW is considered.
    - **IPSG:** BCM of UE_ONLY is considered.
    - **HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA:** BCM of NONE is considered.
    
    - **PCC Rule Error Handling:** If the installation/activation of one or more PCC rules fails, the PCEF includes one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.
      
      If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fails, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.
If a PCC rule was successfully installed/activated, but cannot longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

- **Time of the Day Procedures:** PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

**Important:** In 11.0 and later releases, Rule-Activation-Time / Rule-Deactivation-Time / Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSG time, else the AVP and entire message is rejected. In earlier releases the AVP is successfully parsed only if its value corresponds to a later time than the current IPSG time, else the AVP and entire message is rejected.

In releases prior to 17.0, if “Rule-Deactivation-Time” AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

**Important:** This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx: The Diameter AVP “SN-Firewall-Policy” has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

**Charging Control**

Charging Control is the process of associating packets belonging to a SDF to a charging key, and applying online charging and/or offline charging, as appropriate. Flow-based charging handles differentiated charging of the bearer usage based on real time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, and then no offline charging information is generated.

**Supported Features:**

- Provisioning of Charging-related Information for the IP-CAN Session.
- Provisioning of Charging Addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses or the peer names).
Important: In this release, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

For the purpose of charging correlation between SDF level and application level (for example, IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP-CAN type identifiers are passed from the PCRF to the AF, if such identifiers are available.

For IMS bearer charging, the IP Multimedia Core Network (IM CN) subsystem and the Packet Switched (PS) domain entities are required to generate correlated charging data.

In order to achieve this, the Gateway provides the GGSN Charging Identifier (GCID) associated with the PDP context along with its address to the PCRF. The PCRF in turn sends the IMS Charging Identifier (ICID), which is provided by the P-CSCF, to the Gateway. The Gateway generates the charging records including the GCID as well as the ICID if received from PCRF, so that the correlation of charging data can be done with the billing system.

PCRF also provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF.
  - Select downlink IP CAN bearers based on SDF filters in the PCC rule.
  - Enforce uplink IP flows are transported in the correct IP CAN bearer using the SDF filters within the PCC rule.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be installed, modified, and removed at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.
A third type of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- **Rule Name**: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- **Service Identifier**: The service identifier is used to identify the service or the service component the SDF relates to.
- **Service Data Flow Filter(s)**: The service flow filter(s) is used to select the traffic for which the rule applies.
- **Precedence**: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- **Gate Status**: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- **QoS Parameters**: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), the Allocation and Retention Priority (ARP), and authorized bitrates for uplink and downlink.

**Important**: In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI). Now the entire ARP byte is used for bearer binding (along with QCI). Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled) and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is not supported, so as of now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

- **Charging key (rating group)**
- **Other charging parameters**: The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF will report the usage related to the rule, and so on.

**Important**: In this release, configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

**Important**: ASR5K supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.
In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:
- At IP-CAN session establishment.
- At IP-CAN session modification.

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC rules

The PCRF indicates, via the Rel. 7 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:
- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provision the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:
- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.
- If the PCRF performs the bearer binding, the PCRF may move previously installed or activated PCC rules from one IP CAN bearer to another IP CAN bearer.

**Important:** In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rules report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.
Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

**Selecting a PCC Rule for Uplink IP Packets**

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules.

**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

**Important:** In 11.0 and later releases, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, for two distinct dynamic rules having the same precedence the second rule used to be rejected.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer are discarded.

**Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets**

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules.

**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. The Downlink IP Packet is transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets that do not match any PCC rule of the IP CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Bearer Termination Implications
- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated (for example, for GPRS when the last PDP Context within the IP-CAN session is being terminated) the PCEF contacts the PCRF.
- Request of IP-CAN Bearer Termination: If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF apply the “Request of IP-CAN Session Termination” procedure.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.
The PCEF applies IP CAN specific procedures to terminate the IP CAN session. For GPRS, the GGSN send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP CAN Session Termination” procedure.

In 12.0 and later releases, volume or rule information obtained from PCRF is discarded if the subscriber is going down.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature, which is supported by all products supporting Rel. 7 Gx interface.

License Requirements

The Volume Reporting over Gx 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.

**Important:** In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:


Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

**Important:** Volume Reporting over Gx is applicable only for volume quota.

**Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

**Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

**Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

**Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:
1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.

2. IMSA updates the information to ECS.

3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.

4. For session-level monitoring, the ECS maintains the amount of data usage.

5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the Usage Reporting section.

6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

**Usage Monitoring**

- **Usage Monitoring at Session Level:** PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

  Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

  In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

  - immediate reporting request with monitoring key at rule level
  - immediate reporting request with or without monitoring key at session level
  - explicit disable request at rule level
  - explicit disable request at session level

  In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage
monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.

- **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be the same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- **Usage Monitoring for Dynamic Rules:** If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring key’s usage is reported and the rest of the monitoring keys’ usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring key’s usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys’ usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

### Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.
• **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

• **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

• **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

  Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

• **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

• **Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.**

• **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.
In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

How Rel. 7 Gx Works

This section describes how dynamic policy and charging control for subscribers works with Rel. 7 Gx interface support in GPRS/UMTS networks.

The following figure and table explain the IMSA process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

**Important:** In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.
Figure 37. Rel. 7 Gx IMS Authorization Call Flow

Table 22. Rel. 7 Gx IMS Authorization Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UE (IMS subscriber) requests for primary PDP context activation/creation.</td>
</tr>
<tr>
<td>2</td>
<td>SessMgr allocates an IP address to the UE.</td>
</tr>
<tr>
<td>3</td>
<td>SessMgr requests IMS Authorization, if IMSA is enabled for the APN.</td>
</tr>
<tr>
<td>4</td>
<td>IMSA allocates resources for the IP CAN session and the bearer, and selects the PCRF to contact based on the user's selection key (for example, msisdn).</td>
</tr>
<tr>
<td>5</td>
<td>IMSA requests the DPCA module to issue an auth request to the PCRF.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>6</td>
<td>DPCA sends a CCR initial message to the selected PCRF. This message includes the Context-Type AVP set to PRIMARY and the IP address allocated to the UE. The message may include the Bearer-Usage AVP set to GENERAL. The Bearer-Operation is set to Establishment. The Bearer ID is included if the PCRF does the bearer binding.</td>
</tr>
<tr>
<td>7</td>
<td>PCRF may send preconfigured charging rules in CCA, if a preconfigured rule set for general purpose PDP context is provided in PCRF. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.</td>
</tr>
<tr>
<td>8</td>
<td>DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, eventtriggers, and so on, along with the Bearer ID that corresponds to the rules received from the PCRF to IMSA. IMSA stores the information. If the Bearer ID is absent, and PCRF does the bearer binding, the rule is skipped. Whereas, if the Bearer ID is absent and the PCEF does the bearer binding, the rule is passed onto the ECS to perform bearer binding.</td>
</tr>
<tr>
<td>9</td>
<td>DPCA calls the callback function registered with it by IMSA.</td>
</tr>
<tr>
<td>10</td>
<td>IMSA stores the bearer authorized QoS information and notifies the SessMgr. Other PCRF provided information common to the entire PDP session (event trigger, primary/secondary OCS address, and so on) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.</td>
</tr>
<tr>
<td>11</td>
<td>If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The APN name, primary/secondary OCS server address, and so on are sent to the ECS from the SessMgr.</td>
</tr>
<tr>
<td>12</td>
<td>ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase Id (default rulebase ID from the APN/AAA) and GPRS specific attributes (for example, APN, UMTS QoS, and so on).</td>
</tr>
<tr>
<td>13</td>
<td>OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.</td>
</tr>
<tr>
<td>14</td>
<td>ECS responds to SessMgr with the response message.</td>
</tr>
<tr>
<td>15</td>
<td>SessMgr requests IMSA for the dynamic rules.</td>
</tr>
<tr>
<td>16</td>
<td>IMSA sends the dynamic rules to SessMgr. Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the primary PDP context is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.</td>
</tr>
<tr>
<td>17</td>
<td>SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.</td>
</tr>
<tr>
<td>18</td>
<td>ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.</td>
</tr>
<tr>
<td>19</td>
<td>If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.</td>
</tr>
<tr>
<td>20</td>
<td>Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.</td>
</tr>
<tr>
<td>21</td>
<td>Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).</td>
</tr>
</tbody>
</table>
Configuring Rel. 7 Gx Interface

To configure Rel. 7 Gx interface functionality, the IMS Authorization service must be configured at the context level, and then the APN configured to use the IMS Authorization service.

To configure Rel. 7 Gx interface functionality:

Step 1 Configure IMS Authorization service at the context level for IMS subscriber in GPRS/UMTS network as described in the Configuring IMS Authorization Service at Context Level section.

Step 2 Verify your configuration as described in the Verifying the Configuration section.

Step 3 Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in the Applying IMS Authorization Service to an APN section.

Step 4 Verify your configuration as described in the Verifying Subscriber Configuration section.

Step 5 Optional: Configure the Volume Reporting over Gx feature as described in the Configuring Volume Reporting over Gx section.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

**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.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure

context <context_name>

ims-auth-service <imsa_service_name>

  p-cscf discovery table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }

  p-cscf table { 1 | 2 } row-precedence <precedence_value> { address <ip_address> | ipv6-address <ipv6_address> } [ secondary { address <ip_address> | ipv6-address <ipv6_address> } ]

  policy-control

  diameter origin endpoint <endpoint_name>
```
diameter dictionary <dictionary>

diameter request-timeout <timeout_duration>

diameter host-select table { { { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin } } | prefix-table { 1 | 2 } }

diameter host-select row-precedence <precedence_value> table { { { 1 | 2 } host <host_name> [ realm <realm_id> ] [ secondary host <host_name> [ realm <realm_id> ] ] } | { prefix-table { 1 | 2 } msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to> host <host_name> [ realm <realm_id> ] [ secondary host <sec_host_name> [ realm <secrealm_id> ] algorithm { active-standby | round-robin } ] } } [ -noconfirm ]

diameter host-select reselect subscriber-limit <subscriber_limit> time-interval <duration>

failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } { diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } } { continue | retry-and-terminate | terminate }

end

Notes:
- <context_name> must be the name of the context where you want to enable IMS Authorization service.
- <imsa_service_name> must be the name of the IMS Authorization service to be configured for Rel. 7 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the Command Line Interface Reference for more information on the p-cscf table command.
  
  In 18 and later releases, the syntax for p-cscf table configuration command is:

  p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | secondary { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } [ weight value ]

- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
  
- When configuring the MSISDN prefix range based PCRF selection mechanism:

  To enable the Gx interface to connect to a specific PCRF for a range of subscribers configure msisdn-prefix-from <msisdn_prefix_from> and msisdn-prefix-to <msisdn_prefix_to> with the starting and ending MSISDNs respectively.

  To enable the Gx interface to connect to a specific PCRF for a specific subscriber, configure both msisdn-prefix-from <msisdn_prefix_from> and msisdn-prefix-to <msisdn_prefix_to> with the same MSISDN.

  In StarOS 8.1 and later releases, per MSISDN prefix range table a maximum of 128 rows can be added. In StarOS 8.0 and earlier releases, a maximum of 100 rows can be added.
The MSISDN ranges must not overlap between rows.

- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.

- **Optional:** To configure the Quality of Service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

  ```
  qos-update-timeout <timeout_duration>
  ```

  **Important:** This command is obsolete in release 11.0 and later releases.

- **Optional:** To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

  ```
  signaling-flag { deny | permit }
  signaling-flow permit server-address <ip_address> [ server-port { <port_number> | range <start_number> to <end_number> } ] [ description <string> ]
  ```

- **Optional:** To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

  ```
  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }
  ```

- To configure the PCRF host destinations configured in the GGSN/PCEF, use the `diameter host-select` CLI commands.

- To configure the GGSN/PCEF to use a pre-defined rule when the Gx fails, set the `failure-handling cc-request-type` CLI to `continue`. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

- For provisioning of default charging method, use the following configurations. For this, the AVPs Online and Offline will be sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

  - To send Enable Online:

    ```
    configure
    active-charging service <ecs_service_name>
    charging-action <charging_action_name>
    cca charging credit
    exit
    ```

  - To send Enable Offline:

    ```
    configure
    active-charging service <ecs_service_name>
    rulebase <rulebase_name>
    billing-records rf
    exit
    ```

**Verifying the Configuration**

To verify the IMS Authorization service configuration:
Step 1  Change to the context where you enabled IMS Authorization service by entering the following command:

context <context_name>

Step 2  Verify the IMS Authorization service’s configurations by entering the following command:

show ims-authorization service name <imsa_service_name>

Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the Configuring Rel. 7 Gx Interface section.

configure

    context <context_name>

    apn <apn_name>

    ims-auth-service <imsa_service_name>

    active-charging rulebase <rulebase_name>

    end

Notes:

- <context_name> must be the name of the context in which the IMS Authorization service was configured.
- <imsa_service_name> must be the name of the IMS Authorization service configured for IMS authentication in the context.
- For Rel. 7 Gx, the ECS rulebase must be configured in the APN.
- ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase applies to the entire call. All PDP contexts (bearers) in one call use the same ECS rulebase.
- For predefined rules configured in the ECS, MBR/GBR of a dynamic/predefined rule is checked before it is used for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should have GBR also configured. So for predefined rules, one needs to configure appropriate peak-data-rate, committed-data-rate as per the QCI being GBR QCI or non-GBR QCI. For more information, in the ACS Charging Action Configuration Mode, see the flow limit-for-bandwidth CLI command.
- Provided interpretation of the Gx rulebase is chosen to be ECS group-of-ruledefs, in the Active Charging Service Configuration Mode configure the following command:

policy-control charging-rule-base-name active-charging-group-of-ruledefs

Verifying Subscriber Configuration
Verify the IMS Authorization service configuration for subscriber(s) by entering the following command:

```
show subscribers ims-auth-service <imsa_service_name>
```

<imsa_service_name> must be the name of the IMS Authorization service configured for IMS authentication.

**Configuring Volume Reporting over Gx**

This section describes the configuration required to enable Volume Reporting over Gx.

To enable Volume Reporting over Gx, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
  rulebase <rulebase_name>
    action priority <priority> dynamic-only ruledef <ruledef_name> charging-action <charging_action_name> monitoring-key <monitoring_key>
  exit
  exit
  context <context_name>
    ims-auth-service <imsa_service_name>
    policy-control
      event-update send-usage-report [ reset-usage ]
    end
```

Notes:

- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.

- The `event-update` CLI which enables volume usage report to be sent in event updates is available only in 10.2 and later releases. The optional keyword `reset-usage` enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the usage information as part of event update but not reset at PCEF.

**Gathering Statistics**

This section explains how to gather Rel. 7 Gx 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>
</table>

---

SAE-GW Administration Guide, StarOS Release 17
<table>
<thead>
<tr>
<th>Statistics/Information</th>
<th>Action to perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and statistics specific to policy control in IMS Authorization service.</td>
<td>show ims-authorization policy-control statistics</td>
</tr>
<tr>
<td>Information and statistics specific to the authorization servers used for IMS</td>
<td>show ims-authorization servers ims-auth-service</td>
</tr>
<tr>
<td>Authorization service.</td>
<td></td>
</tr>
<tr>
<td>Information of all IMS Authorization service.</td>
<td>show ims-authorization service all</td>
</tr>
<tr>
<td>Statistics of IMS Authorization service.</td>
<td>show ims-authorization service statistics</td>
</tr>
<tr>
<td>Information, configuration, and statistics of sessions active in IMS Authorization</td>
<td>show ims-authorization sessions all</td>
</tr>
<tr>
<td>service.</td>
<td></td>
</tr>
<tr>
<td>Complete information, configuration, and statistics of sessions active in IMS</td>
<td>show ims-authorization sessions full</td>
</tr>
<tr>
<td>Authorization service.</td>
<td></td>
</tr>
<tr>
<td>Summarized information of sessions active in IMS Authorization service.</td>
<td>show ims-authorization sessions summary</td>
</tr>
<tr>
<td>Complete statistics for active charging service sessions.</td>
<td>show active-charging sessions full</td>
</tr>
<tr>
<td>Information for all rule definitions configured in the service.</td>
<td>show active-charging ruledef all</td>
</tr>
<tr>
<td>Information for all rulebases configured in the system.</td>
<td>show active-charging rulebase all</td>
</tr>
<tr>
<td>Information on all group of ruledefs configured in the system.</td>
<td>show active-charging group-of-ruledefs all</td>
</tr>
<tr>
<td>Information on policy gate counters and status.</td>
<td>show ims-authorization policy-gate {</td>
</tr>
<tr>
<td></td>
<td>counters</td>
</tr>
<tr>
<td>This command is no longer an option in StarOS release 11.0 and beyond.</td>
<td></td>
</tr>
</tbody>
</table>
Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR chassis running StarOS 10.0 or StarOS 11.0 and later releases. This section describes the following topics:

- HAPDSN Rel. 8 Gx Interface Support
- P-GW Rel. 8 Gx Interface Support

HA/PDSN Rel. 8 Gx Interface Support

This section provides information on configuring Rel. 8 Gx interface for HA and PDSN to support policy and charging control for subscribers in CDMA networks.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers in CDMA networks require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this section you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This section describes the following topics:

- Introduction
- Terminology and Definitions
- How it Works
- Configuring HA/PDSN Rel. 8 Gx Interface Support
- Gathering Statistics

Introduction

For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and to do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Gx reference point is located between the Gateway/PCEF and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway/PCEF, and the transmission of traffic plane events from the Gateway/PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application.
The following figure shows the reference points between elements involved in the policy and charging architecture.

**Figure 38. HA/PDSN Rel. 8 Gx PCC Logical Architecture**

Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS).

The following figure shows the interaction between components within the Gateway.

**Figure 39. HA/PDSN Rel. 8 Gx PCC Architecture within PCEF**

License Requirements
The HA/PDSN Rel. 8 Gx 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**

HA/PDSN Rel. 8. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

**Terminology and Definitions**

This section describes features and terminology pertaining to HA/PDSN Rel. 8 Gx functionality.

**Policy Control**

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session.

Policy control comprises the following functions:

- Binding
- Gating Control
- Event Reporting
- QoS Control
- Other Features

**Binding**

In the HA/PDSN Rel. 8 Gx implementation, since there are no bearers within a MIP session the IP-CAN Bearer concept does not apply. Only authorized IP-CAN session is applicable.

**Gating Control**

Gating control is the blocking or allowing of packets belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is open, the packets of the related IP flows are allowed to be forwarded.

**Event Reporting**
**Important:** Unconditional reporting of event triggers from PCRF to PCEF when PCEF has not requested for is not supported.

**Important:** In the HA/PDSN Rel. 8 Gx implementation, only the AN_GW_CHANGE (21) event trigger is supported.

Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF). Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Event trigger reporting from PCEF to PCRF, and provisioning of event triggers happens at IP-CAN session level.

The Event Reporting Function (ERF) located in the PCEF, receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response to the PCRF.

### QoS Control

**Important:** In the HA/PDSN Rel. 8 Gx implementation, only authorized IP-CAN Session is supported.

Provisioning of authorized QoS per IP-CAN bearer, policy enforcement for authorized QoS per QCI, and coordination of authorized QoS scopes in mixed mode are not applicable.

QoS control is the authorization and enforcement of the maximum QoS that is authorized for an SDF. In case of an aggregation of multiple SDFs, the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate. QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.

QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Supported features include:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
- Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
- Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule.

### Other Features

This section describes some of the other features.
PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF communicates the failure to the PCRF by including one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fail, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and includes the Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In the HA/PDSN Gx implementation, the following rule failure codes are supported:

- RATING_GROUP_ERROR (2)
- SERVICE_IDENTIFIER_ERROR (3)
- GW/PCF_MALFUNCTION (4)
- RESOURCES_LIMITATION (5)

If the installation/activation of one or more PCC rules fails during RAR procedure, the RAA command is sent with the Experimental-Result-Code AVP set to DIAMETER_PCC_RULE_EVENT (5142).

Time of the Day Procedures

PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP-CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

When installed, the PCC rule is inactive. If Rule-Activation-Time / Rule-Deactivation-Time is specified, then the PCEF sets the rule active / inactive after that time.

In releases prior to 17.0, if “Rule-Deactivation-Time” AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).

Important: This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx

The Diameter AVP “SN-Firewall-Policy” has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.
Charging Control

**Important:** In the HA/PDSN Rel. 8 Gx implementation, offline charging is not supported.

Charging Control is the process of associating packets belonging to an SDF to a charging key, and applying online charging as appropriate. FBC handles differentiated charging of the bearer usage based on real-time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

Online charging is supported via the Gy interface. In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, then neither online nor offline charging is performed.

Supported Features:

- Provisioning of charging-related information for the IP-CAN Session
- Provisioning of charging addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses)

**Important:** In the HA/PDSN Rel. 8 Gx implementation, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

In the HA/PDSN Rel. 8 Gx implementation, Charging Correlation is not supported. PCRF provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF in case of both uplink and downlink IP flows based on SDF filters in the PCC rule (packet rule matching).
  
  If no PCC rule matches the packet, the packet is dropped.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:
● Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.

● Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

**Important:** A third kind of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

● Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.

● Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.

● Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.

● Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.

● Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.

● QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), and authorized bitrates for uplink and downlink.

● Charging Key (rating group)

● Other charging parameters: The charging parameters define whether online charging interfaces are used, on what level the PCEF will report the usage related to the rule, etc.

**Important:** Configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

**Important:** ASR5K supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW.
After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:
- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:
- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:
- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

**Important:** In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

Selecting a PCC Rule for Uplink IP Packets
If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP-CAN session by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP-CAN session in the order of the precedence of the PCC rules.

**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP-CAN session are discarded.

**Selecting a PCC Rule for Downlink IP Packets**

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP-CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of the IP-CAN session in the order of precedence of the PCC rules.

**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Downlink IP packets that do not match any PCC rule of the IP-CAN session are discarded.

The following procedures are also supported:

- **Indication of IP-CAN Session Termination:** When the IP-CAN session is being terminated the PCEF contacts the PCRF.
- **Request of IP-CAN Session Termination:** If the PCRF decides to terminate an IP-CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP-CAN specific procedures to terminate the IP-CAN session. The HA/PDSN sends a MIP Revocation Request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP-CAN Session Termination” procedure.

- **Use of the Supported-Features AVP during session establishment to inform the destination host about the required and optional features that the origin host supports.**

**How it Works**

This section describes how HA/PDSN Rel. 8 Gx Interface support works.

The following figure and table explain the IMS Authorization process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.
Important: In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 40. HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

Table 24. HA/PDSN Rel. 8 Gx IMS Authorization Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UE (IMS subscriber) requests for MIP Registration Request.</td>
</tr>
<tr>
<td>2</td>
<td>SessMgr allocates an IP address to the UE.</td>
</tr>
<tr>
<td>3</td>
<td>SessMgr requests IMS Authorization, if IMSA is enabled for the subscriber. IMSA service can either be configured in the subscriber template, or can be received from the AAA.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>IMSA allocates resources for the IP-CAN session, and selects the PCRF to contact based on the user's selection key (for example, round-robin).</td>
</tr>
<tr>
<td>5</td>
<td>IMSA requests the DPCA module to issue an auth request to the PCRF.</td>
</tr>
<tr>
<td>6</td>
<td>DPCA sends a CCR initial message to the selected PCRF.</td>
</tr>
<tr>
<td>7</td>
<td>PCRF may send preconfigured charging rules in CCA. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.</td>
</tr>
<tr>
<td>8</td>
<td>DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, etc. IMSA stores the information.</td>
</tr>
<tr>
<td>9</td>
<td>DPCA calls the callback function registered with it by IMSA.</td>
</tr>
<tr>
<td>10</td>
<td>PCRF-provided information common to the entire IP-CAN session (event trigger, primary/secondary OCS address, etc.) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.</td>
</tr>
<tr>
<td>11</td>
<td>If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The primary/secondary OCS server address, etc. are sent to the ECS from the SessMgr.</td>
</tr>
<tr>
<td>12</td>
<td>ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the AAA).</td>
</tr>
<tr>
<td>13</td>
<td>OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.</td>
</tr>
<tr>
<td>14</td>
<td>ECS responds to SessMgr with the response message.</td>
</tr>
<tr>
<td>15</td>
<td>SessMgr requests IMSA for the dynamic rules.</td>
</tr>
<tr>
<td>16</td>
<td>IMSA sends the dynamic rules to SessMgr. Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the MIP session is established, all RAR messages from the PCRF were rejected. Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.</td>
</tr>
<tr>
<td>17</td>
<td>SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.</td>
</tr>
<tr>
<td>18</td>
<td>ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS.</td>
</tr>
<tr>
<td>19</td>
<td>If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.</td>
</tr>
<tr>
<td>20</td>
<td>Depending on the response for the MIP Session Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.</td>
</tr>
</tbody>
</table>
Configuring HA/PDSN Rel. 8 Gx Interface Support

To configure HA/PDSN Rel. 8 Gx Interface functionality:
1. At the context level, configure IMSA service for IMS subscribers as described in the Configuring IMS Authorization Service at Context Level section.
2. Within the same context, configure the subscriber template to use the IMSA service as described in the Applying IMS Authorization Service to Subscriber Template section.
3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

**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.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMSA service at context level for IMS subscribers:

```sh
configure
  context <context_name>

  ims-auth-service <imsa_service_name>

  policy-control
    diameter origin endpoint <endpoint_name>
    diameter dictionary <dictionary>
    diameter request-timeout <timeout_duration>
    diameter host-select table { 1 | 2 } algorithm round-robin
    diameter host-select row-precedence <precedence_value> table { 1 | 2 } host <primary_host_name> [ realm <primary_realm_id> ] [ secondary host <secondary_host_name> [ realm <secondary_realm_id> ] ] [ -noconfirm ]
    failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } { diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } } { continue | retry-and-terminate | terminate }
    exit
  exit

  diameter endpoint <endpoint_name> [ -noconfirm ]

  origin realm <realm_name>
```
Gx Interface Support

Rel. 8 Gx Interface

use-proxy

origin host <host_name> address <ip_address>

no watchdog-timeout

response-timeout <timeout_duration>

connection timeout <timeout_duration>

connection retry-timeout <timeout_duration>

peer <primary_peer_name> [ realm <primary_realm_name> ] address <ip_address> [ port <port_number> ]

peer <secondary_peer_name> [ realm <secondary_realm_name> ] address <ip_address> [ port <port_number> ]

end

Notes:

- `<context_name>` must be the name of the context where you want to enable IMSA service.
- `<imsa_service_name>` must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- To configure the PCRF host destinations configured in the PCEF, use the diameter host-select CLI commands.
- To configure the PCEF to use a pre-defined rule when the Gx fails, set the failure-handling cc-request-type CLI to continue. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

Verifying the IMSA Service Configuration

To verify the IMSA service configuration:

- Change to the context where you enabled IMSA service by entering the following command:
  
  `context <context_name>`

- Verify the IMSA service’s configuration by entering the following command:
  
  `show ims-authorization service name <imsa_service_name>`

Applying IMS Authorization Service to Subscriber Template

After configuring IMSA service at the context-level, within the same context subscriber template must be configured to use the IMSA service for IMS subscribers.

Use the following example to apply IMSA service functionality to subscriber template within the context previously configured in the Configuring IMS Authorization Service at Context Level section.

SAE-GW Administration Guide, StarOS Release 17
configure

context <context_name>

subscriber default

encrypted password <encrypted_password>

ims-auth-service <imsa_service_name>

ip access-group <access_group_name> in

ip access-group <access_group_name> out

ip context-name <context_name>

mobile-ip home-agent <ip_address>

active-charging rulebase <rulebase_name>

end

Notes:

- `<context_name>` must be the name of the context in which the IMSA service was configured.
- `<imsa_service_name>` must be the name of the IMSA service configured for IMS authentication in the context.
- The ECS rulebase must be configured in the subscriber template.
- Provided interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF is chosen to be ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

```
policy-control charging-rule-base-name active-charging-group-of-ruledefs
```

Verifying the Subscriber Configuration

Verify the IMSA service configuration for subscriber(s) by entering the following command in the Exec CLI configuration mode:

```
show subscribers ims-auth-service <imsa_service_name>
```

Notes:

- `<imsa_service_name>` must be the name of the IMSA service configured for IMS authentication.

Gathering Statistics

This section explains how to gather Rel. 8 Gx 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>
</table>

Table 25. Gathering HA/PDSN Rel. 8 Gx Statistics and Information
Statistics/Information | Action to perform
--- | ---
Information and statistics specific to policy control in IMS Authorization service. | show ims-authorization policy-control statistics
Information and statistics specific to the authorization servers used for IMS Authorization service. | show ims-authorization servers ims-auth-service
Information of all IMS Authorization service. | show ims-authorization service all
Statistics of IMS Authorization service. | show ims-authorization service statistics
Information, configuration, and statistics of sessions active in IMS Authorization service. | show ims-authorization sessions all
Complete information, configuration, and statistics of sessions active in IMS Authorization service. | show ims-authorization sessions full
Summarized information of sessions active in IMS Authorization service. | show ims-authorization sessions summary
Complete statistics for active charging service sessions. | show active-charging sessions full
Information for all rule definitions configured in the service. | show active-charging ruledef all
Information for all rulebases configured in the system. | show active-charging rulebase all
Information on all group of ruledefs configured in the system. | show active-charging group-of-ruledefs all
Information on policy gate counters and status. | show ims-authorization policy-gate { counters | status }
This command is no longer an option in StarOS release 11.0 and beyond.

P-GW Rel. 8 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.

- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

**Terminology and Definitions**

This section describes features and terminology pertaining to Rel. 8 Gx functionality.

**Volume Reporting Over Gx**

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

**License Requirements**

The Volume Reporting over Gx 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*.

*Important:* In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

**Supported Standards**

The Volume Reporting over Gx feature is based on the following standard:


**Feature Overview**

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

*Important:* Volume Reporting over Gx is applicable only for volume quota.

*Important:* In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

*Important:* The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.
**Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

**Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the Usage Reporting section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

**Usage Monitoring**

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key:

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level
In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.

- Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys’ usage is reported and the rest of the monitoring keys’ usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys’ usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys’ usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE_REPORT”
trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation timeout set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.
Important: The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).
Rel. 9 Gx Interface

Rel. 9 Gx interface support is available on the Cisco ASR chassis running StarOS 12.2 and later releases.

P-GW Rel. 9 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF reports to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important: ASR5K supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 9 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx 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.

**Important:** In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

**Supported Standards**

The Volume Reporting over Gx feature is based on the following standard:


**Feature Overview**

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

**Important:** Volume Reporting over Gx is applicable only for volume quota.

**Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

**Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

**Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

**Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the Usage Reporting section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP-CAN session.
Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

  Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

  In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

  - immediate reporting request with monitoring key at rule level
  - immediate reporting request with or without monitoring key at session level
  - explicit disable request at rule level
  - explicit disable request at session level

  In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.

  - Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
• Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring key’s usage is reported and the rest of the monitoring keys’ usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring key’s usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys’ usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

• Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

• Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

• IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.
- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF report the accumulated usage for the monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled). This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.

---

**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP-CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx section.

---

**ICSR Support for Volume Reporting over Gx (VoRoGx)**

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.
In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).
Rel. 10 Gx Interface

Rel. 10 Gx interface support is available on the Cisco ASR chassis running StarOS 15.0 and later releases. This section describes the following topics:

- P-GW Rel. 10 Gx Interface Support

P-GW Rel. 10 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Important: ASR5K supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 10 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 10 Volume Reporting over Gx feature.

License Requirements
The Volume Reporting over Gx 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.

**Important:** In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of “Policy Interface” license.

### Supported Standards

The Volume Reporting over Gx feature is based on the following standard:


### Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

**Important:** Volume Reporting over Gx is applicable only for volume quota.

**Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

**Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

**Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

**Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the Usage Reporting section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN
Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

**Usage Monitoring**

- **Usage Monitoring at Session Level:** PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

  In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

  In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

  Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

  In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key:

  - immediate reporting request with monitoring key at rule level
  - immediate reporting request with or without monitoring key at session level
  - explicit disable request at rule level
  - explicit disable request at session level

  In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

  Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

  - **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.

  - **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same...
monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring key’s usage is reported and the rest of the monitoring keys’ usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring key’s usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys’ usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

**Usage Reporting**

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

  For session-level reporting, the actual usage volume is compared with the usage volume threshold.

  For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

  If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

  In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- IP CAN Session Termination: When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the
subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- **Release 12.2 onwards, usage reporting on bearer termination can be added.** When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

  In the case of standard implementation, this must be enabled by CLI configuration.

---

**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP-CAN session and and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the Configuring Volume Reporting over Gx section.

**ICSR Support for Volume Reporting over Gx (VoRoGx)**

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.
To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Use of the Supported-Features AVP on the Gx Interface

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client will, in the first request in a Diameter session indicate the set of features required for the successful processing of the session. If there are features supported by the client that are not advertised as part of the required set of features, the client will provide in the same request this set of optional features that are optional for the successful processing of the session. The server will, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server will support within the same Diameter session. Any further command messages will always be compliant with the list of supported features indicated in the Supported-Features AVPs and features that are not indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported will not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the Gx reference point will be compliant with the requirements for dynamic discovery of supported features and associated error handling.

The base functionality for the Gx reference point is the 3GPP Rel. 7 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the Gx commands. As defined in 3GPP TS 29.229, when extending the application by adding new AVPs for a feature, the new AVPs will have the M bit cleared and the AVP will not be defined mandatory in the command ABNF.

The Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the Gx reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, the Vendor-Id AVP will contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the Gx reference point, the Feature-List-ID AVP will differentiate those lists from one another.

<table>
<thead>
<tr>
<th>Feature bit</th>
<th>Feature</th>
<th>M/O</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Rel8</td>
<td>M</td>
<td>This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits.</td>
</tr>
<tr>
<td>1</td>
<td>Rel9</td>
<td>M</td>
<td>This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.</td>
</tr>
<tr>
<td>3</td>
<td>Rel10</td>
<td>M</td>
<td>This feature indicates the support of base 3GPP Rel-10 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits.</td>
</tr>
<tr>
<td>4</td>
<td>Sponsored Connectivity</td>
<td>O</td>
<td>This feature indicates support for sponsored data connectivity feature. If the PCEF supports this feature, the PCRF may authorize sponsored data connectivity to the subscriber.</td>
</tr>
</tbody>
</table>
In releases prior to 15.0, the Supported-Features AVP was not encoded in CCR-U messages, but it was supported only in CCR-I message. If Rel. 8 dictionary or any dictionary beyond Rel. 8 is used and PCRF does not provide Supported-Features AVP in CCA-I, then the call gets dropped.

In 15.0 and later releases, if PCEF configures Diameter dictionary as release 8, 9 or 10, then PCRF sends Supported-Features AVP so that PCEF will know what feature PCRF supports. If PCEF receives supported features lesser than or greater than requested features then supported feature will be mapped to the lower one.

Whenever the custom dictionary “dpca-custom24” is configured, the Supported-Features AVP including Vendor-Id AVP will be sent in all CCR messages.

**Rule-Failure-Code AVP**

The Rule-Failure-Code AVP indicates the reason that the QoS/PCC rules cannot be successfully installed/activated or enforced. The Rule-Failure-Code AVP is of type Enumerated. It is sent by the PCEF to the PCRF within a Charging-Rule-Report AVP to identify the reason a PCC Rule is being reported.

In releases prior to 15.0, only 11 rule failure codes were defined as the values for this AVP. In 15.0 and later releases, two new rule failure codes INCORRECT_FLOW_INFORMATION (12) and NO_BEARER_BOUND (15) are added. The name of the existing rule failure code 9 is changed to MISSING_FLOW_INFORMATION. For 3GPP Rel. 10, rule failure code 9 maps to GW/PCEF_MALFUNCTION.

**Sponsored Data Connectivity**

With Sponsored Data Connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

Sponsored Data Connectivity feature is introduced in Rel. 10 of 3GPP TS 29.212 specification. If Sponsored Data Connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) who is willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level “SPONSORED_CONNECTIVITY_LEVEL” is added for reporting at Sponsor Connection level and two new AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” have been introduced at the rule level.

Sponsored Data Connectivity will be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the Application Function (AF).

The provisioning of sponsored data connectivity per PCC rule will be performed using the PCC rule provisioning procedure. The sponsor identity will be set using the Sponsor-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. The application service provider identity will be set using the Application-Service-Provider-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. Sponsor-Identity AVP and Application-Service-Provider-Identity AVP will be included if the Reporting-Level AVP is set to the value SPONSORED_CONNECTIVITY_LEVEL.

When receiving the flow based usage thresholds from the AF, the PCRF will use the sponsor identity to generate a monitoring key. The PCRF may also request usage monitoring control, in this case, only the flow based usage is applied for the sponsored data connectivity. If requested, the PCEF may also report the usage to the PCRF.

A new CLI command “diameter encode supported features” has been added in Policy Control Configuration mode to send supported features with Sponsor Identity. For more information on the command, see the Command Line Interface Reference.
Sponsored connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also sponsored connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature will be turned off.

This feature implementation impacts only the Gx dictionary “dpca-custom15”. Also note that this feature is supported only for the dynamic rules.

**Volume Reporting**

For Volume Reporting over Gx, PCRF generates a unique monitoring key based on sponsor identity. Since flows with different monitoring keys are treated differently, flows with sponsor ID are charged differently.
Supported Gx Features

Assume Positive for Gx

In a scenario where both the primary and secondary PCRF servers are overloaded, the PCRF returns an error to P-GW and HSGW. Current behavior for the P-GW and HSGW is to terminate the session if both primary and secondary return a failure or timeout.

This feature is developed to enhance this behavior by applying local policy on the GW to ensure that the subscriber session continues. P-GW / HSGW should implement Assume Positive feature to handle errors and based on the event type implement specific rules.

**Important:** Use of Gx Assume Positive requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The failure handling behavior is enhanced to ensure that the subscriber service is maintained in case of PCRF unavailability. It is also required that the GW reduces the traffic towards the PCRF when receiving a Diameter Too Busy (3004) by stopping the transmission and reception of Diameter messages (CCRs and RARs) to and from the PCRF for a configurable amount of time.

In case of any of the following failures with PCRF, the GW chooses to apply failure handling which results in subscriber termination or to allow browsing without any more policy enforcement.

- TCP link failure
- Application Timer (Tx) expiry
- Result code based failures

In 14.1 and later releases, the PCRF is allowed to fall back to Local Policy for all connection level failures, result code/experimental result code failures. Local Policy may choose to allow the subscriber for a configured amount of time. During this time any subscriber/internal event on the call would be handled from Local Policy. After the expiry of the timer, the subscriber session can be either terminated or else PCRF can be retried. Note that the retry attempt to PCRF happens only when the **timer-expiry event** is configured as **reconnect-to-server**.

The fallback support is added to the failure handling template and the local policy service needs to be associated to IMS Authorization service.

Once the local policy is applied, all PCRF enabled event triggers will be disabled. When the subscriber session is with the local-policy, the GW skips sending of CCR-T and cleans up the session locally.

For a session that was created with active Gx session, the GW sends the CCR-T to primary and on failure sends the CCR-T to the secondary PCRF. If the CCR-T returns a failure from both primary and secondary or times out, the GW cleans up the session locally.

Fallback to Local Policy is done in the following scenarios:

- Tx timer expiry
- Diabase Error
- Result Code Error (Permanent/Transient)
- Experimental Result Code
• Response Timeout

The following points are applicable only in the scenario where reconnect to PCRF is attempted.

• If the subscriber falls back to local-policy because of CCR-I failure, CCR-I will be sent to the PCRF after the timer expiry. On successful CCA-I call will be continued with PCRF or else the call will be continued with local-policy and retry-count will be incremented.

• If the subscriber falls back to local-policy because of the CCR-U failure, IMS Authorization application waits for some event change to happen or to receive an RAR from PCRF.

• In case of event change after the timer expiry, CCR-U will be sent to PCRF. On successful CCA-U message, call will be continued with PCRF or else call will be with local-policy and retry-count will be incremented.

• If RAR is received after the timer-expiry the call will be continued with the PCRF. On expiry of maximum of retries to connect to PCRF, call will be disconnected.

Default Policy on CCR-I Failure

The following parameters are supported for local configuration on P-GW. The configuration parameters are configurable per APN and per RAT Type.

The following fields for a Default Bearer Charging Rule are configurable per APN and per RAT Type:

• Rule Name
• Rating Group
• Service ID
• Online Charging
• Offline Charging
• QCI
• ARP
  • Priority Level
  • QCI
  • QVI
• Max-Requested-Bandwidth
  • UL
  • DL

Flow Description and Flow Status are not configurable but the default value will be set to Any to Any and Flow Status will be set to Enabled.

The following command level fields are configurable per APN and per RAT Type:

• AMBR
  • UL
  • DL
• QCI
• ARP
Gx Back of Functionality

This scenario is applicable when Primary PCRF cluster is unavailable but the secondary PCRF is available to handle new CCR-I messages.

When the chassis receives 3004 result-code then back-off timer will be started for the peer and when the timer is running no messages will be sent to that peer.

The timer will be started only when the value is being configured under endpoint configuration.

Releases prior to 15.0, when the IP CAN session falls back to local policy it remained with local policy until the termination timer expires or the subscriber disconnects. Also, the RAR message received when the local-policy timer was running got rejected with the cause "Unknown Session ID".

In 15.0 and later releases, P-GW/GGSN provides a fair chance for the subscriber to reconnect with PCRF in the event of CCR failure. To support this feature, configurable validity and peer backoff timers are introduced in the Local Policy Service and Diameter endpoint configuration commands. Also, the RAR received when the local-policy timer is running will be rejected with the cause "DIAMETER_UNABLE_TO_DELIVER".

In releases prior to 17.0, rule report was not sent in the CCR messages when PCRF is retried after the expiry of validity timer. In 17.0 and later releases, rule report will be sent to the PCRF during reconnect when the CLI command \texttt{diameter encodeevent-avps local-fallback} is configured under Policy Control Configuration mode.

Support for Volume Reporting in Local Policy

This feature provides support for time based reconnect to PCRF instead of the event based for CCR-U failure scenarios.

In releases prior to 17.0, the following behaviors were observed with respect to the Volume Reporting for Local Policy:

- In the event of CCR-U failure, CCR-U was triggered to PCRF only on receiving subscriber event.
- When a CCR-U failure happened and a call continued without Gx, unreported volume is lost as the threshold is set to infinity. In next CCR-U triggered to PCRF, the cumulative volume was sent to PCRF.
- RAR was rejected with result-code diameter_unable_to_comply (3002) when the validity timer is running.

In 17.0 and later releases, with the timer-based implementation, this feature introduces the following changes to the existing behavior:

- When send-usage-report is configured, the CCR-U with usage report will be sent immediately after the local-policy timer-expiry.
- The unreported usage will not be returned to ECS. Thus, usage since last tried CCR-U will be sent to PCRF.
- RAR will be accepted and the rules received on RAR will be installed even when the timer is running.

Session can be connected to PCRF immediately instead of waiting for subscriber event, and the updated usage report can be sent.

Support for Session Recovery and Session Synchronization

Currently PCRF and ASR5K gateway node are in sync during normal scenarios and when Gx assume positive is not applied. However, there are potential scenarios where the PCRF might have been locally deleted or lost the Gx session.
information and it is also possible that due to the loss of message, gateway node and PCRF can be out of sync on the session state.

While these are rare conditions in the network, the desired behavior is to have PCRF recover the Gx session when it is lost and also to have PCRF and gateway sync the rule and session information. This feature provides functionality to ensure PCRF and gateway can sync on session information and recover any lost Gx sessions. Configuration support has been provided to enable session recovery and session sync features.

In releases prior to 17.0, the implementation is as follows:

- If the PCRF deletes or loses session information during a Gx session update (CCR-U) initiated by the gateway, PCRF will respond back with DIAMETER_UNKNOWN_SESSION_ID resulting in session termination even in the case of CCR-U.
- If the PCRF deletes or loses session information and an Rx message is received, PCRF will not be able to implement corresponding rules and will result in failure of subscriber voice or video calls.
- For subscriber’s existing Rx sessions and active voice/video calls, PCRF will not be able to initiate cleanup of the sessions towards the gateway and can result in wastage of the resources in the network (dedicated bearers not removed) or can result in subscriber not being able to place calls on hold or conference or remove calls from hold.
- For out of sync scenarios, PCRF and gateway could be implementing different policies and can result in wastage of resources or in poor subscriber experience. Existing behavior does not provide for a way to sync the entire session information.

In 17.0 and later releases, the gateway node and PCRF now supports the ability to exchange session information and GW provides the complete subscriber session information to enable PCRF to build the session state. This will prevent the occurrence of the above mentioned scenarios and ensure that GW and PCRF are always in sync. In order to support Gx sync, two new keywords session-recovery and session-sync are added to the diameter encode-supported-features command in Policy Control Configuration mode.

Configuring Gx Assume Positive Feature

To configure Gx Assume Positive functionality:

Step 1 At the global configuration level, configure Local Policy service for subscribers as described in the Configuring Local Policy Service at Global Configuration Level section.

Step 2 At the global configuration level, configure the failure handling template to use the Local Policy service as described in the Configuring Failure Handling Template at Global Configuration Level section.

Step 3 Within the IMS Authorization service, associate local policy service and failure handling template as described in the Associating Local Policy Service and Failure Handling Template section.

Step 4 Verify your configuration as described in the Verifying Local Policy Service Configuration section.

Step 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.
Configuring Local Policy Service at Global Configuration Level

Use the following example to configure Local Policy Service at global configuration level for subscribers:

```
configure

local-policy-service LOCAL_PCC

ruledef 2G_RULE

condition priority 1 apn match .*
exit

ruledef all-plmn

condition priority 1 serving-plmn match .*
exit

actiondef 2G_UPDATE

action priority 1 activate-ambr uplink 18000 downlink 18000

action priority 2 reject-requested-qos
exit

actiondef action1

action priority 2 allow-requested-qos
exit

actiondef allow

action priority 1 allow-session
exit

actiondef delete

action priority 1 terminate-session
exit

actiondef lp_fall

action priority 1 reconnect-to-server
exit

actiondef time

action priority 1 start-timer timer duration 10
exit
```
eventbase default

rule priority 1 event fallback ruledef 2G_RULE actiondef time continue
rule priority 2 event new-call ruledef 2G_RULE actiondef action1
rule priority 3 event location-change ruledef 2G_RULE actiondef action1
rule priority 5 event timer-expiry ruledef 2G_RULE actiondef lp_fall
rule priority 6 event request-qos default-qos-change ruledef 2G_RULE
actiondef allow

end

Notes:
- On occurrence of some event, event will be first matched based on the priority under the eventbase default. For the matched rule and if the corresponding ruledef satisfies, then specific action will be taken.

Configuring Failure Handling Template at Global Configuration Level

Use the following example to configure failure handling template at global configuration level:

```
configure

failure-handling-template <template_name>

msg-type any failure-type any action continue local-fallback

end
```

Notes:
- When the TCP link failure, Application Timer (Tx) expiry, or Result code based failure happens, the associated failure-handling will be considered and if the failure-handling action is configured as local-fallback, then call will fall back to local-fallback mode.

Associating Local Policy Service and Failure Handling Template

Use the following example to associate local policy service and failure handling template:

```
configure

context <context_name>

ims-auth-service <service_name>

associate local-policy-service <lp_service_name>

associate failure-handling <failure-handling-template-name>

end
```

Verifying Local Policy Service Configuration
To verify the local policy service configuration, use this command:

```
show local-policy statistics service <service_name>
```

## Time Reporting Over Gx

This section describes the Time Reporting over Gx feature supported for GGSN in this release.

### License Requirements

No separate license is required for Time Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license. 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.

### Feature Overview

This non-standard Time Usage Reporting over Gx feature is similar to Volume Usage Reporting over Gx. PCRF provides the time usage threshold for entire session or particular monitoring key in CCA or RAR. When the given threshold breached usage report will be sent to PCRF in CCR. This time threshold is independent of data traffic. Apart from the usage threshold breach there are other scenarios where usage report will be send to PCRF.

- **Important:** Time reporting over Gx is applicable only for time quota.
- **Important:** The PCEF only reports the accumulated time usage since the last report for time monitoring and not from the beginning.
- **Important:** If the time usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.
- **Important:** Time usage reporting on bearer termination is supported. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

The following steps explain how Time Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the time monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the time monitoring information from PCRF, the PCEF (ECS) starts tracking the time usage.
4. For session-level monitoring, the ECS maintains the amount of time usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the time usage information per monitoring key.
6. The PCEF continues to track time usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time monitoring does not continue in the PCEF for that IP CAN session.

Limitations

This section lists the limitations for Time Reporting over Gx in this release.

- Only integer monitoring key will be supported like Volume Reporting over Gx
- If the same monitoring key is used for both time and data volume monitoring then disabling monitoring key will disable both time and data usage monitoring.
- If the same monitoring key is used for both time and data usage monitoring and if an immediate report request is received, then both time and volume report of that monitoring key will be sent.

Usage Monitoring

Two levels of time usage reporting are supported:

- Usage Monitoring at Session Level
- Usage Monitoring at Flow Level

Usage Monitoring at Session Level

PCRF subscribes to the session level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL (0).

Usage Monitoring at Flow Level

PCRF subscribes to the flow level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow level monitoring since the rules are associated with the monitoring key and enabling or disabling of usage monitoring at flow level can be controlled by PCRF using it. Usage monitoring is supported for both predefined rules and dynamic rule definition.

Usage Monitoring for Predefined and Static Rules

If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the time being tracked for multiple rules having the same monitoring key. Similarly, usage monitoring information is sent from PCRF for the static rules also.

Usage Monitoring for Dynamic Ruledefs

If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This results in the usage monitoring being done for all the rules associated with that monitoring key.
Usage Reporting

Time usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber usage and checks if the usage threshold provided by PCRF is reached. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "CC-Time" in "Used-Service-Unit" set to track the time usage of the subscriber.

- **Usage Monitoring Disabled:** If PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger.

- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF.

  PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, PCEF sends a CCR with the usage time for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key.

- **PCRF Requested Usage Report:** When PCRF provides the Usage-Monitoring-Information with the Usage-Monitoring-Report set to USAGE_MONITORING_REPORT_REQUIRED, PCEF sends the time usage information. If the monitoring key is provided by PCRF, time usage for that monitoring key is notified to PCRF regardless of usage threshold. If the monitoring key is not provided by PCRF, time usage for all enabled monitoring keys is notified to PCRF.

- **Event Based Reporting:** The event based reporting can be enabled through the CLI command `event-update send-usage-report events`. When an event like gsm change, qos change or revalidation-timeout is configured under this CLI, time usage report is generated whenever that event happens.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track time usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time usage monitoring does not continue in the PCEF for that IP CAN session.

For information on how to configure the Time Reporting over Gx feature, see the Configuring Time Reporting over Gx section.

Configuring Time Reporting over Gx

This section describes the configuration required to enable Time Reporting over Gx.

To enable Time Reporting over Gx, use the following configuration:

```
configure

active-charging service <ecs_service_name>
```
Supported Gx Features

- **rulebase** `<rulebase_name>`
  - **action** **priority** `<priority>` **dynamic-only** **ruledef** `<ruledef_name>` **charging-action** `<charging_action_name>` **monitoring-key** `<monitoring_key>`
  - `exit`
  - `exit`
  - **context** `<context_name>`
    - **ims-auth-service** `<imsa_service_name>`
      - **policy-control**
        - **event-update send-usage-report** [ reset-usage ]
      - `end`

Notes:
- The configuration for enabling Time Reporting over Gx is same as the Volume Reporting over Gx configuration. If a time threshold is received from PCRF then Time monitoring is done, and if a volume threshold is received then Volume monitoring will be done.
- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The `event-update` CLI enables time usage report to be sent in event updates. The optional keyword `reset-usage` enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the time usage information as part of event update but not reset at PCEF.

## Support for Multiple Active and Standby Gx Interfaces to PCRF

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can happen at diabase and application need not select any hosts, this feature is developed to remove the restrictions imposed in the application and allow diabase to pick the peers in a round robin fashion. In addition, this feature will take care of peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command “endpoint-peer-select” as the default behavior is to drop the call if the server discovery fails at application.

When the call is established, IMSA module checks the host selection table/prefix table/host template associated in IMSA service to pick the primary and secondary peers to be contacted. If no host table/prefix table/host template is configured or none of the rows in prefix table are matching or the hosts selected by IMSA are inactive, then based on the CLI configuration the control is given to diabase module which will select the peers in a round robin fashion or terminate the call based on the CLI configuration.

When the CCR message results in a diabase error/Tx expiry/response timeout, then IMSA will let diabase select an alternate route by excluding the peer which resulted in the failure and switch to the peer if the lookup is successful.

When CCR/CCA message is exchanged with the directly connected host selected by diabase and RAR message is received from new host, then IMSA will skip host configuration check and let further communication to happen with the new host. If the directly connected host is selected by application during call establishment, then IMSA will check if the new host is the secondary server per application. When the CCR/CCA message is exchanged with indirectly connected host through DRA which is picked by diabase and RAR message is received from same host through another DRA, then...
IMSA will skip host configuration check and let further communication to happen with the same host through the new DRA. If the DRA is selected by application during call establishment, then IMSA will check if the new DRA is the secondary server per application. Even if RAR message is received from different host though another DRA, IMSA will skip host configuration check and let further communication to happen with the new host through the new DRA.

**Configuring Diameter Peer Selection at Diabase in Failure Scenarios**

The following configuration enables diabase to select the Diameter peers when IMSA fails.

```plaintext
configure
  context context_name
    ims-auth-service service_name
      policy-control
        endpoint-peer-select [ on-host-select-failure | on-inactive-host ]
        { default | no } endpoint-peer-select
    end
```

**Notes:**

- This command is used to perform server selection at diabase when the hosts could not be selected by IMS Authorization application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.
- **on-host-select-failure**: Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.
- **on-inactive-host**: Specifies to perform server selection at diabase when the hosts selected by application are inactive.
- This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at IMS Authorization application.

**Support for Multiple CCR-Uss over Gx Interface**

ASR5K node earlier supported only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update was dropped (like RAT change/ULI change).

In 17.0 and later releases, ASR5K supports multiple CCR-U messages at a time per session through the use of a configurable CLI command “max-outstanding-ccr-u” under IMS Authorization Service configuration mode. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

To support multiple outstanding messages towards PCRF, the following items should be supported:
- Allowing IMSA to send multiple CCR-U messages – This can be achieved through the use of `max-outstanding-ccr-u` command in the IMS Authorization Service configuration mode.

- Queuing of response message for ordering – DPCA should parse the received message irrespective of order in which they are received. IMSA will check whether to forward the response to session manager or queue it locally.

- Peer switch – When multiple CCR-Us are triggered, IMSA will start Tx timer for each request sent out. On first Tx expiry, IMSA/DPCA will do peer switch. That is, IMSA will stop all other requests’ Tx timers and switch to secondary peer (if available) or take appropriate failure handling action.

- Failure handling – On peer switch failure due to Tx expiry, DPCA will take failure handling action based on the configuration present under `ims-auth-service`.

- Handling back pressure – In case of multiple CCR-Us triggered to Primary PCRF and due to Tx timeout all the messages are switched to Secondary PCRF. If Secondary server is already in backpressure state, then IMSA will put first message in the backpressure queue and once after message is processed next pending request will be put into BP queue.

- Volume reporting – In case of multiple CCR-Us for usage report is triggered (for different monitoring keys) and failure handling is configured as “`continue send-ccrt-on-call-termination`”, on first Tx timeout or response timeout, usage report present in all the CCR-Us will be sent to ECS. All the unreported usage will be sent in CCR-T message when the subscriber goes down. If “`event-update send-usage-report`” CLI is present, then there are chances of reporting usage for same monitoring key in multiple CCR-Us.

Though the `max-outstanding-ccr-u` CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

These are the access side updates for which CCR-U might be triggered:

- Bearer Resource Command
- Modify Bearer Request (S-GW change, RAT change, ULI change)
- Modify Bearer Command

These are the following internal updates for which CCR-U is triggered:

- S-GW restoration
- Bearer going down (GGSN, BCM UE_Only)
- ULI/Timezone notification
- Default EPS bearer QoS failure
- APN AMBR failure
- Charging-Rule-Report
- Out of credit / reallocation of credit
- Usage reporting
- Tethering flow detection
- Access network charging identifier

### Configuring Gateway Node to Support Back-to-Back CCR-Us

The following configuration enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

```
configure
```
context context_name

ims-auth-service service_name

policy-control

[ default ] max-outstanding-ccr-u value

end

Notes:
- value must be an integer value from 1 through 12. The default value is 1.

Support for 'RAN/NAS Cause' IE on Gx Interface

New supported feature “Netloc-RAN-NAS-Cause” has been introduced to be in compliance with the Release 12 specification of 3GPP TS 29.212. This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. It requires that the NetLoc feature is also supported.

Important: This feature can be enabled only when the NetLoc feature license is installed.

A new Diameter AVP “RAN-NAS-Release-Cause” will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively, when the NetLoc-RAN-NAS-Cause supported feature is enabled. This AVP will indicate the cause code for the subscriber/bearer termination.

Configuring Supported Feature 'Netloc-RAN-NAS-Cause'

The following configuration enables the supported feature “Netloc-RAN-NAS-Cause”.

configure

context context_name

ims-auth-service service_name

policy-control

diameter encode-supported-features netloc-ran-nas-cause

[ default | no ] diameter encode-supported-features

end

Notes:
- netloc-ran-nas-cause: Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.
- If the supported features “netloc-ran-nas-code” and “netloc” are enabled, then netloc-ran-nas-cause code will be sent to PCRF.
Support ADC Rules over Gx Interface

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard.

ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

**Important:** ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- **TDF-Application-Identifier** – It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.

- **Redirect-Information** – This indicates whether the detected application traffic should be redirected to another controlled address.

- **Mute-Notification** – This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.

- **Application Detection Information** – If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers “APPLICATION_START” and “APPLICATION_STOP” are generated for reporting purpose.

**Limitations**

The limitations for the ADC over Gx feature are:
• ADC does not support group of ruledefs.
• Registration of the duplicate application IDs are not supported.
• Readdress/Redirection for P2P flows will not be supported.
• Redirection happens only on transactions of GET/Response.
• Port based, IP Protocol based, and URL based applications are not supported.
• Pre-configured options (precedence, redirect-server-ip) for dynamic ADC rules are not supported.
• Simultaneous instances of an application for the same subscriber are not distinguished.
• Flow recovery is not supported for application flows.

**Configuring ADC Rules over Gx**

The following configuration enables ADC rules over Gx interface.

```
configure
  context  context_name
    ims-auth-service  service_name
      policy-control
        diameter encode-supported-features adc-rules
          [ default | no ] diameter encode-supported-features
      end
  end
```

**Notes:**

• The keyword “adc-rules” will be available only when the feature-specific license is configured.
• For ADC 6th bit of supported feature will be set.
Chapter 9
Gy Interface Support

This chapter provides an overview of the Gy interface and describes how to configure the Gy interface.

Gy interface support is available on the Cisco system running StarOS 9.0 or later releases for the following products:

- GGSN
- HA
- IPSG
- PDSN
- P-GW

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

This chapter describes the following topics:

- Introduction
- Features and Terminology
- Configuring Gy Interface Support
Introduction

The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

The Gy interface makes use of the Active Charging Service (ACS) / Enhanced Charging Service (ECS) for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Online Charging System (OCS) is the Diameter Credit Control server, which provides the online charging data to the PCEF/GW. With Gy, customer traffic can be gated and billed in an online or prepaid style. Both time- and volume-based charging models are supported. In these models differentiated rates can be applied to different services based on ECS shallow- or deep-packet inspection.

In the simplest possible installation, the system will exchange Gy Diameter messages over Diameter TCP links between itself and one prepay server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

The following figure shows the Gy reference point in the policy and charging architecture.

![PCC Logical Architecture Diagram]

The following figure shows the Gy interface between CTF/Gateway/PCEF/Client running ECS and OCS (CDF/Server). Within the PCEF/GW, the Gy protocol functionality is handled in the DCCA module (at the ECS).
License Requirements

The Gy 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

Gy interface support is based on the following standards:

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

This section describes features and terminology pertaining to Gy functionality.

Charging Scenarios

**Important:** Online charging for events (“Immediate Event Charging” and “Event Charging with Reservation”) is not supported. Only “Session Charging with Reservation” is supported.

Session Charging with Reservation

Session Charging with Unit Reservation is used for credit control of sessions.

Decentralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

Centralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the OCS to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

Decentralized Unit Determination and Decentralized Rating

**Important:** Decentralized Rating is not supported in this release. Decentralized Unit determination is done using CLI configuration.

In this scenario, the CTF requests the OCS to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction of the amount from the subscriber's account is carried out following the conclusion of session establishment.

Basic Operations

**Important:** Immediate Event Charging is not supported in this release. “Reserve Units Request” and “Reserve Units Response” are done for Session Charging and not for Event Charging.

Online credit control uses the basic logical operations “Debit Units” and “Reserve Units”.

- Debit Units Request; sent from CTF to OCS: After receiving a service request from the subscriber, the CTF sends a Debit Units Request to the OCS. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination). For refund purpose, the CTF sends a Debit Units Request to the OCS as well.
Debit Units Response; sent from OCS to CTF: The OCS replies with a Debit Units Response, which informs the CTF of the number of units granted as a result of the Debit Units Request. This includes the case where the number of units granted indicates the permission to render the requested service. For refund purpose, the OCS replies with a Debit Units Response.

Reserve Units Request; sent from CTF to OCS: Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the Reserve Unit Request, and the OCS determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.

Reserve Units Response; sent from OCS to CTF: Response from the OCS which informs the CTF of the number of units that were reserved as a result of the “Reserve Units Request”.

Session Charging with Unit Reservation (SCUR) uses both the “Debit Units” and “Reserve Units” operations. SCUR uses the Session Based Credit Control procedure specified in RFC 4006. In session charging with unit reservation, when the “Debit Units” and “Reserve Units” operations are both needed, they are combined in one message.

**Important:** Cost-Information, Remaining-Balance, and Low-Balance-Indication AVPs are not supported.

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

**Re-authorization**

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer triggers a re-authorization request.

Mid-session service events (re-authorization triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is trigger, the client reports quota usage. The reason for the quota being reported is notified to the server.

**Threshold based Re-authorization Triggers**

The server may optionally include an indication to the client of the remaining quota threshold that triggers a quota re-authorization.

**Termination Action**

The server may specify to the client the behavior on consumption of the final granted units; this is known as termination action.

**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. There are a series of message exchanges 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.

**Important:** Acct-Application-Id is not parsed and if sent will be ignored by the PCEF/GW. In case the Result-Code is not DIAMETER_SUCCESS, the connection to the peer is closed.

- 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 in PCEF/GW and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is taken 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. PCEF/GW only receives this message. 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.

- Tw Timer Expiry Behavior: The connection between the client and the server is taken care by the DIABASE application. When two consecutive Tw timers are expired, the peer state is set to idle and the connection is retried to be established. All the active sessions on the connection are then transferred to the secondary connection if one is configured. All new session activations are also tried on the secondary connection.
  
  There is a connection timeout interval, which is also equivalent to Tw timer, wherein after a CER has been sent to the server, if there is no response received while trying to reestablish connection, the connection is closed and the state set to idle.

**Diameter Credit Control Application**

The Diameter Credit Control Application (DCCA) is a part of the ECS subsystem. For every prepaid customer with Diameter Credit Control enabled, whenever a session comes up, the Diameter server is contacted and quota for the subscriber is fetched.
Quota Behavior

Various forms of quotas are present that can be used to charge the subscriber in an efficient way. Various quota mechanisms provide the end user with a variety of options to choose from and better handling of quotas for the service provider.

Time Quotas

The Credit-Control server can send the CC-Time quota for the subscriber during any of the interrogation of client with it. There are also various mechanisms as discussed below which can be used in conjunction with time quota to derive variety of methods for customer satisfaction.

- Quota Consumption Time: The server can optionally indicate to the client that the quota consumption must be stopped after a period equal to the “Quota Consumption Time” in which no packets are received or at session termination, whichever is sooner. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

If packets are allowed to flow during a CCR (Update)/CCA exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

A locally configurable default value in the client can be used if the server does not send the QCT in the CCA.

- Combinational Quota: Discrete-Time-Period (DTP) and Continuous-Time-Period (CTP) defines mechanisms that extends and generalize the Quota-Consumption-Time for consuming time-quota.
  - Both DTP and CTP uses a “base-time-interval” that is used to create time-envelopes of quota used.
  - Instead of consuming the quota linearly, DTP and CTP consumes the granted quota discretely in chunks of base-time-interval at the start of the each base-time-interval.
  - Selection of one of this algorithm is based on the “Time-Quota-Mechanism” AVP sent by the server in CCA.
  - Reporting usage can also be controlled by Envelope-Reporting AVP sent by the server in CCA during the quota grant. Based on the value of this AVP, the usage can be reported either as the usage per envelope or as usual cumulative usage for that grant.

- Discrete-Time-Period: The base-time-interval defines the length of the Discrete-Time-Period. So each time-envelope corresponds to exactly one Discrete-Time-Period. So when a traffic is detected, an envelope of size equal to Base-Time-Interval is created. The traffic is allowed to pass through the time-envelope. Once the traffic exceeds the base-time-interval another new envelope equal to the base-time-interval is created. This continues till the quota used exceeds the quota grant or reaches the threshold limit for that quota.

- Continuous-Time-Period: Continuous time period mechanism constructs time envelope out of consecutive base-time intervals in which the traffic occurred up to and including a base time interval which contains no traffic. Therefore the quota consumption continues within the time envelope, if there was traffic in the previous base time interval. After an envelope has closed, then the quota consumption resumes only on the first traffic following the closure of the envelope. The envelope for CTP includes the last base time interval which contains no traffic.

The size of the envelope is not constant as it was in Parking meter. The end of the envelope can only be determined retrospectively.
Features and Terminology

- **Quota Hold Time:** The server can specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client understands that the traffic has stopped and the quota is returned to the server. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialized on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

  Alternatively, if this AVP is not present, a locally configurable default value in the client is used. A Quota-Holding-Time value of zero indicates that this mechanism is not used.

- **Quota Validity Time:** The server can optionally send the validity time for the quota during the interrogation with the client. The Validity-Time AVP is present at the MSCC level and applies equally to the entire quota that is present in that category. The quota gets invalidated at the end of the validity time and a CCR-Update is sent to the server with the Used-Service-Units AVP and the reporting reason as VALIDITY_TIME. The entire quota present in that category will be invalidated upon Quota-Validity-Time expiry and traffic in that category will be passed or dropped depending on the configuration, till a CCA-Update is received with quota for that category.

  Validity-Time of zero is invalid. Validity-Time is relative and not absolute.

  In releases prior to 17.0, the AVP “SN-Remaining-Service-Unit” was not sent in the CCR-T and CCR-U messages with reporting Reason FINAL when the FUI action was received as Redirect and the granted units was zero in CCA. In 17.0 and later releases, for the Final-Reporting, the AVP “SN-Remaining-Service-Unit” will be encoded.

  The “SN-Remaining-Service-Unit” AVP behavior is inherited from “Used-Service-Unit” AVP. This Final-Reporting is missing for the Remaining-Service-Unit AVP, which is now incorporated.

**Volume Quota**

The server sends the CC-Total-Octets AVP to provide volume quota to the subscriber. DCCA currently supports only CC-Total-Octets AVP, which applies equally to uplink and downlink packets. If the total of uplink and downlink packets exceeds the CC-Total-Octets granted, the quota is assumed to be exhausted.

If CC-Input-Octets and/or CC-Output-Octets is provided, the quota is counted against CC-Input-Octets and/or CC-Output-Octets respectively.

**Important:** Restricting usages based on CC-Input-Octets and CC-Output-Octets is not supported in this release.

**Units Quota**

The server can also send a CC-Service-Specific-Units quota which is used to have packets counted as units. The number of units per packet is a configurable option.

**Granting Quota**

Gy implementation assumes that whenever the CC-Total-Octets AVP is present, volume quota has been granted for both uplink and downlink.

If the Granted-Service-Unit contains no data, Gy treats it as an invalid CCA.

If the values are zero, it is assumed that no quota was granted.

If the AVP contains the sub AVPs without any data, it is assumed to be infinite quota.
Additional parameters relating to a category like QHT, QCT is set for the category after receiving a valid volume or time grant.

If a default quota is configured for the subscriber, and subscriber traffic is received it is counted against the default quota. The default quota is applicable only to the initial request and is not regranted during the course of the session. If subscriber disconnects and reconnects, the default quota will be applied again for the initial request.

**Requesting Quota**

Quotas for a particular category type can be requested using the Requested-Service-Unit AVP in the CCR. The MSCC is filled with the Rating-Group AVP which corresponds to the category of the traffic and Requested-Service-Unit (RSU) AVP without any data.

The Requested-Service-Unit can contain the CC AVPs used for requesting specific quantity of time or volume grant. Gy CLI can be used to request quota for a category type.

Alternatively quota can also be requested from the server preemptively for a particular category in CCR-I. When the server grants preemptive quota through the Credit control answer response, the quota will be used only when traffic is hit for that category. Quota can be preemptively requested from the Credit Control server from the CLI.

In 12.3 and earlier releases, when no preemptive quota request is present in CCR-I, on hitting server unreachable state for initial request, MSCC AVP with RSU is present in the CCR-I on server retries. Release 14.0 onwards, the MSCC AVP is skipped in the CCR-I on server retries. Corresponding quota usage will be reported in the next CCR-U (MSCC AVP with USU and RSU).

**Reporting Quota**

Quotas are reported to the server for number of reasons including:

- Threshold
- QHT Expiry
- Quota Exhaustion
- Rating Condition Change
- Forced Reauthorization
- Validity Time Expiry
- Final during Termination of Category Instance from Server

For the above cases except for QHT and Final, the Requested-Service-Unit AVP is present in the CCR.

Reporting Reason is present in CCR to let the server know the reason for the reporting of Quota. The Reporting-Reason AVP can be present either in MSCC level or at Used Service Unit (USU) level depending on whether the reason applies to all quotas or to single quota.

When one of these conditions is met, a CCR Update is sent to the server containing a Multiple-Services-Credit-Control AVP(s) indicating the reason for reporting usage in the Reporting-Reason and the appropriate value(s) for Trigger, where appropriate. Where a threshold was reached, the DCCA still has the amount of quota available to it defined by the threshold.

For all other reporting reasons the client discards any remaining quota and either discards future user traffic matching this category or allows user traffic to pass, or buffers traffic according to configuration.

For Reporting-Reason of Rating Condition Change, Gy requires the Trigger Type AVP to be present as part of the CCR to indicate which trigger event caused the reporting and re-authorization request.
For Reporting-Reason of end user service denied, this happens when a category is blacklisted by the credit control server, in this case a CCR-U is sent with used service unit even if the values as zero. When more quota is received from the server for that particular category, the blacklisting is removed.

If a default quota has been set for the subscriber then the usage from the default quota is deducted from the initial GSU received for the subscriber for the Rating Group or Rating Group and Service ID combination.

**Default Quota Handling**

- If default quota is set to 0, no data is passed/reported.
- If default quota is configured and default quota is not exhausted before OCS responds with quota, traffic is passed. Initial default quota used is counted against initial quota allocated. If quota allocated is less than the actual usage then actual usage is reported and additional quota requested. If no additional quota is available then traffic is denied.
- If default quota is not exhausted before OCS responds with denial of quota, gateway blocks traffic after OCS response. Gateway will report usage on default quota even in this case in CCR-U (FINAL) or CCR-T.
- If default quota is consumed before OCS responds, if OCS is not declared dead (see definition in use case 1 above) then traffic is blocked until OCS responds.

**Thresholds**

The Gy client supports the following threshold types:

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

A threshold is always associated with a particular quota and a particular quota type. in the Multiple-Services-Credit-Control AVP, the Time-Quota-Threshold, Volume-Quota-Threshold, and Unit-Quota-Threshold are optional AVPs.

They are expressed as unsigned numbers and the units are seconds for time quota, octets for volume quota and units for service specific quota. Once the quota has reached its threshold, a request for more quotas is triggered toward the server. User traffic is still allowed to flow. There is no disruption of traffic as the user still has valid quota.

The Gy sends a CCR-U with a Multiple-Services-Credit-Control AVP containing usage reported in one or more User-Service-Unit AVPs, the Reporting-Reason set to THRESHOLD and the Requested-Service-Unit AVP without data.

When quota of more than one type has been assigned to a category, each with its own threshold, then the threshold is considered to be reached once one of the unit types has reached its threshold even if the other unit type has not been consumed.

When reporting volume quota, the DCCA always reports uplink and downlink separately using the CC-Input-Octets AVP and the CC-Output-Octets AVP, respectively.

On receipt of more quotas in the CCA the Gy discard any quota not yet consumed since sending the CCR. Thus the amount of quota now available for consumption is the new amount received less any quota that may have been consumed since last sending the CCR.

**Conditions for Reauthorization of Quota**

Quota is re-authorized/requested from the server in case of the following scenarios:

- Threshold is hit
- Quota is exhausted
• Validity time expiry
• Rating condition change:
  • Cellid change: Applicable only to GGSN and P-GW implementations.
  • LAC change: Applicable only to GGSN and P-GW implementations.
  • QoS change
  • RAT change
  • SGSN/Serving-Node change: Applicable only to GGSN and P-GW implementations.

**Discarding or Allowing or Buffering Traffic to Flow**

Whenever Gy is waiting for CCA from the server, there is a possibility of traffic for that particular traffic type to be encountered in the Gy. The behavior of what needs to be done to the packet is determined by the configuration. Based on the configuration, the traffic is either allowed to pass or discarded or buffered while waiting for CCA from the server.

This behavior applies to all interrogation of client with server in the following cases:

• No quota present for that particular category
• Validity timer expiry for that category
• Quota exhausted for that category
• Forced Reauthorization from the server

In addition to allowing or discarding user traffic, there is an option available in case of quota exhausted or no quota circumstances to buffer the traffic. This typically happens when the server has been requested for more quota, but a valid quota response has not been received from the server, in this case the user traffic is buffered and on reception of valid quota response from the server the buffered traffic is allowed to pass through.

**Procedures for Consumption of Time Quota**

• QCT is zero: When QCT is deactivated, the consumption is on a wall-clock basis. The consumption is continuous even if there is no packet flow.

• QCT is active: When QCT is present in the CCA or locally configured for the session, then the consumption of quota is started only at the time of first packet arrival. The quota is consumed normally till last packet arrival plus QCT time and is passed till the next packet arrival.

  If the QCT value is changed during intermediate interrogations, then the new QCT comes into effect from the time the CCA is received. For instance, if the QCT is deactivated in the CCA, then quota consumptions resume normally even without any packet flow. Or if the QCT is activated from deactivation, then the quota consumption resume only after receiving the first packet after CCA.

• QHT is zero: When QHT is deactivated, the user holds the quota indefinitely in case there is no further usage (for volume quota and with QCT for time quota). QHT is active between the CCA and the next CCR.

• QHT is non-zero: When QHT is present in CCA or locally configured for the session, then after a idle time of QHT, the quota is returned to the server by sending a CCR-Update and reporting usage of the quota. On receipt of CCR-U, the server does not grant quota. QHT timer is stopped on sending the CCR and is restarted only if QHT is present in the CCA.

  QHT timer is reset every time a packet arrives.

**Envelope Reporting**
The server may determine the need for additional detailed reports identifying start time and end times of specific activity in addition to the standard quota management. The server controls this by sending a CCA with Envelope-Reporting AVP with the appropriate values. The DCCA client, on receiving the command, will monitor for traffic for a period of time controlled by the Quota-Consumption-Time AVP and report each period as a single envelope for each Quota-Consumption-Time expiry where there was traffic. The server may request envelope reports for just time or time and volume. Reporting the quota back to the server, is controlled by Envelope AVP with Envelope-Start-Time and Envelope-End-Time along with usage information.

**Credit Control Request**

Credit Control Request (CCR) is the message that is sent from the client to the server to request quota and authorization. CCR is sent before the establishment of MIP session, and at the termination of the MIP session. It can be sent during service delivery to request more quotas.

- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

  If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.

- Credit Control Answer - Terminate (CCA-T)

In releases prior to 16.0, CCR-T was immediately sent without waiting for CCA-U if the call was cleared and there was a pending CCA-U. In 16.0 and later releases, if call is cleared when there is a pending update, the gateway will wait for CCA-U to arrive or timeout to happen (whichever happens first).

The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.
The following figure depicts the call flow for a simple call request in the HA Gy implementation.
 Tx Timer Expiry Behavior

A timer is started each time a CCR is sent out from the system, and the response has to arrive within Tx time. The timeout value is configurable in the Diameter Credit Control Configuration mode.

In case there is no response from the Diameter server for a particular CCR, within Tx time period, and if there is an alternate server configured, the CCR is sent to the alternate server after Tw expiry as described in “Tw Timer expiry behavior” section.

It also depends on the Credit-Control-Session-Failover AVP value for the earlier requests. If this AVP is present and is coded to FAILOVER_SUPPORTED then the credit-control message stream is moved to the secondary server, in case it is configured. If the AVP value is FAILOVER_NOT_SUPPORTED, then the call is dropped in case of failures, even if a secondary server is configured.

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, containers are closed only after CCA-U is received successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

Redirection

In the Final-Unit-Indication AVP, if the Final-Action is REDIRECT or Redirect-Server AVP is present at command level, redirection is performed.

The redirection takes place at the end of consumption of quota of the specified category. The GY sends a CCR-Update without any RSU or Rating-Group AVP so that the server does not give any more quotas.

If the Final-Action AVP is RESTRICT_ACCESS, then according to the settings in Restriction-Filter-Rule AVP or Filter-Id AVP, GY sends CCR-Update to the server with used quota.
Triggers

The Diameter server can provide the triggers for which the client should reauthorize a particular category. The triggers can be configured locally as well but whatever trigger is present in the CCA from the server will have precedence.

**Important:** In this release, Gy triggers are not supported for HA.

The trigger types that are supported are:

- SGSN/Serving-Node Change
- QoS Change - Any
- RAT Change
- LAC Change
- CellID Change

On any event as described in the Trigger type happens, the client reauthorizes quota with the server. The reporting reason is set as RATING_CONDITION_CHANGE.

Tariff Time Change

The tariff change mechanism applies to each category instance active at the time of the tariff change whenever the server indicated it should apply for this category.

The concept of dual coupon is supported. Here the server grants two quotas, which is accompanied by a Tariff-Time-Change, in this case the first granted service unit is used until the tariff change time, once the tariff change time is reached the usage is reported up to the point and any additional usage is not accumulated, and then the second granted service unit is used.

If the server expects a tariff change to occur within the validity time of the quota it is granting, then it includes the Tariff-Time-Change AVP in the CCA. The DCCA report usage, which straddles the change time by sending two instances of the Used-Service-Unit AVP, one with Tariff-Change-Usage set to UNIT_BEFORE_TARIFF_CHANGE, and one with Tariff-Change-Usage set to UNIT_AFTER_TARIFF_CHANGE, and this independently of the type of units used by application. Both Volume and Time quota are reported in this way.

The Tariff time change functionality can as well be done using Validity-Time AVP, where in the Validity-Time is set to Tariff Time change and the client will reauthorize and get quota at Validity-Time expiry. This will trigger a lot of reauthorize request to the server at a particular time and hence is not advised.

Tariff-Time-Usage AVP along with the Tariff-Time-Change AVP in the answer message to the client indicates that the quotas defined in Multiple-Services-Credit-Control are to be used before or after the Tariff Time change. Two separate quotas are allocated one for before Tariff-Time-Change and one for after Tariff-Time-Change. This gives the flexibility to the operators to allocate different quotas to the users for different periods of time. In this case, the DCCA should not send the Before-Usage and After-Usage counts in the update messages to the server. When Tariff-Time-Change AVP is present without Tariff-Time-Usage AVP in the answer message, then the quota is used as in single quota mechanism and the client has to send before usage and after usage quotas in the updates to the server.

**Important:** In this release, Gy does not support UNIT_INDETERMINATE value.

Final Unit Indication
The Final-Unit-Indication AVP can be present in the CCA from the server to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP needs to be taken.

**Final Unit Indication at Command Level**

Gy currently does not support FUI AVP at command level. If this AVP is present at command level it is ignored. If the FUI AVP is present at command level and the Final-Unit-Action AVP set to TERMINATE, Gy sends a CCR-Terminate at the expiry of the quota, with all quotas in the USU AVP.

> **Important:** FUI AVP at command level is only supported for Terminate action.

**Final Unit Indication at MSCC Level**

If the Final-Unit-Indication AVP is present at MSCC level, and if the Final-Unit-Action AVP is set to TERMINATE, a CCR-Update is sent at the expiry of the allotted quota and report the usage of the category that is terminated.

For information on redirection cases refer to Redirection section.

**Credit Control Failure Handling**

CCFH AVP defines what needs to be done in case of failure of any type between the client and the server. The CCFH functionality can be defined in configuration but if the CCFH AVP is present in the CCA, it takes precedence. CCFH AVP gives flexibility to have different failure handling.

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

**CCFH with Failover Supported**

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the following behavior takes place:

- **Terminate:** On any Tx expiry for the CCR-I the message is discarded and the session is torn down. In case of CCR-Updates and Terminates the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is torn down.
- **Continue:** On any Tx expiry, the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is still established, but without quota management.
- **Retry and Terminate:** On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

**CCFH with Failover Not Supported**

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to FAILOVER_NOT_SUPPORTED, the following behavior takes place as listed below. Same is the case if there is no secondary server configured on the system.

- **Terminate:** On any Tx expiry, the session is taken down.
- Continue: On any Tx expiry, the session is still established, but without quota management.
- Retry and Terminate: On any Tx expiry, the session is taken down.

**Failover Support**

The CC-Session-Failover AVP and the Credit-Control-Failure-Handling (CCFH) AVP may be returned by the CC server in the CCA-I, and are used by the DCCA to manage the failover procedure. If they are present in the CCA they override the default values that are locally configured in the system.

If the CC-Session-Failover is set to FAILOVER_NOT_SUPPORTED, a CC session will never be moved to an alternative Diameter Server.

If the value of CC-Session-Failover is set to FAILOVER_SUPPORTED, then the Gy attempts to move the CC session to the alternative server when it considers a request to have failed, i.e:

- On receipt of result code “DIAMETER_UNABLE_TO_DELIVER”, “DIAMETER_TOO_BUSY”, or “DIAMETER_LOOP_DETECTED”.
- On expiry of the request timeout.
- On expiry of Tw without receipt of DWA, if the server is connected directly to the client.

The CCFH determines the behavior of the client in fault situations. If the Tx timer expires then based on the CCFH value the following actions are taken:

- CONTINUE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). Note that quota management of other categories is not affected.
- TERMINATE: Terminate the MIP session, which affects all categories.
- RETRY_AND_TERMINATE: Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). The client retries to send the CCR when it determines a failure-to-send condition and if this also fails, the MIP session is then terminated.

After the failover action has been attempted, and if there is still a failure to send or temporary error, depending on the CCFH action, the following action is taken:

- CONTINUE: Allow the MIP session to continue.
- TERMINATE: Terminate the MIP session.
- RETRY_AND_TERMINATE: Terminate the MIP session.

**Recovery Mechanisms**

DCCA supports a recovery mechanism that is used to recover sessions without much loss of data in case of Session Manager failures. There is a constant check pointing of Gy data at regular intervals and at important events like update, etc.

For more information on recovery mechanisms, please refer to the *System Administration Guide*.

**Error Mechanisms**

Following are supported Error Mechanisms.

**Unsupported AVPs**

All unsupported AVPs from the server with “M” bit set are ignored.

**Invalid Answer from Server**
If there is an invalid answer from the server, Gy action is dependent on the CCFH setting:

- In case of continue, the MIP session context is continued without further control from Gy.
- In case of terminate and retry-and-terminate, the MIP session is terminated and a CCR-T is sent to the diameter server.

**Result Code Behavior**

- **DIAMETER_RATING_FAILED**: On reception of this code, Gy discards all traffic for that category and does not request any more quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_END_USER_SERVICE_DENIED**: On reception of this code, Gy temporarily blacklists the category and further traffic results in requesting new quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_CREDIT_LIMIT_REACHED**: On reception of this code, Gy discards all traffic for that category and waits for a configured time, after which if there is traffic for the same category requests quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE**: On reception of this code, Gy allows the session to establish, but without quota management. This is supported only at the command level and not at the MSCC level.
- **DIAMETER_USER_UNKNOWN**: On reception of this code, DCCA does not allow the credit control session to get established, the session is terminated. This result code is supported only at the command level and not at the MSCC level.

For all other permanent/transient failures, Gy action is dependent on the CCFH setting.

**Supported AVPs**

The Gy functionality supports the following AVPs:

- Supported Diameter Credit Control AVPs specified in RFC 4006:
  - **CC-Input-Octets (AVP Code: 412)**: Gy supports this AVP only in USU.
  - **CC-Output-Octets (AVP Code: 414)**: Gy supports this AVP only in USU.
  - **CC-Request-Number (AVP Code: 415)**
  - **CC-Request-Type (AVP Code: 416)**: Gy currently does not support EVENT_REQUEST value.
  - **CC-Service-Specific-Units (AVP Code: 417)**
  - **CC-Session-Failover (AVP Code: 418)**
  - **CC-Time (AVP Code: 420)**: Gy does not support this AVP in RSU.
  - **CC-Total-Octets (AVP Code: 421)**: Gy does not support this AVP in RSU.
  - **Credit-Control-Failure-Handling (AVP Code: 427)**
  - **Final-Unit-Action (AVP Code: 449)**
Supported at Multiple-Services-Credit-Control grouped AVP level and not at command level.

- Final-Unit-Indication (AVP Code: 430):
  Fully supported at Multiple-Services-Credit-Control grouped AVP level and partially supported (TERMINATE) at command level.
- Granted-Service-Unit (AVP Code: 431)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Multiple-Services-Indicator (AVP Code: 455)
- Rating-Group (AVP Code: 432)
- Redirect-Address-Type (AVP Code: 433):
  Gy currently supports only URL (2) value.
- Redirect-Server (AVP Code: 434)
- Redirect-Server-Address (AVP Code: 435)
- Requested-Service-Unit (AVP Code: 437)
- Result-Code (AVP Code: 268)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Subscription-Id (AVP Code: 443)
- Subscription-Id-Data (AVP Code: 444)
- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):
  Gy does NOT support UNIT_INDETERMINEATE (2) value.
- Tariff-Time-Change (AVP Code: 451)
- Used-Service-Unit (AVP Code: 446):
  Gy sends only incremental counts for all the AVPs from the last CCA-U.
- User-Equipment-Info (AVP Code: 458)
- User-Equipment-Info-Type (AVP Code: 459):
  Gy currently supports only IMEISV value.
  Cisco GGSN and P-GW support IMEISV by default.
- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)

- Supported 3GPP specific AVPs specified in 3GPP TS 32.299:
  - 3GPP-Charging-Characteristics (AVP Code: 13)
  - 3GPP-Charging-Id (AVP Code: 2)
  - 3GPP-GGSN-MCC-MNC (AVP Code: 9)
  - 3GPP-GPRS-QoS-Negotiated-Profile (AVP Code: 5)
  - 3GPP-IMSI-MCC-MNC (AVP Code: 8)
  - 3GPP-NSAPI (AVP Code: 10)
- 3GPP-PDP-Type (AVP Code: 3)
- 3GPP-RAT-Type (AVP Code: 21)
- 3GPP-Selection-Mode (AVP Code: 12)
- 3GPP-Session-Stop-Indicator (AVP Code: 11)
- 3GPP-SGSN-MCC-MNC (AVP Code: 18)
- 3GPP-User-Location-Info (AVP Code: 22)
- Base-Time-Interval (AVP Code: 1265)
- Charging-Rule-Base-Name (AVP Code: 1004)
- Envelope (AVP Code: 1266)
- Envelope-End-Time (AVP Code: 1267)
- Envelope-Reporting (AVP Code: 1268)
- Envelope-Start-Time (AVP Code: 1269)
- GGSN-Address (AVP Code: 847)
- Offline-Charging (AVP Code: 1278)
- PDP-Address (AVP Code: 1227)
- PDP-Context-Type (AVP Code: 1247)
  
  This AVP is present only in CCR-I.
- PS-Information (AVP Code: 874)
- Quota-Consumption-Time (AVP Code: 881):
  
  This optional AVP is present only in CCA.
- Quota-Holding-Time (AVP Code: 871):
  
  This optional AVP is present only in the CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.
- Reporting-Reason (AVP Code: 872):
  
  Gy currently does not support the POOL_EXHAUSTED (8) value. It is used in case of credit-pooling which is currently not supported.
- Service-Information (AVP Code: 873):
  
  Only PS-Information is supported.
- SGSN-Address (AVP Code: 1228)
- Time-Quota-Mechanism (AVP Code: 1270):
  
  The Gy server may include this AVP in an Multiple-Services-Credit-Control AVP when granting time quota.
- Time-Quota-Threshold (AVP Code: 868)
- Time-Quota-Type (AVP Code: 1271)
- Trigger (AVP Code: 1264)
- Trigger-Type (AVP Code: 870)
- Unit-Quota-Threshold (AVP Code: 1226)
- Volume-Quota-Threshold (AVP Code: 869)
Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
- Auth-Application-Id (AVP Code: 258)
- Destination-Host (AVP Code: 293)
- Destination-Realm (AVP Code: 283)
- Disconnect-Cause (AVP Code: 273)
- Error-Message (AVP Code: 281)
- Event-Timestamp (AVP Code: 55)
- Failed-AVP (AVP Code: 279)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Origin-Host (AVP Code: 264)
- Origin-Realm (AVP Code: 296)
- Origin-State-Id (AVP Code: 278)
- Redirect-Host (AVP Code: 292)
- Redirect-Host-Usage (AVP Code: 261)
- Redirect-Max-Cache-Time (AVP Code: 262)
- Rating-Group (AVP Code: 432)
- Result-Code (AVP Code: 268)
- Route-Record (AVP Code: 282)
- Session-Id (AVP Code: 263)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.
- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control
Features and Terminology

- Currency-Code (AVP Code: 425)
- Direct-Debiting-Failure-Handling (AVP Code: 428)
- Exponent (AVP Code: 429)
- G-S-U-Pool-Identifier (AVP Code: 453)
- G-S-U-Pool-Reference (AVP Code: 457)
- Requested-Action (AVP Code: 436)
- Service-Parameter-Info (AVP Code: 440)
- Service-Parameter-Type (AVP Code: 441)
- Service-Parameter-Value (AVP Code: 442)
- Unit-Value (AVP Code: 424)
- Value-Digits (AVP Code: 447)

- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Acct-Application-Id (AVP Code: 259)
  - Error-Reporting-Host (AVP Code: 294)
  - Experimental-Result (AVP Code: 297)
  - Experimental-Result-Code (AVP Code: 298)
  - Proxy-Host
  - Proxy-Info
  - Proxy-State

- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:
  - 3GPP-CAMEL-Charging-Info (AVP Code: 24)
  - 3GPP-MS-TimeZone (AVP Code: 23)
  - 3GPP-PDSN-MCC-MNC
  - Authorised-QoS
  - Access-Network-Information
  - Adaptations
  - Additional-Content-Information
  - Additional-Type-Information
  - Address-Data
  - Address-Domain
  - Addressee-Type
  - Address-Type
  - AF-Correlation-Information
  - Alternate-Charged-Party-Address
  - Application-provided-Called-Party-Address
  - Application-Server
- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applc-Info
- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type
- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type
- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initiation-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):
  The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.
- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
• Recipient-SCCP-Address
• Refund-Information
• Remaining-Balance
• Reply-AppId
• Reply-Path-Requested
• Requested-Party-Address
• Role-of-node
• SDP-Answer-Timestamp
• SDP-Media-Component
• SDP-Media-Description
• SDP-Media-Name
• SDP-Offer-Timestamp
• SDP-Session-Description
• SDP-TimeStamp
• Served-Party-IP-Address
• Service-Generic-Information
• Service-ID
• Service-Specific-Data
• Service-Specific-Info
• Service-Specific-Type
• SIP-Method
• SIP-Request-Timestamp
• SIP-Response-Timestamp
• SM-Discharge-Time
• SM-Message-Type
• SM-Protocol-Id
• SMSC-Address
• SMS-Information
• SMS-Node
• SM-Status
• SM-User-Data-Header
• Submission-Time
• Talk-Burst-Exchange
• Talk-Burst-Time
PLMN and Time Zone Reporting

For some implementations of online charging, the OCS requires the PCEF to reporting location-specific subscriber information. For certain subscriber types, subscriber information such as PLMN, Time Zone, and ULI can be sent over the Gy interface as the subscriber changes location, time zone, and serving networks to provide accurate online charging services. Such information can be reported independently from time and volume-based reporting.

PLMN and Time Zone Reporting feature is enabled to support location event reporting based on triggers from Gx, when the following conditions are met:

- Session-based Gy is not initiated due to the absence of charging-actions in rulebase with Credit-Control enabled or due to delayed Gy session initiation.
- PLMN and Time Zone Reporting feature is either enabled in the credit control group or through the use of triggers received from Gx.

If session-based Gy initiation fails or the session goes offline due to configuration or network issues, event-based Gy session will not be initiated.

**Important:** Note that the failure-handling will not be supported for event-based Gy.

Though, in event-based Gy, multiple events can be reported independently and simultaneously this is presently not supported. If an event occurs when the CCA-Event (CCA-E) of the previously reported event is awaited, then the new event is queued and reported only when a CCA-E is received or the message is timed out.

To enable the PLMN and Time Zone Reporting feature, the PCRF shall send the Trigger AVP (Trigger Type 1, Trigger Type 2) at the command level in a CCA.

The Event-based Gy session will be terminated in the following scenarios:
• On termination of the bearer/subscriber (subscriber level Gy).
• Initiation of session-based Gy session (delayed session initiation).
• Once the CCR-E transaction is complete and there are no further events to report.

For information on how to configure this feature, refer to the Gy Interface Support chapter in the administration guide for the product that uses the Gy interface functionality.

Interworking between Session-based Gy and Event-based Gy

If both session-based Gy and event-based Gy mode are activated, then session-based Gy will take precedence i.e. all the events will be reported through CCR-U if the corresponding triggers are enabled. Event-based Gy mode will be active only when session-based Gy has been disabled and has never been activated previously for this session during its lifetime.

OCS Unreachable Failure Handling Feature

The OCS Unreachable Failure Handling feature is required to handle when OCS goes down or unavailable. This feature is otherwise noted as Assume Positive for Gy.

The OCS is considered unavailable/unreachable in the following scenarios:

• PCEF transmits a CCR-U or CCR-I message but no response is received before the specified timeout
• Diameter Watchdog request times out to the current RDR, causing the TCP connection state to be marked down
• Diameter command-level error codes received in a CCA
• If the PCEF is unable to successfully verify transmission of a CCR-T, the PCEF will not assign interim quota, because the user has disconnected.

In 15.0 and later releases, the error result codes can be configured using the CLI command servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [ to-end-result-code ] } } to trigger the server unreachable mode. The same is applicable for the update request also. For more information on the CLI command, see the Credit Control Configuration Mode Commands chapter of the Command Line Interface Reference. However, if the CLI command no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [ to-end-result-code ] } is configured, then the default set of hard-coded error codes are applicable.

The default set is:

• UNABLE_TO_DELIVER 3002
• UNABLE_TOO_BUSY 3004
• LOOP_DETECTED 3005
• ELECTION_LOST 4003

Permanent failures 5001-5999 except 5002, 5003 and 5031.

In 12.2 and later releases, existing failure handling mechanism is enhanced such that the subscriber can be allowed to browse for a pre-configured amount of interim-volume and/or interim-time if OCS becomes unreachable due to transport connection failure or gives an impression that OCS is unreachable owing to slow response for Diameter request messages.
The purpose of this feature is to support Gy based data sessions in the event of an OCS outage. Diameter client allows the user's data session to continue for some fixed quota and then retries the OCS server to restore normal functionality. This feature adds more granularity to the existing failure handling mechanism.

With the implementation of this feature, Gy reporting during outages is supported. A temporary time and/or volume quota is assigned to the user in the event of an OCS outage which will be used during the outage period.

When the OCS returns to service, the GW reports all used quota back to OCS and continues with normal Gy reporting.

For each DCCA-service, CLI control is available for the following options:

- Interim quota volume (in bytes) and quota time (seconds). Both values will apply simultaneously, if configured together and if either quota time or quota volume is exhausted, the Diameter client retries the OCS.

- Option to limit the number of times a session can be assigned a temporary quota. If the user exceeds this amount, the session will be terminated/converted to postpaid.

The quota value is part of the dcca-service configuration, and will apply to all subscribers using that dcca-service. The temporary quota will be specified in volume (bytes) and/or time (seconds) to allow enforcement of both quota tracking mechanisms individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the GW retries the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS.

In the event that the OCS services have not been restored, the GW re-allocates the configured amount of quota and/or time to the user. The GW reports all accumulated used data back to OCS when OCS is back online. If multiple retries and interallocation occur, the GW reports quota used during all allocation intervals. This cycle will continue until OCS services have been successfully restored, or the maximum number of quota assignments has been exhausted.

Support for OCS unreachable CLI commands is added under Diameter Credit Control Configuration mode.

For the P-GW/XGW/GGSN, this behavior will apply to all APNs and subscribers that have online charging enabled by the PCRF. In the HA, this behavior will apply to all users that have online charging enabled by the AAA. Settings will be applied to the dcca-service.

In Release 15.0, the following enhancements are implemented as part of the Assume Positive Gy feature:

- Configurable per error code treatment to enter assume positive mode
- Graceful session restart upon receipt of a 5002 error

**Important:** Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

**Configurable per Error Code Treatment**

This feature allows the customers to configure error result codes using the CLI command “servers-unreachable behavior-triggers” that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported.

Any error result codes from the range 3xxx to 5xxx can be specified using the CLI commands. This feature has been implemented to provide more flexibility and granularity in the way assume positive mode is triggered for error result codes.

**Graceful Session Restart**

Graceful session restart upon receipt of a 5002 error code is supported for server retried CCR-U messages during assume positive state. Also, any unreported usage from the time, server retried CCR-U sent till CCA-I is received, will be reported immediately by triggering CCR-U with usages for the same.
**Important:** Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Any pending updates are aborted once CCA-U with 5002 is received from the server. Also CCR-U is triggered immediately following session restart only if there are any unreported usages pending.

**Important:** When the server responds with 5002 error result code, it does not include any granted service units for the requested rating groups.

For more information on the commands introduced in support of this feature, see the Credit Control Configuration Mode Command chapter in the Command Line Interface Reference.

### Backpressure Handling

Diameter base (Diabase) maintains an outbound stream. When an application wants to write a message into a socket, the message handle of those messages are stored in the outbound stream. Only on receiving the response to the corresponding request, the stored message handle is removed from the outbound stream. In order to rate-limit the message transactions based on the responses received from the server, ASR5k maintains a limit on the number of messages stored in the outbound stream. This is done using "max-outstanding <>" CLI (default value is 256). If the number of messages created by the application exceeds the max-outstanding limit, diabase sends a 'Backpressure' indication to the application to wait till it receives a decongestion indication from diabase to try again.

On receiving a response from the server, the corresponding request message handle will be removed from the outbound stream, creating a slot for another message to be written by the application. In order to intimate this slot availability, decongestion notification is sent to the registered application. The application in turn loops through all sessions and processes the pending trigger to be sent.

When the application loops through the sessions in the system, it traverse the sessions in a sorted order and checks each session whether it has to send a pending CCR-Initial or CCR-Terminate or CCR-Update. When the first session gets the slot to fill the outbound stream, it writes the message into the stream. Now the slot gets back into filled state, reaching the max-outstanding limit again. So the rest of the sessions will still continue to be in backpressed state.

Backpressured request like Credit-Control-Initial and Credit-Control-Terminate are given higher priority over Credit-Control-Update as they are concerned with the creation or termination of a session. So on top of the decongestion notification, DCCA has some internal timers which periodically try to send the message out. So in case of heavy backpressure condition, the probability of CCR-I or CCR-T being sent out is more than CCR-U.

### Gy Backpressure Enhancement

This feature facilitates maintaining a list of DCCA sessions that hit backpressure while creating a message i.e., backpressured list, eliminating the current polling procedure. This will maintain a single queue for all types of messages (CCR-I, CCR-U, CCR-T, CCR-E) that are backpressured. The messages will be sent in FIFO order from the queue.

After processing a session from the backpressure queue DCCA will check for the congestion status of the peer and continue only if the peer has empty slots in the outstanding message queue to accommodate further CCRs.

Releases prior to 16.0, the gateway has a max-outstanding configuration to manage a number of messages that are waiting for response from OCS. When the max-outstanding is configured to a low value, then the frequency to be in congested state is very high.

CPU utilization is very high if the max-outstanding count is low and network is congested.
In 16.0 and later releases, all DCCA sessions associated with the CCR messages that are triggered BACKPRESSURE (when max-outstanding has been reached) will be queued in backpressure list which is maintained per ACS manager instance (credit-control) level.

This list will not have any specific configurable limits on the number of sessions that will be queued in it. This is because there is an inherent limit that is already present which is dependent on the number of subscriber/DCCA sessions.

With this new separate backpressed list, CPU utilization will come down under high backpressure case.

**CC based Selective Gy Session Control**

This section describes the overview and implementation of the Selective Gy Session Control feature based on Charging Characteristics (CC) profile of the subscriber.

This section discusses the following topics for this feature:

- Feature Description
- Configuring CC based Selective Gy Session Control
- Monitoring and Troubleshooting the Selective Gy Session Control Feature

**Feature Description**

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. In Release 17, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The `cc profile cc-profile-index prepaid prohibited` CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging characteristic is selected and used. If there is no matching charging characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.
Relationships to Other Features

This feature can also be used when the CC profile configuration is enabled through the GGSN service. When the CC profile is configured under APN service and GGSN service, the prepaid prohibited configuration for the matching CC profile is applied irrespective of the services.

Limitations

The following are the limitations of this feature:

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session-setup. Once the credit-control-group is selected (after session setup), this feature is not applicable.

Configuring CC based Selective Gy Session Control

The following sections provide the configuration commands to configure the Gy Session Control feature based on the CC profile of the subscriber.

Configuring CC Value

The following commands are used to configure Charging Characteristic values as postpaid/prepaid to disable/enable Gy session towards the OCS.

```plaintext
configure
context context_name

apn apn_name

    cc-profile { cc_profile_index | any } { prepaid-prohibited | credit-control-group cc_group_name }

end
```

Notes:

- `cc_profile_index`: Specifies the CC profile index. `cc_profile_index` must be an integer from 0 through 15.
- `any`: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring “any” CLI command will not override other specific configurations under APN.
- `prepaid-prohibited`: Disables prepaid Gy session for the configured profile index.
- `cc_group_name`: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- `no cc-profile cc_profile_index`: This command falls back to “any” cc-profile behavior irrespective of the CC profile index value configured.

Verifying the Selective Gy Session Control Configuration
Use the following command in Exec mode to display/verify the configuration of Selective Gy Session Control feature.

\[ \text{show configuration} \]

**Monitoring and Troubleshooting the Selective Gy Session Control Feature**

This section provides information regarding show commands and/or their outputs in support of the Selective Gy Session Control Feature

**show active-charging sessions**

The “Credit-Control” field that appears as part of the \[ \text{show active-charging sessions \{ callid | imsi | msisdn \} } \] command output enables the user to determine the credit control state as “On” for online charging enabled session or “Off” for prepaid prohibited session and monitor the subscriber session.
# Configuring Gy Interface Support

To configure Gy interface support:

**Step 1** Configure the core network service as described in this Administration Guide.

**Step 2** Configure Gy interface support as described in the relevant section:
- Configuring GGSN/P-GW/IPSG Gy Interface Support
- Configuring HA/PDSN Gy Interface Support

**Step 3** Configure Event-based Gy support as described in the Configuring PLMN and Time Zone Reporting section.

**Step 4** Optional. Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in the Configuring Server Unreachable Feature section.

**Step 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.

## Configuring GGSN / P-GW / IPSG Gy Interface Support

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

```plaintext
configure
   context <context_name>
      diameter endpoint <endpoint_name>
         origin realm <realm>
         origin host <diameter_host> address <ip_address>
         peer <peer> realm <realm> address <ip_address>
      exit
   exit
   active-charging service <ecs_service_name>
   credit-control [ group <cc_group_name> ]
      diameter origin endpoint <endpoint_name>
```

---

**SAE-GW Administration Guide, StarOS Release 17**
diameter peer-select peer <peer> realm <realm>
diameter pending-timeout <timeout_period>
diameter session failover
diameter dictionary <dictionary>
failure-handling initial-request continue
failure-handling update-request continue
failure-handling terminate-request continue
exit
exit
context <context_name>
apn <apn_name>
  selection-mode sent-by-ms
  ims-auth-service <service>
ip access-group <access_list_name> in
ip access-group <access_list_name> out
ip context-name <context_name>
active-charging rulebase <rulebase_name>
credit-control-group <cc_group_name>
end

Notes:
- For information on configuring IP access lists, refer to the Access Control Lists chapter in the System Administration Guide.
- For more information on configuring ECS ruledefs, refer to the ACS Ruledef Configuration Mode Commands chapter in the Command Line Interface Reference.
- For more information on configuring ECS charging actions, refer to the ACS Charging Action Configuration Mode Commands chapter in the Command Line Interface Reference.
- For more information on configuring ECS rulebases, refer to the ACS Rulebase Configuration Mode Commands chapter in the Command Line Interface Reference.

Configuring HA / PDSN Gy Interface Support

To configure HA / PDSN Gy interface support, use the following configuration:
configure

context <context_name>

diameter endpoint <endpoint_name>

  origin realm <realm>

  origin host <diameter_host> address <ip_address>

  peer <peer> realm <realm> address <ip_address>

exit

exit

active-charging service <ecs_service_name>

ruledef <ruledef_name>

  ip any-match = TRUE

exit

charging-action <charging_action_name>

  content-id <content_id>

  cca charging credit rating-group <rating_group>

exit

rulebase <rulebase_name>

  action priority <action_priority> ruledef <ruledef_name> charging-action <charging_action_name>

exit

credit-control [ group <cc_group_name> ]

diameter origin endpoint <endpoint_name>

diameter peer-select peer <peer> realm <realm>

diameter pending-timeout <timeout>

diameter session failover

diameter dictionary <dictionary>

failure-handling initial-request continue

failure-handling update-request continue

failure-handling terminate-request continue
pending-traffic-treatment noquota buffer

pending-traffic-treatment quota-exhausted buffer

exit

context <context_name>

subscriber default

   ip access-group <acl_name> in
   ip access-group <acl_name> out
   ip context-name <context_name>
   active-charging rulebase <rulebase_name>
   credit-control-group <cc_group_name>

end

Notes:

- For information on configuring IP access lists, refer to the Access Control Lists chapter in the System Administration Guide.
- For more information on configuring ECS ruledefs, refer to the ACS Ruledef Configuration Mode Commands chapter in the Command Line Interface Reference.
- For more information on configuring ECS charging actions, refer to the ACS Charging Action Configuration Mode Commands chapter in the Command Line Interface Reference.
- For more information on configuring ECS rulebases, refer to the ACS Rulebase Configuration Mode Commands chapter in the Command Line Interface Reference.

Configuring PLMN and Time Zone Reporting

PLMN and Time Zone Reporting feature requires a credit-control group to be defined in the APN or subscriber configuration or there must be a default credit-control group configured. The following CLI commands are available to enable/disable PLMN and Time Zone Reporting feature:

To enable PLMN and Time Zone Reporting through subscriber-template, use the following configuration:

configure

   context <context_name>

   subscriber name <subscriber_name>

   dns primary <primary_ipaddress>
   dns secondary <secondary_ipaddress>
   ip access-group test in
ip access-group test out
ip context-name <context_name>
credit-control-client event-based-charging
active-charging rulebase <rulebase_name>
exit
end

Notes:

- The `credit-control-client event-based-charging` command should be used to enable PLMN and Time Zone Reporting.

  For more information on configuring PLMN and Time Zone Reporting feature, refer to the Command Line Interface Reference.

To enable PLMN and Time Zone Reporting through APN template, use the following configuration:

```
configure
  context <context_name>
  apn <apn_name>
    selection-mode sent-by-ms
    accounting-mode none
    ip access-group test in
    ip access-group test out
    ip context-name <context_name>
    ip address pool name <pool_name>
    credit-control-client event-based-charging
    active-charging rulebase <rulebase_name>
  exit
  end
```

Rest of the parameters needed for Event-based Gy such as dictionary, endpoint will be picked from the credit-control group.

In a scenario where the triggers are configured through the CLI command and another set of triggers are also received from Gx, then the triggers from Gx will have a higher priority.
Configuring Server Unreachable Feature

The Server Unreachable feature requires a failure handling behavior to be defined in the Diameter Credit Control configuration. The following CLI commands are available to enable/disable OCS Unreachable Failure Handling feature:

To enable OCS Unreachable Failure Handling feature, use the following configuration:

```
configure
require active-charging

active-charging service <service_name>

credit-control

servers-unreachable { initial-request | update-request } { continue | terminate } [ { after-interim-volume <bytes> | after-interim-time <seconds> } + server-retries <retry_count> ]

servers-unreachable behavior-triggers { initial-request | update-request } transport-failure [ response-timeout | tx-expiry ]

servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [ to end-result-code ] } }

servers-unreachable behavior-triggers update-request { result-code { any-error | result-code [ to end-result-code ] } }

end
```

Notes:

- This CLI command “servers-unreachable { initial-request | update-request } { continue | terminate }[ { after-interim-volume <bytes> | after-interim-time <seconds> } + server-retries <retry_count> ]” allows configuring interim-volume and interim-time in the following ways:
  - after-interim-volume <bytes> alone followed by server-retries.
  - after-interim-time <seconds> alone followed by server-retries.
  - after-interim-volume <bytes> after-interim-time <seconds> followed by server-retries.

- This CLI command “servers-unreachable behavior-triggers” is used to trigger the servers-unreachable failure handling at either Tx expiry or Response timeout (This CLI is similar to retry-after-tx-expiry in “failure-handling update-request continue retry-after-tx-expiry” command.).

- This CLI command “servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [ to end-result-code ] } }” is used to trigger the servers-unreachable failure handling based on the configured Diameter error result codes.

For more information on configuring this feature, refer to the Command Line Interface Reference.

Gathering Statistics

This section explains how to gather Gy 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.
### Statistics/Information

<table>
<thead>
<tr>
<th>Statistics/Information</th>
<th>Action to perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete statistics for ECS sessions.</td>
<td><code>show active-charging sessions full</code></td>
</tr>
<tr>
<td>Detailed information for the Active Charging Service (ACS)</td>
<td><code>show active-charging service all</code></td>
</tr>
<tr>
<td>Information on all rule definitions configured in the service.</td>
<td><code>show active-charging ruledef all</code></td>
</tr>
<tr>
<td>Information on all charging actions configured in the service.</td>
<td><code>show active-charging charging-action all</code></td>
</tr>
<tr>
<td>Information on all rulebases configured in the service.</td>
<td><code>show active-charging rulebase all</code></td>
</tr>
<tr>
<td>Statistics of the Credit Control application, DCCA.</td>
<td><code>show active-charging credit-control statistics</code></td>
</tr>
<tr>
<td>States of the Credit Control application's sessions, DCCA.</td>
<td><code>show active-charging credit-control session-states [ rulebase &lt;rulebase_name&gt; ] [ content-id &lt;content_id&gt; ]</code></td>
</tr>
</tbody>
</table>
Chapter 10
ICAP Interface Support

This chapter provides information on configuring the external Active Content Filtering servers for a core network service subscriber. This chapter also describes the configuration and commands that are used to implement this feature.

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 respective product Administration Guide, before using the procedures in this chapter.

The following products currently support ICAP interface functionality:

- GGSN
- P-GW
ICAP Interface Support Overview

This feature supports streamlined ICAP interface to leverage Deep Packet Inspection (DPI) to enable external application servers to provide their services without performing DPI, and without being inserted in the data flow. For example with an external Active Content Filtering (ACF) Platform.

A high-level view of the streamlined ICAP interface support for external ACF is shown in the following figure:

Figure 45.  High-Level View of Streamlined ICAP Interface with external ACF

The system with ECS is configured to support DPI and the system uses this capability for content charging as well. WAP and HTTP traffic is content filtered over the ICAP interface. RTSP traffic that contains adult content can also be content filtered on the ICAP interface. Only the RTSP Request packets will be considered for content filtering over the ICAP interface.

If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the DPI function. The URL of the GET/POST request is extracted and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the application server. The application server checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked, or redirected by answering to the GET/POST with:

- A 200 OK message if the request is accepted.
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber must be redirected.
- Deny-response code 200 for RTSP requests is not supported. Only 403 “Forbidden” deny-response code will be supported.

Depending on the response received, the system with ECS will either pass the request unmodified, or discard the message and respond to the subscriber with the appropriate redirection or block message.

Content charging is performed by the Active Charging Service (ACS) only after the request has been controlled by the application server. This guarantees the appropriate interworking between the external application and content-based billing. In particular, this guarantees that charging will be applied to the appropriate request in case of redirection, and
that potential charging-based redirections (i.e. Advice of Charge, Top Up page, etc.) will not interfere with the decisions taken by the application server.

Functions of the ACF include:

- Retrieval of subscriber policies based on the subscriber identity passed in the ICAP message
- Determining the appropriate action (permit, deny, redirect) to take for the type of content based on subscriber profile
- Communication of the action (permit, deny, or redirect) decision for the URL back to the ACS module

**Failure Action on Retransmitted Packets**

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- **WSP CO:**
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.

- **HTTP:**
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.
ICAP Interface Support Overview

- Content Insert: Retransmitted packets are dropped and not charged.
- Redir: Retransmitted packets are dropped and not charged.
- Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
- Terminate flow: Retransmitted packets are dropped and not charged.

RTSP:
The following scenarios describe the failure actions where an RTSP request is received from the client. If ICAP is enabled, then the request goes to the ICAP server for content filtering.

- Allow: If the failure action configured is “allow”, the RTSP request packet is sent out after applying the appropriate disposition action. Here, the flow remains the same as in the case if the ICAP response received is 200 OK.
- Content Insert: If the failure action configured is “content-insertion <string of size 1 to 128>”, then this failure action for RTSP request will not be supported. Instead the failure action “Discard” for such an RTSP request will be supported.
- Redirect-URL: If the failure action configured is “redirect-url <string of size 1 to 128>”, then a TCP FIN_ACK packet with an RTSP “302 Moved Temporarily” response header is inserted towards the client containing the said URL for redirection. A TCP RST packet is inserted towards the server. The underlying TCP connection is thus closed. If the RTSP client wants to retry to the redirected URL, the opening of a new TCP connection must be initiated.
- Discard: If the failure action configured is “discard”, then the RTSP request packet received from the client is quietly discarded and no notification is sent to the client.
- Terminate flow: If the failure action configured is “terminate-flow”, then the TCP connection is torn down by injecting a TCP FIN-ACK towards the client and a RST packet towards the server. However, no notification will be sent to the RTSP client and the server regarding this flow termination.

Supported Networks and Platforms
This feature supports ST16 and Cisco Chassis for the core network services configured on the system.

License Requirements
External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface 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.
ICAP Interface Support

Configuring ICAP Interface Support

This section describes how to configure the Content Filtering Server Group (CFSG) through Internet Content Adaptation Protocol (ICAP) interface between ICAP client and ACF server (ICAP server).

Important: This section provides the minimum instruction set for configuring external content filtering servers on ICAP interface on the system. For more information on commands that configure additional parameters and options, refer to CFSG Configuration Mode Commands chapter in Command Line Interface Reference.

To configure the system to provide ICAP interface support for external content filtering servers:

Step 1  Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in the Creating ICAP Server Group and Address Binding section.

Step 2  Specify the active content filtering server (ICAP server) IP addresses and configure other parameters for ICAP server group by applying the example configuration in the Configuring ICAP Server and Other Parameters section.

Step 3  Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in the Configuring ECS Rulebase for ICAP Server Group section.

Step 4  Optional. Configure the charging action to forward HTTP/RTSP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in the Configuring Charging Action for ICAP Server Group section.

Step 5  Verify your ICAP interface and external content filtering server group configuration by following the steps in the Verifying the ICAP Server Group Configuration section.

Step 6  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

Creating ICAP Server Group and Address Binding

Use the following example to create the ICAP server group and bind the IP addresses:

```
configure

context <icap_ctxt_name> [ -noconfirm ]

    content-filtering server-group <icap_svrgrp_name> [ -noconfirm ]

        origin address <ip_address>

    end

```

Notes:

- `<ip_address>` is local IP address of the CFSG endpoint.
Configuring ICAP Server and Other Parameters

Use the following example to configure the active content filtering (ICAP server) and other related parameters:

```
configure

context <icap_context_name>

ccontent-filtering server-group <icap_server_grp_name>

icap server <ip_address> [ port <port_number> ] [ max <max_msgs>] [ priority <priority> ] [ standby ]

deny-message <msg_string>

response-timeout <timeout>

connection retry-timeout <retry_timeout>

failure-action { allow | content-insertion <content_string> | discard | redirect-url <url> | terminate-flow }

dictionary { custom1 | custom2 | custom3 | standard }

end
```

Notes:

- In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In release 8.0, only one ICAP Server can be configured per Content Filtering Server Group.

- The `standby` keyword can be used to configure the ICAP server as standby. A maximum of ten active and standby ICAP servers per Content Filtering Server Group can be configured. The active and standby servers under the same server group can be configured to work in active-standby mode.

- The maximum outstanding request per ICAP connection configured using the optional `max <max_msgs>` keyword is limited to one. Therefore, any other value configured using the `max` keyword will be ignored.

- Optional. To configure the ICAP URL extraction behavior, in the Content Filtering Server Group configuration mode, enter the following command:

```
url-extraction { after-parsing | raw }
```

By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.

Configuring ECS Rulebase for ICAP Server Group

Use the following example to configure the content filtering mode to ICAP server mode in the ECS rulebase for content filtering:

```
configure

require active-charging [ optimized-mode ]

active-charging service <acs_svc_name> [ -noconfirm ]
```
ICAP Interface Support

Configuring ICAP Interface Support

rulebase <rulebase_name> [ -noconfirm ]

content-filtering mode server-group <cf_server_group>

dead

Notes:

- In release 8.1, the optimized-mode keyword enables ACS in the Optimized mode, wherein ACS functionality is managed by SessMgs. In release 8.1, ACS must be enabled in the Optimized mode.
- In release 8.3, the optimized-mode keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.
- In release 8.0 and release 9.0 and later, the optimized-mode keyword is not available.

Configuring Charging Action for ICAP Server Group

Use the following example to configure the charging action to forward HTTP/WAP GET request to ICAP server for content processing:

configure

active-charging service <acs_svc_name>

charging-action <charging_action_name> [ -noconfirm ]

content-filtering processing server-group

dead

Verifying the ICAP Server Group Configuration

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

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

These instructions are used to verify the configuration for this feature.

Step 1 Verify your ICAP Content Filtering Server Group configuration by entering the following command in Exec Mode:

show content-filtering server-group

The following is a sample output. In this example, an ICAP Content Filtering server group named icap_cfsg1 was configured.

Content Filtering Group: icap_cfsg1
Context: icap1
Origin Address: 1.2.3.4
ICAP Address(Port): 1.2.3.4(1344)
Max Outstanding: 256
Priority: 1
Response Timeout: 30(secs) Connection Retry Timeout: 30(secs)
Dictionary: standard
Timeout Action: terminate-flow
Deny Message: "Service Not Subscribed"
URL-extraction: after-parsing
Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria: 1

Step 2 Verify any configuration error in your configuration by entering the following command in Exec Mode:

```
show configuration errors
```
Chapter 11
L2TP Access Concentrator

This chapter describes the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) functionality support on Cisco® ASR 5x00 chassis 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 respective product Administration Guide, before using the procedures in this chapter.

**Important:** The L2TP Access Concentrator 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*.

When enabled though the session license and feature use key, the system supports L2TP for encapsulation of data packets between it and one or more L2TP Network Server (LNS) nodes. In the system, this optional packet encapsulation, or tunneling, is performed by configuring L2TP Access Concentrator (LAC) services within contexts.

**Important:** The LAC service uses UDP ports 13660 through 13668 as the source port for sending packets to the LNS.
Applicable Products and Relevant Sections

The LAC feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

<table>
<thead>
<tr>
<th>Applicable Product(s)</th>
<th>Refer to Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDSN/FA/HA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supported LAC Service Configurations for PDSN Simple IP</td>
</tr>
<tr>
<td></td>
<td>• Supported LAC Service Configuration for Mobile IP</td>
</tr>
<tr>
<td></td>
<td>• Configuring Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• RADIUS and Subscriber Profile Attributes Used</td>
</tr>
<tr>
<td></td>
<td>• Configuring Local Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</td>
</tr>
<tr>
<td></td>
<td>• Configuring LAC Services</td>
</tr>
<tr>
<td></td>
<td>• Modifying PDSN Services for L2TP Support</td>
</tr>
<tr>
<td>GGSN/SGSN/FA/P-GW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supported LAC Service Configurations for the GGSN</td>
</tr>
<tr>
<td></td>
<td>• Supported LAC Service Configuration for Mobile IP</td>
</tr>
<tr>
<td></td>
<td>• Configuring Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• RADIUS and Subscriber Profile Attributes Used</td>
</tr>
<tr>
<td></td>
<td>• Configuring Local Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• Configuring LAC Services</td>
</tr>
<tr>
<td></td>
<td>• Modifying APN Templates to Support L2TP</td>
</tr>
<tr>
<td>ASN GW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supported LAC Service Configuration for Mobile IP</td>
</tr>
<tr>
<td></td>
<td>• Configuring Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• RADIUS and Subscriber Profile Attributes Used</td>
</tr>
<tr>
<td></td>
<td>• Configuring Local Subscriber Profiles for L2TP Support</td>
</tr>
<tr>
<td></td>
<td>• Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</td>
</tr>
<tr>
<td></td>
<td>• Configuring LAC Services</td>
</tr>
</tbody>
</table>
Supported LAC Service Configurations for PDSN Simple IP

LAC services can be applied to incoming PPP sessions using one of the following methods:

- **Attribute-based tunneling**: This method is used to encapsulate PPP packets for only specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

- **PDSN Service-based compulsory tunneling**: This method of tunneling is used to encapsulate all incoming PPP traffic from the R-P interface coming into a PDSN service, and tunnel it to an LNS peer for authentication. It should be noted that this method does not consider subscriber configurations, since all authentication is performed by the peer LNS.

Each LAC service is bound to a single system interface configured within the same system context. It is recommended that this context be a destination context as displayed in the following figure.

**Figure 46. LAC Service Configuration for SIP**

*PDSN Configuration*

**Attribute-based Tunneling**

This section describes the working of attribute-based tunneling and its configuration.
How The Attribute-based L2TP Configuration Works

The following figure and the text that follows describe how Attribute-based tunneling is performed using the system.

1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The PDSN service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for PDSN Simple IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.
Important: These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

Step 1  Configure the subscriber profiles according to the information and instructions located in the Configuring Subscriber Profiles for L2TP Support section of this chapter.

Step 2  Configure one or more LAC services according to the information and instructions located in the Configuring LAC Services section of this chapter.

Step 3  Configure the PDSN service(s) with the tunnel context location according to the instructions located in the Modifying PDSN Services for L2TP Support section of this chapter.

Step 4  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

PDSN Service-based Compulsory Tunneling

This section describes the working of service-based compulsory tunneling and its configuration.

How PDSN Service-based Compulsory Tunneling Works

PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

Accounting start and interim accounting records are still sent to the local RADIUS server configured in the system’s AAA Service configuration. When the L2TP session setup is complete, the system starts its call counters and signals the RADIUS server to begin accounting. The subscriber name for accounting records is based on the NAI-constructed name created for each session.

PDSN service-based compulsory tunneling requires the modification of one or more PDSN services and the configuration of one or more LAC services.

The following figure and the text that follows describe how PDSN service-based compulsory tunneling is performed using the system.
1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service detects its tunnel-type parameter is configured to L2TP and its tunnel-context parameter is configured to the Destination context.
3. The PDSN forwards all packets for the session to a LAC service configured in the Destination context. If multiple LAC services are configured, session traffic will be routed to each using a round-robin algorithm.
4. The LAC service initiates an L2TP tunnel to one of the LNS peers listed as part of its configuration.
5. Session packets are passed to the LNS over a packet data network for authentication.
6. The LNS authenticates the session and returns an Access-Accept to the PDSN.
7. The PDSN service initiates accounting for the session using a constructed NAI.
   Session data traffic is passed over the L2TP tunnel established in step 4.

Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP

This section provides a list of the steps required to configure L2TP compulsory tunneling support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.
Step 1  Configure one or more LAC services according to the information and instructions located in the Configuring LAC Services section of this chapter.

Step 2  Configure the PDSN service(s) according to the instructions located in the Modifying PDSN Services for L2TP Support section of this chapter.

Step 3  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.
Supported LAC Service Configurations for the GGSN and P-GW

As mentioned previously, L2TP is supported through the configuration of LAC services on the system. Each LAC service is bound to a single system interface configured within the same system destination context as displayed in the following figure.

Figure 49. GGSN LAC Service Configuration

LAC services are applied to incoming subscriber PDP contexts based on the configuration of attributes either in the GGSN/’s Access Point Name (APN) templates or in the subscriber’s profile. Subscriber profiles can be configured locally on the system or remotely on a RADIUS server.

LAC service also supports domain-based L2TP tunneling with LNS. This method is used to create multiple tunnels between LAC and LNS on the basis of values received in “Tunnel-Client-Auth-ID” or “Tunnel-Server-Auth-ID” attribute received from AAA Server in Access-Accept as a key for tunnel selection and creation. When the LAC needs to establish a new L2TP session, it first checks if there is any existing L2TP tunnel with the peer LNS based on the value of key “Tunnel-Client-Auth-ID” or “Tunnel-Server-Auth-ID” attribute. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

If LAC service needs to establish a new tunnel for a new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message. If all available peer-LNS are exhausted, LAC service will reject the call.
L2TP tunnel parameters are configured within the APN template and are applied to all subscribers accessing the APN. However, L2TP operation will differ depending on the subscriber’s PDP context type as described below:

- **Transparent IP**: The APN template’s L2TP parameter settings will be applied to the session.
- **Non-transparent IP**: Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.
- **PPP**: The APN template’s L2TP parameter settings will be applied and all of the subscriber’s PPP packets will be forwarded to the specified LNS.

More detailed information is located in the sections that follow.

**Transparent IP PDP Context Processing with L2TP Support**

The following figure and the text that follows describe how transparent IP PDP contexts are processed when L2TP tunneling is enabled.

1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming
sessions. If no outbound information is configured, the subscriber’s International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

1. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
2. The GGSN passes data received from the MS to a LAC service.
3. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
4. The LNS un-encapsulates the packets and processes them as needed. The processing includes IP address allocation.

Non-transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 51. Non-transparent IP PDP Context Call Processing with L2TP Tunneling

1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber’s username is sent to the peer LNS.

3. The GGSN service authenticates the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server. As part of the authentication, the RADIUS server returns an Access-Accept message. The message may include attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

If these attributes are supplied, they take precedence over those specified in the APN template.

4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.

5. The GGSN passes data received from the MS to a LAC service.

6. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.

7. The LNS un-encapsulates the packets and processes them as needed. The processing includes authentication and IP address allocation.

**PPP PDP Context Processing with L2TP Support**

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

**Figure 52. PPP PDP Context Call Processing with L2TP Tunneling**
1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.

2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured.

   Note that L2TP support could also be configured in the subscriber’s profile. If the APN is not configured for L2TP tunneling, the system will attempt to authenticate the subscriber. The tunneling parameters in the subscriber’s profile would then be used to determine the peer LNS.

3. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.

4. The GGSN passes the PPP packets received from the MS to a LAC service.

5. The LAC service encapsulates the PPP packets and forwards it to the appropriate Gi interface for delivery to the LNS.

6. The LNS un-encapsulates the packets and processes them as needed. The processing includes PPP termination, authentication (using the username/password provided by the subscriber), and IP address allocation.

**Configuring the GGSN or P-GW to Support L2TP**

This section provides a list of the steps required to configure the GGSN or P-GW to support L2TP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a GGSN or P-GW.

1. Configure the APN template to support L2TP tunneling according to the information and instructions located in the *Modifying APN Templates to Support L2TP* section of this chapter.

   **Important:** L2TP tunneling can be configured within individual subscriber profiles as opposed/or in addition to configuring support with an APN template. Subscriber profile configuration is described in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

2. Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*. 

---

**L2TP Access Concentrator**

**Supported LAC Service Configurations for the GGSN and P-GW**

**SAE-GW Administration Guide, StarOS Release 17**

438
Supported LAC Service Configuration for Mobile IP

LAC services can be applied to incoming MIP sessions using attribute-based tunneling. Attribute-based tunneling is used to encapsulate PPP packets for specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

Each LAC service is bound to a single system interface within the same system context. It is recommended that this context be a destination context as displayed in figure below.

How The Attribute-based L2TP Configuration for MIP Works

The following figure and the text that follows describe how Attribute-based tunneling for MIP is performed using the system.
1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The HA service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

**Configuring Attribute-based L2TP Support for HA Mobile IP**

This section provides a list of the steps required to configure attribute-based L2TP support for use with HA Mobile IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as an HA.

**Step 1** Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

**Step 2** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
Step 3  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*. 
Configuring Subscriber Profiles for L2TP Support

This section provides information and instructions on the following procedures:

- RADIUS and Subscriber Profile Attributes Used
- Configuring Local Subscriber Profiles for L2TP Support
- Configuring Local Subscriber
- Verifying the L2TP Configuration

**Important:** Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

RADIUS and Subscriber Profile Attributes Used

Attribute-based L2TP tunneling is supported through the use of attributes configured in subscriber profiles stored either locally on the system or remotely on a RADIUS server. The following table describes the attributes used in support of LAC services. These attributes are contained in the standard and VSA dictionaries.

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>Local Subscriber Attribute</th>
<th>Description</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-Type</td>
<td>tunnel12tp</td>
<td>Specifies the type of tunnel to be used for the subscriber session</td>
<td>L2TP</td>
</tr>
<tr>
<td>Tunnel-Server-Endpoint</td>
<td>tunnel12tp peer-address</td>
<td>Specifies the IP address of the peer LNS to connect tunnel to.</td>
<td>IPv4 address in dotted-decimal format, enclosed in quotation marks</td>
</tr>
<tr>
<td>Tunnel-Password</td>
<td>tunnel12tp secret</td>
<td>Specifies the shared secret between the LAC and LNS.</td>
<td>Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks</td>
</tr>
<tr>
<td>Tunnel-Private-Group-ID</td>
<td>tunnel12tp tunnel-context</td>
<td>Specifies the name of the destination context configured on the system in which the LAC service(s) to be used are located.</td>
<td>Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks</td>
</tr>
</tbody>
</table>

**Important:** If the LAC service and egress interface are configured in the same context as the core service or HA service, this attribute is not needed.
## RADIUS Attribute

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>Local Subscriber Attribute</th>
<th>Description</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunne1-Preference</td>
<td>tunnel12tp preference</td>
<td>Configures the priority of each peer LNS when multiple LNS nodes are configured.</td>
<td>Integer from 1 to 65535</td>
</tr>
</tbody>
</table>
| SN-Tunnel-Load-Balancing | loadbalance-tunnel-peer | A vendor-specific attribute (VSA) used to provides a selection algorithm defining how an LNS node is selected by the RADIUS server when multiple LNS peers are configured within the subscriber profile. | • Random - Random LNS selection order, the Tunnel-Preference attribute is not used in determining which LNS to select.  
• Balanced - LNS selection is sequential balancing the load across all configured LNS nodes, the Tunnel-Preference attribute is not used in determining which LNS to select.  
• Prioritized - LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. |
| Client-Endpoint | local-address | Specifies the IP address of a specific LAC service configured on the system that to use to facilitate the subscriber’s L2TP session. This attribute is used when multiple LAC services are configured. | IPv4 address in dotted decimal notation. (xxx.xxx.xxx.xxx) |

### RADIUS Tagging Support

The system supports RADIUS attribute tagging for tunnel attributes. These “tags” organize together multiple attributes into different groups when multiple LNS nodes are defined in the user profile. Tagging is useful to ensure that the system groups all the attributes used for a specific server. If attribute tagging is not supported by your specific RADIUS server, the system implicitly organizes the attributes in the order that they are listed in the access accept packet.

### Configuring Local Subscriber Profiles for L2TP Support

This section provides information and instructions for configuring local subscriber profiles on the system to support L2TP.
Configuring Subscriber Profiles for L2TP Support

Important: The configuration of RADIUS-based subscriber profiles is not discussed in this document. Please refer to the documentation supplied with your RADIUS server for further information.

Important: This section provides the minimum instruction set for configuring local subscriber profile for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the LAC Service Configuration Mode Commands chapter in the Command Line Interface Reference.

To configure the system to provide L2TP support to subscribers:

Step 1 Configure the “Local” subscriber with L2TP tunnel parameters and the load balancing parameters with action by applying the example configuration in the Configuring Local Subscriber section.

Step 2 Verify your L2TP configuration by following the steps in the Verifying the L2TP Configuration section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

Configuring Local Subscriber

Use the following example to configure the Local subscriber with L2TP tunnel parameters. Optionally you can configure load balancing between multiple LNS servers:

```
configure
    context <ctxt_name> [-noconfirm]
    subscriber name <subs_name>
    tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [ encrypted ]
    secret <secret_string> | tunnel-context <context_name> | local-address <local_ip_address>
}
    load-balancing { random | balanced | prioritized }
end
```

Notes:
- `<ctxt_name>` is the system context in which you wish to configure the subscriber profile.
- `<lns_ip_address>` is the IP address of LNS server node and `<local_ip_address>` is the IP address of system which is bound to LAC service.

Verifying the L2TP Configuration

These instructions are used to verify the L2TP configuration.

Step 1 Verify that your L2TP configurations were configured properly by entering the following command in Exec Mode in specific context:
show subscriber configuration username user_name

The output of this command is a concise listing of subscriber parameter settings as configured.

**Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes**

As with other services supported by the system, values for subscriber profile attributes not returned as part of a RADIUS Access-Accept message can be obtained using the locally configured profile for the subscriber named default. The subscriber profile for default must be configured in the AAA context (i.e. the context in which AAA functionality is configured).

As a time saving feature, L2TP support can be configured for the subscriber named default with no additional configuration for RADIUS-based subscribers. This is especially useful when you have separate source/AAA contexts for specific subscribers.

To configure the profile for the subscriber named default, follow the instructions above for configuring a local subscriber and enter the name default.
Configuring LAC Services

Important: Not all commands, keywords and functions may be available. Functionality is dependent on platform and license(s).

This section provides information and instructions for configuring LAC services on the system allowing it to communicate with peer LNS nodes.

Important: This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the LAC Service Configuration Mode Commands chapter in the Command Line Interface Reference.

To configure the LAC services on system:

Step 1 Configure the LAC service on system and bind it to an IP address by applying the example configuration in the Configuring LAC Service section.

Step 2 Optional. Configure LNS peer information if the Tunnel-Service-Endpoint attribute is not configured in the subscriber profile or PDSN compulsory tunneling is supported by applying the example configuration in the Configuring LNS Peer section.

Step 3 Verify your LAC configuration by following the steps in the Verifying the LAC Service Configuration section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

Configuring LAC Service

Use the following example to create the LAC service and bind the service to an IP address:

```
configure

    context <dst_ctxt_name> [-noconfirm]

    lac-service <service_name>

    bind address <ip_address>

end
```

Notes:

- `<dst_ctxt_name>` is the destination context where you want to configure the LAC service.
Configuring LNS Peer

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure

context <dst_ctxt_name> [ -noconfirm ]

lac-service <service_name>

tunnel selection-key tunnel-server-auth-id

peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
{[encrypted] isakmp-secret <secret> }] [description <text>] [ preference <integer>]

load-balancing { random | balanced | prioritized }
end
```

Notes:

- `<dst_ctxt_name>` is the destination context where the LAC service is configured.

Verifying the LAC Service Configuration

These instructions are used to verify the LAC service configuration.

**Step 1** Verify that your LAC service configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show lac-service name service_name
```

The output given below is a concise listing of LAC service parameter settings as configured.

```
Service name: vpn1
Context: isp1
Bind: Done
Local IP Address: 192.168.2.1
First Retransmission Timeout: 1 (secs)
Max Retransmission Timeout: 8 (secs)
Max Retransmissions: 5
Max Sessions: 500000 Max Tunnels: 32000
Max Sessions Per Tunnel: 512
Data Sequence Numbers: Enabled Tunnel Authentication: Enabled
```
Keep-alive interval: 60  Control receive window: 16
Max Tunnel Challenge Length: 16
Proxy LCP Authentication: Enabled
Load Balancing: Random
Service Status: Started
Newcall Policy: None
Modifying PDSN Services for L2TP Support

PDSN service modification is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but can not determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.

**Important:** This section provides the minimum instruction set for modifying PDSN service for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

**Step 1**  
Modify the PDSN service to support L2TP by associating LAC context and defining tunnel type by applying the example configuration in the *Modifying PDSN Service* section.

**Step 2**  
Verify your configuration to modify PDSN service by following the steps in the *Verifying the PDSN Service for L2TP Support* section.

**Step 3**  
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying PDSN Service

Use the following example to modify the PDSN service to support L2TP by associating LAC context and defining tunnel type:

```
configure
  context <source_ctxt_name> [ -noconfirm ]
  pdsn-service <pdsn_service_name>
    ppp tunnel-context <lac_context_name>
    ppp tunnel-type { l2tp | none }
  end
```

Notes:

- `<source_ctxt_name>` is the name of the source context containing the PDSN service, which you want to modify for L2TP support.
• `<pdsn_service_name>` is the name of the pre-configured PDSN service, which you want to modify for L2TP support.
• `<lac_context_name>` is typically the destination context where the LAC service is configured.

Verifying the PDSN Service for L2TP Support

These instructions are used to verify the PDSN service configuration.

**Step 1** Verify that your PDSN is configured properly by entering the following command in Exec Mode in specific context:

```
show pdsn-service name pdsn_service_name
```

The output of this command is a concise listing of PDSN service parameter settings as configured.
Modifying APN Templates to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.

**Important:** This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

**Step 1** Modify the APN template to support L2TP with LNS server address and other parameters by applying the example configuration in the *Assigning LNS Peer Address in APN Template* section.

**Step 2** Optional. If L2TP will be used to tunnel transparent IP PDP contexts, configure the APN’s outbound username and password by applying the example configuration in the *Configuring Outbound Authentication* section.

**Step 3** Verify your APN configuration by following the steps in the *Verifying the APN Configuration* section.

**Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Assigning LNS Peer Address in APN Template

Use following example to assign LNS server address with APN template:

```plaintext
configure

context <dst_ctxt_name> [-noconfirm]

apn <apn_name>

    tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret <l2tp_secret> ] [ preference <integer> ] [ tunnel-context <l2tp_context_name> ] [ local-address <local_ip_address> ] [ crypto-map <map_name> { [ encrypted ] isakmp-secret <crypto_secret> } ]

end
```

**Notes:**

- `<dst_ctxt_name>` is the name of system destination context in which the APN is configured.
- `<apn_name>` is the name of the pre-configured APN template which you want to modify for the L2TP support.
- `<lns_address>` is the IP address of LNS server node and `<local_ip_address>` is the IP address of system which is bound to LAC service.
Configuring Outbound Authentication

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure

context <dst_ctxt_name> [ -noconfirm ]
apn <apn_name>
  outbound { [ encrypted ] password <pwd> | username <name> }
end
```

Notes:

- `<dst_ctxt_name>` is the destination context where APN template is configured.
- `<apn_name>` is the name of the pre-configured APN template which you want to modify for the L2TP support.

Verifying the APN Configuration

These instructions are used to verify the APN configuration.

**Step 1** Verify that your APN configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show apn name <apn_name>
```

The output is a concise listing of APN parameter settings as configured.
Chapter 12
Mobile IP Registration Revocation

This chapter describes Registration Revocation for Mobile-IP and Proxy Mobile-IP 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 this administration guide before using the procedures in this chapter.

Important: This license is enabled by default; however, not all features are supported on all platforms and other licenses may be required for full functionality as described in this chapter.
Overview

Registration Revocation is a general mechanism whereby either the HA or the FA providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

Mobile IP Registration Revocation can be triggered at the FA by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)

**Important:** Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the HA can initiate the revocation for Proxy-MIP calls.

Mobile IP Registration Revocation can be triggered at the HA by any of the following:

- Administrative clearing of calls
- Inter-Access Gateway handoff. This releases the binding at the previous access gateway/FA
- Session Manager software task outage resulting in the loss of FA sessions (for sessions that could not be recovered)
- Session Idle timer expiry (when configured to send Revocation)
- Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested, etc.)

The FA and the HA negotiate Registration Revocation support when establishing a Mobile IP call. Revocation support is indicated to the Mobile Node (MN) from the FA by setting the 'X' bit in the Agent Advertisement to MN. However, the MN is not involved in negotiating the Revocation for a call or in the Revocation process. It only gets notified about it. The X bit in the Agent Advertisements is just a hint to the MN that revocation is supported at the FA but is not a guarantee that it can be negotiated with the HA.

At the FA, if revocation is enabled and a FA-HA SPI is configured, the Revocation Support extension is appended to the RRQ received from the MN and protected by the FA-HA Authentication Extension. At the HA, if the RRQ is accepted, and the HA supports revocation, the HA responds with an RRP that includes the Revocation Support extension. Revocation support is considered to be negotiated for a binding when both sides have included a Revocation Support Extension during a successful registration exchange.

**Important:** The Revocation Support Extension in the RRQ or RRP must be protected by the FA-HA Authentication Extension. Therefore, an FA-HA SPI must be configured at the FA and the HA for this to succeed.

If revocation is enabled at the FA, but an FA-HA SPI is not configured at the FA for a certain HA, then FA does not send Revocation Support Extension for a call to that HA. Therefore, the call may come up without Revocation support negotiated.
If the HA receives an RRQ with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with “FA Failed Authentication” error.

If the FA receives a RRP with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with “HA Failed Authentication” error.

Also note that Revocation support extension is included in the initial, renewal or handoff RRQ/RRP messages. The Revocation extension is not included in a Deregistration RRQ from the FA and the HA will ignore them in any Deregistration RRQs received.
Configuring Registration Revocation

Support for MIP Registration Revocation requires the following configurations:

- **FA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.
- **HA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.

**Important:** These instructions assume that the system was previously configured to support subscriber data sessions for a core network service with FA and/or an HA according to the instructions described in the respective product Administration Guide.

**Important:** Commands used in the configuration samples 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.

### Configuring FA Services

Configure FA services to support MIP Registration Revocation by applying the following example configuration:

```bash
configure
  context <context_name>
    fa-service <fa_service_name>
      revocation enable
      revocation max-retransmission <number>
      revocation retransmission-timeout <time>
    end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

### Configuring HA Services

Configure HA services to support MIP Registration Revocation by applying the following example configuration:

```bash
configure
  context <context_name>
    ha-service <ha_service_name>
```

SAE-GW Administration Guide, StarOS Release 17
revocation enable

revocation max-retransmission <number>

revocation retransmission-timeout <time>

end

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.
Chapter 13
Multi-Protocol Label Switching (MPLS) Support

This chapter describes the system’s support for BGP/MPLS VPN and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on specific systems. 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.

When enabled through a feature license key, the system supports MPLS to provide a VPN connectivity from the system to the corporate’s network.

**Important:** This release provides BGP/MPLS VPN for directly connected PE routers only.

MP-BGP is used to negotiate the routes and segregate the traffic for the VPNs. The network node learns the VPN routes from the connected Provider Edge (PE), while the PE populates its routing table with the routes provided by the network functions.

This chapter includes following sections:

- Overview
- Supported Standards
- Supported Networks and Platforms
- Licenses
- Benefits
- Configuring BGP/MPLS VPN with Static Labels
- Configuring BGP/MPLS VPN with Dynamic Labels
Overview

As seen in the following scenario, the chassis can be deployed as a router while supporting BGP/MPLS-VPN in a network.

- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Provider Edge (PE)
- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Autonomous System Border Router (ASBR)

Chassis as MPLS-CE Connecting to PE

![Chassis as MPLS-CE Connected to PE](image)

The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the Configuring BGP/MPLS VPN with Static Labels section and refer Configuring BGP/MPLS VPN with Dynamic Labels for dynamic label configuration.

The system is in a separate autonomous system (AS) from the Provider Edge (PE). It communicates with the PE and all VPN routes are exchanged over MP-BGP. Routes belonging to different VPNs are logically separated, using separate virtual route forwarding tables (VRFs).

Routes for each VPN are advertised as VPN-IPv4 routes, where route distinguishers are prepended to regular IPv4 routes to allow them to be unique within the routing table. Route targets added to the BGP extended community attributes identify different VPN address spaces. The particular upstream BGP peer routing domain (VPN), from which a route is to be imported by the downstream peer into an appropriate VRF, is identified with an extended community in the advertised NLRI.

A unique label is also received or advertised for every VPN route.

The Customer Edge (CE) also advertises routes to the PE using NLRIs that include route distinguishers to differentiate VPNs, an extended community to identify VRFs, and a MPLS-label, which will later be used to forward data traffic. There is a single MPLS-capable link between the CE and the PE. MP-BGP communicates across this link as a TCP session over IP. Data packets are sent bidirectionally as MPLS encapsulated packets.

This solution does not use any MPLS protocols. The MPLS label corresponding to the immediate upstream neighbor can be statically configured on the downstream router, and similarly in the reverse direction.

When forwarding subscriber packets in the upstream direction to the PE, the CE encapsulates packets with MPLS headers that identify the upstream VRF (the label sent with the NLRI) and the immediate next hop. When the PE receives a packet it swaps the label and forward.
The CE does not run any MPLS protocol (LDP or RSVP-TE).
When receiving data packets in the downstream direction from the PE, the label is checked to identify the destination VRF. Then the packet is de-encapsulated into an IP packet and sent to the session subsystem for processing.

**Important:** MPLS ping/trace route debugging facilities are not supported.

### Chassis as MPLS-CE Connected to ASBR

**Figure 56. Chassis as MPLS-CE Connected to ASBR**

The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the Configuring BGP/MPLS VPN with Static Labels section and refer Configuring BGP/MPLS VPN with Dynamic Labels for dynamic label configuration.

This scenario differs from the MPLS-CE with PE scenario in terms of peer functionality even though MPLS-CE functionality does not change. Like the MPLS-CE with PE scenario, MPLS-CE system maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session.

The peer in this scenario is not a PE router but an Autonomous System Border Router (ASBR). The ASBR does not need to maintain any VRF configuration. The PE routers use IBGP to redistribute labeled VPN-IPv4 routes either to an ASBR or to a route reflector (of which the ASBR is a client). The ASBR then uses the eBGP to redistribute those labeled VPN-IPv4 routes to an MPLS-CE in another AS. Because of the eBGP connection, the ASBR changes the next-hop and labels the routes learned from the iBGP peers before advertising to the MPLS-CE. The MPLS-CE is directly connected to the eBGP peering and uses only the the MP-eBGP to advertise and learn routes. The MPLS-CE pushes/pops a single label to/from the ASBR, which is learned over the MP-eBGP connection. This scenario avoids the configuration of VRFs on the PE, which have already been configured on the MPLS-CE.

### Engineering Rules

- Up to 250 virtual routing tables per context.
- Up to 5000 “host routes” spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Up to 1024 VRFs per chassis.
Supported Standards

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

- RFC 4364, BGP/MPLS IP VPNs
- RFC 3032, MPLS Label Stack Encoding

**Important:** One or more sections of above mentioned IETF are partially supported for this feature. For more information on Statement of Compliance, contact your Cisco account representative.
Supported Networks and Platforms

This feature supports all ASR 5x00 platforms with StarOS Release 9.0 or later running with network function services.
Licenses

Multi-protocol label switching (MPLS) 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.
Benefits

MPLS provides networks with a more efficient way to manage applications and move information between locations. MPLS prioritizes network traffic, so administrators can specify which applications should move across the network ahead of others.
Configuring BGP/MPLS VPN with Static Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with static MPLS label support.

The base configuration, as described in the Routing chapter in this guide, must be completed prior to attempt the configuration procedure described below.

**Important:** The feature described in this chapter is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

**Important:** Commands used in the configuration samples 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.

To configure the system for BGP/MPLS VPN:

**Step 1** Create a VRF on the router and assign a VRF name by applying the example configuration in the Create VRF with Route-distinguisher and Route-target section.

**Step 2** Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in the Set Neighbors and Enable VPNv4 Route Exchange section.

**Step 3** Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in the Configure Address Family and Redistribute Connected Routes section. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.

**Step 4** Configure IP Pools with MPLS labels for input and output by applying the example configuration in the Configure IP Pools with MPLS Labels section.

**Step 5** Optional. Bind DHCP service to work with MPLS labels for input and output in corporate networks by applying the example configuration in the Bind DHCP Service for Corporate Servers section.

**Step 6** Optional. Bind AAA/RADIUS server group in corporate network to work with MPLS labels for input and output by applying the example configuration in the Bind AAA Group for Corporate Servers section.

**Step 7** Save your configuration as described in the System Administration Guide.

Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second ip vrf command creates the route-distinguisher and route-target.

```
configure

   context <context_name> -noconfirm

   ip vrf <vrf_name>
```
Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

```
configure
  context <context_name>
    router bgp <as_number>
      neighbor <ip_address> remote-as <AS_num>
      address-family vpnv4
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
    exit
    interface <bind_intfc_name>
      ip address <ip_addr_mask_combo>
    end
```
Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with MPLS labels for input and output.

```config
configure

calendar <context_name> -noconfirm

ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name> mpls-label input <in_label_value> output <out_label_value1> nexthop-forwarding-address <ip_addr_bgp_neighbor>
end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with MPLS labels for input and output in Corporate network.

```config
configure

calendar <dest_ctxt_name>

interface <intfc_name> loopback

ip vrf forwarding <vrf_name>

ip address <bind_ip_address subnet_mask>

exit

dhcp-service <dhcp_svc_name>

dhcp ip vrf <vrf_name>

bind address <bind_ip_address> [nexthop-forwarding-address <nexthop_ip_address> [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]]]

dhcp server <ip_address>
end
```

Notes:
- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword `nexthop-forwarding-address <ip_address> mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]` applies DHCP over MPLS traffic.

Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with MPLS labels for input and output in Corporate network.
configure

context <dest_ctxt_name>

aaa group <aaa_grp_name>

radius ip vrf <vrf_name>

radius attribute nas-ip-address address <nas_address> nexthop-forwarding-address <ip_address> mpls-label input <in_mpls_label_value> output <out_mpls_label_value>

radius server <ip_address> encrypted key <encrypt_string> port <iport_num>

end

Notes:

- **aaa_grp_name** is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.

- Optional keyword `nexthop-forwarding-address<ip_address> mpls-label input <in_mpls_label_value> output <out_mpls_label_value>` associates AAA group for MPLS traffic.
Configuring BGP/MPLS VPN with Dynamic Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with dynamic MPLS label support.

The base configuration, as described in the Routing chapter in this guide, must be completed prior to attempt the configuration procedure described below.

**Important:** The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

**Important:** Commands used in the configuration samples 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.

To configure the system for BGP/MPLS VPN:

**Step 1** Create a VRF on the router and assign a VRF name by applying the example configuration in the Create VRF with Route-distinguisher and Route-target section.

**Step 2** Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in the Set Neighbors and Enable VPNv4 Route Exchange section.

**Step 3** Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in the Configure Address Family and Redistribute Connected Routes section. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.

**Step 4** Configure IP Pools with dynamic MPLS labels by applying the example configuration in the Configure IP Pools with MPLS Labels section.

**Step 5** Optional. Bind DHCP service to work with dynamic MPLS labels in corporate networks by applying the example configuration in the Bind DHCP Service for Corporate Servers section.

**Step 6** Optional. Bind AAA/RADIUS server group in corporate network to work with dynamic MPLS labels by applying the example configuration in the Bind AAA Group for Corporate Servers section.

**Step 7** Optional. Modify the configured IP VRF, which is configured to support basic MPLS functionality, for mapping between DSCP bit value and experimental (EXP) bit value in MPLS header for ingress and egress traffic by applying the example configuration in the DSCP and EXP Bit Mapping section.

**Step 8** Save your configuration as described in the System Administration Guide.

**Create VRF with Route-distinguisher and Route-target**

Use this example to first create a VRF on the router and assign a VRF name. The second ip vrf command creates the route-distinguisher and route-target.

```
configure
```

SAE-GW Administration Guide, StarOS Release 17
Multi-Protocol Label Switching (MPLS) Support

Configuring BGP/MPLS VPN with Dynamic Labels

context <context_name> -noconfirm

ip vrf <vrf_name>

router bgp <as_number>

ip vrf <vrf_name>

route-distinguisher {<as_value> | <ip_address>} <rt_value>

route-target export {<as_value> | <ip_address>} <rt_value>

route-target import {<as_value> | <ip_address>} <rt_value>
end

Notes:

- If export and import route targets are the same, alternate command `route-target both {<as_value>|<ip_address>} <rt_value>` can be used in place of `route-target import` and `route-target export` commands.

Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

configure

context <context_name>

mpls bgp forwarding

router bgp <as_number>

neighbor <ip_address> remote-as <AS_num>

address-family vpnv4

neighbor <ip_address> activate

neighbor <ip_address> send-community both

exit

interface <bind_intfc_name>

ip address <ip_addr_mask_combo>

end
Configure Address Family and Redistributed Connected Routes

Use this example to configure the address-family and to redistribute the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```bash
configure
context <context_name>
router bgp <as_number>
  address-family ipv4 <type> vrf <vrf_name>
    redistribute connected
end
```

Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with dynamic MPLS labels.

```bash
configure
context <context_name> -noconfirm
  ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name>
end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with dynamic MPLS labels in Corporate network.

```bash
configure
context <dest_ctxt_name>
  interface <intfc_name> loopback
    ip vrf forwarding <vrf_name>
    ip address <bind_ip_address subnet_mask>
  exit
dhcp-service <dhcp_svc_name>
  dhcp ip vrf <vrf_name>
  bind address <bind_ip_address>
  dhcp server <ip_address>
```
end

Notes:
- To ensure proper operation, DHCP functionality should be configured within a destination context.

**Bind AAA Group for Corporate Servers**

Use this example to bind AAA server groups with dynamic MPLS labels in Corporate network.

```
configure
  context <dest_ctxt_name>
    aaa group <aaa_grp_name>
      radius ip vrf <vrf_name>
      radius attribute nas-ip-address address <nas_address>
      radius server <ip_address> encrypted key <encrypt_string> port <iport_num>
  end
```

Notes:
- `aaa_grp_name` is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.

**DSCP and EXP Bit Mapping**

Use this example to modify the configured IP VRF to support QoS mapping.

```
configure
  context <context_name>
    ip vrf <vrf_name>
      mpls map-dscp-to-exp dscp <dscp_bit_value> exp <exp_bit_value>
      mpls map-exp-to-dscp exp <exp_bit_value> dscp <dscp_bit_value>
  end
```
Chapter 14
Network Mobility (NEMO)

This chapter describes the system’s support for NEMO 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 Cisco ASR 5x00 Packet Data Network Gateway Administration Guide, before using the procedures in this chapter.

This chapter includes the following sections:

- NEMO Overview
- NEMO Configuration
NEMO Overview

When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

The following figure shows a high-level view of LTE NEMOv4 Architecture.

Figure 57. NEMO Overview

Use Cases

The following use cases are supported by NEMO in LTE:

1. **Stationary** - Applications, like branch offices, with a mobile router that does not require mobility.
2. **Nomadic** - Applications that use a mobile router that does not move while in service, but that may be moved to a different location and brought back on service (e.g. a kiosk showing up in a mall one day and in a different location the next day or month).
3. **Moveable** - Applications that need to maintain Dynamic Mobile Network Routing (DMNR) service operational while moving and crossing PDSN boundaries, such as public safety vehicles. Service continuity is handled by the mobility protocols (Mobile IP in 3G and GTP in LTE).
Features and Benefits

The system supports the usage of dynamically learned, overlapping customer prefixes. These prefixes are advertised via BGP.

MIPv4-based NEMO Control Plane

The following figure shows a high-level view of the NEMO control plane.

![NEMO Control Plane Diagram]

NEMO includes the following features:

- **Collocated-Care-of-Address mode**
  
  The Cisco NEMO MR is expected to use the Collocated-Care-of-Address mode to establish a NEMO MIPv4 session with NEMO4G-HA and as one of the IP endpoints of the NEMO GRE Tunnel for the transport of user traffic.

- **MR-HADDR**
  
  NEMO4G-HA supports a potential “dummy” MR-HADDR address that would be configured in every MR within the same Enterprise or across all served Enterprises (same IP address).

- **Dynamic advertisement of WAN-IP Pools and learned LAN prefixes**
  
  eBGP is used to advertise the Enterprise WAN-IP Pools and the LAN prefixes learned via NEMO for the associated Enterprise.

- **N-MHAE credentials**
  
  NEMO4G-HA supports local authentication for the NEMO MIPv4 RRQ based on preconfigured N-MHAE-SPI/KEY values on a per Enterprise basis (one unique set for all MRs belonging to the same Enterprise) or on a global basis (one unique set for all Enterprises).

- **LAN prefixes**
  
  - NEMO4G-HA accepts a minimum of zero LAN prefixes and a maximum of eight prefixes per mobile router. Anything beyond eight prefixes shall be silently discarded.
  - NEMO4G-HA supports any prefix length (including /32).
  - NEMO4G-HA supports dynamic prefix updates.
Network Mobility (NEMO)

NEMO Overview

- NEMO4G-HA removes from the associated Enterprise VRF routing table any prefixes that are not included in a scheduled or ad-hoc NEMO MIPv4 re-registration request from a given MR (assuming these were present in a previous NEMO MIPv4 RRQ). E-PGW shall update the external VRF router of the removal of such prefixes on the next eBGP update.

- NEMO4G-HA accepts and installs any new prefixes that are included in a scheduled or ad-hoc NEMO MIPv4 re-registration request to the associated Enterprise VRF routing table, as long as it doesn't exceed the maximum number of supported prefixes per MR (up to eight). E-PGW shall update the external VRF router of the newly installed prefixes on the next eBGP update. NEMO4G-HA shall accept NEMO MIPv4 RRQs that do not include any prefixes in the first initial RRQ and it shall accept prefixes advertised in subsequent RRQs.

- In case of a prefix whose IP address or mask is changed on the MR, the MR will remove the old IP address/mask and add the new IP address/mask prefix in a scheduled or ad-hoc NEMO MIPv4 re-registration request and NEMO4G-HA shall remove the old route and add the new route corresponding to the new prefix to the Enterprise VRF routing table.

- Overlapping IP addressing
  NEMO4G-HA supports private and overlapping IP addressing across multiple Enterprises for the WAN IP pools, MR-HADDR, and LAN prefixes.

NEMO MR Authorization

NEMO4G-HA authorizes a NEMO MIPv4 session only if a NEMO permission has been assigned to the underlying PDN connection. NEMO permission should be assigned to the underlying PDN connection via either local configuration (APN parameter) or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter is supported to enable NEMO permission at the APN/PDN level within the P-GW service.

MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client. NEMO4G-HA processes the first of three Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The three Cisco-specific NVSEs are placed after the MIPv4 “Identification” field and before the mandatory MIPv4 “Mobile-Home-Authentication-Extension.” NEMO4G-HA accepts the LAN prefixes (up to eight) encoded in the first Cisco-specific NVSE (vendor-type = 9). NEMO4G-HA is not expected to process the other two Cisco-specific NVSEs with vendor-type = 49, which carry the Internal Interface ID of the MR’s Roaming Interface and the MR’s Roaming Interface Bandwidth in Kbps, respectively.

Cisco-specific NVSEs follow RFC 3025 “Mobile IP Vendor/Organization Specific Extensions.”

GRE Encapsulation

User traffic shall be encapsulated over a GRE tunnel between the MR NEMO client and NEMO4G-HA. The IP endpoints of the GRE tunnel shall be the IPv4 assigned to the MR modem during the Enterprise PDN connection setup and the IPv4 address of the NEMO4G-HA service on the E-PGW.

NEMO4G-HA shall remove the GRE encapsulation before it forwards the outbound traffic towards the Enterprise VPN via the associated SGi VLAN interface. Inbound traffic received through the same SGi VLAN interface shall be encapsulated into a GRE tunnel before it's passed to the E-PGW service for forwarding to the MR through the proper GTP/PMIP tunnel.
Session Interactions

The following session interaction scenarios are supported between NEMO and the underlying PDN connection made over eHRPD or LTE access.

In the following circumstances, NEMO4G-HA shall withdraw the associated prefix routes from the Enterprise VRF routing table, update the eBGP neighbors and free up all internal resources allocated for the underlying PDN connection and NEMO session:

- When the eHRPD terminates the underlying PDN connection (PPP-VSNCP-Term-Req sent to MR and PMIP-BU with lifetime = 0 sent to E-PGW).
- When the MR terminates the PPP/PDN connection when accessing the network via eHRPD.
- After an eUTRAN (LTE) detach procedure initiated by the MR or MME.

NEMO4G-HA shall not be able to process any NEMO MIPv4 RRQs if there’s no underlying PDN connection associated to those RRQs (PMIPv6 or GTP). In other words, NEMO MIPv4 RRQs can be accepted and processed only if an Enterprise PDN connection has been established with E-PGW by the mobile router.

NEMO4G-HA shall silently ignore NEMO MIPv4 RRQs if the underlying PDN connection associated to each of those RRQs does not have the NEMO permission indication. This applies to both eHRPD and LTE access.

NEMO4G-HA shall forward (not drop) user data using MIP or GRE tunneling (UDP/434 or IP Protocol/47, respectively) to the external enterprise VRF if such data is not destined to the NEMO4G-HA IP address. This applies to PDN connections that have or do not have the NEMO Permission indication. This shall also apply to both eHRPD and LTE access.

Any failure on either the authentication or authorize of a NEMO MIPv4 session shall not affect the underlying PDN connection established between the mobile router and the E-PGW via eHRPD or LTE. For example, if the security credentials do not match between the MR NEMO client and NEMO4G-HA, NEMO4G-HA can reject the NEMO MIPv4 RRQ, but the associated PDN connection shall not be terminated.

NEMO Session Timers

NEMO4G-HA uses the registration lifetime value locally configured, even though MR's may use the maximum possible value (65534).

NEMO4G-HA can process ad-hoc NEMO RRQ messages.

Enterprise-wide Route Limit Control

NEMO4G-HA supports a control mechanism to limit the maximum number of prefixes/routes that a given enterprise can register, including the pools for WAN IP assignments.

When the maximum number of routes is reached, a syslog message is generated. Once the number of routes goes under the limit, a syslog message is generated for notification.

Forced Fragmentation

E-PGW forces IP packet fragmentation even for IP packets with the DF-bit set.

Redundancy/Reliability

The LTE NEMO solution supports intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.
LTE NEMO Call Flow

The following figure describes the call flow of the NEMOv4 solution.

Figure 59. NEMOv4 Call Flow

1. The Cisco MR eHWIC establishes first a connection to the IMS PDN to register to the LTE Network. The eHWIC's User Id must be properly provisioned on the HSS/SPR to be successfully authenticated.

2. After the Cisco MR eHWIC registers with the LTE network and establishes a connection to the IMS PDN, then it connects to the appropriate Enterprise PDN based on the locally configured Enterprise APN.
   - During the PDN authorization procedure using S6b, the 3GPP AAA assigns a NEMO permission via AVP. The AVP is also be available as an APN parameter on the E-PGW to allow NEMO service at the PDN/Enterprise level.
   - E-PGW assigns the MR eHWIC an IPv4 address from the Enterprise IPv4 pool assigned during PDN authentication.
   - E-PGW creates the proper flows internally to forward packets to the corresponding VRF external to the E-PGW platform using the IPv4 pool configuration on the egress context.
   - The MR eHWIC passed on the assigned IPv4 address to the NEMO application (also called WAN-IPv4 address).

3. The MR NEMO application initiates a Mobile IPv4 registration request (RRQ) using the following local configuration and the IPv4 address assigned to the eHWIC during the Enterprise PDN attach procedure.
Network Mobility (NEMO)

NEMO Overview

The NEMO MIPv4 RRQ will be carried as a regular user packet over the mobility connection, either GTP in LTE and PPP/PMIPv6 in eHRPD. The NEMO MIPv4 RRQ includes the following key parameters:

- **CCOA** - IPv4 address assigned to the eHWIC modem during the Enterprise PDN connection setup (WAN-IP). The MR NEMO application will use the CCOA/WAN-IP address as the source of all NEMO packets sent to NEMO4G-HA (control and tunneled user traffic).
- **MR-HADDR** - Mandatory IPv4 address preconfigured in the MR NEMO application. MR-HADDR is normally used as the source of all NEMO control packets sent to the NEMO4G-HA. However, the MR NEMO application will use the CCOA as the source for all NEMO packets (control and tunneled user traffic). Therefore, NEMO4G-HA will ignore the preconfigured MR-HADDR included in the RRQ, but it will still include it in the NEMO MIPv4 RRP.
- **Home Agent Address** - Preconfigured IPv4 address that the MR NEMO application uses as the destination for all NEMO control and GRE tunneled user data (NEMO4G-HA's IPv4 Address).
- **Explicit LAN Prefixes** - Locally attached IPv4 networks preconfigured on the MR NEMO application. LAN prefixes will be encoded in the same Cisco NVSE extension currently used in the NEMO solution for 3G. The Cisco NVSE included in the NEMOv4 MIP RRQ is in the form of a TLV.
- **N-MHAE** - Mandatory NEMO MN-HA Authentication Extension that includes the SPI and the authenticator computed using a pre-shared Key. Both SPI and Key are preconfigured in the MR NEMO application as well.
- **NEMO-Tunnel flags** such as, but not limited to, “Reverse Tunnel,” “Direct Termination,” “Tunnel Encapsulation” = GRE.

4. NEMO4G-HA sends a MIP registration response (RRP) back to the MR after it performs the following tasks:
   - Authenticate the RRQ using the N-MHAE information included in the RRQ.
   - Authorize the NEMO service based on the NEMO permission attribute assigned to the associated Enterprise PDN connection.
   - Accept the prefixes advertised in the Cisco NVSE extension included in the NEMO MIPv4 RRQ.
     - The learned prefixes will have to adhere to the current rules of valid pool routes. The minimum valid mask length is /13 and pool routes can not include 0.0.0.0 or 255.255.255.255.
     - NEMO4G-HA will accept a minimum of 0 prefixes and a maximum of 8 prefixes. Anything beyond 8 prefixes will be silently discarded.
     - NEMO4G-HA will also check that the new resultant enterprise route count (total number of VRF routes) do not exceed the route limit potentially configured for the given enterprise. If the preconfigured route limit is exceeded, then NEMO4G-HA will reject the NEMO MIP RRQ. Otherwise, NEMO4G-HA will install the accepted prefixes in the internal VRF associated with the Enterprise PDN.
     - eBGP would then propagate the new NEMO routes to the external VRF as part of the next BGP update.

5. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table to route all traffic through the LTE connection.
   - Outbound packets are encapsulated over GRE using the CCOA/WAN-IP address as the source and the NEMO4G-HA-Service IPv4 address as the destination of the tunnel.
   - Inbound packets are encapsulated over GRE as well from the NEMO4G-HA to the MR NEMO application. The source of the GRE tunnel is the NEMO4G-HA-Service IPv4 address and the destination is the CCOA/WAN-IP address.
Engineering Rules

- Up to 100 virtual routing tables per context. This allows up to 100 BGP-VPNs per context.
- Up to 5k host routes spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Up to 1024 VRFs per chassis.

Supported Standards

- IETF RFC 3025 (February 2001) “Mobile IP Vendor/Organization Specific Extensions”
- IETF RFC 1191 (November 1990) “Path MTU Discovery”
NEMO Configuration

**Important:** Commands used in the configuration samples 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.

To configure the system for NEMO:

1. Create a VRF on the router and assign a VRF-ID by applying the example configuration in the Create a VRF section.
2. Set the neighbors and address family to exchange routing information with a peer router by applying the example configuration in the Set Neighbors and Address Family section.
3. Redistribute connected routes between routing domains by applying the example configuration in the REDistribute Connected Routes section.
4. Allow the P-GW to use the NEMO service by applying the example in the Configure and Enable NEMO in APN Profile section.
5. Create a NEMO HA by applying the example in the Create a NEMO HA section.
6. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Sample Configuration

```plaintext
context egress

interface corp1-outbound
  ip address 192.168.1.1 255.255.255.0

exit

ip vrf corp1
ip pool corp1-test 10.1.1.1 255.255.255.0 private vrf corp1
nexthop-forwarding-address 192.168.1.2 overlap vlanid 50
router bgp 100
  address-family ipv4 vrf corp1
    neighbor 192.168.1.2 remote-as 300
    neighbor 192.168.1.2 allow-default-vrf-connection
    redistribute connected
```
Create a VRF

Use this example to first create a VRF on the router and assign a VRF-ID.

configure

context <context_name> -noconfirm

ip vrf <vrf_name>

ip pool <pool_name> <pool_address> private vrf <vrf_name>

next-hop-forwarding-address <ip_address> overlap vlanid <vlan_id>
Set Neighbors and Address Family

Use this example to set the neighbors and address family to exchange routing information with a peer router.

```bash
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
      ip vrf <vrf_name>
        neighbor <ip_address> remote-as <AS_num>
        address-family <type>
        neighbor <ip_address> activate
    end
end
```

Redistribute Connected Routes

Use this example to redistribute connected routes between routing domains.

```bash
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
      ip vrf <vrf_name>
        address-family <type> vrf <vrf_name>
        redistribute connected
        exit
        redistribute connected
    end
end
```

Configure and Enable NEMO in APN Profile

Use this example to configure and enable NEMO in an APN profile.

```bash
configure
  context <context_name>
```
apn <apn_name>
  permission nemo
ip context-name <name>
ip address pool name <pool_name>
end

Create a NEMO HA

Use this example to create a NEMO HA.

configure
  context <context_name>
    ha-service <ha_service_name>
      mn-ha-spi spi-number <number> encrypted secret <enc_secret>
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address <ip_address>
    end
Chapter 15
Operator Policy

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

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

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

This document includes the following information:

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

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

A Look at Operator Policy on an SGSN

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

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

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

A Look at Operator Policy on an S-GW

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

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

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

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

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

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

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

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

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

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

**Call Control Profile**

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

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

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

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

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

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

APN Profile

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

For example:

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

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

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

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

IMEI-Profile (SGSN only)

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

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

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

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

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

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

APN Remap Table

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

• An APN is provided in the Activation Request that does not match with any of the subscribed APNs; either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN would reject the Activation Request. It is possible to correct the APN, creating a valid name so that the Activation Request is not rejected.

• In some cases, an operator might want to force certain devices/users to use a specific APN. For example, all iPhone4 users may need to be directed to a specific APN. In such situations, the operator needs to be able to override the selected APN.

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

• APN aliasing - maps incoming APN to a different APN based on partial string match (MME and SGSN) or matching charging characteristic (MME and SGSN).

• Wildcard APN - allows APN to be provided by the SGSN when wildcard subscription is present and the user has not requested an APN.

• Default APN - allows a configured default APN to be used when the requested APN cannot be used — for example, the APN is not part of the HLR subscription.
APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

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

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

**Operator Policies**

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

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

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

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

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

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

---

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

---

**IMSI Ranges**

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

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

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

Figure 60. Operator Policy Selection Logic
Operator Policy Configuration

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

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

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

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

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

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

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

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

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

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

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

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

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide.

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

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

Configuring the Call Control Profile for an SGSN

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

```
call-control-profile <profile_name>>
  attach allow access-type umts location-area-list instance <list_id>
  authenticate attach
  location-area-list instance <instance> area-code <area_code>
  sgsn-number <E164_number>
end
```

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

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

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

```
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.

```
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

imei-profile <profile_name>
    ggsn-address 211.211.123.3
    direct-tunnel not-permitted-by-ggsn (SGSN only)
    associate apn-remap-table remap1
```
Notes:
- It is optional to configure an IMEI profile. An operator policy can include IMEI profiles and/or APN profiles.
- This profile will only become valid when it is associated with an operator policy.

**APN Remap Table Configuration**

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

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

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

```
configure

apn-remap-table <table_name>
  apn-selection-default first-in-subscription
  wildcard-apn pdp-type ipv4 network-identifier <apn_net_id>
  blank-apn network-identifier <apn_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.
Operator Policy Configuration

```
configure

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

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

**Associating Operator Policy Components on the MME**

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

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

Use the following example to configure operator policy component associations:

```
configure

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

lte-policy

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

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

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

## Configuring Accounting Mode for S-GW

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

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

```
configure

calendar <sgw_context_name>

    sgw-service <sgw_srv_name>

        accounting mode radius-diameter

    end

end
```

Notes:

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

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

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

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

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

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

```
[local]asr5x00# show operator-policy full name oppolicy1

Operator Policy Name = oppolicy1

Call Control Profile Name : ccprofile1
  Validity : Valid

APN Remap Table Name : remap1
  Validity : Valid

IMEI Range 711919739 to 711919777

IMEI Profile Name : imeiprofil
  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 16
Proxy-Mobile IP

This chapter describes system support for Proxy Mobile IP 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 before using the procedures in this chapter.

Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:
- Overview
- How Proxy Mobile IP Works in 3GPP2 Network
- How Proxy Mobile IP Works in 3GPP Network
- How Proxy Mobile IP Works in WiMAX Network
- How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication
- Configuring Proxy Mobile-IP Support
Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

**Important:** Proxy Mobile IP 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*.

The Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

<table>
<thead>
<tr>
<th>Applicable Product(s)</th>
<th>Refer to Sections</th>
</tr>
</thead>
</table>
| PDSN                  | • Proxy MobileIP in 3GPP2 Service  
                    | • How Proxy Mobile IP Works in 3GPP2 Network  
                    | • Configuring FA Services  
                    | • Configuring Proxy MIP HA Failover  
                    | • Configuring HA Services  
                    | • Configuring Subscriber Profile RADIUS Attributes  
                    | • RADIUS Attributes Required for Proxy Mobile IP  
                    | • Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN  
                    | • Configuring Default Subscriber Parameters in Home Agent Context |
| GGSN                  | • Proxy MobileIP in 3GPP Service  
                    | • How Proxy Mobile IP Works in 3GPP Network  
                    | • Configuring FA Services  
                    | • Configuring Proxy MIP HA Failover  
                    | • Configuring HA Services  
                    | • Configuring Subscriber Profile RADIUS Attributes  
                    | • RADIUS Attributes Required for Proxy Mobile IP  
                    | • Configuring Default Subscriber Parameters in Home Agent Context  
                    | • Configuring APN Parameters |
### Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber’s profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider’s network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider’s network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

### Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber’s profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).
The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider’s network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber’s profile take precedence over the configuration of the APN.

**Proxy Mobile IP in WiMAX Service**

For subscriber sessions using Proxy Mobile, subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber’s profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider’s network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.
How Proxy Mobile IP Works in 3GPP2 Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1**: The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.
- **Scenario 2**: The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

**Scenario 1: AAA server and PDSN/FA Allocate IP Address**

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.
How Proxy Mobile IP Works in 3GPP2 Network

Figure 61. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

Table 28. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.</td>
</tr>
<tr>
<td>2</td>
<td>The PCF and PDSN/FA establish the R-P interface for the session.</td>
</tr>
<tr>
<td>3</td>
<td>The PDSN/FA and MN negotiate Link Control Protocol (LCP).</td>
</tr>
<tr>
<td>4</td>
<td>Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.</td>
</tr>
</tbody>
</table>
### How Proxy Mobile IP Works in 3GPP2 Network

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>The PDSN/FA sends an Access Request message to the RADIUS AAA server.</td>
</tr>
<tr>
<td>6</td>
<td>The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN’s Home Address (IP address) and the IP address of the HA to use.</td>
</tr>
<tr>
<td>7</td>
<td>The PDSN/FA sends a PPP Authentication Response message to the MN.</td>
</tr>
<tr>
<td>8</td>
<td>The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.</td>
</tr>
<tr>
<td>9</td>
<td>The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN’s home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</td>
</tr>
<tr>
<td>10</td>
<td>While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.</td>
</tr>
<tr>
<td>11</td>
<td>The HA responds with a Proxy Mobile IP Registration Response after validating the home address against its pool. The HA also creates a mobile binding record (MBR) for the subscriber session.</td>
</tr>
<tr>
<td>12</td>
<td>The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.</td>
</tr>
<tr>
<td>13</td>
<td>While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.</td>
</tr>
<tr>
<td>14</td>
<td>Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.</td>
</tr>
<tr>
<td>15</td>
<td>Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.</td>
</tr>
<tr>
<td>16</td>
<td>The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.</td>
</tr>
<tr>
<td>17</td>
<td>The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.</td>
</tr>
<tr>
<td>18</td>
<td>The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface.</td>
</tr>
<tr>
<td>19</td>
<td>The PDSN/FA and the PCF terminate the R-P session.</td>
</tr>
<tr>
<td>20</td>
<td>The HA and the AAA server stop accounting for the session.</td>
</tr>
<tr>
<td>21</td>
<td>The PDSN and the AAA server stop accounting for the session.</td>
</tr>
</tbody>
</table>

### Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.
Figure 62. HA Assigned IP Address Proxy Mobile IP Call Flow

Table 29. HA Assigned IP Address Proxy Mobile IP Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.</td>
</tr>
<tr>
<td>2</td>
<td>The PCF and PDSN/FA establish the R-P interface for the session.</td>
</tr>
<tr>
<td>3</td>
<td>The PDSN/FA and MN negotiate Link Control Protocol (LCP).</td>
</tr>
<tr>
<td>4</td>
<td>Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td>The PDSN/FA sends an Access Request message to the RADIUS AAA server.</td>
</tr>
<tr>
<td>6</td>
<td>The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.</td>
</tr>
<tr>
<td>7</td>
<td>The PDSN/FA sends a PPP Authentication Response message to the MN.</td>
</tr>
<tr>
<td>8</td>
<td>The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.</td>
</tr>
<tr>
<td>9</td>
<td>The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</td>
</tr>
<tr>
<td>10</td>
<td>While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.</td>
</tr>
<tr>
<td>11</td>
<td>The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.</td>
</tr>
<tr>
<td>12</td>
<td>The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.</td>
</tr>
<tr>
<td>13</td>
<td>While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.</td>
</tr>
<tr>
<td>14</td>
<td>Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.</td>
</tr>
<tr>
<td>15</td>
<td>Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.</td>
</tr>
<tr>
<td>16</td>
<td>The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.</td>
</tr>
<tr>
<td>17</td>
<td>The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.</td>
</tr>
<tr>
<td>18</td>
<td>The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface</td>
</tr>
<tr>
<td>19</td>
<td>The PDSN/FA and the PCF terminate the R-P session.</td>
</tr>
<tr>
<td>20</td>
<td>The HA and the AAA server stop accounting for the session.</td>
</tr>
<tr>
<td>21</td>
<td>The PDSN and the AAA server stop accounting for the session.</td>
</tr>
</tbody>
</table>
How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network. The following figure and the text that follows describe a a sample successful Proxy Mobile IP session setup call flow in 3GPP service.

**Figure 63. Proxy Mobile IP Call Flow in 3GPP**

![Proxy Mobile IP Call Flow in 3GPP](image-url)
Table 30. Proxy Mobile IP Call Flow in 3GPP Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.</td>
</tr>
<tr>
<td>2</td>
<td>The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the MS to place it into PPP mode. The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information. Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.</td>
</tr>
<tr>
<td>3</td>
<td>The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.</td>
</tr>
<tr>
<td>4</td>
<td>The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, “C” indicates the control signalling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).</td>
</tr>
<tr>
<td>5</td>
<td>The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact. Note that Proxy Mobile IP support can also be determined by attributes in the user’s profile. Attributes in the user’s profile supersede APN settings. If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to a AAA server.</td>
</tr>
<tr>
<td>6</td>
<td>If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.</td>
</tr>
<tr>
<td>7</td>
<td>If Proxy Mobile IP support was either enabled in the APN or in the subscriber’s profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS’s home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</td>
</tr>
<tr>
<td>8</td>
<td>The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.</td>
</tr>
<tr>
<td>9</td>
<td>The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.</td>
</tr>
<tr>
<td>10</td>
<td>The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.</td>
</tr>
<tr>
<td>11</td>
<td>The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.</td>
</tr>
<tr>
<td>12</td>
<td>The MT, will respond to the TE’s IPCP Config-Request with an IPCP Config-Ack message. The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.</td>
</tr>
<tr>
<td>13</td>
<td>The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>14</td>
<td>The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.</td>
</tr>
<tr>
<td>15</td>
<td>The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).</td>
</tr>
<tr>
<td>16</td>
<td>The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.</td>
</tr>
<tr>
<td>17</td>
<td>The GGSN returns a Delete PDP Context Response message to the SGSN.</td>
</tr>
<tr>
<td>18</td>
<td>The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.</td>
</tr>
<tr>
<td>19</td>
<td>The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to.</td>
</tr>
<tr>
<td>20</td>
<td>The SGSN returns a Deactivate PDP Context Accept message to the MS.</td>
</tr>
<tr>
<td>21</td>
<td>The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.</td>
</tr>
<tr>
<td>22</td>
<td>For each accounting message received from the GGSN, the CG responds with an acknowledgement.</td>
</tr>
</tbody>
</table>
How Proxy Mobile IP Works in WiMAX Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

**Scenario 1: AAA server and ASN GW/FA Allocate IP Address**

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.
Figure 64. AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile Node (MN) secures a traffic channel over the airlink with the BS.</td>
</tr>
<tr>
<td>2</td>
<td>The BS and ASN GW/FA establish the R6 interface for the session.</td>
</tr>
<tr>
<td>3</td>
<td>The ASN GW/FA and MN negotiate Link Control Protocol (LCP).</td>
</tr>
<tr>
<td>4</td>
<td>Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.</td>
</tr>
</tbody>
</table>
How Proxy Mobile IP Works in WiMAX Network

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>The ASN GW/FA sends an Access Request message to the RADIUS AAA server.</td>
</tr>
<tr>
<td>6</td>
<td>The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the MN’s Home Address (IP address) and the IP address of the HA to use.</td>
</tr>
<tr>
<td>7</td>
<td>The ASN GW/FA sends an EAP Authentication Response message to the MN.</td>
</tr>
<tr>
<td>8</td>
<td>The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.</td>
</tr>
<tr>
<td>9</td>
<td>The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN’s home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</td>
</tr>
<tr>
<td>10</td>
<td>While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.</td>
</tr>
<tr>
<td>11</td>
<td>The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it’s pool. The HA also creates a mobile binding record (MBR) for the subscriber session.</td>
</tr>
<tr>
<td>12</td>
<td>The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.</td>
</tr>
<tr>
<td>13</td>
<td>While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.</td>
</tr>
<tr>
<td>14</td>
<td>Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.</td>
</tr>
<tr>
<td>15</td>
<td>Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.</td>
</tr>
<tr>
<td>16</td>
<td>The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.</td>
</tr>
<tr>
<td>17</td>
<td>The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session.</td>
</tr>
<tr>
<td>18</td>
<td>The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface</td>
</tr>
<tr>
<td>19</td>
<td>The ASN GW/FA and the BS terminate the R6 session.</td>
</tr>
<tr>
<td>20</td>
<td>The HA and the AAA server stop accounting for the session.</td>
</tr>
<tr>
<td>21</td>
<td>The ASN GW and the AAA server stop accounting for the session.</td>
</tr>
</tbody>
</table>

---

**Scenario 2: HA Allocates IP Address**

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.
How Proxy Mobile IP Works in WiMAX Network

**Figure 65.** HA Assigned IP Address Proxy Mobile IP Call Flow

**Table 32.** HA Assigned IP Address Proxy Mobile IP Call Flow Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile Node (MN) secures a traffic channel over the airlink with the BS.</td>
</tr>
<tr>
<td>2</td>
<td>The BS and ASN GW/FA establish the R6 interface for the session.</td>
</tr>
<tr>
<td>3</td>
<td>The ASN GW/FA and MN negotiate Link Control Protocol (LCP).</td>
</tr>
<tr>
<td>4</td>
<td>Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td>The ASN GW/FA sends an Access Request message to the RADIUS AAA server.</td>
</tr>
<tr>
<td>6</td>
<td>The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.</td>
</tr>
<tr>
<td>7</td>
<td>The ASN GW/FA sends an EAP Authentication Response message to the MN.</td>
</tr>
<tr>
<td>8</td>
<td>The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.</td>
</tr>
<tr>
<td>9</td>
<td>The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</td>
</tr>
<tr>
<td>10</td>
<td>While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.</td>
</tr>
<tr>
<td>11</td>
<td>The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.</td>
</tr>
<tr>
<td>12</td>
<td>The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.</td>
</tr>
<tr>
<td>13</td>
<td>While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.</td>
</tr>
<tr>
<td>14</td>
<td>Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.</td>
</tr>
<tr>
<td>15</td>
<td>Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.</td>
</tr>
<tr>
<td>16</td>
<td>The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.</td>
</tr>
<tr>
<td>17</td>
<td>The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.</td>
</tr>
<tr>
<td>18</td>
<td>The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface.</td>
</tr>
<tr>
<td>19</td>
<td>The ASN GW/FA and the BS terminate the R6 session.</td>
</tr>
<tr>
<td>20</td>
<td>The HA and the AAA server stop accounting for the session.</td>
</tr>
<tr>
<td>21</td>
<td>The ASN GW and the AAA server stop accounting for the session.</td>
</tr>
</tbody>
</table>
How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers. Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool. The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.
Table 33. Proxy-MIP Call Setup using CHAP Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On connecting to WiFi network, MS first send DNS query to get PDIF IP address</td>
</tr>
<tr>
<td>2</td>
<td>MS receives PDIF address from DNS</td>
</tr>
<tr>
<td>3</td>
<td>MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP address in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDIF service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Response. PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.</td>
</tr>
<tr>
<td>5</td>
<td>On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload which contains the NAI, SA, TSi, TSr, CP (requesting IP address and DNS address) payloads. MS will not include AUTH payload to indicate that it will use EAP methods.</td>
</tr>
<tr>
<td>6</td>
<td>On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA servers are selected based on domain profile, default subscriber template or default domain configurations. PDIF includes Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details are explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Request from MS.</td>
</tr>
<tr>
<td>7</td>
<td>PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Payload AVP contents and sends IKE_AUTH Response back to MS in the EAP payload. PDIF allows IDr and CERT configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is configured to do so.</td>
</tr>
<tr>
<td>8</td>
<td>MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AUTH Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challenge received from MS.</td>
</tr>
<tr>
<td>9</td>
<td>The AAA server sends the DEA back to the PDIF with Result-Code AVP as “success.” The EAP-Payload AVP message also contains the EAP result code with “success.” The DEA also contains the IMSI for the user, which is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions such as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.</td>
</tr>
<tr>
<td>10</td>
<td>PDIF sends the IKE_AUTH Response back to MS with the EAP payload.</td>
</tr>
<tr>
<td>11</td>
<td>MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed from the keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS Notify payload also.</td>
</tr>
<tr>
<td>12</td>
<td>PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH payload computed from the MSK. PDIF does not assign any IP address for the MS pending second authentication. Nor will the PDIF include any configuration payloads. a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify payload is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 session by sending INFORMATIONAL (Delete) Request. b. If ANOTHER_AUTH_FOLLOWS Notify payload is not present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. However, if proxy-mip-required is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ. When PDIF receives the Proxy-MIP RR, it takes the Home Address (and DNS addresses if any) and sends the IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. In either case, IKEv2 setup will finish at this stage and IPSec tunnel gets established with a Tunnel Inner Address (TIA).</td>
</tr>
<tr>
<td>13</td>
<td>MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include the NAI. This NAI may be completely different from the NAI used in the first authentication.</td>
</tr>
</tbody>
</table>
## How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

### Step Description

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14   | On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second authentication methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP methods may be either EAP-Passthru or EAP-Terminated.  
   a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload including challenge.  
   b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC.  
   c. MS processes the IKE_AUTH Response:  
      - If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the challenge, compute the response and send IKE_AUTH Request with EAP payload including Challenge and Response.  
      - If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the MS sends legacy-Nak with EAP-GTC. |
| 15(a) | PDIF receives the new IKE_AUTH Request from MS. If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Access Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.). |
| 15(b) | If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_AUTH Response with EAP-GTC. |
| 16   | PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success. |
| 17   | PDIF receives the final IKE_AUTH Request with AUTH payload. |
| 18   | PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Agent if `proxy-mip-required` is enabled. The HA address may be received from the RADIUS server in the Access Accept (Step 16) or may be locally configured. PDIF may also remember the HA address from the first authentication received in the final DEA message. |
| 19   | If `proxy-mip-required` is disabled, PDIF assigns the IP address from the local pool. |
| 20   | PDIF received proxy-MIP RRP and gets the IP address and DNS addresses. |
| 21   | PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also sets up the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by including the CP payload with the IP address and optionally the DNS addresses. This completes the setup. |
| 22   | PDIF sends a RADIUS Accounting start message. |

### Important: For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.
Figure 67. Proxy-MIP Call Setup using PAP Authentication

Table 34. Proxy-MIP Call Setup using PAP Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.</td>
</tr>
<tr>
<td>16</td>
<td>PDIF then initiates EAP-GTC procedure, and requests a password from MS.</td>
</tr>
<tr>
<td>17</td>
<td>MS includes an authentication password in the EAP payload to PDIF.</td>
</tr>
<tr>
<td>18</td>
<td>Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Name attribute and PAP-password.</td>
</tr>
<tr>
<td>19</td>
<td>Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may include Framed-IP-Address attribute.</td>
</tr>
<tr>
<td>20</td>
<td>The attribute content in the Access Accept message is encoded as EAP payload with EAP success when PDIF sends the IKE_AUTH Response to the MS.</td>
</tr>
<tr>
<td>21</td>
<td>The MS and PDIF now have a secure IPSec tunnel for communication.</td>
</tr>
<tr>
<td>22</td>
<td>PDIF sends an Accounting START message.</td>
</tr>
</tbody>
</table>
Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:

**Important:** Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.

**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

```plaintext
configure

context <context_name>

fa-service <fa_service_name>

proxy-mip allow

proxy-mip max-retransmissions <integer>

proxy-mip retransmission-timeout <seconds>

proxy-mip renew-percent-time percentage

fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number { encrypted secret enc_secret | secret secret } [ description string ] [ hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } ] replay-protection { timestamp | nonce } [ timestamp-tolerance tolerance ]

authentication mn-ha allow-noauth

end
```
Notes:

- The `proxy-mip max-retransmissions` command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- `proxy-mip retransmission-timeout` configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
- `proxy-mip renew-percent-time` configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50%, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of 600 seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after 300 seconds have passed.

- Use the `fa-ha-spi remote-address` command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the Command Line Interface Reference for the full command syntax.

**Important:** Note that FA-HA SPIs must be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the `authentication mn-ha allow-noauth` command to configure the FA service to allow communications from the HA without authenticating the HA.

Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- 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.

Proceed to the optional Configuring Proxy MIP HA Failover section to configure Proxy MIP HA Failover support or skip to the Configuring HA Services section to configure HA service support for Proxy Mobile IP.

Configuring Proxy MIP HA Failover

Use this example to configure Proxy MobileIP HA Failover:

**Important:** This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:
configure

context <context_name>

fa-service <fa_service_name>

    proxy-mip ha-failover [ max-attempts <max_attempts> | num-attempts- before-switching <num_attempts> | timeout <seconds> ]

Notes:
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec
  mode command save configuration. For additional information on how to verify and save configuration
  files, refer to the System Administration Guide and the Command Line Interface Reference.

Configuring HA Services

Use the following configuration example to configure HA services to support Proxy Mobile IP.

configure

context <context_name>

    ha-service <ha_service_name>

**Important:** Note that FA-HA SPIs must be configured for the Proxy MIP feature to work while it is optional for
regular MIP. Also note that the above syntax assumes that FA-HA SPIs were previously configured as part of the HA
service as described in respective product Administration Guide. The replay-protection and timestamp- 
tolerance keywords should only be configured when supporting Proxy Mobile IP.

fa-ha-spi remote-address <fa_ip_address> spi-number <number> { encrypted secret
    <enc_secret> | secret <secret> } [ description <string> ] [ hash-algorithm | hmac-md5 | md5 | rfc2002-md5 ] replay-protection { timestamp | nonce } | timestamp-tolerance
    <tolerance> ]

    authentication mn-ha allow-noauth
    authentication mn-aaa allow-noauth

end

Notes:
- Repeat this example as needed to configure additional HA services to support Proxy-MIP.
- 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.

To verify the configuration of the HA service:

context <context_name>

    show ha-service name <ha_service_name>
Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

**Important:** Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

### RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

<table>
<thead>
<tr>
<th>Attribute (SN- or SN1-)</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
</table>
| SN-Subscriber-Permission OR SN1-Subscriber-Permission | Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute **must** be set to Simple IP. | None (0)  
Simple IP (0x01)  
Mobile IP (0x02)  
Home Agent Terminated Mobile IP (0x04) |
| SN-Proxy-MIP OR SN1-Proxy-MIP | Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute **must** be enabled to support Proxy Mobile IP. | Disabled - do not perform compulsory Proxy-MIP (0)  
Enabled - perform compulsory Proxy-MIP (1) |
| SN-Simultaneous-SIP-MIP OR SN1-Simultaneous-SIP-MIP | Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services. | Disabled (0)  
Enabled (1) |

**Important:** Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will **not** allow simultaneous Simple IP and Mobile IP sessions for the MN.
### Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

```bash
configure
c
context <context_name>
  subscriber name <subscriber_name>
  permission pdsn-simple-ip
  proxy-mip allow
  inter-pdsn-handoff require ip-address
  mobile-ip home-agent <ha_address>
  <optional> mobile-ip home-agent <ha_address> alternate
  ip context-name <context_name>
end
```

Verify that your settings for the subscriber(s) just configured are correct.

```bash
show subscribers configuration username <subscriber_name>
```

**Notes:**

- Configure the system to enforce the MN’s use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the `inter-pdsn-handoff require ip-address` command.

- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the `mobile-ip home-agent ha_address alternate` command to specify the secondary, or alternate HA.

### Attribute Table

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-PDSN-Handoff-Req-IP-Addr OR SN1-PDSN-Handoff-Req-IP-Addr</td>
<td>Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.</td>
<td>Disabled - do not reject (0) • Enabled - reject (1)</td>
</tr>
<tr>
<td>3GPP2-MIP-HA-Address</td>
<td>This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>
• Repeat this example as needed to configure additional FA services to support Proxy-MIP.
• Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

```sh
configure
context <context-name>
    subscriber name <subscriber_name>
    proxy-mip require
```

**Note**

*subscriber_name* is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

### Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

```sh
configure
context <context_name>
    ip context-name <context_name>
end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Configuring APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.

**Important:** This is an optional configuration. In addition, attributes returned from the subscriber’s profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

These instructions assume that you are at the root prompt for the Exec mode:

```
[local] host_name#`

---

530

**SAE-GW Administration Guide, StarOS Release 17**
Step 1 Enter the configuration mode by entering the following command:

`configure`

The following prompt appears:

```
[local] host_name(config)#
```

Step 2 Enter context configuration mode by entering the following command:

```
context <context_name>
```

`context_name` is the name of the system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>] host_name(config-ctx)#
```

Step 3 Enter the configuration mode for the desired APN by entering the following command:

```
apn <apn_name>
```

`apn_name` is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). The following prompt appears:

```
[<context_name>] host_name(config-apn)#
```

Step 4 Enable proxy Mobile IP for the APN by entering the following command:

```
proxy-mip required
```

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

Step 5 Optional. GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:

```
proxy-mip null-username static-homeaddr
```

This command will enable the accepting of MIP Registration Request without NAI extensions in this APN.

Step 6 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local] host_name#
```

Step 7 Repeat step 1 through step 6 as needed to configure additional APNs.

Step 8 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a detailed listing of configured APN parameter settings.

Step 9 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.
Configuring Proxy Mobile-IP Support
Chapter 17
Rf Interface Support

This chapter provides an overview of the Diameter Rf interface and describes how to configure the Rf interface.

Rf interface support is available on the Cisco system running StarOS 10.0 or later releases for the following products:

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

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

This chapter describes the following topics:

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

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, S-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/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, S-GW, HSGW, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).
The following figure shows the Rf interface between CTF and CDF.

**Figure 68.  Charging Architecture**

![Charging Architecture Diagram]

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

**Figure 69.  Logical Offline Charging Architecture**

![Logical Offline Charging Architecture Diagram]
Charging Collection Function

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

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

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

Charging Trigger Function

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

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

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

Dynamic Routing Agent

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a 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 (Release 9)
Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

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

Basic Principles

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

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

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

Table 36. 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 37. Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

<table>
<thead>
<tr>
<th>Diameter Message</th>
<th>Triggering SIP Method/ISUP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR [Start]</td>
<td>SIP 200 OK acknowledging an initial SIP INVITE</td>
</tr>
</tbody>
</table>

SAE-GW Administration Guide, StarOS Release 17
### Diameter Message | Triggering SIP Method/ISUP Message
---|---
| ISUP:ANM (applicable for the MGCF) | ISUP:ANM (applicable for the MGCF)  
ACR [Interim]  
SIP 200 OK acknowledging a SIP  
RE-INVITE or SIP UPDATE [e.g. change in media components]  
Expiration of AVP [Acct-Interim-Interval]  
SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE  
ACR [Stop]  
SIP BYE message (both normal and abnormal session termination cases)  
ISUP:REL (applicable for the MGCF)  
ACR [Event]  
SIP 200 OK acknowledging non-session related SIP messages, which are:  
- SIP NOTIFY  
- SIP MESSAGE  
- SIP REGISTER  
- SIP SUBSCRIBE  
- SIP PUBLISH  
SIP 200 OK acknowledging an initial SIP INVITE  
SIP 202 Accepted acknowledging a SIP REFER or any other method  
SIP Final Response 2xx (except SIP 200 OK)  
SIP Final/Redirection Response 3xx  
SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up  
SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure  
SIP CANCEL, indicating abortion of a SIP session set-up

### Event Based Charging

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

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

### Session Based Charging

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

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

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

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

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

Table 38. 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 expiries of Tw without a DWA, the peer is considered to be down.

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

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

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

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

Rf Interface Failures/Error Conditions

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

DRA/CCF Connection Failure

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

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

No Reply from CCF

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

Detection of Message Duplication

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

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

CCF Detected Failure

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

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

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

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers “Service Data Volume Limit” and “Service Data Time Limit”. 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/HRPD/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 70. Rf Call Flow for Event Based Charging**

**Table 39. Rf Call Flow Description for Event Based Charging**

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

The following figure and table explain the simple Rf call flow for session based charging.
### Figure 71. Rf Call Flow for Session Based Charging

![Call Flow Diagram](image)

### Table 40. Rf Call Flow Description for Session Based Charging

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

To configure Rf interface support:

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

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

3. Enable Rf accounting in ACS as described in the Enabling Rf Interface in Active Charging Service section.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN P-GW Rf Interface Support
   - Configuring HSGW Rf Interface Support
   - Configuring P-CSCFS-CSCF Rf Interface Support
   - Configuring S-GW Rf Interface Support
5. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

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

Enabling Rf Interface in Active Charging Service

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

```
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, S-GW, HSGW and CCF for Change-Condition triggers:

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target S-GW/HSGW/Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.
- When multiple change conditions occur, the precedence of reporting change conditions is as follows for S-GW and HSGW only:
  - Normal/Abnormal Release (Stop)
  - Management Intervention (Stop)
  - RAT Change
  - UE Timezone Change
  - Serving Node PLMN Change
  - Max Number of Changes in Charging conditions
  - Volume Limit
  - Time Limit
• Service Data Volume Limit
• Service Data Time Limit
• Service Idled out
• Serving Node Change
• User Location Change
• QoS Change

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

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

Table 41. P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/E-HRPD/GGSN

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

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

Time 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>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>YES, NO</td>
<td>YES, Will include SDC that corresponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volume Limit, Service Data Time Limit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partial FDR</td>
<td>Final FDR</td>
<td>SDC Level</td>
</tr>
<tr>
<td>Stop</td>
<td>Management Intervention</td>
<td>YES</td>
<td>NO, YES</td>
<td>YES, Will include SDC that corresponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volume Limit, Service Data Time Limit)</td>
</tr>
</tbody>
</table>

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 populated in the ACR Interim. 
4. CCF creates the partial record.

Management intervention will close the PDN session from P-GW/GGSN.
Configuring Rf Interface Support

To configure Rf Interface Support, use the following configuration:

```
configure

context <context_name>

hsgw-service<service_name>

   associate accounting-policy <policy_name>

   exit

exit

policy accounting <policy_name>

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

accounting-keys qci

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

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

max-containers { containers | fill-buffer }

exit

end
```
Notes:

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

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

- VOLUME_LIMIT
- TIME_LIMIT

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting(PDN Session based accounting)</th>
<th>EPS bearer level reporting(PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>YE S</td>
<td>Normal Release for all bearers. When PDN session/PDN Session per QCI is closed, C-C in both level will have Normal Release.</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>YE S</td>
<td>Abnormal Release for all bearers</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Abnormal Release</td>
<td>YES NO</td>
<td>NO</td>
<td>N/A</td>
<td>Abnormal Release for the specific bearer that is released. N/A N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>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>N/A</td>
<td>The container for this change condition will be cached by the HSGW and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger. For APN-AMBR change, containers (TDVs) for all existing non-GBR bearers will be cached.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partia UD R</td>
<td>Final UD R</td>
<td>C-C on PS-Information Level</td>
<td>QoS-Change - added to TDV for the bearer that the trigger affected, ACR sent when MaxCCC is reached (if Max CC is provisioned)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C-C on TDV Level</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC on PS-Information Level</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC on TDV Level</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interim</td>
<td>Volume Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Volume Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to HSGW through various interfaces. The charging profile will be provisioned in the HSS.</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Time Limit</td>
<td>YES</td>
<td>YES NO</td>
<td>Time Limit for all bearers</td>
<td>Time Limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Time Limit</td>
<td>The Time Limit is configured as part of the Charging profile and the Charging Characteristics AVP will carry this charging profile that will passed on from the HSS/AAA to HSGW through various interfaces. The charging profile will be provisioned in the HSS.</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 NO NO N/A</td>
<td>Serving Node Change-added to TDV for all bearers, ACR sent when MaxCCC is reached (if MaxCC is configured)</td>
<td>N/A</td>
<td>Serving Node Change-added to TDV, ACR sent when MaxCCC is reached (if MaxCC is configured)</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>N/A</td>
<td>Serving Node PLMN Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions )</td>
<td>User Location Change</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>RAT Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>UE Timezone Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>TariffTime Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### ACR Message | Change-Condition Value | CCF Response to Change-Condition Value | PDN Connection level reporting(PDN Session based accounting) | EPS bearer level reporting(PDN Session per QCI accounting) | Comments
---|---|---|---|---|---
N/A | Service Idled Out | N/A | N/A | N/A | N/A | N/A | N/A
N/A | Service Specific Unit Limit | N/A | N/A | N/A | N/A | N/A | N/A
Interim | Max Number of Changes in Charging Conditions | YES | YES | NO | Max Number of Changes in Charging | TDV corresponds to change condition that occurred (Qos-Change or ULI change or Normal Bearer Release or Abnormal Bearer Release or Serving Node Change) | Max Number of Changes in Charging | TDV corresponds to change condition that occurred (Qos-Change or ULI change or Serving Node Change) | This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. The Max Number of Changes in Charging Conditions is set at 10. Example: [1] Max Number of Changes in Charging Conditions set at S-GW = 2. [2] When Change Condition 1 takes place an ACR[interim] is sent and Traffic-Data-Volumes added to the UDR.
(continued)
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting(PDN Session based accounting)</th>
<th>EPS bearer level reporting(PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Management Intervention</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Management intervention will close the PDN session from P-GW.</td>
</tr>
</tbody>
</table>
Configuring Rf Interface Support

### SAE-GW Administration Guide, StarOS Release 17

#### Configuring Rf Interface Support

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim</td>
<td>-</td>
<td>Addition of Container YES, Partial UDR NO, Final UDR NO</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Configuring P-CSCF/S-CSCF Rf Interface Support

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

```
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
```
Enabling Charging for SIP Methods

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

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

**Important:** Please note that charging is disabled by default.

To enable the charging for all SIP methods except REGISTER, use the following configuration:

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

To enable the charging only for INVITE SIP method, use the following configuration:

```
configure
context vpn
cscf service pcscf
  no charging
  exclude invite
```
Configuring S-GW Rf Interface Support

To configure S-GW Rf interface support, use the following configuration:

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

Notes:

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

Similarly, if the event trigger is one of the following, the containers will be released:
- VOLUME_LIMIT
- TIME_LIMIT
- PLMN_CHANGE
- TIMEZONE_CHANGE

Table 43. S-GW and CCF Behavior for Change-Condition in ACR[Stop] and ACR[Interim] for LTE

<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting(PDN Session based accounting)</th>
<th>EPS bearer level reporting(PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Normal Release</td>
<td>YES</td>
<td>NO</td>
<td>YE S</td>
<td>Normal Release for all bearers, Normal Release, Normal Release, Normal Release, When PDN session/PDN Session per QCI is closed, C-C in both level will have Normal Release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Normal Release</td>
<td>YES NO NO</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Stop</td>
<td>Abnormal Release</td>
<td>YES NO YES</td>
<td>Abnormal Release</td>
<td>Abnormal Release for all bearers</td>
<td>Abnormal Release</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>Abnormal Release</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>---------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>None (as this change condition is a counter for the Max Number of Changes in Charging Conditions)</td>
<td>QoS-Change</td>
<td>YES NO NO</td>
<td>N/A</td>
<td>N/A</td>
<td>The container for this change condition will be cached by the S-GW and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger. For APN-AMBR change, containers (TDVs) for all existing non-GBR bearers will be cached.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C-C on PS-Information Level</td>
<td>C-C on TDV Level</td>
<td>CC on PS-Information Level</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partial UDR</td>
<td>Final UDR</td>
<td></td>
</tr>
<tr>
<td>Interim</td>
<td>Volume Limit</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>Volume Limit for all bearers</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Time Limit</td>
<td>YES</td>
<td>Time Limit for all bearers</td>
<td>Time Limit</td>
<td>The Time Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry the charging profile identifier that is passed from HSS to S-GW via MME. The charging profile value can be configured in the HSS on a per APN basis.</td>
</tr>
<tr>
<td>N/A</td>
<td>Serving Node Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting (PDN Session based accounting)</td>
<td>EPS bearer level reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Serving Node PLMN Change</td>
<td>YES</td>
<td>YES NO</td>
<td>Serving Node PLMN Change for all bearers</td>
<td>PLMN change noticed at the S-GW, without S-GW relocation. eNB/MME may change and belong to a new PLMN (rural operator) or eNB may change with no MME/S-GW relocation; however eNB belongs to new serving network. This Change Condition is required as S-GW could support a MME owned by a rural operator. With S-GW relocation, the old S-GW terminates the Diameter charging session &amp; the new S-GW starts a Diameter charging session (S-GW-Change AVP included).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partia l UDR</td>
<td>Fina l UDR</td>
<td>C-C on PS-Information Level</td>
<td>CC on PS-Information Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td></td>
<td>C-C on TDV Level</td>
<td>CC on TDV Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level Reporting (PDN Session based accounting)</td>
<td>EPS bearer level Reporting (PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of Container</td>
<td>Partial UDR</td>
<td>Final UDR</td>
<td>C-C on PS Information Level</td>
</tr>
<tr>
<td>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>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>RAT Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>RAT Change</td>
</tr>
<tr>
<td>Interim</td>
<td>UE Timezone Change</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>UE Timezone</td>
</tr>
<tr>
<td>N/A</td>
<td>Tariff Time Change</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Idled Out</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>Service Specific Unit Limit</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ACR Message</td>
<td>Change-Condition Value</td>
<td>CCF Response to Change-Condition Value</td>
<td>PDN Connection level reporting(PDN Session based accounting)</td>
<td>EPS bearer level reporting(PDN Session per QCI accounting)</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Interim</td>
<td>Max Number of Changes in Charging Conditions</td>
<td>YES</td>
<td>NO</td>
<td>Max Number of Changes in Charging</td>
<td>TDV corresponds to change condition that occurred (Qos-Change or ULI change or Normal Bearer Termination, Abnormal Bearer Termination.)</td>
</tr>
</tbody>
</table>

This ACR [Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. The Max Number of Changes in Charging Conditions is set at 10.

Example: [1] Max Number of Changes in Charging Conditions set at S-GW = 2. [2] When Change Condition 1 takes place no ACR [interim] is sent, but S-GW will store the container data for this change condition. (continued)
<table>
<thead>
<tr>
<th>ACR Message</th>
<th>Change-Condition Value</th>
<th>CCF Response to Change-Condition Value</th>
<th>PDN Connection level reporting (PDN Session based accounting)</th>
<th>EPS bearer level reporting (PDN Session per QCI accounting)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[3] Change Condition 2 takes place. An ACR Interim is sent. Now Max Number of Changes in Charging conditions is populated in the PS-Information and the both the TDVs for the Change condition 1 and Change Condition 2 is populated in the 2 TDVs. Please note the TDVs need to be in the order that they are created so that the Billing Mediation system is not confused with the usage data sequence. [4] CCF creates the partial record.</td>
</tr>
<tr>
<td>N/A</td>
<td>Management Intervention</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Management intervention will close the PDN session from P-GW.</td>
</tr>
</tbody>
</table>
### ACR Message | Change-Condition Value | CCF Response to Change-Condition Value | PDN Connection level reporting (PDN Session based accounting) | EPS bearer level reporting (PDN Session per QCI accounting) | Comments
---|---|---|---|---|---
Interim | - | YES | NO | NO | N/A | N/A | N/A

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

---

### Gathering Statistics

This section explains how to gather Rf and related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

<table>
<thead>
<tr>
<th>Statistics/Information</th>
<th>Action to perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete statistics for Diameter Rf accounting sessions</td>
<td>show diameter aaa-statistics</td>
</tr>
</tbody>
</table>

The following is a sample output of the `show diameter aaa-statistics` command:

```
Authentication Servers Summary
-----------------------------

Message Stats :
Total MA Requests: 0 Total MA Answers: 0
MAR - Retries: 0 MAA Timeouts: 0
MAA - Dropped: 0
Total SA Requests: 0 Total SA Answers: 0
```
SAR - Retries: 0 SAA Timeouts: 0
SAA - Dropped: 0
Total UA Requests: 0 Total UA Answers: 0
UAR - Retries: 0 UAA Timeouts: 0
UAA - Dropped: 0
Total LI Requests: 0 Total LI Answers: 0
LIR - Retries: 0 LIA Timeouts: 0
LIA - Dropped: 0
Total RT Requests: 0 Total RT Answers: 0
RTR - Rejected: 0
Total PP Requests: 0 Total PP Answers: 0
PPR - Rejected: 0
Total DE Requests: 0 Total DE Answers: 0
DEA - Accept: 0 DEA - Reject: 0
DER - Retries: 0 DEA Timeouts: 0
DEA - Dropped: 0
Total AA Requests: 0 Total AA Answers: 0
AAR - Retries: 0 AAA Timeouts: 0
AAA - Dropped: 0
ASR: 0 ASA: 0
RAR: 0 RAA: 0
STR: 0 STA: 0
STR - Retries: 0
Message Error Stats:
Diameter Protocol Errs: 0 Bad Answers: 0
Unknown Session Reqs: 0 Bad Requests: 0
Request Timeouts: 0 Parse Errors: 0
Request Retries: 0
Session Stats:
Total Sessions: 0 Freed Sessions: 0
SessionTimeouts: 0 Active Sessions: 0
STR Termination Cause Stats:
Diameter Logout: 0 Service Not Provided: 0
Bad Answer: 0 Administrative: 0
Link Broken: 0 Auth Expired: 0
User Moved: 0 Session Timeout: 0
User Request: 0 Lost Carrier 0
Lost Service: 0 Idle Timeout 0
NAS Session Timeout: 0 Admin Reset 0
Admin Reboot: 0 Port Error: 0
NAS Error: 0 NAS Request: 0
NAS Reboot: 0 Port Unneeded: 0
Port Preempted: 0 Port Suspended: 0
Service Unavailable: 0 Callback: 0
User Error: 0 Host Request: 0
Accounting Servers Summary
---------------------------
Message Stats :
Total AC Requests: 0 Total AC Answers: 0
ACR-Start: 0 ACA-Start: 0
ACR-Start Retries: 0 ACA-Start Timeouts: 0
ACR-Interim: 0 ACA-Interim: 0
ACR-Interim Retries: 0 ACA-Interim Timeouts: 0
ACR-Event: 0 ACA-Event: 0
ACR-Stop: 0 ACA-Stop: 0
ACR-Stop Retries: 0 ACA-Stop Timeouts: 0
ACA-Dropped: 0
AC Message Error Stats:
Diameter Protocol Errs: 0 Bad Answers: 0
Unknown Session Reqs: 0 Bad Requests: 0
Request Timeouts: 0 Parse Errors: 0
Request Retries: 0
Chapter 18
Routing Behind the Mobile Station on an APN

The routing behind the Mobile Station (MS) feature enables the routing of packets to IPv4 addresses that do not belong to the PDN Session (the MS), but exist behind it. The network address of the destination can be different than the Mobile Station address.

- Feature Description
- How It Works
- Configuring Routing Behind the Mobile Station
- Monitoring and Troubleshooting the Routing Behind the Mobile Station
Feature Description

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the “mobile router.” If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session.
How It Works

Routing Behind the Mobile Station on an APN

The following rules apply:

- AAA interface of GGSN/P-GW supports receiving "Framed Route AVP" in Radius Access-Accept Message from the Radius Server.
- AAA interface of GGSN/P-GW supports maximum 16 "Framed Route AVP" in Radius Access-Accept Message.
- GGSN/P-GW does not accept framed route with destination address as 0.0.0.0 and/or netmask as 0.0.0.0.
- GGSN/P-GW does not accept framed route where gateway address in the route is not matching with the address that would be assigned to Mobile station.
- GGSN/P-GW ignores duplicate framed routes.
- GGSN/P-GW supports controlling enabling/disabling of this feature through CLI in APN Configuration.
- GGSN/P-GW supports controlling number of framed-routes to be installed through this feature.
- GGSN/P-GW supports controlling number of hosts (addresses) supported behind the mobile station per route.
- The routing behind an MS is supported only for IPv4 PDP contexts.
- Packets routed behind the MS share the same 3GPP QoS settings of the MS.
Configuring Routing Behind the Mobile Station

The routing behind the MS feature enables the routing of packets to IPv4 addresses that do not belong to the PDN Session (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- The Framed-Route (attribute 22) as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the profile of a user and contain at least one route, and up to 16 routes for each MS that is to use the routing behind the MS feature.

When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the RADIUS authentication and authorization phase of the PDN Session creation. If routing behind the MS has not been enabled using the network-behind-mobile command in access-point configuration mode, the GGSN ignores the Framed-Route attribute.

When the MS session is no longer active, the routes are deleted.

- Static routes are not configured. The configuration of the routing behind the mobile station feature (Framed Route, attribute 22) and static routes at the same time is not supported.

Configuration Overview

To enable routing behind a Mobile Station perform the following steps:

Step 1  Create an APN Profile. Refer to the Creating an APN Profile section.

Step 2  Enable or disable a Network behind Mobile Station for APN. Refer to the Enabling Routing Behind the Mobile Station section.

Creating an APN Profile

Use the following example to create an APN profile on the P-GW/SAEGW/S-GW:

```bash
config

    context context_name

        apn apn_name

end
```

Notes:

- The apn name must be an alphanumeric string from 1 to 64 characters in length.
- Once you have created an APN profile, you will enter the Access Point Profile Configuration Mode.
Enabling Routing Behind the Mobile Station

To enable routing behind an MS, use the following steps command in access-point configuration mode:

```
config

network-behind-mobile { max-addresses-behind-mobile max_addrs | max-subnets max_subnets }

{ default | no } network-behind-mobile

end
```

Notes:

- **default**
  Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

- **no**
  Disables the network behind mobile station functionality on the APN.

- **max-addresses-behind-mobile max_addrs**
  Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

- **max-subnets max_subnets**
  Specifies the maximum number of subnets that can be enabled for a call in the APN.
  `max_subnets` must be an integer from 1 through 16.
  Default: 10

Verifying the Routing Behind the Mobile Station

To verify the routing behind the mobile station configuration, use the following show commands.

1. `Router# show ip route vrf vpn_am2`

```
"*" indicates the Best or Used route. S indicates Stale.

Destination Nexthop Protocol Prec Cost Interface
*17.18.19.20/32 10.7.104.2 bgp 20 0 bgp_neighbour (nhlfe-ix:3)
*17.18.19.21/32 0.0.0.0 connected 0 0 vpn_am2lb1
*40.40.41.0/24 0.0.0.0 connected 0 0
*41.40.41.0/24 0.0.0.0 connected 0 0
*42.40.41.0/24 0.0.0.0 connected 0 0
*43.40.41.0/24 0.0.0.0 connected 0 0
```
*44.40.41.0/24 0.0.0.0 connected 0 0
*45.40.41.0/24 0.0.0.0 connected 0 0
*46.40.41.0/24 0.0.0.0 connected 0 0
*47.40.41.0/24 0.0.0.0 connected 0 0
*48.40.41.0/24 0.0.0.0 connected 0 0
*49.40.41.0/24 0.0.0.0 connected 0 0
*106.106.0.0/16 0.0.0.0 connected 0 0 pool pool_test_3
Total route count : 13
Unique route count: 13
Connected: 12 BGP: 1

2. show subscribers pgw-only full all

Username: starent
Subscriber Type : Visitor
Status : Online/Active
State : Connected
Auto Delete : No
Idle time : 00h00m50s
MS TimeZone : n/a Daylight Saving Time: n/a
Access Type: gtp-pdn-type-ipv4 Network Type: IP
Access Tech: eUTRAN pgw-service-name: PGW21
Callid: 0db5d3a3 IMSI: 123456789012345
Protocol Username: starent MSISDN: 9326737733
Interface Type: S5S8GTP Low Access Priority: N/A
Emergency Bearer Type: N/A
IMS-media Bearer: No
S6b Auth Status: N/A
Access Peer Profile: default
Acct-session-id (Cl): 141414650F55554B
Routing Behind the Mobile Station on an APN

Configuring Routing Behind the Mobile Station

ThreeGPP2-correlation-id (C2): 17767C4D / 6SKdW=2
Card/Cpu: 12/0 Sessmgr Instance: 47
Bearer Type: Default Bearer-Id: 5
Bearer State: Active
IP allocation type: local pool
IPv6 allocation type: N/A
IP address: 106.106.0.5
Framed Routes: Framed Routes Source: RADIUS
40.40.41.0 255.255.255.0 106.106.0.5
41.40.41.0 255.255.255.0 106.106.0.5
43.40.41.0 255.255.255.0 106.106.0.5
44.40.41.0 255.255.255.0 106.106.0.5
45.40.41.0 255.255.255.0 106.106.0.5
46.40.41.0 255.255.255.0 106.106.0.5
47.40.41.0 255.255.255.0 106.106.0.5
48.40.41.0 255.255.255.0 106.106.0.5
49.40.41.0 255.255.255.0 106.106.0.5
42.40.41.0 255.255.255.0 106.106.0.5
ULI:
TAI-ID:
MCC: 214 MNC: 365
TAC: 0x6789
ECGI-ID:
MCC: 214 MNC: 365
ECI: 0x1234567
Accounting mode: None APN Selection Mode: Sent by MS
MEI: 112233445567788 Serving Nw: MCC=123, MNC=765
charging id: 257250635 charging chars: normal
Source context: EPC2 Destination context: ISP1
S5/S8/S2b/S2a-APN: cisco.com
SGi-APN: cisco.com
APN-OI: n/a
Restoration priority level: n/a
traffic flow template: none
IMS Auth Service: IMSGx
active input ipv4 acl: IPV4ACL active output ipv4 acl: IPV4ACL
active input ipv6 acl: active output ipv6 acl:
ECS Rulebase: cisco
Bearer QoS:
QCI: 5
ARP: 0x04
PCI: 0 (Enabled)
PL: 1
PVI: 0 (Enabled)
MBR Uplink (bps): 0 MBR Downlink (bps): 0
GBR Uplink (bps): 0 GBR Downlink (bps): 0
PCRF Authorized Bearer QoS:
QCI: n/a
ARP: n/a
PCI: n/a
PL: n/a
PVI: n/a
MBR uplink (bps): n/a MBR downlink (bps): n/a
GBR uplink (bps): n/a GBR downlink (bps): n/a
Downlink APN AMBR: n/a Uplink APN AMBR: n/a
P-CSCF Address Information:
Primary IPv6: n/a
Secondary IPv6: n/a
Tertiary IPv6 : n/a
Primary IPv4 : n/a
Secondary IPv4: n/a
Tertiary IPv4 : n/a

Access Point MAC Address: N/A

pgw c-teid: [0x8000002f] 2147483695 pgw u-teid: [0x8000002f] 2147483695
sgw c-teid: [0x50010001] 1342242817 sgw u-teid: [0x60010001] 1610678273
ePDG c-teid: N/A ePDG u-teid: N/A
cgw c-teid: N/A cgw u-teid: N/A

ePDG c-addr: N/A ePDG u-addr: N/A
cgw c-addr: N/A cgw u-addr: N/A

Downlink APN AMBR: 16534000 bps Uplink APN AMBR: 16534000 bps

Mediation context: None Mediation no early PDUs: Disabled

Mediation No Interims: Disabled Mediation Delay PBA: Disabled

input pkts: 0 output pkts: 0
input bytes: 0 output bytes: 0
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0
input pkts dropped due to lorc : 0 output pkts dropped due to lorc : 0
input bytes dropped due to lorc : 0

in packet dropped suspended state: 0 out packet dropped suspended state: 0
in bytes dropped suspended state: 0 out bytes dropped suspended state: 0

in packet dropped overcharge protection: 0 out packet dropped overcharge protection: 0
in bytes dropped overcharge protection: 0 out bytes dropped overcharge protection: 0

in packet dropped sgw restoration state: 0 out packet dropped sgw restoration state: 0
in bytes dropped sgw restoration state: 0 out bytes dropped sgw restoration state: 0
pk rate from user(bps): 0 pk rate to user(bps): 0
ave rate from user(bps): 0 ave rate to user(bps): 0
sust rate from user(bps): 0 sust rate to user(bps): 0
pk rate from user(pps): 0 pk rate to user(pps): 0
ave rate from user(pps): 0 ave rate to user(pps): 0
sust rate from user(pps): 0 sust rate to user(pps): 0
link online/active percent: 65
ipv4 bad hdr: 0 ipv4 ttl exceeded: 0
ipv4 fragments sent: 0 ipv4 could not fragment: 0
ipv4 input acl drop: 0 ipv4 output acl drop: 0
ipv4 bad length trim: 0
ipv4 input mcast drop: 0 ipv4 input bcast drop: 0
ipv6 input acl drop: 0 ipv6 output acl drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv6 input css down drop: 0 ipv6 output css down drop: 0
ipv4 output xoff pkts drop: 0 ipv4 output xoff bytes drop: 0
ipv6 output xoff pkts drop: 0 ipv6 output xoff bytes drop: 0
ipv6 input ehrpd-access drop: 0 ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0 output pkts dropped (0 mbr): 0
ip source violations: 0 ipv4 output no-flow drop: 0
ipv6 egress filtered: 0
ipv4 proxy-dns redirect: 0 ipv4 proxy-dns pass-thru: 0
ipv4 proxy-dns drop: 0
ipv4 proxy-dns redirect tcp connection: 0
ipv6 bad hdr: 0 ipv6 bad length trim: 0
ip source violations no acct: 0
ip source violations ignored: 0
dormancy total: 0 handoff total: 0
ipv4 icmp packets dropped: 0
APN AMBR Input Pkts Drop: 0 APN AMBR Output Pkts Drop: 0
APN AMBR Input Bytes Drop: 0 APN AMBR Output Bytes Drop: 0
Monitoring and Troubleshooting the Routing Behind the Mobile Station

Routing Behind the Mobile Station Show Command(s) and/or Outputs

show apn name <apn_name>

...  
proxy-mip: Disabled
proxy-mipv6: Disabled
proxy-mip null-username static home address: Disabled

Network Behind Mobile Station: Enabled

Maximum subnets behind Mobile station: 10
Maximum Addresses Behind Mobile Station: 16777214

Tunnel peer load-balancing : random
L3-to-L2 tunnel address-policy no-alloc-validate
tunnel address-policy alloc-validate
NPU QoS Traffic Priority: Derive from packet DSCP

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

The following topics are covered in this appendix:

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

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

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

The following guidelines apply to the above session events:

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

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

The following guidelines apply to record elements:

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

<table>
<thead>
<tr>
<th>Event Number</th>
<th>Description</th>
<th>Format</th>
<th>Size (bytes)</th>
<th>Applicable Event Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Event identity (ID 1 – ID 6)</td>
<td>Integer [1-6]</td>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Event Result (3GPP 29.274 Cause Code)</td>
<td>Integer [1-255]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>IMSI</td>
<td>Integer (15 digits)</td>
<td>15</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>IMEISV</td>
<td>Integer (16 digits)</td>
<td>16</td>
<td>All</td>
</tr>
<tr>
<td>5</td>
<td>Start Time (GMT)</td>
<td>MM/DD/YYYY HH:MM:SS: _MS(millisecond accuracy)</td>
<td>18</td>
<td>All</td>
</tr>
<tr>
<td>6</td>
<td>End Time (GMT)</td>
<td>MM/DD/YYYY HH:MM:SS: _MS(millisecond accuracy)</td>
<td>18</td>
<td>2, 4</td>
</tr>
<tr>
<td>7</td>
<td>Protocol (GTPv2)</td>
<td>String</td>
<td>5</td>
<td>All</td>
</tr>
<tr>
<td>8</td>
<td>Disconnect code (ASR 5x00)</td>
<td>Integer [1-999]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>9</td>
<td>Trigger Event (3GPP 29.274 request cause code)</td>
<td>Integer [1-15]</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>10</td>
<td>Origination Node</td>
<td>String (CLLI)</td>
<td>10</td>
<td>All</td>
</tr>
<tr>
<td>11</td>
<td>Origination Node Type</td>
<td>String (SGW</td>
<td>HSGW</td>
<td>PGW</td>
</tr>
<tr>
<td>12</td>
<td>EPS Bearer ID(Default)</td>
<td>Integer [0-15]</td>
<td>1 or 2</td>
<td>All</td>
</tr>
<tr>
<td>13</td>
<td>APN Name</td>
<td>String</td>
<td>34 to 255</td>
<td>All</td>
</tr>
<tr>
<td>14</td>
<td>PGW IP Address</td>
<td>IPv4 or IPv6 address</td>
<td>7 to 55</td>
<td>All</td>
</tr>
<tr>
<td>15</td>
<td>UE IPv4 Address</td>
<td>IPv4 address</td>
<td>7 to 15</td>
<td>All</td>
</tr>
<tr>
<td>16</td>
<td>UE IPv6 Address</td>
<td>IPv6 address</td>
<td>3 to 55</td>
<td>All</td>
</tr>
<tr>
<td>Event Number</td>
<td>Description</td>
<td>Format</td>
<td>Size (bytes)</td>
<td>Applicable Event Numbers</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------</td>
<td>----------------------------------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Uplink AMBR</td>
<td>Integer (0-40000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>18</td>
<td>Downlink AMBR</td>
<td>Integer (0-40000000000)</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 (0-40000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>25</td>
<td>Downlink MBR (bps)</td>
<td>Integer (0-40000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>26</td>
<td>Uplink GBR (bps)</td>
<td>Integer (0-40000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>27</td>
<td>Downlink GBR (bps)</td>
<td>Integer (0-40000000000)</td>
<td>1 to 10</td>
<td>All</td>
</tr>
<tr>
<td>28</td>
<td>Downlink Packets Sent (interval)</td>
<td>Integer (0-40000000000)</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 (0-500000000000)</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 (0-500000000000)</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>
<tr>
<td>35</td>
<td>S1u IP Address of eNodeB</td>
<td>IPv4 or IPv6 address</td>
<td>7 to 55</td>
<td>All</td>
</tr>
</tbody>
</table>
Active-to-Idle Transitions

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

Table 45. 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

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

<table>
<thead>
<tr>
<th>Cause Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request</strong></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Local Detach</td>
</tr>
<tr>
<td>3</td>
<td>Complete</td>
</tr>
<tr>
<td>4</td>
<td>RAT changed from 3GPP to Non-3GPP</td>
</tr>
<tr>
<td>5</td>
<td>ISR deactivation</td>
</tr>
<tr>
<td>6</td>
<td>Error Indication received from RNC/eNodeB</td>
</tr>
<tr>
<td><strong>Accept</strong></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Request accepted</td>
</tr>
<tr>
<td>17</td>
<td>Request accepted partially</td>
</tr>
<tr>
<td>18</td>
<td>New PDN type due to network preference</td>
</tr>
<tr>
<td>19</td>
<td>New PDN type due to single address bearer only</td>
</tr>
<tr>
<td><strong>Reject</strong></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Context Not Found</td>
</tr>
<tr>
<td>65</td>
<td>Invalid Message Format</td>
</tr>
<tr>
<td>66</td>
<td>Version not supported by nextpeer</td>
</tr>
<tr>
<td>67</td>
<td>Invalid length</td>
</tr>
<tr>
<td>68</td>
<td>Service not supported</td>
</tr>
<tr>
<td>69</td>
<td>Mandatory IE incorrect</td>
</tr>
<tr>
<td>70</td>
<td>Mandatory IE missing</td>
</tr>
<tr>
<td>71</td>
<td>Reserved</td>
</tr>
<tr>
<td>72</td>
<td>System failure</td>
</tr>
<tr>
<td>73</td>
<td>No resources available</td>
</tr>
<tr>
<td>74</td>
<td>Semantic error in the TFT operation</td>
</tr>
<tr>
<td>75</td>
<td>Syntactic error in the TFT operation</td>
</tr>
<tr>
<td>76</td>
<td>Semantic errors in packet filter(s)</td>
</tr>
<tr>
<td>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>77</td>
<td>Syntactic errors in packet filter(s)</td>
</tr>
<tr>
<td>78</td>
<td>Missing or unknown APN</td>
</tr>
<tr>
<td>79</td>
<td>Unexpected repeated IE</td>
</tr>
<tr>
<td>80</td>
<td>GRE key not found</td>
</tr>
<tr>
<td>81</td>
<td>Relocation failure</td>
</tr>
<tr>
<td>82</td>
<td>Denied in RAT</td>
</tr>
<tr>
<td>83</td>
<td>Preferred PDN type not supported</td>
</tr>
<tr>
<td>84</td>
<td>All dynamic addresses are occupied</td>
</tr>
<tr>
<td>85</td>
<td>UE context without TFT already activated</td>
</tr>
<tr>
<td>86</td>
<td>Protocol type not supported</td>
</tr>
<tr>
<td>87</td>
<td>UE not responding</td>
</tr>
<tr>
<td>88</td>
<td>UE refuses</td>
</tr>
<tr>
<td>89</td>
<td>Service denied</td>
</tr>
<tr>
<td>90</td>
<td>Unable to page UE</td>
</tr>
<tr>
<td>91</td>
<td>No memory available</td>
</tr>
<tr>
<td>92</td>
<td>User authentication failed</td>
</tr>
<tr>
<td>93</td>
<td>APN access denied - no subscription</td>
</tr>
<tr>
<td>94</td>
<td>Request rejected</td>
</tr>
<tr>
<td>95</td>
<td>P-TMSI Signature mismatch</td>
</tr>
<tr>
<td>96</td>
<td>IMSI not known</td>
</tr>
<tr>
<td>97</td>
<td>Semantic error in the TAD operation</td>
</tr>
<tr>
<td>98</td>
<td>Syntactic error in the TAD operation</td>
</tr>
<tr>
<td>99</td>
<td>Reserved Message Value Received</td>
</tr>
<tr>
<td>100</td>
<td>Remote peer not responding</td>
</tr>
<tr>
<td>101</td>
<td>Collision with network initiated request</td>
</tr>
<tr>
<td>102</td>
<td>Unable to page UE due to Suspension</td>
</tr>
<tr>
<td>103</td>
<td>Conditional IE missing</td>
</tr>
<tr>
<td>104</td>
<td>APN Restriction type Incompatible with currently active PDN connection</td>
</tr>
<tr>
<td>105</td>
<td>Invalid overall length of the triggered response message and a piggybacked initial message</td>
</tr>
<tr>
<td>106</td>
<td>Data forwarding not supported</td>
</tr>
<tr>
<td>107</td>
<td>Invalid reply from remote peer</td>
</tr>
<tr>
<td>116 to 239</td>
<td>Spare. This value range is reserved for Cause values in rejection response message.</td>
</tr>
<tr>
<td>Cause Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td><strong>Sub-Causes</strong></td>
<td></td>
</tr>
<tr>
<td>NO_INFORMATION</td>
<td></td>
</tr>
<tr>
<td>ABORTED_BY_SESSION_DELETION</td>
<td></td>
</tr>
<tr>
<td>NO_RESPONSE_FROM_MME</td>
<td></td>
</tr>
<tr>
<td>INTERNALLY_TRIGGERED</td>
<td></td>
</tr>
<tr>
<td>BEARERS_IN_MULTIPLE_PDN_CONNECTIONS</td>
<td></td>
</tr>
<tr>
<td>EXPECTED_BEARERS_MISSING_IN_MESSAGE</td>
<td></td>
</tr>
<tr>
<td>UNEXPECTED_BEARERS_PRESENT_IN_MESSAGE</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 20
S-GW Restoration Support

This chapter describes the S-GW Restoration support feature.

- Feature Description
- How it Works
- Configuring SGW Restoration Support
- Monitoring and Troubleshooting S-GW Restoration Support
Feature Description

S-GW Restoration helps in handling the S-GW failure in the EPC network. It allows affected PDNs that fail due to S-GW to be restored by selecting another S-GW to serve the affected PDNs. This avoids unnecessary flooding of signaling for PDN cleanup.

The P-GW maintains the sessions in case path failure is detected or if S-GW restart is detected during recovery IE on GTP-C signaling. The P-GW will ensure that any dropped packets in this scenario are not charged. The P-GW also rejects any bearer additions or modification requests received for the PDN connection maintained after the S-GW failure detection. This occurs until the PDN is restored.

Once the session has been restored by the MME and the P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW, then the P-GW continues forwarding any received downlink data and start charging them.

When a subscriber is in S-GW restoration phase, all RARs (except for Session Termination) reject the PCEF. The P-GW rejects all internal updates which can trigger CCR-U towards the PCRF. The P-GW triggers a CCR-U with AN-GW changes for the PDNs that are restored if the S-GW has changed on restoration.

The MME/S4-SGSN is locally configured to know that the P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at the P-GW, it supports it for all S-GWs/MMEs.

**Important:** Only MME/S4-SGSN triggered S-GW restoration procedure will be supported. S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.

The P-GW Restart Notification may also be used to signal that the peer P-GW has failed and not restarted. In this case, the P-GW Restart Notification contains a cause value: P-GW not responding. While sending the PRN, the S-GW includes the cause with this new cause value depending on the echo response.

Relationships to Other Features

GTP-C path failure detection should be enabled for enabling this feature.
How it Works

Changes at P-GW

If a path failure is detected at the Demux, then the path failure notification is sent to all session managers at the P-GW. Next, the session manager cleans up the ongoing transactions. Once all the transactions are deleted, the sessmgr-egtpc deletes the tunnels by adding them into the pacing queue.

The P-GW will not delete the session immediately after detecting path failure with the S-GW restoration in place. The P-GW discards downlink packets received for a maintained PDN connection and stops charging for maintained PDN connections after an S-GW failure that has not been restored.

The MME/S4-SGSN controls the pace of the S-GW relocations to avoid core network node overload. The MME/S4-SGSN prioritizes the S-GW relocation for UEs engaged in a Service Request for RAU/TAU procedures over UEs which are not engaged in any mobility product procedure and do not have a signaling connection to MME/S4-SGSN.

If a session is marked for S-GW restoration and if a new request results in context replacement, then the existing session is aborted followed by a new request indication event.

Changes at the E-GTPC

When the Demux informs the eGTP-C about the path failure, abort all active procedures. The abort procedure indicates to the P-GW if S-GW restoration is enabled for the session. Add all the session in the queue and start the session hold timer for S-GW. The MME restores these sessions by relocating sessions to the new or the same S-GW. When the MBReq is received at the P-GW and if the session is marked with S-GW restoration, then the S-GW flag is reset. At this point, the session hold timer expires and S-GW restoration is removed.

Changes at the MME and SGSN

When the MME and SGSN detects path failure towards the S-GW and the MME supports S-GW restoration, then MME relocates sessions from the failed S-GW to another S-GW. Currently, S-GW restoration is not supported in MME and SGSN.

Demux Failure Detection

The EGTPIN manager detects a path failure and informs all session managers about the failure. Then, the session manager gets the path failure notification and S-GW restoration is enabled so it will stop all ongoing transactions. The Sessmgr-egtpc informs the P-GW-drv about the path failure. The P-GW deletes the session.

Next, the eGTP-C starts the session hold timer. If the MME triggers the S-GW service restoration before the session hold up timer, then sessions from the old S-GW will move to the new S-GW. This ensures that no sessions are handed over and none are deleted.

Once the session hold timer expires, all the sessions with that peer are cleaned up. At this point, new sessions are not moved to the new S-GW.
**Important**: If the S-GW goes down and comes back up in a very short interval, then the P-GW will not detect the path failure. In this case, S-GW restoration does not occur. If the old S-GW comes up again before the hold timer expires, then there is a chance that only some partial sessions move to the new S-GW. In this case, the eGTP-C does not need to delete the remaining sessions with that peer. The eGTP-C will stop the timer.

If the session manager detects the path failure, then it informs the Demux manager. The above scenario still occurs in this case.

After detecting the path failure, the Demux will not send ECHO messages towards the S-GW. If the new session addition occurs or a new session is restored from the node, then the Demux sends the ECHO messages towards the peer.

**Standards Compliance**

The S-GW Restoration functionality complies with the following standards:

- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
Configuring S-GW Restoration Support

The session-hold timer is a configurable parameter. The operator can configure this parameter using the `egtpc sgw-restoration session-hold timeout seconds` CLI command.

The `sgw-restoration` keyword enables S-GW restoration functionality and configure session hold timeout on a P-GW service.

When the P-GW detects that the peer S-GW is down (detection is based on restart counter change or PATH failure due to an ECHO response failure), it moves all PDN sessions associated with the peer S-GW to the SGW-RESTORATION-STATE. Also the P-GW starts a timer with the value provided for session-hold timeout per peer S-GW. After timer expiry, the P-GW cleans up all the sessions which are in the SGW-RESTORATION-STATE.

**Important:** By default, S-GW restoration support will not be enabled.

Sample Configuration

Use the following example to enable S-GW Restoration Support.

```
configure
  context context_name
    pgw-service service_name
      egtpc sgw-restoration session-hold timeout seconds
        { default | no } egtpc sgw-restoration session-hold
    end
```

Notes:
- `session-hold timeout` configures session hold timer for S-GW restoration.
- `seconds` must be an integer from 1 to 3600. Default: 0 (disabled).
- On S-GW failure indication, the P-GW checks if the S-GW restoration feature is enabled or not. If enabled, the P-GW maintains all the affected sessions for session-hold timeout. After session-hold timeout, the P-GW cleans all the sessions which are not recovered yet.

Verifying the S-GW Configuration

To verify the S-GW Restoration configuration, use the following command:

```
show pgw-service all
```

The following fields have been added to display configuration information for S-GW restoration.
- EGTP SGW Restoration Handling
- Session Hold Timer
- Timeout
Monitoring and Troubleshooting S-GW Restoration Support

This section includes show commands in support of the S-GW Restoration.

S-GW Show Commands

This section provides information regarding show commands and/or their outputs in support of the S-GW Restoration.

show ims-authorization policy-control statistics

The following fields have been added to display the statistics introduced in support of S-GW Restoration Support.

- SGW Restoration
- RAR Reject
- Internal Updates Dropped
- Revalidation Timeout
- Pending Updates

show pgw-service statistics all

The following counters have been added to display S-GW Restoration Support.

- SGW Restoration Statistics
- PDNs Total
- In Restoration State
- Recovered
- Released
- Drops During SGW Restoration State
- Packets
- Bytes

show subscribers pgw-only full all

The following fields and counters have been added to display S-GW Restoration Support.

- Bearer State
- in packet dropped sgw restoration state
- in bytes dropped sgw restoration state
- out packet dropped sgw restoration state
- out bytes dropped sgw restoration state
Chapter 21
Traffic Policing and Shaping

This chapter describes the support of per subscriber Traffic Policing and Shaping feature on Cisco’s Chassis and explains the commands and RADIUS attributes that are used to implement this feature. 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.

**Important:** Traffic Policing and Shaping 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*.

This chapter included following procedures:

- Overview
- Traffic Policing Configuration
- Traffic Shaping Configuration
- RADIUS Attributes
Overview

This section describes the traffic policing and shaping feature for individual subscriber. This feature is comprised of two functions:

- Traffic Policing
- Traffic Shaping

Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APN of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.

- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.

- **Burst-size:** The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber’s “bucket”. Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop:** The offending packet is discarded.

- **Transmit:** The offending packet is passed.

- **Lower the IP Precedence:** The packet’s ToS bit is set to “0”, thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet’s ToS bit was already set to “0”, this action is equivalent to “Transmit”.

Traffic Shaping

Traffic Shaping is a rate limiting method similar to the Traffic Policing, but provides a buffer facility for packets exceeded the configured limit. Once the packet exceeds the data-rate, the packet queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data system can be configured to either drop the packets or kept for the next scheduled traffic session.

**Important:** Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.
Traffic Policing Configuration

Traffic Policing is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

Important: In 3GPP service attributes received from the RADIUS server supersede the settings in the APN.

Important: Commands used in the configuration samples 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.

Configuring Subscribers for Traffic Policing

Important: Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Step 1 Configure local subscriber profiles on the system to support Traffic Policing by applying the following example configurations:

Step a To apply the specified limits and actions to the downlink (data to the subscriber):

```plaintext
configure

context <context_name>

subscriber name <user_name>

qos traffic-police direction downlink

end
```

Step b To apply the specified limits and actions to the uplink (data from the subscriber):

```plaintext
configure

context <context_name>

subscriber name <user_name>

qos traffic-police direction uplink

end
```

Notes:
• There are numerous keyword options associated with the `qos traffic-police direction { downlink | uplink }` command.

• Repeat for each additional subscriber to be configured.

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the `ip user-datagram-tos-copy` command in the Subscriber Configuration mode is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the `ip qos-dscp` command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

---

**Step 2** Verify the subscriber profile configuration by applying the following example configuration:

```plaintext
context <context_name>

show subscriber configuration username <user_name>
```

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the `System Administration Guide` and the `Command Line Interface Reference`.

---

**Configuring APN for Traffic Policing in 3GPP Networks**

This section provides information and instructions for configuring APN template’s QoS profile in support of Traffic Policing.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used. Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the table below.

**Table 47. Permitted Values for Committed and Peak Data Rates in GTP Messages**

<table>
<thead>
<tr>
<th>Value (bps)</th>
<th>Increment Granularity (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From 1000 to 63,000</td>
<td>1,000 (e.g. 1000, 2000, 3000, ... 63000)</td>
</tr>
<tr>
<td>From 64,000 to 568,000</td>
<td>8,000 (e.g. 64000, 72000, 80000, ... 568000)</td>
</tr>
<tr>
<td>From 576,000 to 8,640,000</td>
<td>64,000 (e.g. 576000, 640000, 704000, ... 8640000)</td>
</tr>
<tr>
<td>From 8,700,000 to 16,000,000</td>
<td>100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)</td>
</tr>
</tbody>
</table>

**Step 1** Set parameters by applying the following example configurations:

**Step a** To apply the specified limits and actions to the downlink (the Gn direction):

```plaintext
configure
```
Traffic Policing and Shaping

Traffic Policing Configuration

context <context_name>
apn <apn_name>
qos rate-limit downlink
end

Step b  To apply the specified limits and actions to the uplink (the Gi direction):

configure
context <context_name>
apn <apn_name>
qos rate-limit uplink
end

Notes:

• There are numerous keyword options associated with qos rate-limit { downlink | uplink } command.

• Optionally, configure the maximum number of PDP contexts that can be facilitated by the APN to limit the APN’s bandwidth consumption by entering the following command in the configuration:

max-contents primary <number> total <total_number>

• Repeat as needed to configure additional Qos Traffic Policing profiles.

Important: If a “subscribed” traffic class is received, the system changes the class to background and sets the following: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

Step 2  Verify that your APNs were configured properly by entering the following command:

show apn { all | name <apn_name> }

The output is a concise listing of configured APN parameter settings.

Step 3  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.
Traffic Shaping Configuration

Traffic Shaping is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

**Important:** In 3GPP, service attributes received from the RADIUS server supersede the settings in the APN.

**Important:** Commands used in the configuration samples 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.

**Important:** Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

Configuring Subscribers for Traffic Shaping

This section provides information and instructions for configuring local subscriber profiles on the system to support Traffic Shaping.

**Important:** Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

**Step 1** Set parameters by applying the following example configurations:

**Step a** To apply the specified limits and actions to the downlink (data to the subscriber):

```plaintext
configure
context <context_name>
subscriber name <user_name>
qos traffic-shape direction downlink
end
```

**Step b** To apply the specified limits and actions to the uplink (data to the subscriber):

```plaintext
configure
context <context_name>
subscriber name <user_name>
qos traffic-shape direction uplink
```
Notes:

- There are numerous keyword options associated with `qos traffic-shape direction { downlink | uplink }` command.
- Repeat for each additional subscriber to be configured.

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the `ip user-datagram-tos-copy` command in the Subscriber Configuration mode is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the `ip qos-dscp` command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

**Step 2** Verify the subscriber profile configuration by applying the following example configuration:

```plaintext
context <context_name>

show subscriber configuration username <user_name>
```

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

### Configuring APN for Traffic Shaping in 3GPP Networks

This section provides information and instructions for configuring APN template’s QoS profile in support of Traffic Shaping.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system converts this to a value that is permitted by GTP as shown in the following table.

**Table 48. Permitted Values for Committed and Peak Data Rates in GTP Messages**

<table>
<thead>
<tr>
<th>Value (bps)</th>
<th>Increment Granularity (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From 1000 to 63,000</td>
<td>1,000 (e.g. 1000, 2000, 3000, ... 63000)</td>
</tr>
<tr>
<td>From 64,000 to 568,000</td>
<td>8,000 (e.g. 64000, 72000, 80000, ... 568000)</td>
</tr>
<tr>
<td>From 576,000 to 8,640,000</td>
<td>64,000 (e.g. 576000, 640000, 704000, ... 86400000)</td>
</tr>
<tr>
<td>From 8,700,000 to 16,000,000</td>
<td>100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)</td>
</tr>
</tbody>
</table>

**Step 1** Set parameters by applying the following example configurations.
**Step a**  To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
    qos rate-limit downlink
  end
```

**Step b**  To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
  context <context_name>
    apn <apn_name>
    qos rate-limit uplink
  end
```

**Step 2**  Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

**Step 3**  Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*. 
RADIUS Attributes

Traffic Policing for CDMA Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for CDMA subscribers (PDSN, HA) configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 49. RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-QoS-Tp-DnIk (or SN1-QoS-Tp-DnIk)</td>
<td>Enable/disable traffic policing in the downlink direction.</td>
</tr>
<tr>
<td>SN-Tp-DnIk-Committed-Data-Rate (or SN1-Tp-DnIk-Committed-Data-Rate)</td>
<td>Specifies the downlink committed-data-rate in bps.</td>
</tr>
<tr>
<td>SN-Tp-DnIk-Peak-Data-Rate (or SN1-Tp-DnIk-Committed-Data-Rate)</td>
<td>Specifies the downlink peak-data-rate in bps.</td>
</tr>
<tr>
<td>SN-Tp-DnIk-Burst-Size (or SN1-Tp-DnIk-Burst-Size)</td>
<td>Specifies the downlink burst-size in bytes. <strong>NOTE:</strong> It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.</td>
</tr>
<tr>
<td>SN-Tp-DnIk-Exceed-Action (or SN1-Tp-DnIk-Exceed-Action)</td>
<td>Specifies the downlink exceed action to perform.</td>
</tr>
<tr>
<td>SN-Tp-DnIk-Violate-Action (or SN1-Tp-DnIk-Violate-Action)</td>
<td>Specifies the downlink violate action to perform.</td>
</tr>
<tr>
<td>SN-QoS-Tp-UpIk (or SN1-QoS-Tp-UpIk)</td>
<td>Enable/disable traffic policing in the uplink direction.</td>
</tr>
</tbody>
</table>
### Traffic Policing and Shaping

#### RADIUS Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)</td>
<td>Specifies the uplink committed-data-rate in bps.</td>
</tr>
<tr>
<td>SN-Tp-Uplk-Peak-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)</td>
<td>Specifies the uplink peak-data-rate in bps.</td>
</tr>
<tr>
<td>SN-Tp-Uplk-Burst-Size (or SN1-Tp-Uplk-Burst-Size)</td>
<td>Specifies the uplink-burst-size in bytes.</td>
</tr>
</tbody>
</table>

**Important:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-Tp-Uplk-Exceed-Action (or SN1-Tp-Uplk-Exceed-Action)</td>
<td>Specifies the uplink exceed action to perform.</td>
</tr>
<tr>
<td>SN-Tp-Uplk-Violate-Action (or SN1-Tp-Uplk-Violate-Action)</td>
<td>Specifies the uplink violate action to perform.</td>
</tr>
</tbody>
</table>

### Traffic Policing for UMTS Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for UMTS subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

**Table 50. RADIUS Attributes Required for Traffic Policing Support for UMTS Subscribers**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN-QoS-Conversation-Class (or SN1-QoS-Conversation-Class)</td>
<td>Specifies the QOS Conversation Traffic Class.</td>
</tr>
<tr>
<td>SN-QoS-Streaming-Class (or SN1-QoS-Streaming-Class)</td>
<td>Specifies the QOS Streaming Traffic Class.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>SN-QoS-Interactive1-Class (or SN1-QoS-Interactive1-Class)</td>
<td>Specifies the QOS Interactive Traffic Class.</td>
</tr>
<tr>
<td>SN-QoS-Interactive2-Class (or SN1-QoS-Interactive2-Class)</td>
<td>Specifies the QOS Interactive2 Traffic Class.</td>
</tr>
<tr>
<td>SN-QoS-Interactive3-Class (or SN1-QoS-Interactive3-Class)</td>
<td>Specifies the QOS Interactive3 Traffic Class.</td>
</tr>
<tr>
<td>SN-QoS-Background-Class (or SN1-QoS-Background-Class)</td>
<td>Specifies the QOS Background Traffic Class.</td>
</tr>
<tr>
<td>SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)</td>
<td>This compound attribute simplifies sending QoS values for Traffic Class (the above attributes), Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.</td>
</tr>
</tbody>
</table>
Appendix A
S-GW Engineering Rules

This appendix provides Serving Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5x00 for your network deployment. General and network-specific rules are located in the appendix of the System Administration Guide for the specific network type.

The following rules are covered in this appendix:

- Interface and Port Rules
- S-GW Service Rules
- S-GW Subscriber Rules
## Interface and Port Rules

The assumptions and rules discussed in this section pertain to Ethernet line cards and the type of interfaces they facilitate.

### Assumptions

Overall assumptions for the S5/S8 and S11 interfaces used in the LTE EPC between Serving Gateway and PDN-GW are listed below.

- GTPv2-C is the signaling protocol used on the S5/S8 and S11 interfaces. Message and IE definitions comply with 3GPP 29.274.
- S5 and S11 interfaces use IPv6 transport as defined in 29.274, section 10.
- MSISDN is assumed to be sent by MME in initial attach.
- MEI will always be retrieved by MME from UE and sent on S11 during initial attach and UE Requested PDN connectivity procedure.
- MME will always send UE time zone information.
- The default bearer does not require any TFT.
- The PCO IE in Create Session Request shall contain two DNS server IP addresses. [S5/S8]
- UE's location change reporting support is required. [S5/S8]
- The S-GW does not verify the content of the IEs which are forwarded on the S5/S8 interface from the S11 interface. The P-GW verifies the content of all the IEs received on the S5/S8 interface.

### S1-U/S11 Interface Rules

The following engineering rules apply to the S1-U0/S11 interface:

- An S1-U0/S11 interface is created once the IP address of a logical interface is bound to an S-GW service.
- The logical interface(s) that will be used to facilitate the S1-U0/S11 interface(s) must be configured within an “ingress” context.
- S-GW services must be configured within an “ingress” context.
- At least one S-GW service must be bound to each interface, however, multiple S-GW services can be bound to a single interface if secondary addresses are assigned to the interface.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S1-U0/S11 interface can be limited.

### S5/S8 Interface Rules

This section describes the engineering rules for the S5 interface for communications between the Mobility Access Gateway (MAG) service residing on the S-GW and the Local Mobility Anchor (LMA) service residing on the P-GW.
MAG to LMA Rules

The following engineering rules apply to the S5/S8 interface from the MAG service to the LMA service residing on the P-GW:

- An S5/S8 interface is created once the IP address of a logical interface is bound to an MAG service.
- The logical interface(s) that will be used to facilitate the S5/S8 interface(s) must be configured within the egress context.
- MAG services must be configured within the egress context.
- MAG services must be associated with an S-GW service.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S5/S8 interface can be limited.
S-GW Service Rules

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

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

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance. Only create a large number of services only 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 understanding 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.
Appendix B

P-GW Engineering Rules

This appendix provides PDN 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 and Configuration Guide for the specific network type.

The following rules are covered in this appendix:

- Interface and Port Rules
- P-GW Context and Service Rules
- P-GW Subscriber Rules
Interface and Port Rules

The rules discussed in this section pertain to the Ethernet 10/100 line card, the Ethernet 1000 line card and the four-port Quad Gig-E line card and the type of interfaces they facilitate, regardless of the application.

S2a Interface Rules

This section describes the engineering rules for the S2a interface for communications between the Mobility Access Gateway (MAG) service residing on the HSGW and the Local Mobility Anchor (LMA) service residing on the P-GW.

LMA to MAG

The following engineering rules apply to the S2a interface from the LMA service to the MAG service residing on the HSGW:

- An S2a interface is created once the IP address of a logical interface is bound to an LMA service.
- The logical interface(s) that will be used to facilitate the S2a interface(s) must be configured within an ingress context.
- LMA services must be configured within an ingress context.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S2a interface can be limited in order to allow higher bandwidth per subscriber.

S5/S8 Interface Rules (GTP)

The following engineering rule applies to the S5/S8 interface from the P-GW to the S-GW:

- P-GW preserves an IP address between S2a interface (PMIPv6) and S5/S8 interface (GTP) when the user moves between Wi-Fi and LTE if a common P-GW is used as the anchor point between the two services.
P-GW Context and Service Rules

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

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

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

- The system supports unlimited peer HSGW/MAG addresses per P-GW.
  - The system maintains statistics for a maximum of 8192 peer HSGWs per P-GW service.
  - If more than 8192 HSGWs are attached, older statistics are identified and overwritten.
  - PMIPv6 does not support any peer level statistics (per MAG level statistics).
- The system supports 65,000 S-GW addresses per P-GW.
  - The system maintains statistics for all peer S-GWs per P-GW service.
- The system maintains statistics for a maximum of 64,000 peer P-GWs per HSGW or S-GW service.
- There are a maximum of 8 P-GW assignment tables per context and per chassis.
- The total number of entries per table and per chassis is limited to 256.
P-GW Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- Default subscriber templates may be configured on a per P-GW service.