S-GW Administration Guide, StarOS Release 21.24

First Published: 2021-06-30

Last Modified: 2023-02-25

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

CONTENTS

About this Guide

Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with CUPS products. References to any CUPS products or features are for informational purposes only. Please contact your Cisco Account or Support representative for any questions about parity between this product and any CUPS products.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

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.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

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

Command Syntax Conventions	Description
{ keyword or *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

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*
- *IPSec Reference*
- *MME 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

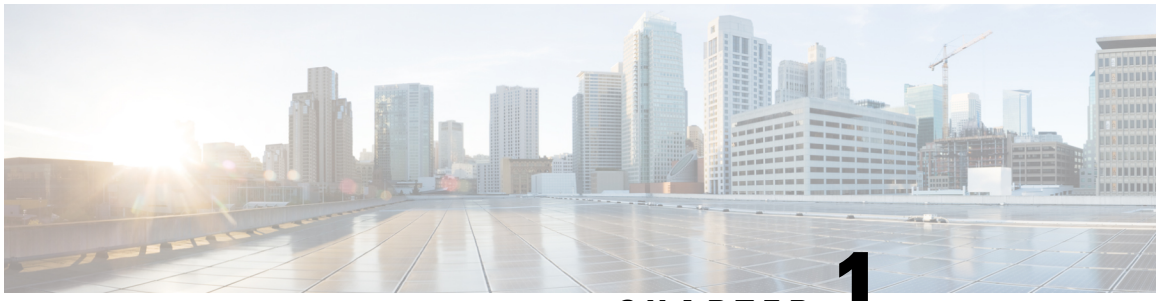
Use the following path selections to access the S-GW documentation:

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

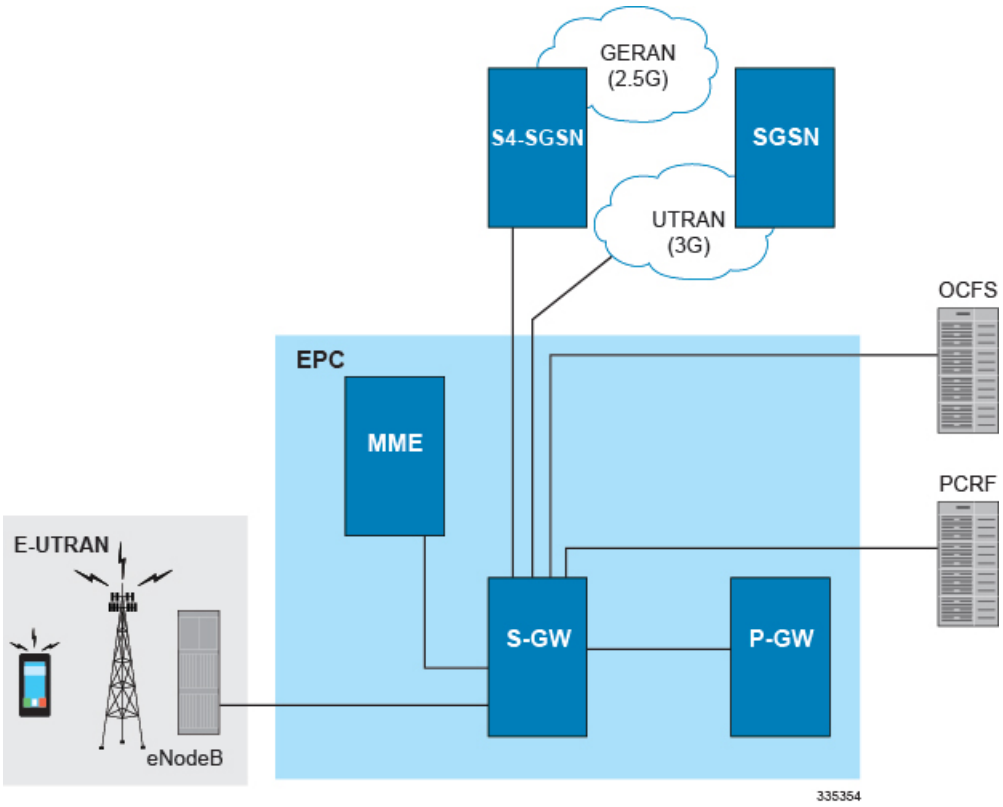
Serving Gateway Overview

The Cisco® ASR 5500 core platform provides wireless carriers with a flexible solution that functions as a Serving Gateway (S-GW) in Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks.

Product Description

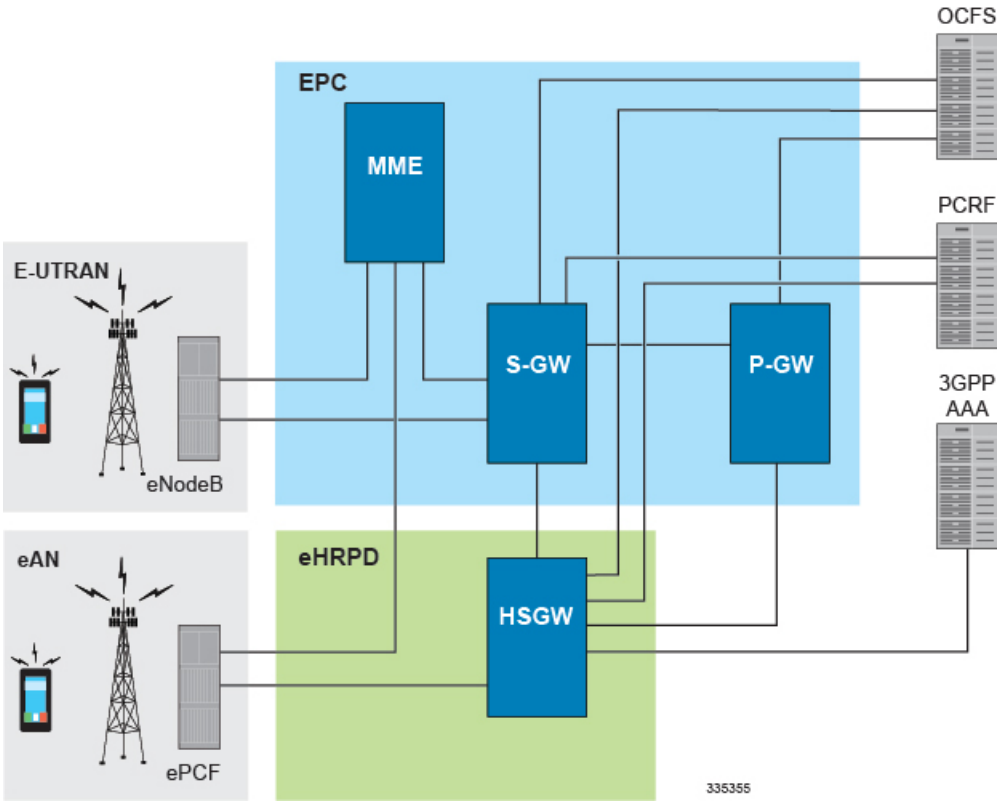
The Serving Gateway routes and forwards data packets from the UE and acts as the mobility anchor during inter-eNodeB handovers. Signals controlling the data traffic are received on the S-GW from the MME which determines the S-GW that will best serve the UE for the session. Every UE accessing the EPC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

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



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

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



The functions of the S-GW include:

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

Platform Requirements

The S-GW service runs on a Cisco® ASR 5500 Series chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the *Installation Guide* for the chassis and/or contact your Cisco account representative.

Licenses

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

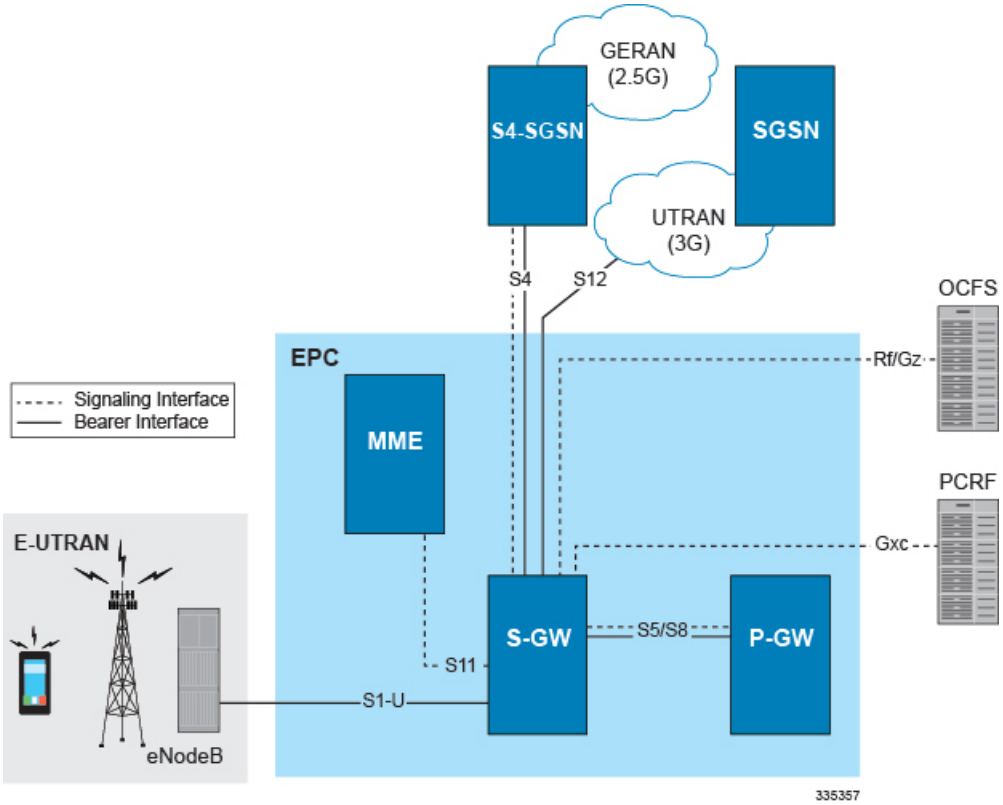
Network Deployment(s)

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

Serving Gateway in the E-UTRAN/EPC Network

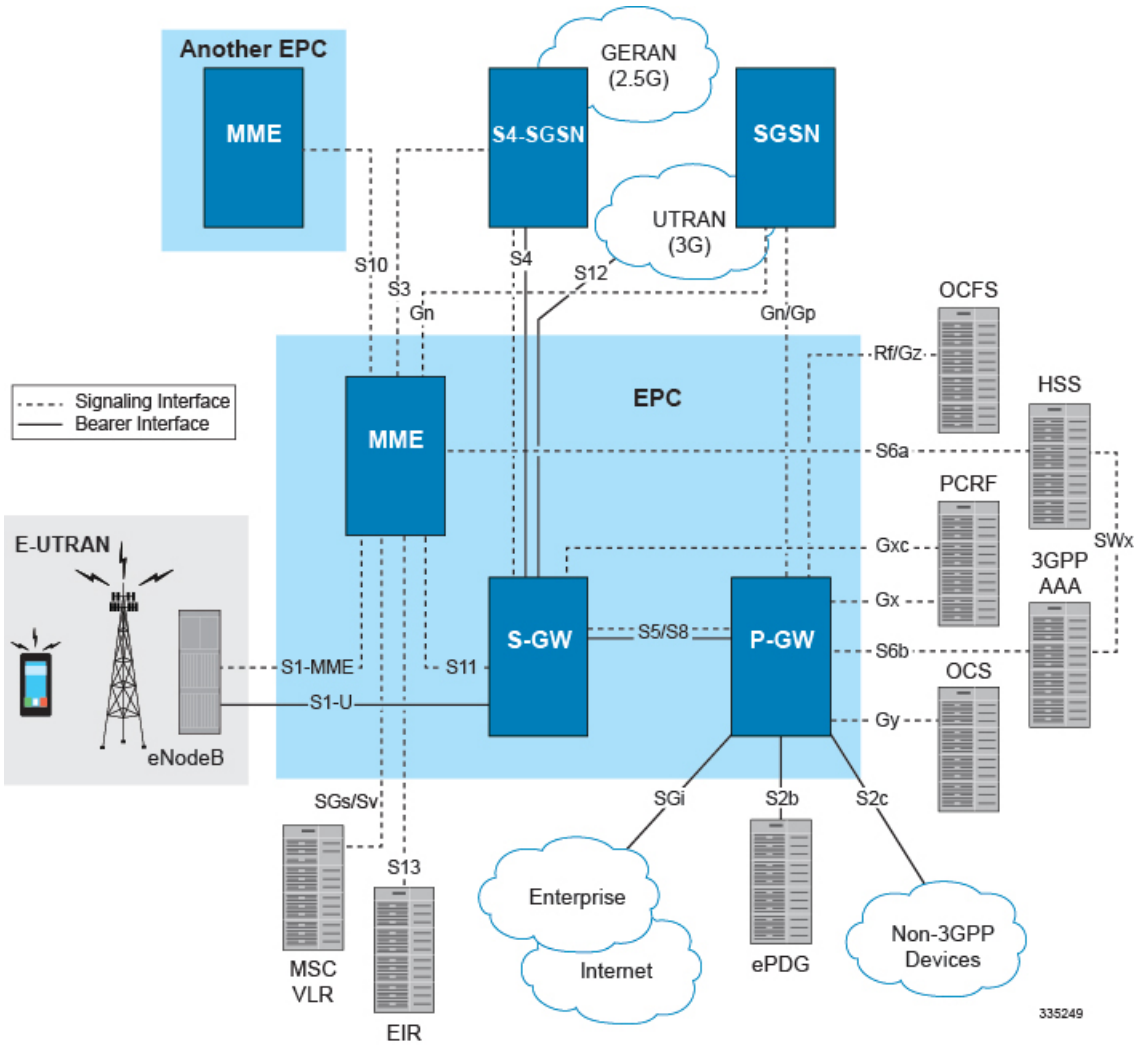
The following figure displays the specific network interfaces supported by the S-GW. Refer to Supported Logical Network Interfaces (Reference Points), on page 5 for detailed information about each interface.

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



The following figure displays a sample network deployment of an S-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

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



Supported Logical Network Interfaces (Reference Points)

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

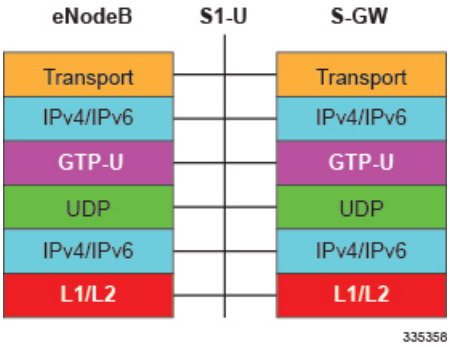
S1-U Interface

This reference point provides bearer channel tunneling between the eNodeB and the S-GW. It also supports eNodeB path switching during handovers. The S-GW provides the local mobility anchor point for inter-eNodeB hand-overs. It provides inter-eNodeB path switching during hand-overs when the X2 handover interface between base stations cannot be used. The S1-U interface uses GPRS tunneling protocol for user plane (GTP-Uv1). GTP encapsulates all end user IP packets and it relies on UDP/IP transport. The S1-U interface also supports IPSec IKEv2. This interface is defined in 3GPP TS 23.401.

Supported protocols:

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

Figure 5: Supported Protocols on the S1-U Interface



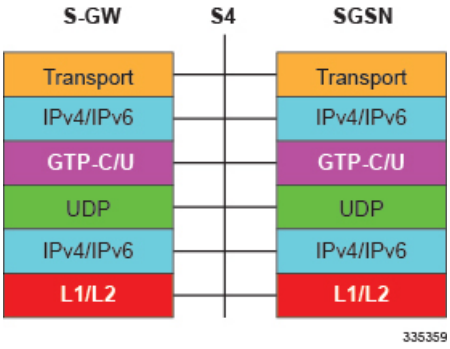
S4 Interface

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

Supported protocols:

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

Figure 6: Supported Protocols on the S4 Interface



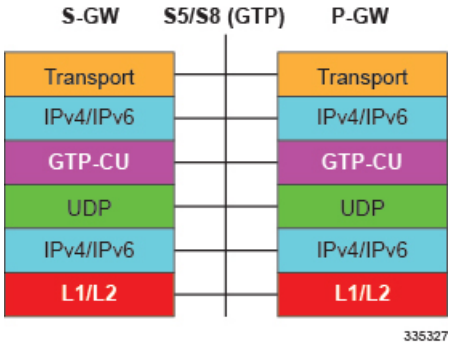
S5/S8 Interface

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

Supported protocols:

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

Figure 7: Supported Protocols on the S5/S8 Interface



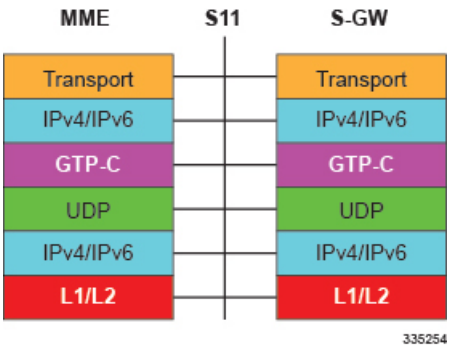
S11 Interface

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

Supported protocols:

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

Figure 8: Supported Protocols on the S11 Interface



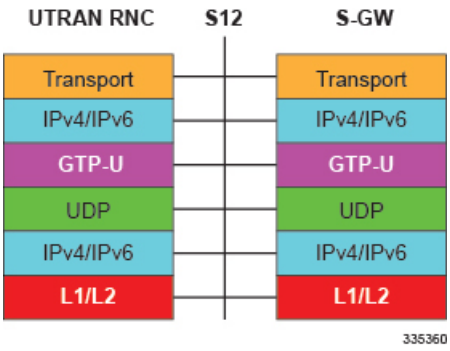
S12 Interface

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

Supported protocols:

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

Figure 9: Supported Protocols on the S12 Interface



Gz Interface

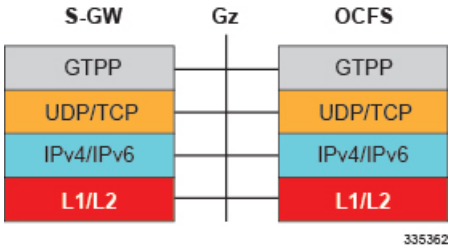
The Gz reference interface enables offline accounting functions on the S-GW. The S-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage. The Gz interface and offline accounting functions are used primarily in roaming scenarios where the foreign P-GW does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

Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6

- Data Link Layer: ARP
- Physical Layer: Ethernet

Figure 10: Supported Protocols on the Gz Interface



Rf Interface

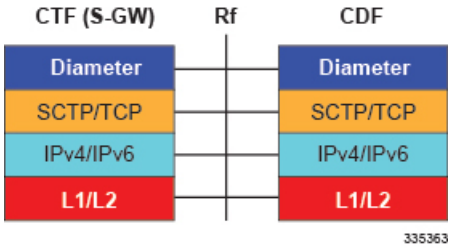
Important The Rf interface is not supported on the S-GW.

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

Supported protocols:

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

Figure 11: Supported Protocols on the Rf Interface



Features and Functionality - Base Software

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

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*.

3GPP Release 12 Cause-Code IE Support

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

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

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

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

Abnormal Bearer Termination Cause in CDR

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

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

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

ANSI T1.276 Compliance

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

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

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

These measures are applicable to the ASR 5500 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.

Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

Important For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

Bulk Statistics Support

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

When used in conjunction with an element management system, the data can be parsed, archived, and graphed.

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

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **MAG**: Provides MAG service statistics
- **S-GW**: Provides S-GW node-level service statistics

- **IP Pool**: Provides IP pool statistics
- **APN**: Provides Access Point Name statistics

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

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

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

The Bulk Statistics Server component of an element management system parses collected statistics and stores the information in its PostgreSQL database. It can also generate XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

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

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

CDR Support for Including LAPI (Signaling Priority)

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

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

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

Circuit Switched Fall Back (CSFB) Support

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

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

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

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

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

Closed Subscriber Group Support

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

- 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

Collision Counter Support in the GTP Layer

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

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

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

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

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

Sample output:

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

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

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

Congestion Control

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

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

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operational thresholds that are configured for the system as described in the *Thresholding Configuration Guide*. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

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

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

Dedicated Bearer Timeout Support on the S-GW

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

Downlink Delay Notification

This feature is divided between the following:

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

Value Handling

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

Throttling

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

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

EPS Bearer ID and ARP Support

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

In order to support MPS requirement for Priority Paging in the network for MPS subscriber, DDN message has been enhanced to support passing ARP and EBI information. When the S-GW sends a Downlink Data Notification message, it shall include both EPS Bearer ID and ARP. If the Downlink Data Notification is triggered by the arrival of downlink data packets at the S-GW, the S-GW shall include the EPS Bearer ID and ARP associated with the bearer on which the downlink data packet was received. If the Downlink Data Notification is triggered by the arrival of control signaling, the S-GW shall include the EPS Bearer ID and ARP, if present in the control signaling. If the ARP is not present in the control signaling, the S-GW shall include the ARP in the stored EPS bearer context. If multiple EPS Bearers IDs are reported in the Downlink

Data Notification message, the S-GW shall include all the EBI values and the ARP associated with the bearer with the highest priority (lowest ARP value). For more information, see TS 23.401 (section 5.3.4.3) and 29.274 (section 7.2.11). Details are discussed in CR-859 of 3GPP specifications.

DSCP Ingress and Egress and DSCP Marking at the APN Profile

This feature will provide an operator with a configuration to set the DSCP value per APN profile, so different APNs can have different DSCP markings as per QOS requirements for traffic carried by the APN. In addition, the **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.

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

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

Micro-checkpoints were configurable only with the **micro-checkpoint-periodicity** option in the **timeout idle** command in APN Configuration Mode.

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

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

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

Event Reporting

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

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

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

Event Log #	Description
New Events	
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: %s, error code %d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>]Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-%d Ran out of session handles"
140075	Represents error_log1 in format "[IMSI <IMSI>]%s"
Modified Events	
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)"
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=%s(%d) event=%s(%d)"

Event Log #	Description
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-%d: Request to %s bearer rejected. Reason: %s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code %d"
12774	Represents pgw_purge_invalid_crr in format "[IMSI <IMSI>] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <%u>."
12858	Represnts ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <%u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <%u>:pf_id_bitmap 0x%x and tft_opcode: %d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <%u> rejected, due to <%s>."
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <%u>, due to <%s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<%s>,[event:<%s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call."
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0x%x> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN %s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] %s"
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d"

Event Log #	Description
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr %d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] %s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <%s> in state <%s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <%s> in state <%s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <%s> in state <%s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] %s"

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

IP Access Control Lists

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

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

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

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)

Important The Diameter Rf offline charging interface is not supported on the S-GW.

Routing and Miscellaneous Features

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

LIPA Support

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

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

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

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

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

Location Reporting

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

ULI data reported in GTPv2 messages includes:

- **TAI-ID:** Tracking Area Identity

- **MCC: MNC:** Mobile Country Code, Mobile Network Code
- **TAC:** Tracking Area Code

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

Mapping High Throughput Sessions on Session Managers

Session managers are upgraded to manage several high throughput sessions without sharing the core and without creating a bottleneck on the CPU load.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is checkpointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.

Note

- The selection of session managers for non-high throughput sessions remains the same in the existing setup.
- Non-high throughput sessions are placed along with the high throughput sessions on the same session manager.

Limitations

Managing high throughput sessions on a session manager has the following limitations:

- The following scenarios may result in placing two high throughput sessions on a session manager:
  - Initial attach from eHRPD/2G/3G sessions.
  - IP addresses – both IPv4 and IPv6, are placed on the same session manager.
  - For an S-GW, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
  - For a collapsed call, the second Create Session Request (PDN) from a UE lands directly on a session manager which has the first PDN of the same UE.
  - In a Multi-PDN call from a UE that is capable of DCNR. For example: VoLTE and Internet capable of DCN will be placed on the same session manager.
- The DCNR flag is not defined by 3GPP for Wi-Fi. Therefore, a session cannot be assigned to a session manager during a Wi-Fi to LTE handover with the DCNR flag set.
- This feature manages and supports distribution of high throughput sessions on a session manager but does not guarantee high throughput for a subscriber.

- In some cases, the round robin mechanism could place a high throughput session on a session manager that was already loaded with other high throughput sessions.

MME Restoration Support

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

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

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

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

MME Restoration Standards Extension

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

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

S-GW NTSR Enhancement

When the Network Triggered Service Restoration (NTSR) feature is enabled on the S-GW and it detects an MME failure. If the subscriber served by the failed MME receives any downlink data packets, then the S-GW selects an alternate MME from the NTSR pool in round-robin fashion. The S-GW then sends a Downlink Data Notification (DDN) to the selected MME. This round robin selection of an MME is per sessmgr instance and not system wide.

Previously, operators could configure a maximum of five MME IP addresses in an NTSR pool. To efficiently interoperate with networks containing more than five MMEs, the S-GW has been enhanced so that 10 MME IP addresses can be configured in the NTSR pool. The configured MME IP addresses can be IPv4, IPv6, or a combination of both IPv4 and IPv6.

This feature improves load balancing of DDN messages in the network during an MME failure.

The existing **ntsr-pool** command in *Global Configuration Mode* is used to configure the MME peer IP addresses. The maximum number of MMEs that can be configured has been increased from five to a maximum of 10.

The existing **show ntsr-pool full all** command in Exec Mode is used to view the configured NTSR pool-id, the NTSR Pool type, and the IP addresses of the MME peers. The command output will now show a maximum of 10 MME peer IP addresses.

Multiple PDN Support

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

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

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

Important Up to 11 multiple PDN connections are supported.

Node Functionality GTP Echo

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

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

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

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

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

Important Offline Charging is not supported on the S-GW.

Important Online Charging is not supported on the S-GW.

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

The ASR 5500 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks.

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

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.

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.

Optimization for egtpinmgr Recovery

Restarting the egtpinmgr task took a significant amount of time for recovery. Hence, the outage time when the GGSN, P-GW, SAEGW, and S-GW were unable to accept any new calls during egtpinmgr recovery was high.

The software is enhanced to optimize the recovery outage window in the event of an egtpinmgr task restart; this has been achieved by optimizing the internal algorithms of egtpinmgr recovery and the data structures required. In addition, recovery time now is dependent only on the number of unique IMSIs and not on the number of sessions for an IMSI.

Peer GTP Node Profile Configuration Support

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

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

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

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

P-GW Restart Notification Support

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

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

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

QoS Bearer Management

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

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

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

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

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

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

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

by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

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

Removal of Private Extension-based Overcharging Support

Prior to StarOS release 21.0, the Cisco P-GW and S-GW supported the sending and receiving of overcharging protection data via both a non-3GPP Private Extension Information Element (IE), and a 3GPP Indication IE.

However, since 3GPP support to exchange overcharging protection data exists, no operators were using the Overcharging Private Extension (OCP) based solution. It was also reported by some operators that the Private Extension IE carrying overcharging protection data sent by the P-GW was leading to issues at S-GWs of other vendors.

As a result, support for Private Extension-based Overcharging Support is being removed from the Cisco P-GW and S-GW. This has the benefit of preventing unexpected scenarios occurring due to the decoding of a Private Extension ID carrying overcharging protection data at the P-GW/S-GW of other vendors.

Previous and New Behavior for the P-GW

The following table describes the previous and new behavior at the P-GW for Create Session Request (CSReq) and Create Session Response (CSRsp) messages due to the removal of Private Extension Overcharging Support.

Table 2: Previous and New Behavior: CSReq and CSRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support

Scenario No.	IE Carrying OCP Capability Received from S-GW in CSReq	Old Behavior: IE carrying OCP Capability Sent to S-GW in CSRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in CSRsp
1	Indication IE	Indication IE	No change. Indication IE will be sent in CSRsp.
2	Private Extension IE	Both Private Extension and Indication IEs.	Private Extension IE received from S-GW is ignored. Indication IE is sent in CSRsp.
3	None	Both Private Extension and Indication IEs.	Only Indication IE is sent in CSRsp.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from S-GW is ignored. Only Indication IE is sent in CSRsp.

The following table describes the previous and new behavior in Modify Bearer Request (MBReq) and Modify Bearer Response (MBRsp) messages due to the removal of Private Extension Overcharging Support.

Table 3: Previous and New Behavior: MBRreq and MBRsp Messages at P-GW Due to Removal of Private Extension Overcharging Support

Scenario No.	IE carrying OCP Capability Received from S-GW in MBReq	Old Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp	New Behavior: IE Carrying OCP Capability Sent to S-GW in MBRsp
1	Indication IE	Indication IE	No Change. Indication IE is sent in MBRsp messages.
2	Private Extension IE	Private Extension IE	Private Extension IE received from S-GW is ignored. Indication IE is sent in MBRsp message.
3	None	Both Private Extension and Indication IEs.	Only the Indication IE is sent in MBRsp message.
4	Both Private Extension and Indication IEs.	Indication IE	Private Extension IE received from the S-GW is ignored. Only the Indication IE is sent in the MBRsp message.

Previous and New Behavior for the S-GW

The following table describes the previous and new behavior in Create Session Response (CSRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

Table 4: Previous and New Behavior: CSRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
12	Indication IE	No change. OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in CSRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **Private Extension IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in CSRsp	New Behavior: IE Carrying OCP Capability Received from PGW in CSRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in CSRsp	New Behavior: IE Carrying OCP Capability Sent to MME in CSRsp
3	Both Private Extension IE and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only OCP capability received as a part of the Indication IE is accepted.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **Private Extension IE and Indication IE**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, then the Private Extension IE is forwarded to the MME in CSRsp as would be done for any unknown Private Extension IE.
4	None	No change.	None	No change.

The following table describes the previous and new behavior in Modify Bearer Response (MBRsp) messages at the S-GW due to the removal of Private Extension Overcharging Support.

Table 5: Previous Behavior and New Behavior: MBRsp Messages at the S-GW Due to the Removal of Private Extension Overcharging Support

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
1	Indication IE	No change. OCP capability received as part of Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.
2	Private Extension IE	OCP capability received as part of Private Extension IE is ignored.	If gtpc private-extension overcharge-protection is disabled at egtpc service level: **None**. If gtpc private-extension overcharge-protection is enabled at egtpc service level: **Indication IE**.	Since the CLI command is deprecated, neither one of the two IEs is sent in the MBRsp to the MME for the OCP capability.
3	Both Private Extension ID and Indication IE	OCP capability received as part of the Private Extension IE is ignored. Only the OCP capability received as part of the Indication IE is accepted.	Indication IE	No change. Indication IE is sent in MBRsp.

Scenario No.	Old Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	New Behavior: IE Carrying OCP Capability Received from P-GW in MBRsp	Old Behavior: IE Carrying OCP Capability Sent to MME in MBRsp	New Behavior: IE Carrying OCP Capability Sent to MME in MBRsp
4	None	None	None	No change.

Important In StarOS releases 21.0 and later, the S-GW will send a MBReq message with only the indication IE for the Pause/Start Charging procedure. The private extension IE is not sent.

Important If the S-GW receives only the private extension IE from the P-GW in the CSRsp/MBRsp message, then the S-GW ignores the private extension IE. As a result, the S-GW assumes that Overcharging Protection is NOT enabled for the P-GW. So, in this scenario, even if the overcharging condition is met at the S-GW, the S-GW will not send a MBReq message for Charging pause to the P-GW.

Rf Diameter Accounting

Important Rf Diameter Accounting is not supported on the S-GW.

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

The Rf reference interface enables offline accounting functions on the HSGW in accordance with 3GPP Release 8 specifications. In an LTE application the same reference interface is also supported on the S-GW and P-GW platforms. The Cisco gateways use the Charging Trigger Function (CTF) to transfer offline accounting records via a Diameter interface to an adjunct Charging Data Function (CDF) / Charging Gateway Function (CGF). The HSGW and Serving Gateway collect charging information for each mobile subscriber UE pertaining to the radio network usage while the P-GW collects charging information for each mobile subscriber related to the external data network usage.

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

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

S-GW Collision Handling

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

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

The enhanced behavior is as follows:

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

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

Viewing S-GW Collision Statistics

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

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

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

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 Gxc. The trace can be initiated using multiple methods:

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

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

The session level trace function consists of trace activation followed by triggers. The EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5500 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

Caution As subscriber level trace is a CPU intensive activity the maximum number of concurrently monitored trace sessions per Cisco S-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

Support for One Million S1-U Peers on the S-GW

Due to customer business requirements and production forecasts, support has been added to the StarOS for one million S1-U connections on a single S-GW.

The S1-U interface is the user plane interface carrying user data between an eNodeB and an S-GW received from the terminal. The StarOS now has the capability to scale the number of S1-U peers to one million per VPN context.

A new CLI command has been added to enable operators to set the number of S1-U peers for which statistics should be collected. The limit is restricted to less than one million peers (128k) due to StarOS memory limitations.

How it Works

The gtpumgr uses the following guidelines while allocating peers:

- When a session installation comes from the Session Manager, a peer is created. If statistics are maintained at the Session Manager, the gtpumgr also creates the peer record with the statistics.
- Peer records are maintained per service.
- The number of peers is maintained at the gtpumgr instance level. The limit is one million S1-U peers per gtpumgr instance.
- If the limit of one million peers is exceeded, then peer creation fails. It causes a call installation failure in the gtpumgr, which leads to an audit failure if an audit is triggered.

The feature changes impact all the interfaces/services using the gtpu-service including GGSN/S4-SGSN/SGW/PGW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW for:

- The Gn and Gp interfaces of the General Packet Radio Service (GPRS)
- The Iu, Gn, and Gp interfaces of the UMTS system
- The S1-U, S2a, S2b, S4, S5, S8, and S12 interfaces of the Evolved Packet System (EPS)

Recovery/ICSR Considerations

- After a session manager/gtpumgr recovery or after an ICSR switchover, the same set of peers configured for statistics collection is recovered.
  - Peers with 0 sessions and without statistics are not recovered.
  - Peers with 0 sessions and with statistics are recovered.

- Peers with Extension Header Support disabled are recovered.

- While upgrading from a previous release, ensure the newer release chassis **gtpu peer statistics threshold** is equal to or greater than the previous release. This ensures that the GTPU peer statistics are preserved during the upgrade. For example, if you are upgrading from release 19.0 to 20.2, and the 19.0 system has 17,000 GTPU sessions, then configure the threshold on the 20.2 chassis to 17,000 as well.

Configuration/Restrictions

- Due to the large number of GTP-U entities connecting to the StarOS, Cisco recommends disabling the GTP-U Path Management feature.
- The configured threshold is not the hard upper limit for statistics allocation because of the distributed nature of system. It is possible that total GTP-U peers with statistics exceeds the configured threshold value to some extent.
- It is assumed that all 1,000,000 peers are not connected to the node in a point-to-point manner. They are connected through routers.
- There will not be any ARP table size change for the StarOS to support this feature.

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 then 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 then 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 a the condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in an element management system.

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

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

ULI Enhancements

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

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

- RAN/NAS Cause IE within bearer context of Delete Bearer Command message.
- The S-GW ignores the ULI received as call is going down so there is no point in updating the CDR.

Support for ULI and ULI Timestamp in Delete Bearer Command message had already been added.

Now, when a new ULI is received in the Delete Bearer Command message, a S-GW CDR is initiated.

Features and Functionality - Optional Enhanced Feature Software

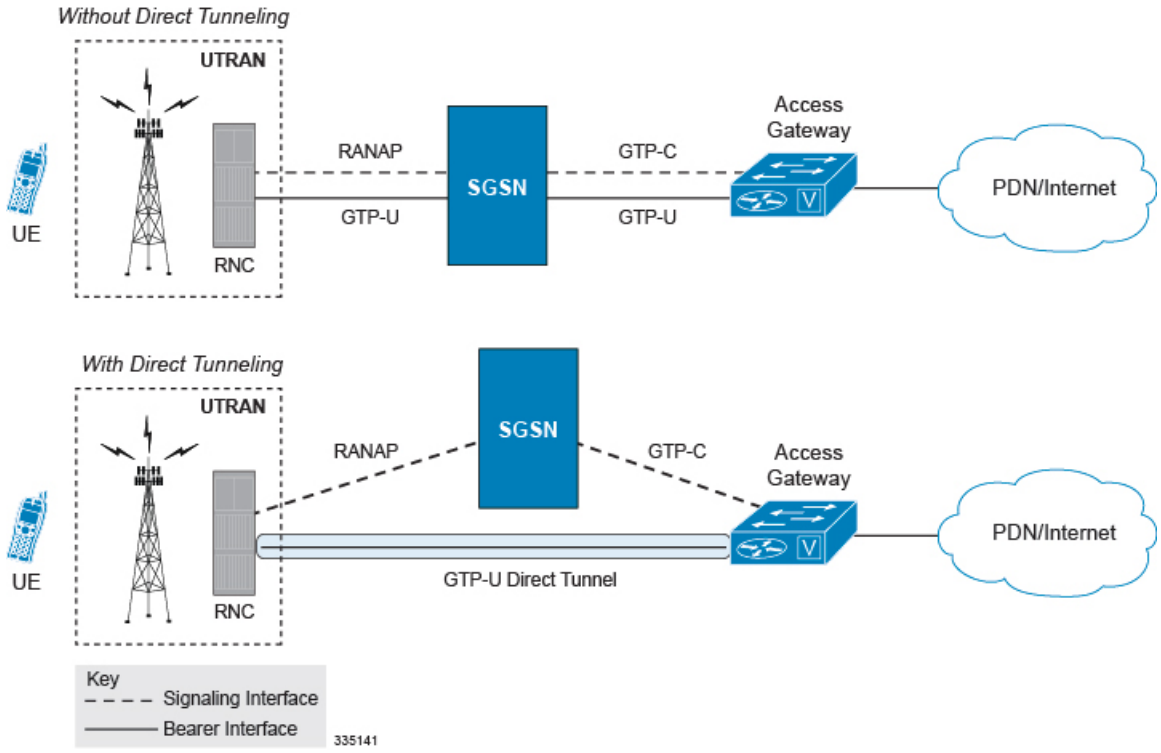
This section describes the optional enhanced features and functions for the S-GW service.

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

Direct Tunnel

In accordance with standards, one tunnel functionality enables the SGSN to establish a direct tunnel at the user plane level - a GTP-U tunnel, directly between the RAN and the S-GW.

Figure 12: GTP-U with Direct Tunnel



In effect, a direct tunnel reduces data plane latency as the tunnel functionality acts to remove the SGSN from the data plane and limit the SGSN to the control plane for processing. This improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services). Additionally, direct tunnel functionality implements the standard SGSN optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

Typically, the SGSN establishes a direct tunnel at PDP context activation using an Update PDP Context Request towards the S-GW. This means a significant increase in control plane load on both the SGSN and S-GW components of the packet core. Hence, deployment requires highly scalable S-GWs since the volume and frequency of Update PDP Context messages to the S-GW will increase substantially. The ASR 5500 platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

Important For more information on direct tunnel support, refer to the *Direct Tunnel for 4G (LTE) Networks* chapter in this guide.

Intelligent Paging for ISR

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

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

Inter-Chassis Session Recovery

The ASR 5500 platform provide industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

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

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

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

Interchassis Communication

Chassis configured to support ICSR communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier
- chassis priority
- chassis MAC address

Checkpoint Messages

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

Important For more information on inter-chassis session recovery support, refer to the *Interchassis Session Recovery* chapter in *System Administration Guide*.

IP Security (IPSec) Encryption

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

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

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

Important You must purchase an IPSec license to enable IPSec. For more information on IPSec support, refer to the *IPSec Reference*.

Lawful Intercept

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

Layer 2 Traffic Management (VLANs)

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

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

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

New Call Policy for Stale Sessions

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

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

New Standard QCI Support

New Standard QCI Support is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

The P-GW/SAEGW/S-GW support additional new 3GPP-defined standard QCIs. QCIs 65, 66, 69, and 70 are now supported for Mission Critical and Push-to-Talk (MC/PTT) applications. These new standard QCIs are supported in addition to the previously supported QCIs of 1 through 9, and operator-defined QCIs 128 through 254.

The StarOS will continue to reject QCIs 10 through 127 sent by the PCRF.

For detailed information on this feature, refer to the *New Standard QCI Support* chapter in this guide.

Overcharging Protection Support

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

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

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

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

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

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

Once the criterion to signal "stop charging" is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. The MBReq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.

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

P-GW will resume charging downlink packets when either of these conditions is met:

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

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

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

Paging Policy Differentiation

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.

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.

Important P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Important For more information on paging policy differentiation, refer to the *Paging Policy Differentiation* chapter in this guide.

3GPP Release 12 Load and Overload Support

Use of 3GPP Release 12 (R12) Load and Overload Support requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

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

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

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

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

- Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

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

Important 3GPP R12 Load and Overload Support is a license-controlled feature. Contact your Cisco representative for more information on licensing requirements.

Important For more information on this feature, refer to the *GTP-C Load and Overload Control Support on the P-GW, SAEGW, and S-GW* chapter in this guide.

3GPP R12 Load and Overload Factor Calculation Enhancement

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

A new CLI command is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.

Operation

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

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

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

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

Separate Paging for IMS Service Inspection

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

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

Session Recovery Support

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

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

S-GW Paging Enhancements

Use of S-GW Paging requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

S-GW Paging includes the following scenarios:

Scenario 1: S-GW sends a DDN message to the MME/S4-SGSN nodes. MME/S4-SGSN responds to the S-GW with a DDN Ack message. While waiting for the DDN Ack message from the MME/S4-SGSN, if the S-GW receives a high priority downlink data, it does not resend a DDN to the MME/S4-SGSN.

Scenario 2: If a DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN, S-GW does not send DDN.

Scenario 3: DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received. DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.

To handle these scenarios, the following two enhancements have been added to the DDN functionality:

- High Priority DDN at S-GW
- MBR-DDN Collision Handling

These enhancements support the following:

- Higher priority DDN on S-GW and SAEGW, which helps MME/S4-SGSN to prioritize paging.
- Enhanced paging KPI and VoLTE services.
- DDN message and mobility procedure so that DDN is not lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A new CLI command **ddn temp-ho-rejection mbr-guard-timer** has been introduced to enable the guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.
- TAU/RAU with control node change triggered DDNs.

In addition to the above functionality, to be compliant with 3GPP standards, support has been enhanced for Downlink Data Notification message and Mobility procedures. As a result, DDN message and downlink data which triggers DDN is not lost. This helps improve paging KPI and VoLTE success rates in scenarios where DDN is initiated because of SIP invite data.

Important For more information on this functionality, refer to the *S-GW Paging Enhancements* chapter in this guide.

How the Serving Gateway Works

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

The S-GW supports the following network flows:

• GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network, on page 44

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

The following topics and procedure flows are included:

• Subscriber-initiated Attach (initial), on page 44
• Subscriber-initiated Detach, on page 47

Subscriber-initiated Attach (initial)

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

Figure 13: Subscriber-initiated Attach (initial) Call Flow

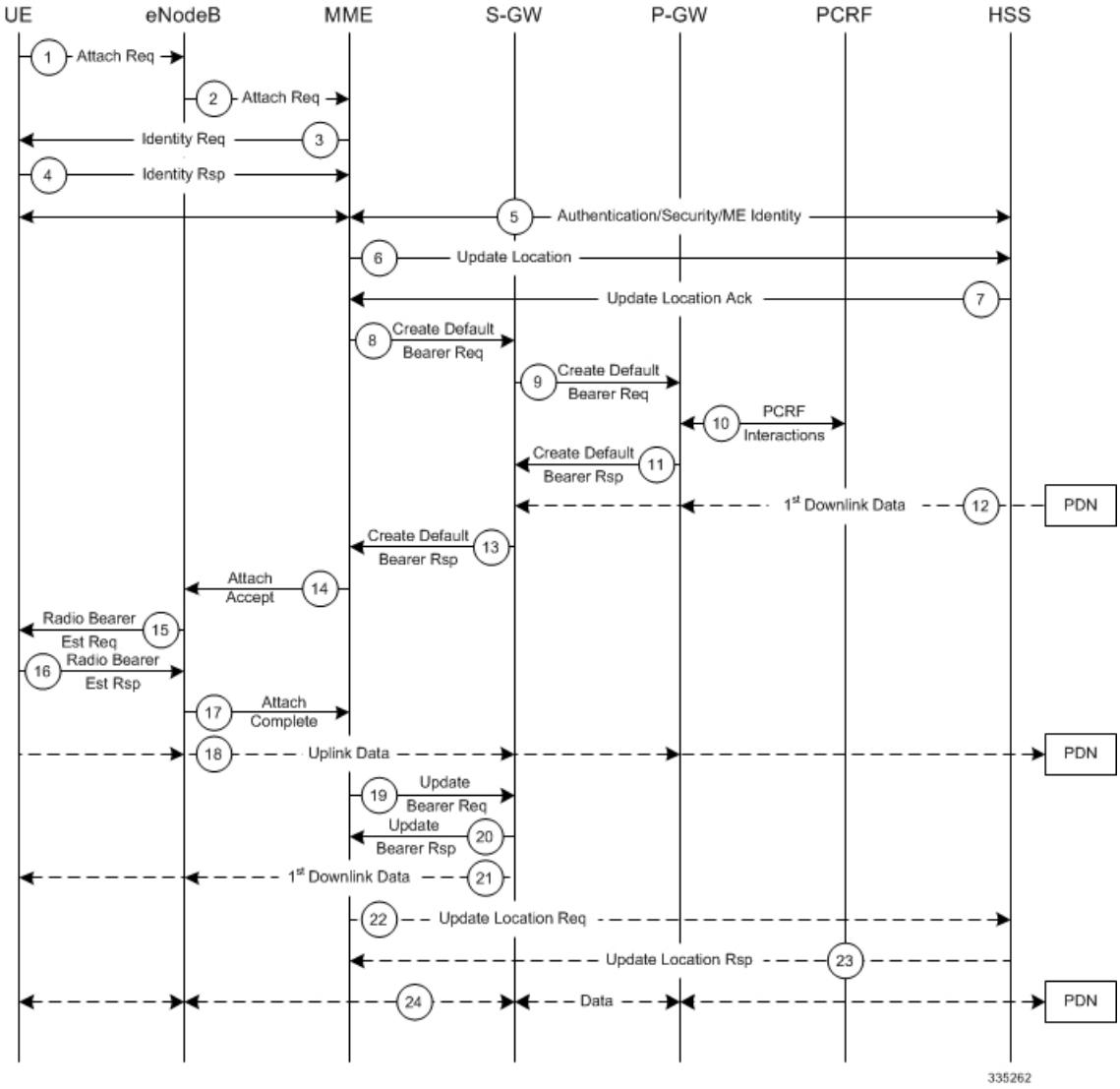


Table 6: Subscriber-initiated Attach (initial) Call Flow Description

Step	Description
1	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.
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an MME selection function. The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.

Step	Description
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	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.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	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.
8	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.
9	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.
10	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.
11	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.
12	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
13	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.
14	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.
15	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.

Step	Description
16	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
17	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
18	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunneled to the S-GW and P-GW.
19	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
20	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
21	The S-GW sends its buffered downlink packets.
22	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.
23	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
24	Bidirectional data is passed between the UE and PDN.

Subscriber-initiated Detach

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

Figure 14: Subscriber-initiated Detach Call Flow

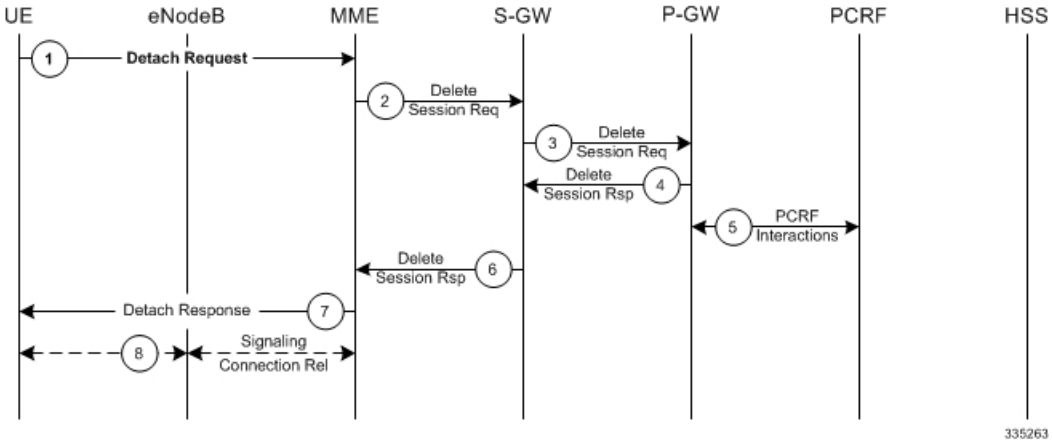


Table 7: Subscriber-initiated Detach Call Flow Description

Step	Description
1	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.
2	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.

Step	Description
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	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.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	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.
8	The MME releases the S1-MME signaling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

Supported Standards

The S-GW service complies with some of the standards in the following standards categories:

- 3GPP References, on page 48
- 3GPP2 References, on page 51
- IETF References, on page 51
- Object Management Group (OMG) Standards, on page 51

3GPP References

Release 12 3GPP References

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

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

Release 11 3GPP References

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

Release 10 3GPP References

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

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

Release 9 Supported Standards

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

Release 8 Supported Standards

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification

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

3GPP2 References

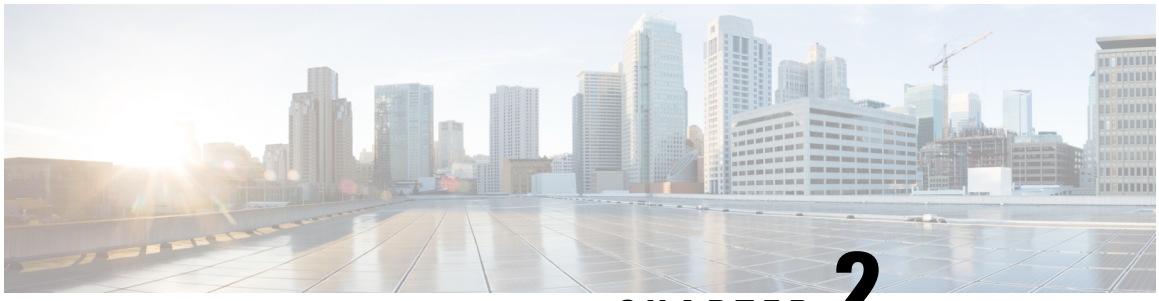
- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

IETF References

- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (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 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3775: Mobility Support in IPv6
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5213: Proxy Mobile IPv6
- Internet-Draft: Proxy Mobile IPv6
- Internet-Draft: GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft: Binding Revocation for IPv6 Mobility, work in progress

Object Management Group (OMG) Standards

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



CHAPTER 2

Serving Gateway Configuration

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

Important Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

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

This chapter includes the following topics:

Configuring the System as a Standalone eGTP S-GW

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

Information Required

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

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

Required Local Context Configuration Information

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

Table 8: Required Information for Local Context Configuration

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

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 9: Required Information for S-GW Ingress Context Configuration

Required Information	Description
S-GW ingress context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW ingress context is recognized by the system.
Accounting policy name	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.
S1-U/S11 Interface Configuration (To/from eNodeB/MME) **Note** The configuration provided in this guide assumes a shared S1-U/S11 interface. These interfaces can be separated to support a different network architecture. The information below applies to both.	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name (for S1-U/S11 interface)	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service bound to the S1-U/S11 interface will be recognized by the system.
IP address	S1-U/S11 interface IPv4 or IPv6 address.
S-GW Service Configuration	
S-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S-GW service is recognized by the system. Multiple names are needed if multiple S-GW services will be used.
eGTP Ingress Service Configuration	
eGTP S1-U/S11 ingress service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP S1-U/S11 ingress service is recognized by the system.

Required S-GW Egress Context Configuration Information

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

Table 10: Required Information for S-GW Egress Context Configuration

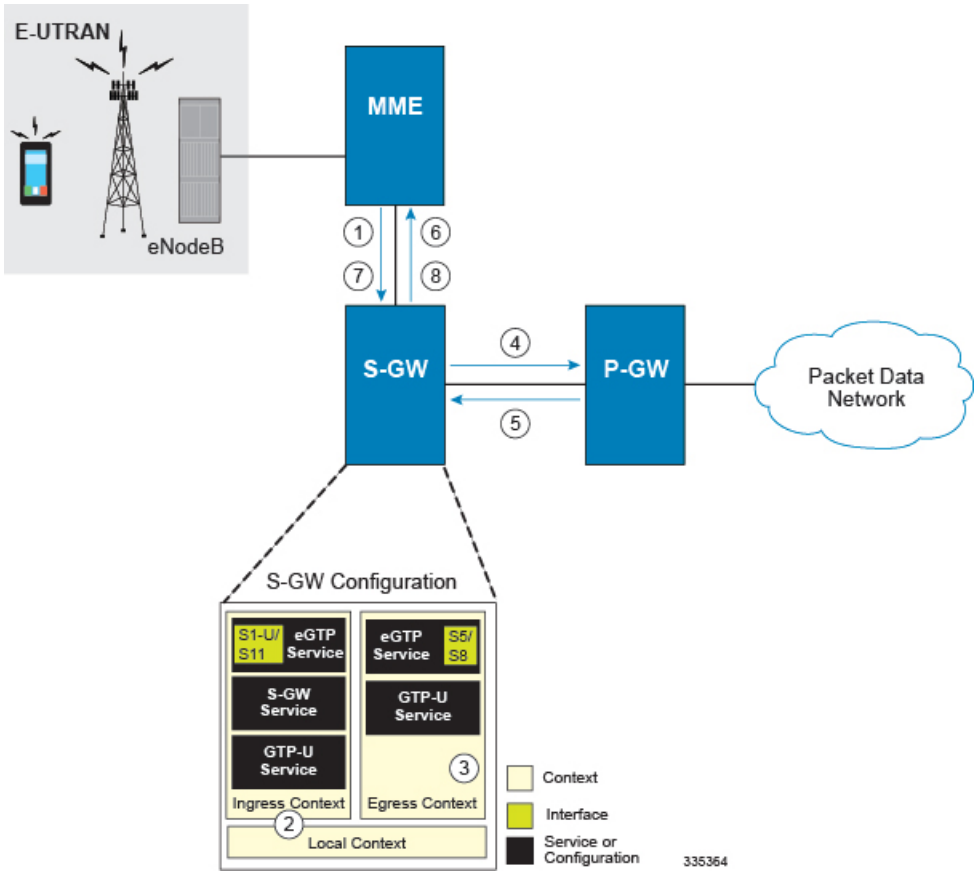
Required Information	Description
S-GW egress context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW egress context is recognized by the system.
S5/S8 Interface Configuration (To/from P-GW)	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name (for S5/S8 interface)	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.
IP address	S5/S8 interface IPv4 or IPv6 address.
eGTP Egress Service Configuration	
eGTP Egress Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP egress service is recognized by the system.

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 15: eGTP S-GW Call Processing Using a Single Ingress and Egress Context

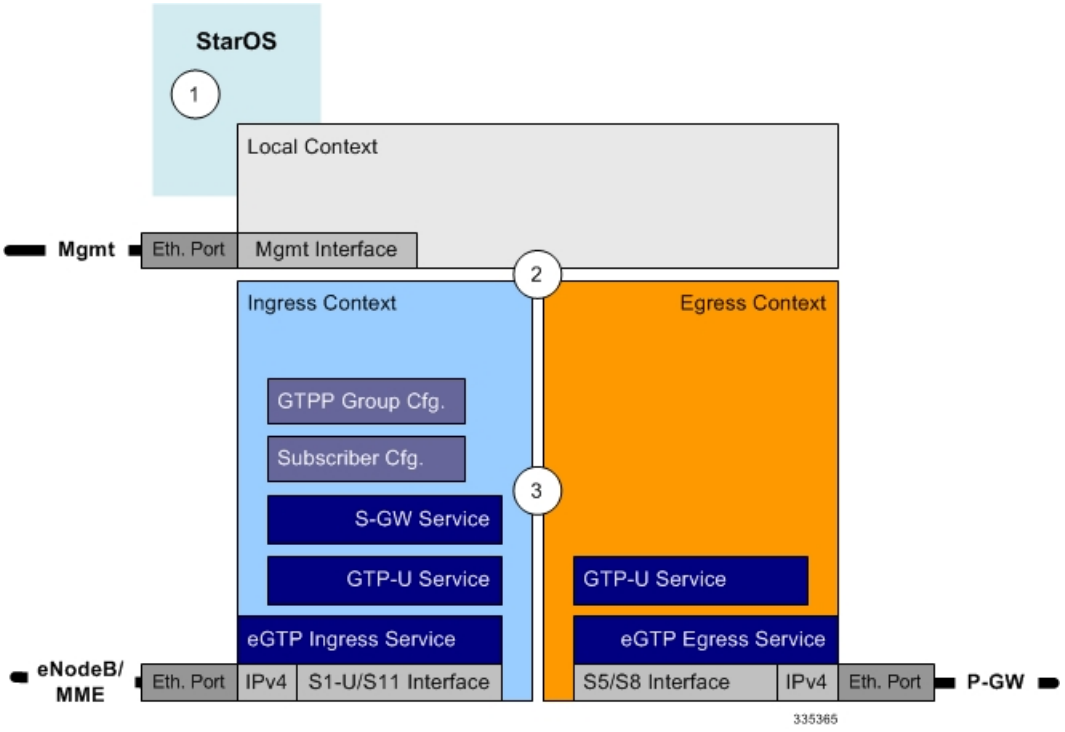


1. A subscriber session from the MME is received by the S-GW service over the S11 interface.
2. The S-GW service determines which context to use to access PDN services for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation 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 a standalone eGTP S-GW, review the following graphic and subsequent steps.

Figure 16: eGTP S-GW Configurable Components



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

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in theInitial Configuration, on page 58.

Step 3 Configure the system to perform as an eGTP S-GW and set basic S-GW parameters such as eGTP interfaces and an IP route by applying the example configurations presented in the eGTP Configuration, on page 61.

Step 4 Verify and save the configuration by following the instruction in the Verifying and Saving the Configuration, on page 62.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in the Modifying the Local Context, on page 59.

Step 2 Create an ingress context where the S-GW and eGTP ingress service will reside by applying the example configuration in the Creating an S-GW Ingress Context, on page 59.

Step 3 Create an eGTP ingress service within the newly created ingress context by applying the example configuration in the Creating an eGTP Ingress Service, on page 60.

Step 4 Create an S-GW egress context where the eGTP egress services will reside by applying the example configuration in the Creating an S-GW Egress Context, on page 60.

Step 5 Create an eGTP egress service within the newly created egress context by applying the example configuration in the Creating an eGTP Egress Service, on page 60.

Step 6 Create a S-GW service within the newly created ingress context by applying the example configuration in the Creating an S-GW Service, on page 60.

Modifying the Local Context

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

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

Creating an S-GW Ingress Context

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

```
configure
  context <ingress_context_name> -noconfirm
    subscriber default
    exit
  interface <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> <ingress_context_name>
   end
```

Notes:

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

Creating an eGTP Ingress Service

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

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

Creating an S-GW Egress Context

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

```
configure
  context <egress_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <address>
        tunnel-mode ipv6ip
          source interface <name>
          destination address <ipv4 or ipv6 address>
          end
configure
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <egress_context_name>
    end
```

Notes:

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

Creating an eGTP Egress Service

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

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

Creating an S-GW Service

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

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

eGTP Configuration

Step 1 Set the system's role as an eGTP S-GW and configure eGTP service settings by applying the example configuration in the Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings, on page 61.

Step 2 Configure the S-GW service by applying the example configuration in the Configuring the S-GW Service, on page 62.

Step 3 Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring an IP Route, on page 62.

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

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

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

Notes:

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

Configuring the S-GW Service

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

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

Configuring an IP Route

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

```
configure
   context <egress_context_name>
      ip route <pgw_ip_addr/mask> <sgw_next_hop_addr> <sgw_intrfc_name>
      end
```

Verifying and Saving the Configuration

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

Configuring Optional Features on the eGTP S-GW

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

Configuring the GTP Echo Timer

The GTP echo timer on the ASR 5500 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:

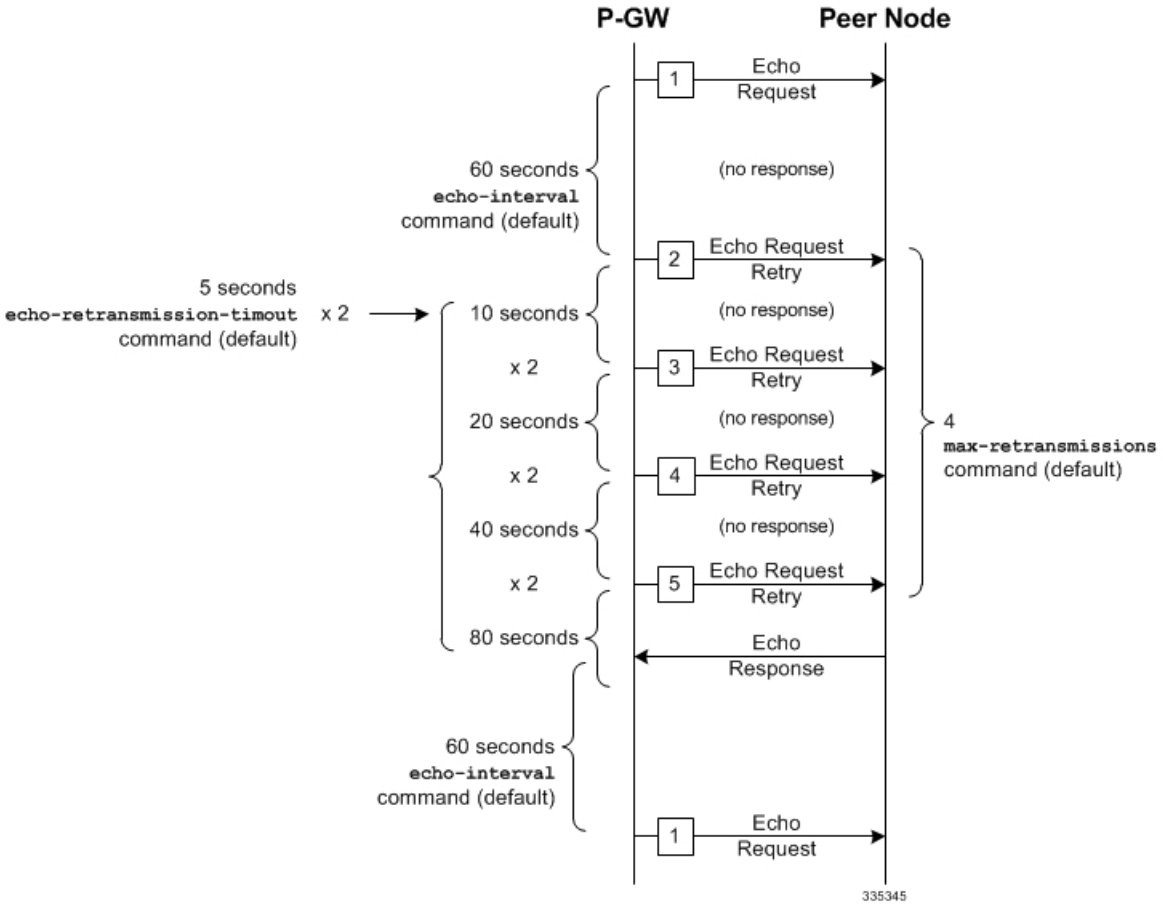
eGTP-C

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

Notes:

- This configuration can be used in either the ingress context supporting the S1-U and/or S11 interfaces with the eNodeB and MME respectively; and the egress context supporting the S5/S8 interface with the P-GW.
- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above:

Figure 17: Failure and Recovery Scenario: Example 1



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

GTP-U

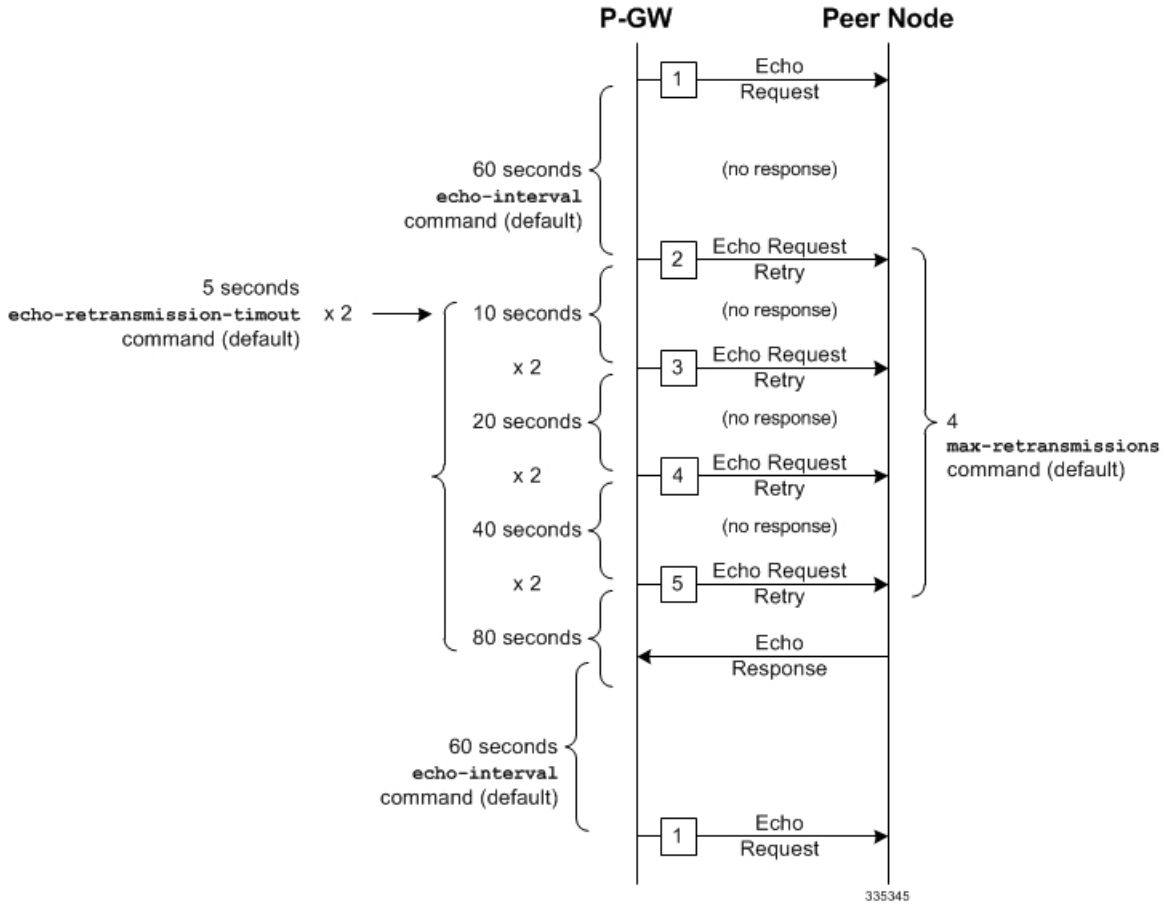
```
configure
   context <context_name>
      gtpu-service <gtpu_service_name>
         echo-interval <seconds>
         echo-retransmission-timeout <seconds>
         max-retransmissions <num>
         end
```

Notes:

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

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

Figure 18: Failure and Recovery Scenario: Example 2



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

Dynamic GTP Echo Timer Configuration

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

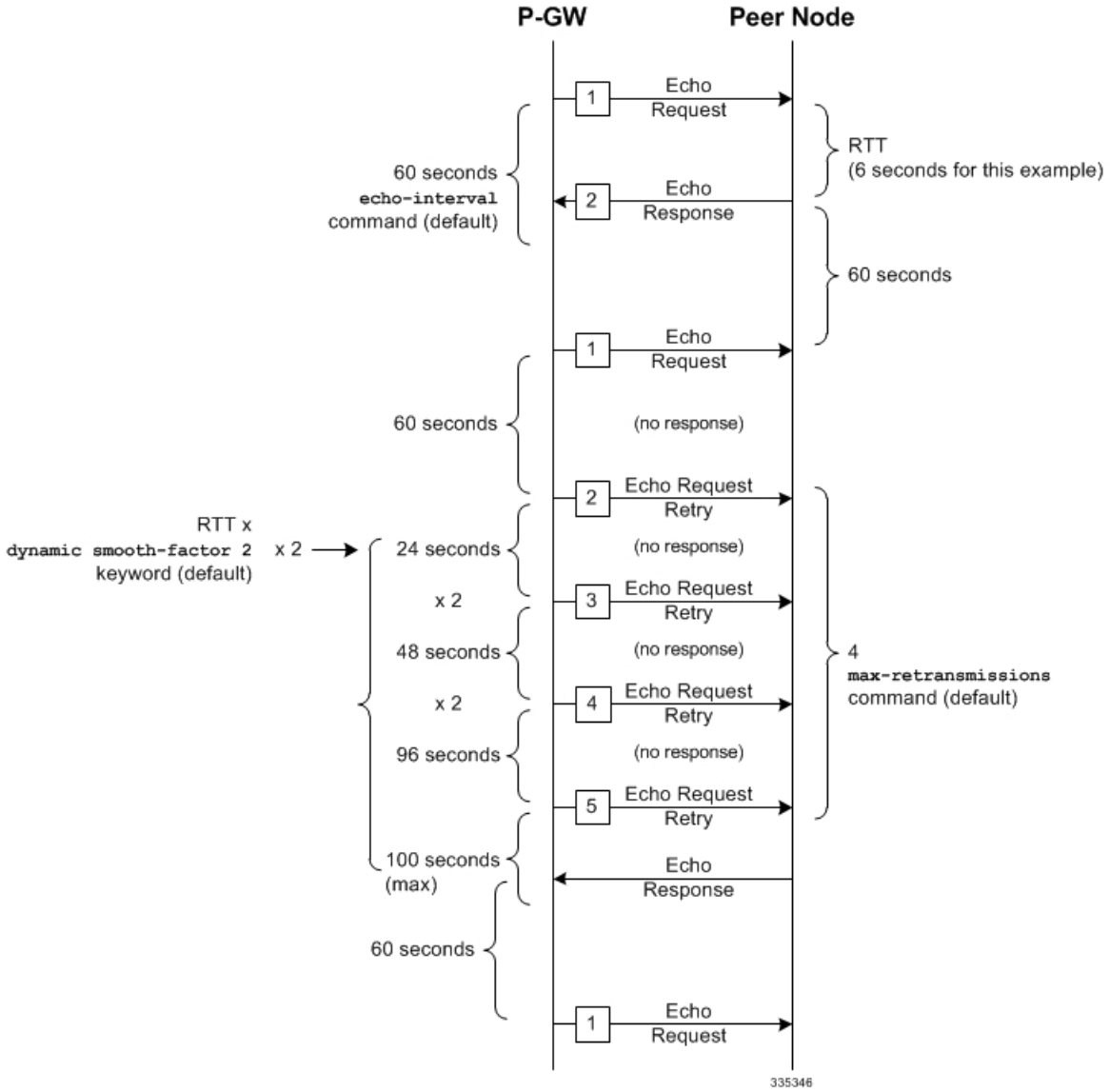
eGTP-C

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

Figure 19: Failure and Recovery Scenario: Example 3



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

GTP-U

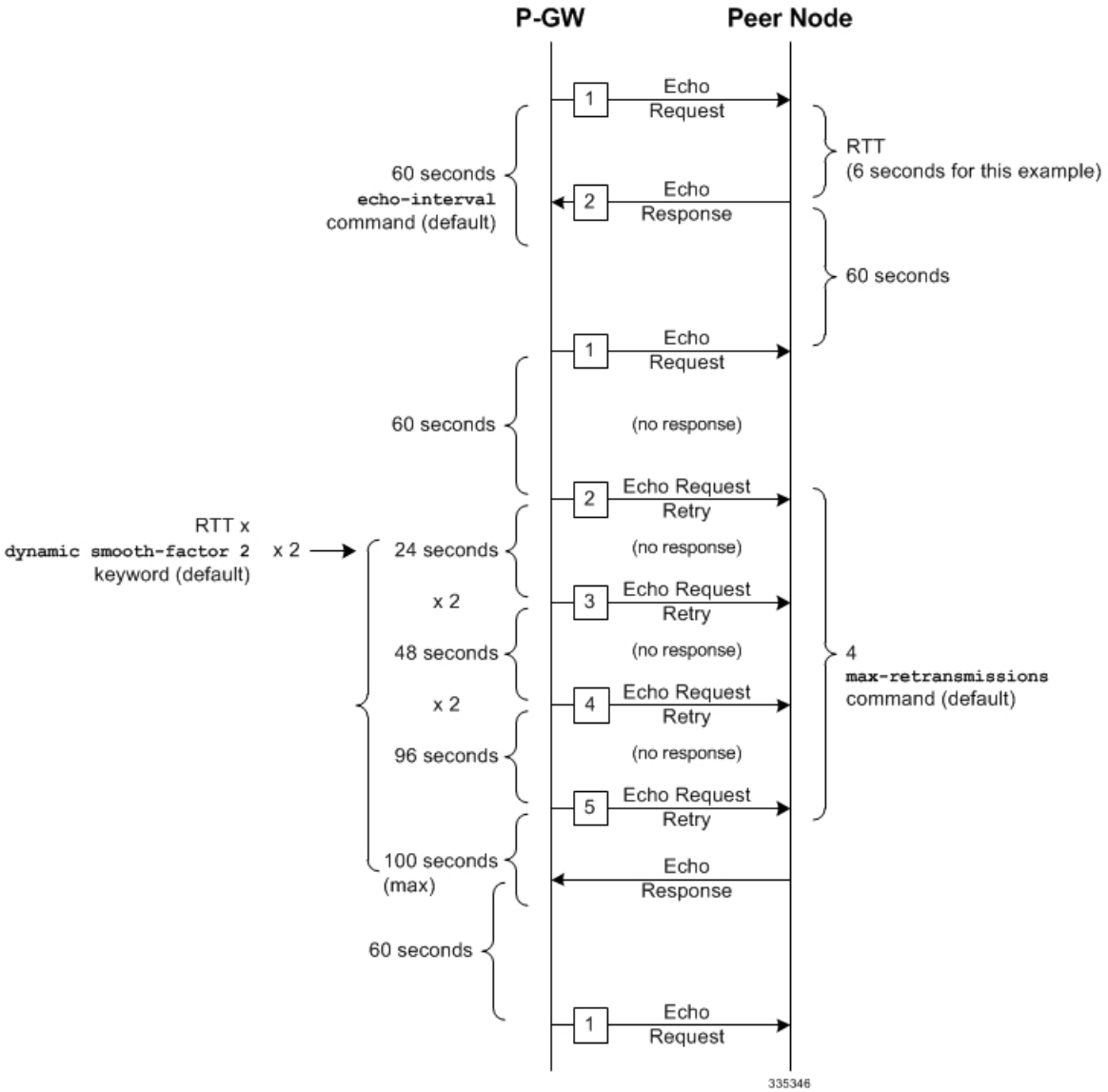
```
configure
  context <context_name>
    gtpu-service <gtpu_service_name>
      echo-interval <seconds> dynamic smooth-factor <multiplier>
```

```
echo-retransmission-timeout <seconds>
max-retransmissions <num>
end
```

Notes:

- This configuration can be used in either the ingress context supporting the S1-U interfaces with the eNodeB and the egress context supporting the S5/S8 interface with the P-GW.
- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above and an example round trip timer (RTT) of six seconds:

Figure 20: Failure and Recovery Scenario: Example 4



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

Configuring GTPP Offline Accounting on the S-GW

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

```
configure
  gtpp single-source
    context <ingress_context_name>
      subscriber default
        accounting mode gtpp
        exit
      gtpp group default
        gtpp charging-agent address <gz_ipv4_address>
        gtpp echo-interval <seconds>
        gtpp attribute diagnostics
        gtpp attribute local-record-sequence-number
        gtpp attribute node-id-suffix <string>
        gtpp dictionary <name>
        gtpp server <ipv4_address> priority <num>
        gtpp server <ipv4_address> priority <num> node-alive enable
        exit
      policy accounting <gz_policy_name>
        accounting-level {type}
        operator-string <string>
        cc profile <index> buckets <num>
        cc profile <index> interval <seconds>
        cc profile <index> volume total <octets>
        exit
      sgw-service <sgw_service_name>
        accounting context <ingress_context_name> gtpp group default
        associate accounting-policy <gz_policy_name>
        exit
      exit
    context <ingress_context_name>
      interface <gz_interface_name>
        ip address <address>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gz_interface_name> <ingress_context_name>
    end
```

Notes:

- **gtpp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- **gtpp** is the default option for the **accounting mode** command.
- An accounting mode configured for the call-control profile will override this setting.

- **accounting-level** types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the Accounting Profile Configuration Mode Commands chapter in the *Command Line Interface Reference* for more information on this command.

Configuring Diameter Offline Accounting on the S-GW

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

Important Diameter Offline Accounting is not supported on the S-GW.

```
configure
  operator-policy name <policy_name>
    associate call-control-profile <call_cntrl_profile_name>
    exit
  call-control-profile <call_cntrl_profile_name>
    accounting mode radius-diameter
    exit
  lte-policy
    subscriber-map <map_name>
      precendence <number> match-criteria all operator-policy-name
<policy_name>
      exit
    exit
  context <ingress_context_name>
    policy accounting <rf_policy_name>
      accounting-level {type}
      operator-string <string>
      exit
    sgw-service <sgw_service_name>
      associate accounting-policy <rf_policy_name>
      associate subscriber-map <map_name>
      exit
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    diameter endpoint <rf_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
```

```
      route-entry peer <rf_cfg_name>
      exit
    exit
  context <ingress_context_name>
    interface <rf_interface_name>
      ip address <rf_ipv4_address>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <ingress_context_name>
    end
```

Notes:

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

Configuring APN-level Traffic Policing on the S-GW

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

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

Notes:

- For the **qos rate-limit** command, the actions supported for **violate-action** and **exceed-action** are: **drop**, **lower-ip-precedence**, and **transmit**.

Configuring X.509 Certificate-based Peer Authentication

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

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

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

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

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

Notes:

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

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

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

Notes:

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

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

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

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

Creating and Configuring an IPSec Transform Set

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

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

Notes:

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

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <sgw_context_name>
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.

- The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```
configure
   context <sgw_context_name>
      crypto template <crypto_template_name> ikev2-dynamic
         ikev2-ikesa transform-set list <name1> . . . <name6>
         ikev2-ikesa rekey
         payload <name> match childsa match ipv4
            ipsec transform-set list <name1> . . . <name4>
            rekey
            end
```

Notes:

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

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

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

```
configure
   context <sgw_ingress_context_name>
      gtpu-service <gtpu_ingress_service_name>
         bind ipv4-address <s1-u_interface_ip_address> crypto-template
<enodeb_crypto_template>
         exit
      egtp-service <egtp_ingress_service_name>
         interface-type interface-sgw-ingress
         associate gtpu-service <gtpu_ingress_service_name>
         gtpc bind address <s1u_interface_ip_address>
         exit
      exit
   context <sgw_egress_context_name>
      gtpu-service <gtpu_egress_service_name>
         bind ipv4-address <s5_interface_ip_address> crypto-template
<enodeb_crypto_template>
         exit
      egtp-service <egtp_egress_service_name>
         interface-type interface-sgw-egress
         associate gtpu-service <gtpu_egress_service_name>
         gtpc bind address <s5_interface_ip_address>
         exit
      exit
   context <sgw_ingress_context_name>
      sgw-service <sgw_service_name> -noconfirm
```

```
egtp-service ingress service <egtp_ingress_service_name>
egtp-service egress context <sgw_egress_context_name>
end
```

Notes:

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

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

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

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

Creating and Configuring a Crypto Access Control List

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

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

Notes:

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

Creating and Configuring an IPSec Transform Set

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

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

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.

- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <sgw_context_name>
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

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

Creating and Configuring a Crypto Map

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

```
configure
  context <sgw_ingress_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      ikev2-ikesa transform-set list <name1> . . . <name6>
      payload <name> match ipv4
        lifetime <seconds>
```

```
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
    interface <s1-u_intf_name>
      ip address <ipv4_address>
      crypto-map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s1_u_intf_name> <sgw_ingress_context_name>
    end
```

Notes:

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

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

```
configure
  context <sgw_egress_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
    interface <s5_intf_name>
      ip address <ipv4_address>
      crypto map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
      no shutdown
      bind interface <s5_intf_name> <sgw_egress_context_name>
      end
```

Notes:

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

Configuring 3GPP Release 12 Load Control Support

3GPP R12 Load Control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

Use the following example to configure this feature:

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

Notes:

- The **inclusion-frequency** parameter determines how often the Load control information element is sent to the peer(s).
- The total of the three **weightage** parameters should not exceed 100.
- The **associate** command is used to associate the Load Control Profile with an existing S-GW service.

Configuring 3GPP Release 12 Overload Control Support

3GPP R12 Overload Control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Use the following example to configure this feature.

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

Notes:

- The **inclusion-frequency** parameter determines how often the Overload control information element is sent to the peer(s).
- The total of the three **weightage** parameters should not exceed 100.
- **validity-period** configures how long the overload control information is valid. Valid entries are from 1 to 3600 seconds. The default is 600 seconds.
- The **associate** command is used to associate the Overload Control Profile with an existing S-GW service.

Configuring S4 SGSN Handover Capability

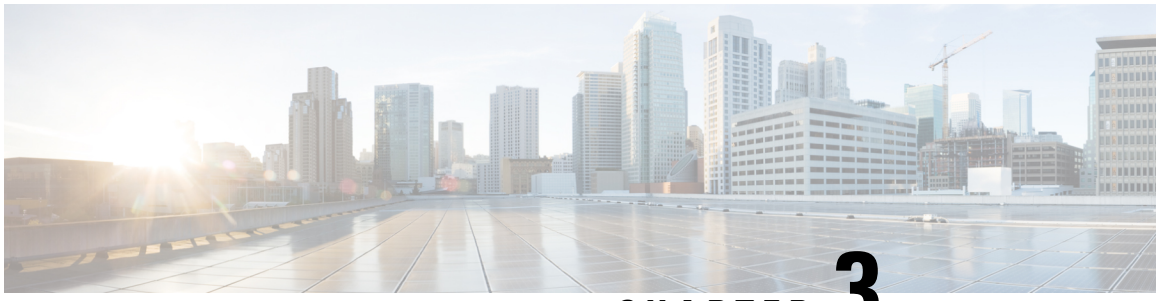
This configuration example configures an S4 interface supporting inter-RAT handovers between the S-GW and an S4 SGSN.

Use the following example to configure this feature:

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

Notes:

- The S4 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.



CHAPTER 3

Monitoring the Service

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

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

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

Monitoring System Status and Performance

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

Table 11: System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Congestion-Control Information	
View Congestion-Control Statistics	**show congestion-control statistics { a11mgr | ipsecmgr }**
View Subscriber Information	
View session resource status	**show resources session**
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*

To do this:	Enter this command:
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	**show subscribers all**
View Statistics for Subscribers using S-GW Services on the System	
View statistics for subscribers using any S-GW service on the system	**show subscribers sgw-only full**
View statistics for subscribers using a specific S-GW service on the system	**show subscribers sgw-service** *service_name*
View Statistics for Subscribers using MAG Services on the System	
View statistics for subscribers using any MAG service on the system	**show subscribers mag-only full**
View statistics for subscribers using a specific MAG service on the system	**show subscribers mag-service** *service_name*
View Session Subsystem and Task Information	
Display Session Subsystem and Task Statistics **Important** Refer to the StarOS Tasks 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 Session Manager statistics	**show session subsystem facility sessmgr all**
View MAG Manager statistics	**show session subsystem facility magmgr all**
View Session Recovery Information	
View session recovery status	**show session recovery status [verbose]**
View Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View S-GW Service Information	
View S-GW service statistics	**show sgw-service statistics all**
Verify S-GW services	**context** *sgw_context_name* **show sgw-service all |grep Status** **show mag-service all |grep Status**
View GTP Information	
View eGTP-C service statistics for a specific service	**show egtpc statistics egtpc-service** *name*
View eGTP-C service information for a specific service	**show egtpc-service** *name*

To do this:	Enter this command:
View GTP-U service statistics for all GTP-U data traffic on the system	**show gtpu statistics**
View eGTP-U service information for a specific service	**show gtpu-service** *name*
View QoS/QCI Information	
View QoS Class Index to QoS mapping tables	**show qci-qos-mapping table all**

Configuring the S-GW to Include IMSI/IMEI in Logging Events

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

Table 12: New and Modified System Event Logs with IMSI/IMEI in System Event Log Details

Event Log	Description
New Events	
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: s, error code d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>]Sessmgr-d Recover call from CRR failed for callid:0xx reason=s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-d Ran out of session handles"
140075	Represents error_log1 in format "[IMSI <IMSI>]s"
Modified Events	
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=s(d) state=s(d) event=s(d)"
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=s(d) event=s(d)"
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-d: Request to s bearer rejected. Reason: s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code d"

Event Log	Description
12774	Represents pgw_purge_invalid_crr in format "[IMSI <IMSI>] Local s TEID [lu] Collision: Clp Connect Time: lu, Old Clp Callid: d, Old Clp Connect Time: lu s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <u>."
12858	Represnts ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <u>:pf_id_bitmap 0xx and tft_opcode: d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <u> rejected, due to <s>."
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <u>, due to <s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<s>,[event:<s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call."
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0xx> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] s"
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code d"
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "

Event Log	Description
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <s> in state <s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <s> in state <s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <s> in state <s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] s"

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

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

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

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

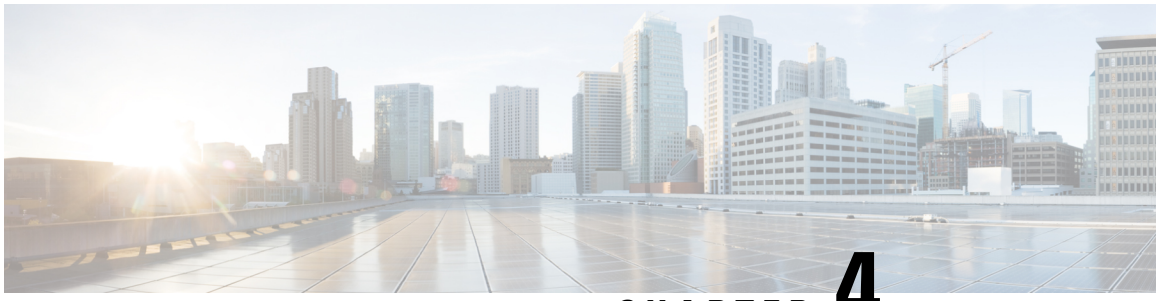
Notes:

- **no** disables the inclusion of the IMSI/IMEI in system event logs of type error and critical
- To determine if **logging include-ueid** is enabled on the S-GW, use the **show configuration** command in Exec Mode. This command will indicate one of the following:
  - logging include-ueid (when enabled)
  - no logging include-ueid (when disabled)

Clearing Statistics and Counters

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

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



CHAPTER 4

5G Non Standalone

This chapter describes the 5G Non Standalone (NSA) feature in the following sections:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

The 5G NSA solution for SAEGW supports Secondary RAT Usage IE during GnGp handover.	21.22
The 5G NSA solution for SAEGW supports dcca-custom1, dcca-custom7 and dcca-custom8 dictionaries.	21.11
The 5G NSA solution for SAEGW supports the following functionality: • P-GW Custom Dictionaries support over Gz for extended bitrate • S-GW Custom Dictionaries support over Gz for extended bitrate • P-GW Custom Dictionaries support over Gy and Rf for extended bitrate • S-GW support of Secondary RAT Data Usage Report in Gz CDRs	21.10
The 5G NSA solution for SAEGW supports the following functionality: • P-GW support of Secondary RAT Data Usage Report in Gz CDRs • P-GW support of Secondary RAT Data Usage Report in Rf CDRs • S-GW and P-GW support of statistics for DCNR PDNs	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
The 5G NSA solution for SAEGW supports the following functionality: • Feature License • Dedicated Bearers • Gy interface • URLLC QCI	21.8
First introduced.	21.6

Feature Description

Important 5G NSA feature is license controlled from release 21.8 onwards. Contact your Cisco account representative for detailed information on specific licensing requirements.

The 5G NSA solution for SAEGW supports the following functionalists:

- **High Throughput**

  5G NR offers downlink data throughput up to 20 Gbps and uplink data throughput up to 10 Gbps. Some interfaces in EPC have the support to handle (encode/decode) 5G throughput. For example, NAS supports up to 65.2 Gbps (APN-AMBR) and S5/S8/S10/S3 (GTP-v2 interfaces) support up to 4.2 Tbps. The

diameter interfaces S6a and Gx support only up to 4.2Gbps throughput, S1-AP supports only up to 10 Gbps and NAS supports up to 10 Gbps (MBR, GBR). New AVP/IE have been introduced in S6a, Gx , S1-AP, and NAS interfaces to support 5G throughput. See the *How It Works* section for more information.

- **DCNR Support on P-GW:**

  Supports configuration of DCNR feature at the P-GW-service, by configuring “Extended-BW-NR” feature in IMSA service. Advertises the DCNR feature support by sending “Extended-BW-NR” feature bit in “Feature-List-ID-2” towards PCRF. Forwards AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" in CCR messages when it receives APN-AMBR values greater than 4.2Gbps from MME/S-GW. Decodes the extended AVP "Extended-APN-AMBR-UL" and "Extended-APN-AMBR-DL" when it is received from PCRF.

- Sends AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when it receives MBR and GBR values greater than 4.2Gbps from MME/S-GW. Decodes the AVP "Extended-Max-Requested-BW-UL", "Extended-Max-Requested-BW-DL", "Extended-GBR-UL" and "Extended-GBR-DL" when received from PCRF. Supports dedicated bearer establishment with extended QoS. Sends AVP Extended-Max-Requested-BW-UL and "Extended-Max-Requested-BW-DL" in Gy records.

- **Ultra Low Latency Support**:

  Supports 5G requirements of Ultra-Reliable and Low Latency Communications (URLLC). 3GPP introduced URLCC QCI 80 (Non-GBR resource type), QCI 82 and 83 (GBR resource type). P-GW establishes default bearers with URLLC QCI 80, which is typically used by low latency eMBB applications. P-GW establishes dedicated bearers with URLLC QCI 82 and 83 (also with QCI 80 if dedicated bearers of Non-GBR type to be established), which is typically used by discrete automation services (industrial automation).

- **ICSR Support**

  With release 21.10 onwards ICSR for 5G NSA on SAEGW is supported.

- **Dynamic S-GW and P-GW selection by MME for DCNR capable UE**

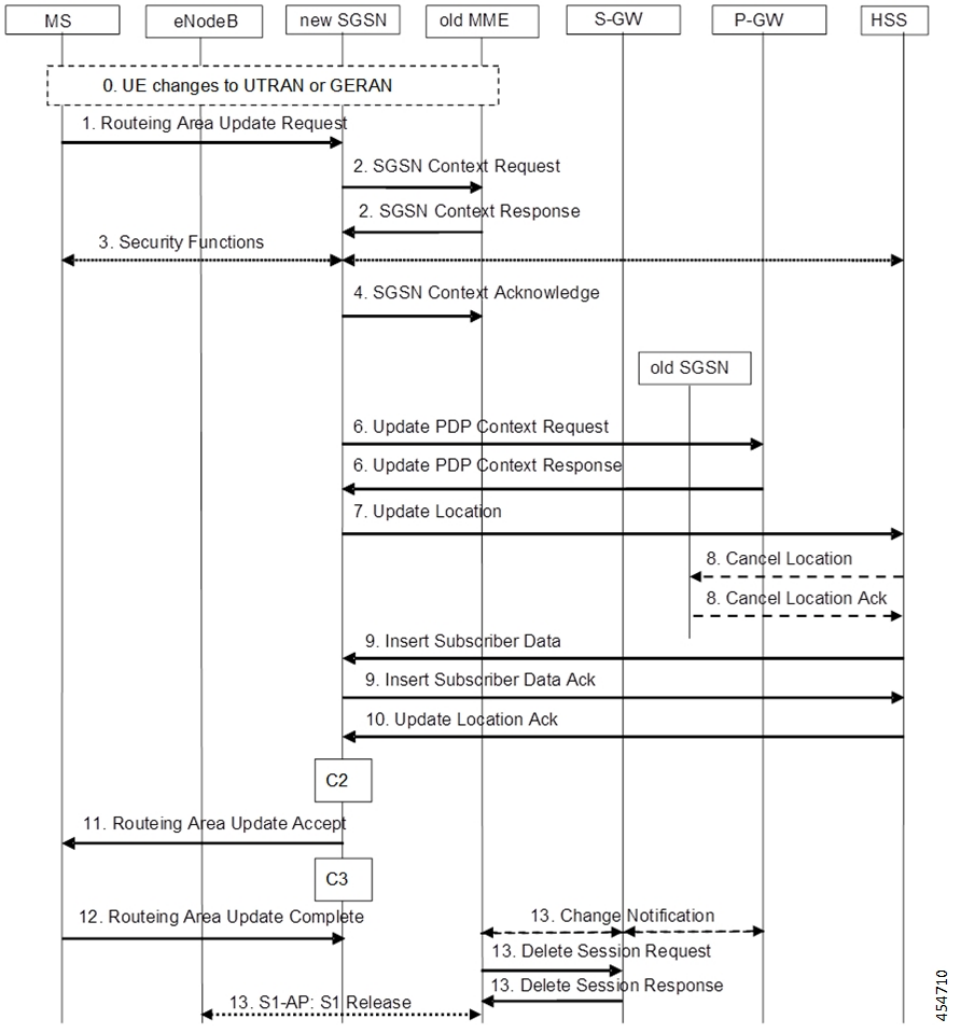
  When DCNR capable UE attempts to register in MME and when all DCNR validations are successful (for example DCNR feature configuration on MME, HSS not sending access-restriction for NR, and son on), the MME sets “UP Function Selection Indication Flags” IE with DCNR flag set to 1 in “Create Session Request” message. This feature is relevant for CUPS architecture to help SGW-C and PGW-C to select SGW-U and PGW-U which supports dual connectivity with NR. When S-GW receives this IE over S11, it sends this IE over S5 to P-GW. S-GW ignores IE if it receives it in Non-CUPS deployment.

- **P-GW Secondary RAT Usage Data Report Handling:**

  P-GW supports custom24 and custom44 for Gz and aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries for Rf to support Secondary RAT Data Usage Report in CDRs.

Support for Secondary RAT Usage During GnGp Handover

This feature supports the Secondary RAT usage reported in change notification request during 4G to 3G handover. The support is for handling the change notification with Secondary RAT Usage during the GnGp handover. Step 13 is added in the following diagram in support of this feature. The usage must be reported in next CDR generation.



IMSI Not Known

If there's no context found for IMSI specified in Secondary RAT Usage IE of change notification request Message, it returns the change notification response with cause value "IMSI/IMEI not known".

Limitations

Following are the known limitations for this feature:

- This feature only supports the handling of the secondary RAT usage IE.
- During the 4G to 3G handover, dedicated bearers are retained and Secondary RAT usage is reported for both Default and Dedicated bearers.

Enabling Secondary RAT Data Usage Report

Use the following configuration to enable Secondary RAT Data Usage Report:

```
configure
  context context_name
    pgw-service service_name
      dcnr
      end
```

Note The GGSN service associated with the P-GW service must have the DCNR enabled using the preceding CLI.

- **Statictics support for DCNR PDNs:**

  S-GW and P-GW statistics support for DCNR PDNs

- **S-GW Secondary RAT Usage Data Report Handling:**

  S-GW supports custom24 and custom6 dictionaries to support Secondary RAT Data Usage Report in CDRs over Gz.

- **P-GW Custom Dictionaries Support over Gz:**

  P-GW supports Custom44 and Custom24 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Multiple Presence Reporting Area Support:**

  S-GW supports Multiple-PRA action and Multiple-PRA Information over S11/S4 and S5/S8 interfaces. P-GW supports Multiple-PRA Action and Multiple-PRA Information over S5/S8 and Gx interfaces.

- **S-GW Custom Dictionaries Support over Gz :**

  S-GW supports custom24 and custom6 dictionaries to support sending the following AVPs when it receives MBR, GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gx:**

P-GW supports dpca-custom15, dpca-custom11, dpca-custom23, dpca-custom19 and dpca-custom17, dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

- Extended-Max-Requested-BW-UL
- Extended-Max-Requested-BW-DL
- Extended-GBR-DL
- Extended-GBR-UL
- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Gy:**

  P-GW supports dcca-custom1, dcca-custom7, dcca-custom8, dcca-custom13 and dcca-custom26 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **P-GW Custom Dictionaries Support over Rf:**

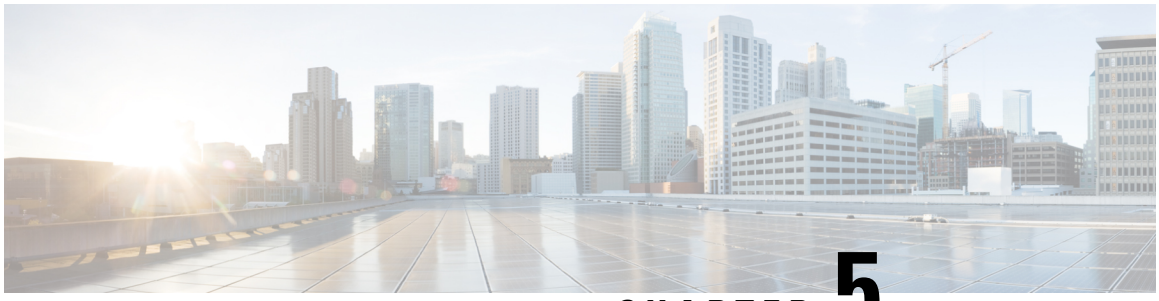
  P-GW supports aaa-custom3, aaa-custom4 and aaa-custom6 dictionaries to support sending the following AVPs when it receives GBR and APN-AMBR values greater than 4.2Gbps:

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

Multiple Presence Reporting Area

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

Note This feature is introduced in release 21.9.1. For more information, refer to the *Presence Reporting Area* chapter in the *P-GW Administration Guide*.



CHAPTER 5

Collision Handling on the P-GW/SAEGW/S-GW

Feature Description

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

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

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

Relationships to Other Features

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

How It Works

Collision Handling

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

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

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

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

Sample output:

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

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

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

Example Collision Handling Scenarios

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

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

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

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

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

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

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

DBCmd/MBreq Collision Handling:

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

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

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

The CLI command **collision handling** provides more flexibility in configuring the handling of the DBCmd message and MBReq message collision scenario. Also refer to Configuring DBcmd Message Behavior, on page 96 in this document for instructions on how to configure the behavior for this collision handling scenario.

MBReq/CBreq Parallel Processing; Handling CBRsp:

The P-GW/S-GW handles the following example collision scenario:

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

Handling UBrsp when Transaction is Suspended:

The P-GW/S-GW handles the following example collision scenario:

When the P-GW/S-GW receives an UBRsp message, then the P-GW/S-GW handles the UBRsp message for the suspended transaction. As a result, The UBRsp message will be buffered until the MBRsp message is sent out.

Collision Handling of MBR over MBR for Drop and Retry

To avoid collision over Modify bearer request (mbreq) message over mbreq, the MME supports collision of MBR over MBR Drop and Retry functionality through a `mbreq-over-mbreq drop` CLI configuration under the egtp-service. The following functions occur:

- MME sends modify bearer request when service request modify bearer request is in pending state
- S-GW drops the E-RAB procedure modify bearer request message
- MME retries the dropped MBR until first MBR response.

Limitations

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

Standards Compliance

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

Configuring Collision Handling

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

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

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

Configuring DBcmd Message Behavior

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

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

NOTES:

- **collision-handling dbcmd-over-mbreq** : Configures collision handling of DBcmd when MBreq is pending.
- **drop**: Drop the DBcmd message when the MBreq message is pending.
- **queue**: Queue the DBcmd message when the MBreq is message is pending.

  The default behavior is to abort the MBReq message and handle the DBcmd message.

Verifying the Configuration

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

```
show egtpc service all
     Collision handling: DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or <Abort
 MBreq and handle Dbcmd>
```

Monitoring the Collision Handling Feature

This section describes how to monitor the collision handling feature.

Collision Handling Show Command(s) and/or Outputs

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

show configuration

The output of this command indicates if collision handling for the DBcmd message when the MBreq message is pending is enabled or disabled or for the mbreq over mbreq drop messages:

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

show egtp-service all | name

The output of this command indicates how the P-GW is configured to handle the DBcmd Message when the MBreq message for the Default Bearer is pending at due to Drop MBreq or Abort MBreq and handle MBreq scenarios:

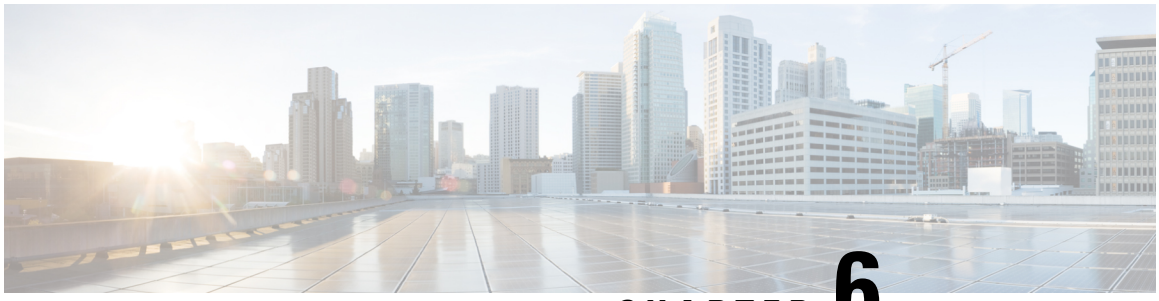
- Collision handling:
  - MBreq when MBreq pending

show egtp statistics verbose

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

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

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



CHAPTER 6

Session Tracing

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

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

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

The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

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

Session Tracing Overview

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

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

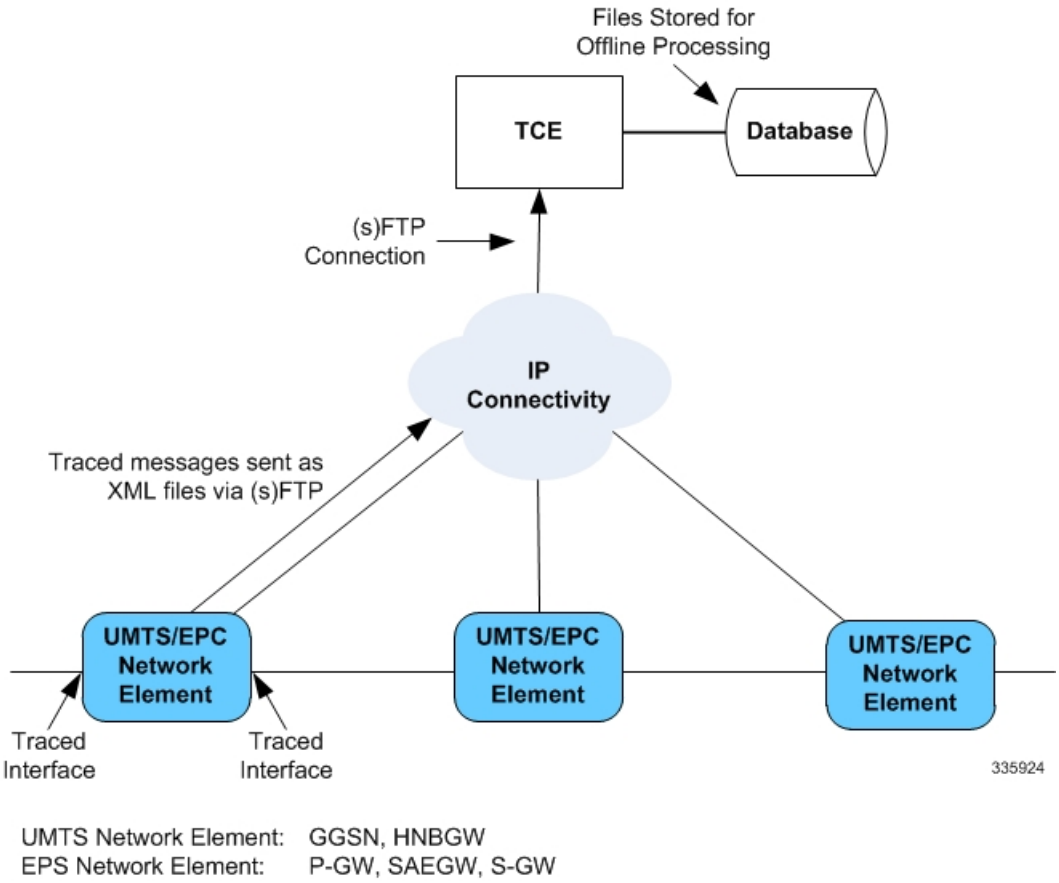
All monitored activity is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a File Transfer Protocol (FTP) or secure FTP (sFTP) connection.

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

Important Only the SFTP option supports for Session Trace function. FTP does not support for the Session Trace function.

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

Figure 21: Session Tracing Architecture



Session Trace Types

There are three types of session trace functions available.

- **Management Trace:** The operator sends an activation request via the CLI directly to the UMTS/EPC network element where the trace is to be initiated. The network element establishes the trace session and waits for a configured trigger event to start actively tracing. When management-initiated trace activations are executed at the network element, they are never propagated to other NEs whether or not it is involved in the actual recording of the call.
- **Random Trace**: Enables or disables the subscriber session trace functionality based on a the random trace on the UMTS/EPC network element. The trace control and configuration parameters are configured directly in the specified network element through the **random trace** CLI command. There is no propagation of trace parameters in random based trace activation. This NE shall not propagate the received data to any other NEs whether or not it is involved in the actual recording of the call. If enabled, the subscriber selection will be based on random logic all instances of session on the specified UMTS/EPC network element.
- **Signaling Trace**: With a signaling based activation, the trace session is indicated to the UMTS/EPC network element across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active). Signaling based activations are always propagated to neighboring NEs even if the current NE does not participate in the trace (either they not enabled by configuration or not present in the configured trace parameters).

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

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

Session Trace Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, an (S)FTP connection to the Trace Collection Entity (TCE) is established if one does not already exist. The NE will store up to 2 MB of XML data on its local disk to allow for the (S)FTP connection to be established and the files to be pushed to or pulled from the TCE.

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

Session Trace Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session

to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Data Collection

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

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

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

Data Forwarding

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

Note the following:

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

Supported Standards

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

- 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 Functionality

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

1. Enabling Session Tracing, on page 103
2. Configuring a Session Trace Template for the Management Trace Function, on page 104
3. Configuring a Management Session Trace, on page 108
4. Configuring a Signaling Session Trace, on page 109
5. Configuring a Random Trace, on page 110

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

Important Not all combinations of Session Trace configuration types are allowed on the SAEGW. For details on the supported session trace configuration types, refer to Supported SAEGW Session Trace Configurations, on page 114 in this document.

Enabling Session Tracing

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

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

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

```
config
   session trace network-element { all | ggsn | hnbgw | mme | pgw | saegw
 | sgw } [  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** : Enables Session Tracing functionality on the specified network element. To enable session tracing for all supported network elements, enter **all**.
- **file-type { a-type | b-type }**: Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. Note that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs. The default is **a-type**.
- **tce-mode** : Specifies that trace files are stored locally and must be pulled by the TCE (**none**) or trace files are pushed to the TCE (**push**). The default is **none**.
- **transport** : Specifies the method by which the trace files are pushed to the TCE (either **ftp** or **sftp**.) The default is **sftp**.

- **username**: Must be specified if the **tce-mode** is **push**.
- **password**: Must be specified if the **tce-mode** is **push**.
- **encrypted**: Specifies that the password used to push files to the TCE server will be encrypted.
- **password**: Specifies the password to use to push files to the TCE server. The user name can be from 1 to 31 alphanumeric characters.
- **collection-timer**: Specifies the amount of time, in seconds, to wait from initial activation/data collection before data is reported to TCE. The default is 10 seconds.
- **retry-timer**: Specifies the amount of time, in seconds, to wait before retrying a file transfer if the previous transfer failed. The default is 60 seconds.

Example:

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

Verifying that Session Tracing is Enabled

Use the following example to verify that session tracing functionality is enabled on the UMTS/EPC network element:

```
show session trace statistics
```

The output indicates for which NEs session tracing is enabled, and also indicates the configured trace type, where applicable. For example:

```
Network element status:
      MME:      Enabled      Cell-Trace: Disabled
      S-GW:    Enabled
SAEGW Enabled
            PGW:                    Trace-Type: None
            SGW:                    Trace-Type: None
```

Disabling Session Trace Functionality

Use the following example to disable session tracing functionality:

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

Configuring a Session Trace Template for the Management Trace Function

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

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

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

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

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

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

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

```
interface interface_name
end
```

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

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

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

GGSN

Available **ggsn** interfaces include:

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

HNBGW

Available **hnbgw** interfaces are:

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

MME

Available **mme** interfaces include:

- **all**: Specifies that all MME interfaces are to be traced.
- **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.

- **s13**: Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.
- **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

P-GW

Available **pgw** interfaces are:

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

SAEGW

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

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

- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

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

S-GW

The available **sgw** interfaces are:

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

Verifying the Session Trace Template Configuration

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

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

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

Disabling the Session Trace Template Configuration

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

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

Disabling the Session Trace Template Configuration per Network Element and Subscriber

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

```
no session trace subscriber network-element { ggsn | hnbgw | mme | pgw |
 saegw | sgw } template-name template_name { imsi id | imei id } trace-ref
 trace_ref_value collection-entity ip_address
```

Configuring a Management Session Trace

Session tracing functionality must be enabled before a management trace can be configured. Refer to Enabling Session Tracing, on page 103 for the procedure.

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

```
session trace subscriber network-element { ggsn | hnbgw | mme | pgw |
saegw | sgw } template-name template_name { imei id | imsi id } { all |
interface } } trace-ref id collection-entity ip_address
```

Notes:

- **template-name**: Specifies the name of the session trace template to use for this session trace. Session trace templates are configured in *Global Configuration Mode* using the **template-session-trace** command. Management traces executed in Exec mode will use the specified template.
- **imsi** *id*: Specifies the International Mobile Subscriber Identification Number for the subscriber.
- **imei** *id*: Specifies the International Mobile Equipment Identification number for the subscriber.
- **trace-ref**: Specifies the Trace Reference for this subscriber management trace. It must be composed of the Mobile Country Code (MCC) + the Mobile Network Code (MNC) + a 3 byte octet string Trace ID. Example: 31001212349.
- **collection-entity**: Specifies the IP address of the Trace Collection Entity (TCE) to which the trace file generated will be sent. The IP address must be in IPv4 format.

Example:

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

```
config
  session trace network-element saegw
  end
config
  template-session-trace network-element saegw template-name saegw_all
    func-pgw interface all
    func-sgw interface all
    end
session trace subscriber network-element saegw template-name saegw_all imsi
123456789012345 trace-ref 123456789012 collection-entity 209.165.200.225
```

Verifying the Management Trace Configuration

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

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

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

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

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

```
NE Type: SAEGW
            PGW:                    Trace-Type:                    M
            SGW:                    Trace-Type:                    M
......
Traced Interfaces:
PGW:
      <P-GW interfaces configured for the trace.>
SGW:
      <S-GW interfaces configured for the trace.>
```

Disabling the Management Trace Configuration

To disable the management trace configuration from Exec Mode:

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

Configuring a Signaling Session Trace

Session trace functionality must be enabled before a signaling session trace can be configured. Refer to Enabling Session Tracing, on page 103 for the procedure.

To configure a signaling session trace:

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

Notes:

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

Example:

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

session trace signaling network-element *saegw*

Verifying the Signaling Session Trace Configuration

To verify the signaling session trace configuration:

show session trace statistics

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

```
Network element status:
......
SAEGW Enabled
          PGW:                    Trace-Type: S
          SGW:                    Trace-Type: S
```

Disabling the Signaling Session Trace

To deactivate signaling trace on the SAEGW:

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

Configuring a Random Trace

Session trace functionality first must be enabled on the UMTS/EPC network element before a random trace can be configured. Refer to Enabling Session Tracing, on page 103 in this chapter for the procedure.

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

To configure a random session trace:

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

Notes:

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

GGSN

Available **ggsn** interfaces are:

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

- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

HNBGW

Available **hnbgw** interfaces are:

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

P-GW

Available P-GW interfaces are:

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

SAEGW

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

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

- **all**: Specifies that all **func-pgw** interfaces configured under an SAEGW are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.

- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.

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

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

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

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

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

Example:

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

```
session trace random 40 network-element saegw func-pgw interface s5 func-sgw
 interface all collection-entity 209.165.200.225
```

Verifying the Random Trace Configuration

To verify the random session trace configuration:

show session trace statistics

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

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

Disabling the Random Trace for a Specific Network Element

To disable random session tracing for a specific network element:

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

Monitoring the Session Trace Functionality

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

show session trace statistics

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

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

show session trace subscriber network-element trace-ref

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

show session trace trace-summary

This command provides the trace-ref value of all session traces, broken down 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 13: Supported Session Trace Configurations on the SAEGW

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	When M traces are enabled for Func-SGW, Func-PGW and cal type Collapsed botl S-GW control messages (gtpv2) a P-GW control messages shall be traced in 1 SAEGW trace file.
R	R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	S	Collapsed	Yes	Yes	1 SAEGW trace file generated	

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M+S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	When M+S trac enabled for Func-S-GW, Func-P-GW an type collapsed b -SGW control messages (gtpv P-GW control messages shall traced in 2 SAE trace files. One file due to Management an due to Signaling files have the sa contents.
M+R	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	R	Collapsed	No	No	None	Not a valid trac configuration
R	S	Collapsed	No	No	None	Not a valid trac configuration
M	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M	Collapsed	No	Yes	1 SAEGW trace file generated	
M	S	Collapsed	No	Yes	1 SAEGW trace file generated	
S	M	Collapsed	Yes	No	1 SAEGW trace file generated	
M+S	M	Collapsed	Yes	No	2 SAEGW trace files generated	P-GW Trace is generated
M	M+S	Collapsed	No	Yes	2 SAEGW trace files generated, but S-GW trace not generated	S-GW Trace is generated
M+S	S	Collapsed	Yes	Yes	2 SAEGW trace files generated	
S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M+R	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M+R	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M+R	Collapsed	No	Yes	1 SAEGW trace file generated	
M	n/a	Pure S	Yes	No	1 SAEGW trace file generated	Config for func-P-G is not applicable fo Pure S calls
S	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
M+S	n/a	Pure S	Yes	No	2 SAEGW trace files generated	
M+R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R+S	n/a	Pure S	No	No	None	Not a valid trace configuration.
n/a	M	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	S	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	M+S	Pure P	No	Yes	2 SAEGW trace file generated	
n/a	M+R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R+S	Pure P	No	Yes	None	Not a valid trace configuration

Session Trace File Example

This section provides an example of a signaling trace file.

Figure 22: Signaling Trace File Example (1 of 3)

```
<<<<OUTBOUND  10:04:53:997 Eventid:141005(3)
[MME-S11]GTPv2C Tx PDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x000004D3, 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/GPRS ATT/DET: 0
                        MO & MT SMS: 0
                        PDP CONTEXT: 0

                    GGSN:
                        MBMS CONTEXT: 0
                        PDP CONTEXT: 0

                    MME:
                        HANDOVERS: 1
                        BEARER ACT/MOD/DEL: 1
                        UE INIT PDN DISC: 1
                        INIT ATT/TAU/DET: 1
                        SERVICE REQUEST: 1
                        UE INIT PDN CON REQ: 1
```

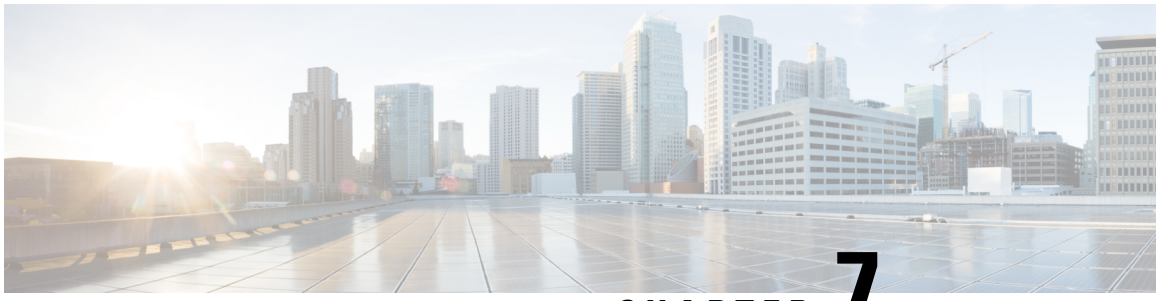
335925

Figure 23: 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
                                                                        335926
```

Figure 24: 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                          335927
```



CHAPTER 7

Backup and Recovery of Key KPI Statistics

This feature allows the backup of GGSN, P-GW, SAEGW, and/or S-GW counters for recovery of key KPI counter values after a session manager (SessMgr) restart.

This chapter includes the following information:

Feature Description

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

How It Works

A key set of counters used in KPI computation will be backed up for recovery if a SessMgr task restarts. The counters that will be backed up are determined by the KPIs typically used in several operator networks.

The backup of counters is enabled or disabled via configuration. The configuration specifies the product (GGSN, P-GW, SAEGW, and/or S-GW) for which counters will be backed up and also a time interval for the backup of the counters.

Architecture

When this feature is enabled (see *Configuring Backup Statistics Feature* below), the GGSN, P-GW, SAEGW, and/or S-GW only backs up the counters maintained at the SessMgr. The recovery function does not need to be configured or started as it occurs automatically as needed when the feature is enabled.

The counters are backed up to the AAAMgr that is paired with the SessMgr.

Checkpointing

Node-level statistics are checkpointed at AAAMgr. Once statistics are backed up for a specific product, all the associated services, such as eGTP-C and GTP-U statistics, are also checkpointed.

Recovery

When SessMgr restarts, recovery is performed by receiving all the stored statistics from the mapped AAAMgr and the recovered values are added to the backup counters maintained at per-service level. This will not impact session recovery time as the backed up counters are pushed to SessMgr only after session recovery is complete.

Since session recovery is complete, the session managers may start processing calls. In such cases, the counters will continue to be incremented. The recovered values of the corresponding counters will always be added to the existing counters. Gauge counters are checkpointed but not recovered.

Order of Statistics Collection

The upper limit of checkpoint messaging is a maximum of 1 MB. Before picking any node to checkpoint, available memory is checked. If memory is insufficient, the whole node is discarded.

Since there is 1 MB limit, nodes/statistics to checkpoint are prioritized as follows:

1. SAEGW statistics:
   - P-GW and S-GW service node-level statistics collected
2. P-GW service node configuration will store the following statistics:
   - P-GW, eGTP-C ingress, GTP-U ingress, per-interface (s2a, s2b, s5s8), and GGSN (if associated) statistics collected
   - SAEGW associated P-GW service statistics not collected
3. S-GW service node configuration will store the following statistics:
   - S-GW, eGTP-C ingress/egress, and GTP-U ingress/egress statistics collected
   - SAEGW associated S-GW service statistics not collected
4. GGSN statistics:
   - GGSN service statistics, if not associated with P-GW service, collected
5. Session disconnect reasons collected if GGSN/P-GW/SAEGW/S-GW is enabled

Error Handling

If adding new statistics is going to cause overflow of 1 MB buffer, that service and the corresponding node will not be included. Checkpointing of any further nodes will also be stopped. Error level log will be flagged if total memory requirement goes above 1 MB.

Limitations

- A backup interval must be specified and counters are backed up only at the specified interval. For example, if the backup interval is specified as 5 minutes, then counters are backed up every 5 minutes. Suppose backup happened at Nth minute and the configured backup interval is for every 5 minutes, then if a task crash happens at N+4 minutes, the GGSN, P-GW, SAEGW, and/or S-GW recovers only the values backed up at Nth minute and the data for the past 4 minutes is lost.
- Only statistics maintained at the SessMgr are backed up. Statistics at other managers are not backed up or recovered.
- The following statistics are not considered for backup:
  - APN-level statistics
  - eGTP-C APN-QCI statistics
  - DemuxMgr statistics
- The CLI command **clear statistics** will not trigger checkpoint to delete the node statistics on AAAMgr. New checkpoint after timer expiry will overwrite the statistics.
- Maximum of 1 MB of statistics will be stored on AAAMgr. Services after the maximum size limit are not backed up.
- Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.
- If SessMgr restarts and AAAMgr restarts before SessMgr recovers statistics from AAAMgr, then backed up statistics are lost.
- This feature is not applicable for ICSR.

Configuring Backup Statistics Feature

For the Backup and Recovery of Key KPI Statistics feature to work, it must be enabled by configuring the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

Configuration

The following CLI commands are used to manage the functionality for the backing up of the key KPI statistics feature.

Enabling

The following configures the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW and enables the Backup and Recovery of Key KPI Statistics feature.

```
configure
     statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

Setting the Backup Interval

The following command configures the number of minutes (0 to 60) between each backup of the statistics. When the backup interval is not specified, a default value of 5 minutes is used as the backup interval

```
configure
     statistics-backup-interval minutes
     exit
```

Important Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.

Disabling

The following configures the GGSN, P-GW, SAEGW, and/or S-GW to disable the backing up of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

```
configure
     no statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

Verifying the Backup Statistics Feature Configuration

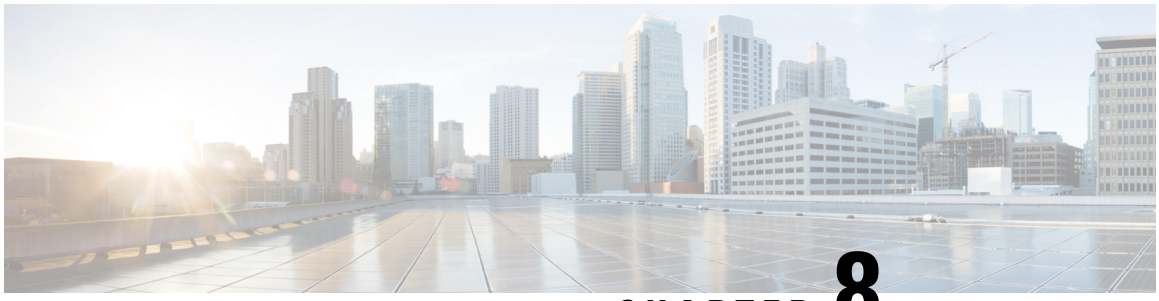
Use either the **show configuration** command or the **show configuration verbose** command to display the feature configuration.

If the feature was enabled in the configuration, two lines similar to the following will appear in the output of a **show configuration [verbose]** command:

```
statistics-backup  pgw
statistics-backup-interval 5
```

Notes:

- The interval displayed is 5 minutes. 5 is the default. If the **statistics-backup-interval** command is included in the configuration, then the 5 would be replaced by the configured interval number of minutes.
- If the command to disable the feature is entered, then no statistics-backup line is displayed in the output generated by a **show configuration [verbose]** command.



CHAPTER 8

Bulkstats for GTP-C Messages by ARP Value

This chapter describes StarOS support for the Bulkstats for GTP-C Messages by ARP Value feature on the P-GW, SAE-GW, and S-GW.

Feature Description

To comply with the "Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority" to support emergency calls over Voice over LTE (VoLTE), several Key Performance Indicators (KPIs) have been introduced with this feature. This feature is utilized to collect statistics for total number of GTP-C messages received for Enhanced Multimedia Priority Service (eMPS) session for specified interval (in minutes). The list of GTP-C messages are defined in accordance with the GIR document. As part of this feature:

- The S-GW will generate peg counts of the total number of received GTP-C messages containing an Allocation and Retention Priority (ARP), chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW level.
- The P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the specific P-GW level.
- The peg counts for GTP-C messages are broken down by message type similar to existing GTP-C message counters. The bulkstats are broken down by applicable S-GW and P-GW service and S5, S8, S11, and S4 interfaces.

Bulkstats are added for eMPS session/message.

Piggy-back Message

For piggy-back messages, if either of the messages have matching ARP or result into converting non-eMPS session to eMPS session, then both messages are counted as eMPS message and corresponding statistics for both messages are incremented.

If Modify Bearer Request is piggy-backed with Create Bearer Response on S11 interface of S-GW and Create Bearer Response result into converting non-eMPS session into eMPS session, then Modify Bearer Response statistics will not increment for this Modify Bearer Request.

Bulkstats Collection and Reset

Bulkstats are added under eGTP-C Schema and pgw-egtpc-s5s8 Schema. These eMPS bulkstats in eGTP-C Schema and pgw-egtpc-s5s8 Schema holds value only for a bulkstat interval, that is, value of these bulkstats shows number of eMPS messages exchanged during the bulkstat interval.

Limitations

This section identifies the known limitations of the feature:

- Peer level and APN level statistics are not collected.
- MPS statistics recovery is not supported.
- MPS statistics are not collected for CSReq, DDNReq, and change notification messages rejected by demux with ARP for eMPS sessions.
- MPS statistics are not collected for retried/re-transmitted messages.

Licensing

Important Bulkstats for GTP-C Messages by ARP Value feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Performance Indicator Changes

S-GW Ingress S4 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S4 interface of S-GW Ingress:

- **show egtpc statistics interface sgw-ingress interface-type s4**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s4**: Displays interface level GTP-C message statistics for S4 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s4**
  - **s4**: Interface type S4 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as

bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.

- **Create Session Request (Total RX)**: This counter will be incremented by S-GW when it receives Create session request message on S4 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create session response message on S4 interface containing an ARP value configured in MPS Profile.

S-GW Ingress S11 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S11 interface of S-GW Ingress:

- **show egtpc statistics interface sgw-ingress interface-type s11**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s11**: Displays interface level GTP-C message statistics for S11 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s11**
  - **s11**: Interface type S11 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total RX)**: This counter will be incremented by S-GW when it receives Create session request message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create session response message on S11 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Modify Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Modify Bearer response message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Create Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Create Bearer response message on S11 interface containing an ARP value configured in MPS Profile.
- **Downlink Data Notification (Total TX)**: This counter will be incremented by S-GW when it transmits Downlink Data Notification message on S11 interface containing an ARP value configured in MPS Profile.

- **Downlink Data Notification Ack (Total RX)**: This counter will be incremented by S-GW when it receives Downlink Data Notification Ack message on S11 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Update Bearer request message on S11 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Update Bearer response message on S11 interface containing an ARP value configured in MPS Profile.

S-GW Egress GTP-based S5/S8 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S5/S8 interface of S-GW Egress:

- **show egtpc statistics interface sgw-egress interface-type s5s8**
  - **interface-type**: Displays interface level GTP-C message statistics
  - **s5s8**: Displays interface level GTP-C message statistics for S5/S8 interface
- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type sgw-s5s8**
  - **sgw-s5s8**: Interface type S5/S8 for S-GW eGTP-C interface

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total TX)**: This counter will be incremented by S-GW when it transmits Create session request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total RX)**: This counter will be incremented by S-GW when it receives Create session response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total TX)**: This counter will be incremented by S-GW when it transmits Modify Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total RX)**: This counter will be incremented by S-GW when it receives Modify Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Create Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Create Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total RX)**: This counter will be incremented by S-GW when it receives Update Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.

- **Update Bearer Response (Total TX)**: This counter will be incremented by S-GW when it transmits Update Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.

P-GW Ingress GTP-based S5/S8 Interface

The following CLI commands are modified to display the eMPS session related GTP-C message statistics for S5/S8 interface of P-GW Ingress:

- **show egtpc statistics interface pgw-ingress interface-type s5s8**
- **show egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface-type s5s8**
  - **s5s8**: Interface type S5/S8 for P-GW eGTP-C interface.

The output of the above CLI commands displays the following new parameters:

- **Total eMPS Statistics**: Cumulative GTP-C message statistics for messages received/transmitted on eMPS Sessions.
- **Current interval eMPS Statistics**: GTP-C message statistics for messages received/transmitted on eMPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current MPS Statistics will be same as Total MPS Statistics.
- **Create Session Request (Total RX)**: This counter will be incremented by P-GW when it receives Create session request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Session Response (Total TX)**: This counter will be incremented by P-GW when it transmits Create session response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Request (Total RX)**: This counter will be incremented by P-GW when it receives Modify Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Modify Bearer Response (Total TX)**: This counter will be incremented by P-GW when it transmits Modify Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Request (Total TX)**: This counter will be incremented by P-GW when it receives Create Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Create Bearer Response (Total RX)**: This counter will be incremented by P-GW when it receives Create Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Request (Total TX)**: This counter will be incremented by P-GW when it transmits Update Bearer request message on S5/S8 interface containing an ARP value configured in MPS Profile.
- **Update Bearer Response (Total RX)**: This counter will be incremented by P-GW when it receives Update Bearer response message on S5/S8 interface containing an ARP value configured in MPS Profile.

clear egtpc

The following CLI commands are modified to clear eMPS statistics at interface level and eGTP-C service level:

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**: Clears interface statistics along with eMPS statistics for all eGTP-C services of P-GW Ingress type and S5/S8 interface.
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s4 | s11 | sgw-s5s8]**: Clears interface statistics along with eMPS statistics for all eGTP-C services of S-GW Ingress type and S4 or S11 interface/S-GW Egress type and S5/S8 interface.
- **clear egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface [s5s8]**: Clears interface statistics along with eMPS statistics for all P-GW eGTP-C services and S5/S8 interface.
- **clear egtpc statistics egtp-service** *sgw_egptc_service_name* **interface [s11 | s4 | sgw-s5s8]**: Clears interface statistics along with eMPS statistics for all S-GW eGTP-C services and S4 or S11 or S5/S8 interface.

P-GW eGTP-C S5/S8 Schema

The following new bulk statistics variables are added to the P-GW eGTP-C S5/S8 schema in support of this feature:

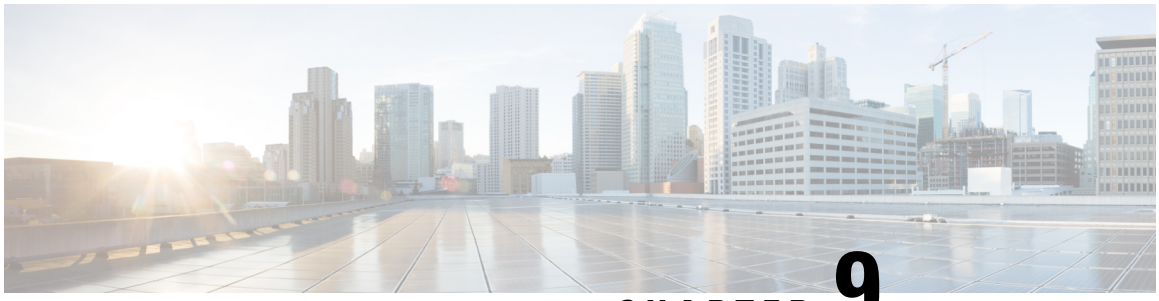
- tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-modbearerreq-emps – The total number of tunnel - modify bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-modbearerresp-emps – The total number of tunnel - modify bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-crebearerreq-emps – The total number of tunnel - create bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-crebearerresp-emps – The total number of tunnel - create bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-updbearerreq-emps – The total number of tunnel - update bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-updbearerresp-emps – The total number of tunnel - update bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.

eGTP-C Schema

The following new bulk statistics variables are added to the eGTP-C schema in support of this feature:

- s11-tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.

- s11-tun-recv-modbearerreq-emps – The total number of tunnel - modify bearer request - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-modbearerresp-emps – The total number of tunnel - modify bearer response - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-crebearerreq-emps – The total number of tunnel - create bearer request - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-crebearerresp-emps – The total number of tunnel - create bearer response - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-updbearerreq-emps – The total number of tunnel - update bearer request - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-updbearerresp-emps – The total number of tunnel - update bearer response - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-sent-ddnreq-emps – The total number of downlink data notification - messages sent by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s11-tun-recv-ddnack-emps – The total number of downlink data notificatino acknowledge - messages received by the system for eMPS subscriber on interface s11. This stat is for current bulkstat interval only.
- s4-tun-recv-cresessreq-emps – The total number of tunnel - create session request - messages received by the system for eMPS subscriber on interface s4. This stat is for current bulkstat interval only.
- s4-tun-sent-cresessresp-emps – The total number of tunnel - create session response - messages sent by the system for eMPS subscriber on interface s4. This stat is for current bulkstat interval only.
- tun-sent-cresessreq-emps – The total number of tunnel - create session request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-cresessresp-emps – The total number of tunnel - create session response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-modbearerreq-emps – The total number of tunnel - modify bearer request - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-modbearerresp-emps – The total number of tunnel - modify bearer response - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-crebearerreq-emps – The total number of tunnel - create bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-crebearerresp-emps – The total number of tunnel - create bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-recv-updbearerreq-emps – The total number of tunnel - update bearer request - messages received by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.
- tun-sent-updbearerresp-emps – The total number of tunnel - update bearer response - messages sent by the system for eMPS subscriber on interface s5s8. This stat is for current bulkstat interval only.



CHAPTER 9

Disable Cause Source Enhancement

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • SAEGW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *S-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

This feature introduces configuration changes that would allow you to configure the S-GW, including SAEGW instances, to disable the Cause Source bit functionality in Cause IE. If this configuration is enabled, S-GW and SAEGW always set the Cause Source Bit in Cause IE to zero.

Configuring cause-source

The **gtpc disable cause source** command has been introduced in support of this feature.

```
configure
    context context_name
       egtp-service egtp_service_name
          [ no | default ] gtpc disable cause-source
          end
```

Notes:

- **disable:** Disables functionality at egtpc level
- **cause-source:** Disables cause source Bit in Cause IE.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands and bulk statistics available to support of this feature.

Show Commands and/or Outputs

This section provides information regarding show commands and their outputs for the Disable Cause Source feature.

show egtp-service name egtp

This command displays the following output:

```
Service name                        : egtp_sgwi1….
Reject S2b HO(No UE Context)        : Disabled
GTPC Cause Source bit in Cause IE   : [Enabled/Disabled]
```

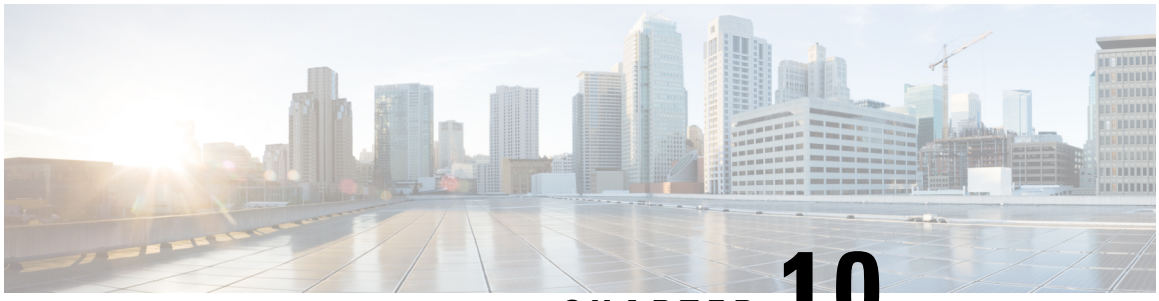
Troubleshooting

The following commands can be used for troubleshooting:

- The following commands can be used for checking current status of this feature:

  show egtp-service name *service_name*

- Monitor protocol CLI can be enabled to check GTPV2 protocol trace. In the protocol trace output cause source bit in Cause IE can be checked.



CHAPTER 10

Direct Tunnel for 4G (LTE) Networks

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

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

- Serving GPRS Support Node (S4-SGSN)
- Serving Gateway (S-GW)
- PDN Gateway (P-GW)

Important Direct Tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The following sections are included in this chapter:

Direct Tunnel for 4G Networks - Feature Description

The amount of user plane data will increase significantly during the next few years because of High Speed Packet Access (HSPA) and IP Multimedia Subsystem technologies. Direct tunneling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates.

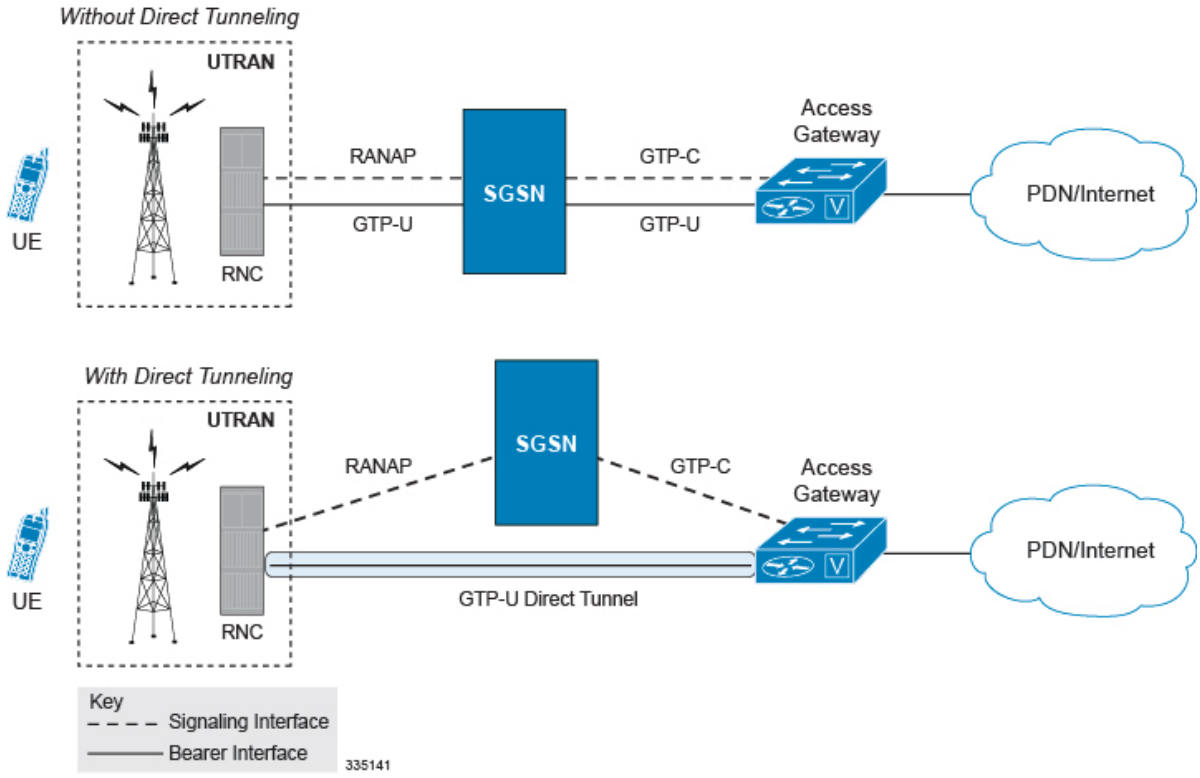
Direct Tunnel (DT) offers a solution that optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

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*.

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

Once a direct tunnel is established, the S4-SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

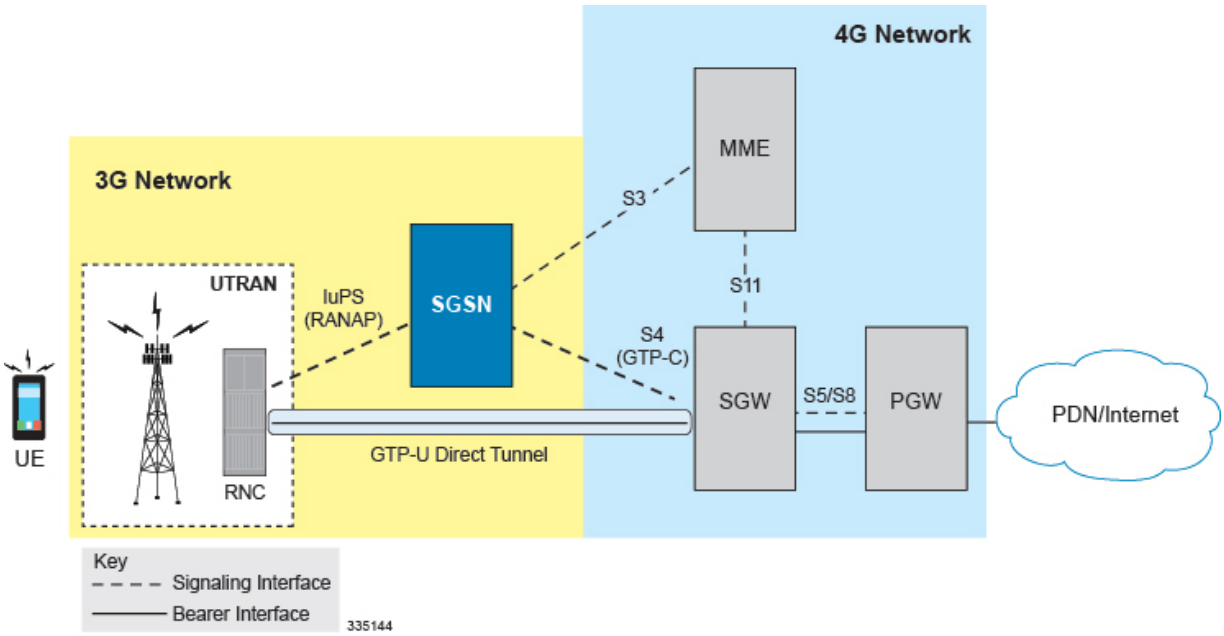
Figure 25: GTP-U Direct Tunneling



A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the S4-SGSN/S-GW to handle the user plane processing.

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

Figure 26: Direct Tunneling - LTE Network, S12 Interface



A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

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

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

Scenarios that vary at S4-SGSN when direct tunneling is enabled, as compared to DT on a 2G or 3G SGSN using the Gn interface, include:

- RAB Release
- Iu Release
- Error Indication from RNC

- Downlink Data Notification from S-GW
- Downlink Data Error Indication from S-GW
- MS Initiated PDP Modification
- P-GW Initiated PDP Modification while the UE is IDLE
- HLR/HSS Initiated PDP Modification
- Session Recovery with Direct Tunnel

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

How It Works

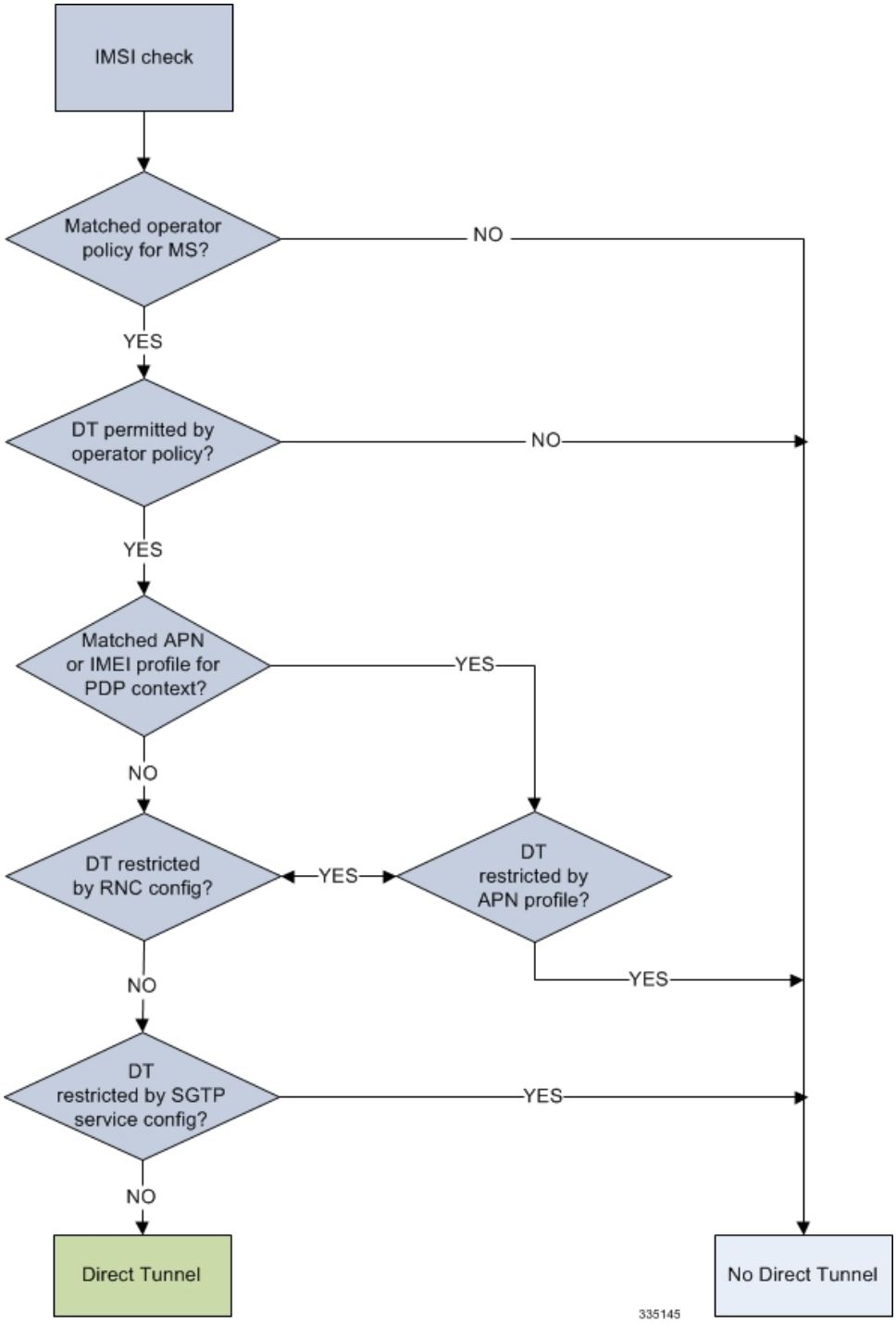
DT functionality enables direct user plane tunnel between RNC and SGW within the PS domain. With direct tunneling the S4-SGSN provides the RNC with the TEID and user plane address of the S-GW, and also provides the S-GW with the TEID and user plane address of the RNC.

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

DT Establishment Logic

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

Figure 27: Direct Tunneling - Establishment Logic



Establishment of Direct Tunnel

The S4-SGSN uses the S12 interface for DT.

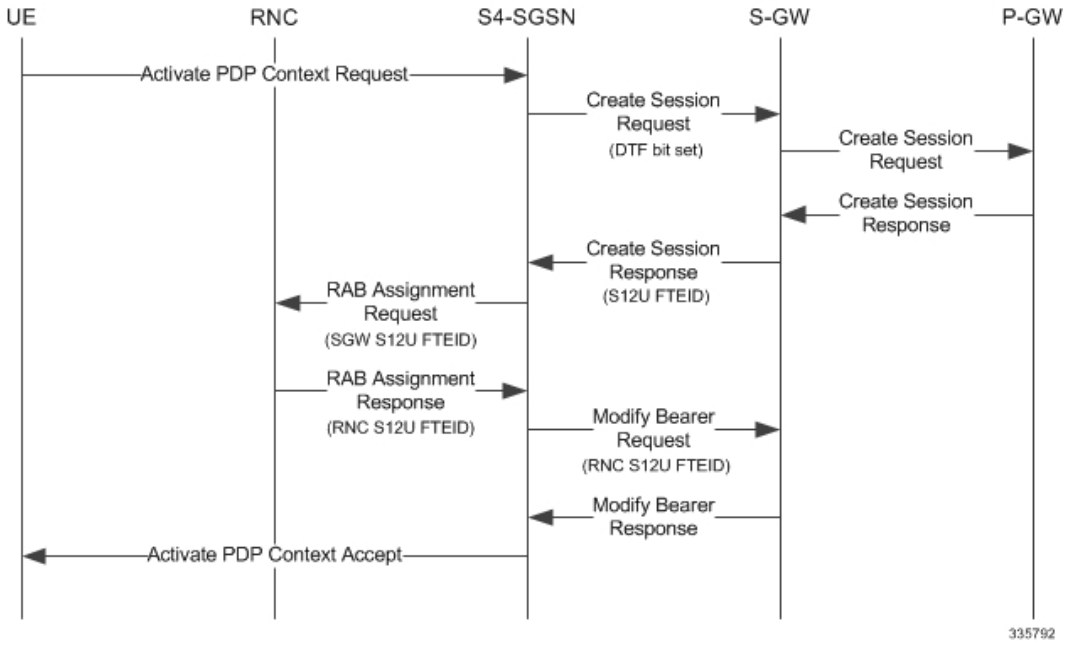
Direct Tunnel Activation for Primary PDP Context

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

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

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

Figure 28: Primary PDP Activation with Direct Tunnel

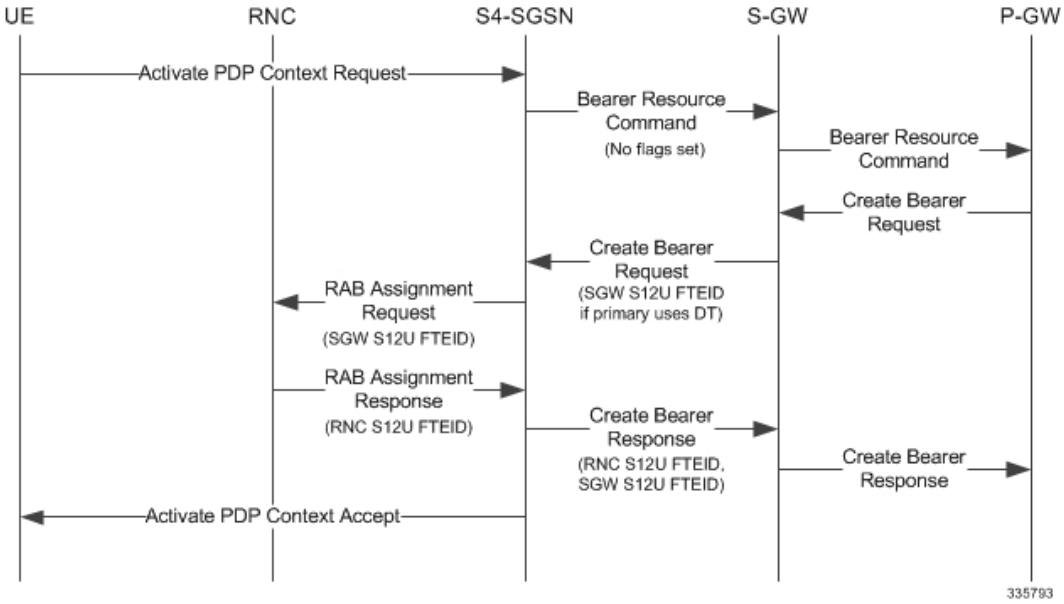


Direct Tunnel Activation for UE Initiated Secondary PDP Context

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

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

Figure 29: Secondary PDP Activation with Direct Tunnel



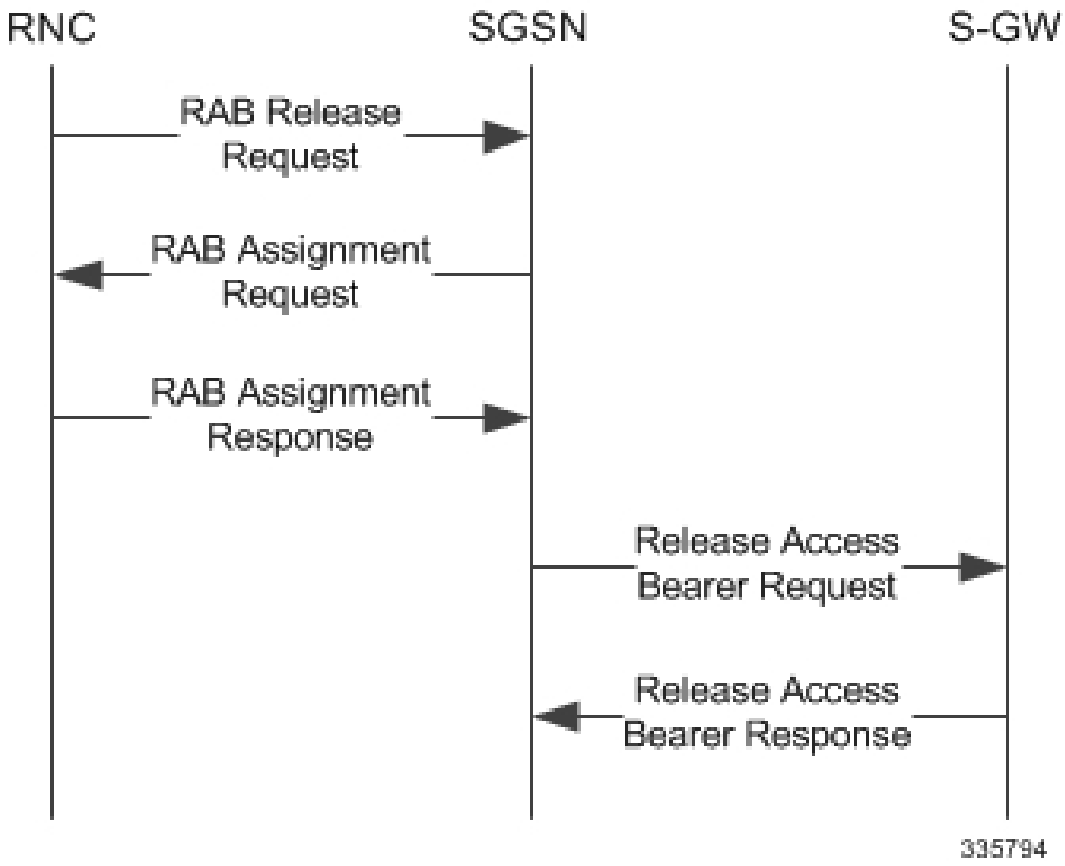
RAB Release with Direct Tunnel

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

Upon receiving the Release Access Bearer Request, the S-GW removes the S12 U RNC FTEID. If any downlink data appears, the S-GW sends a Downlink Data Notification because it does not have a user plane FTEID with which to forward data.

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

Figure 30: RAB Release Procedure with Direct Tunnel



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

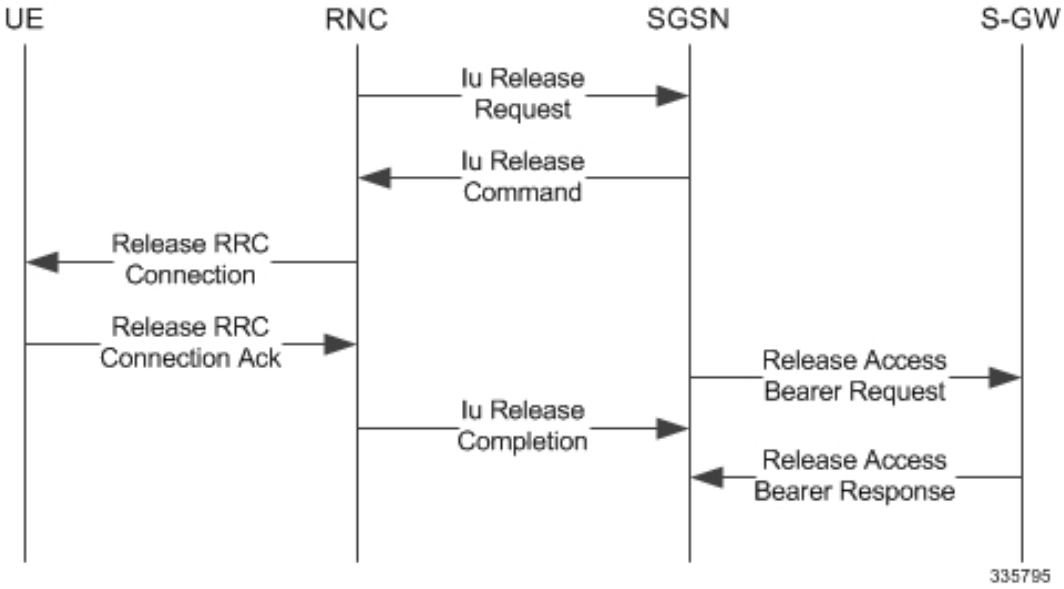
Iu Release with Direct Tunnel

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

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

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

Figure 31: Iu Release Procedure with Direct Tunnel

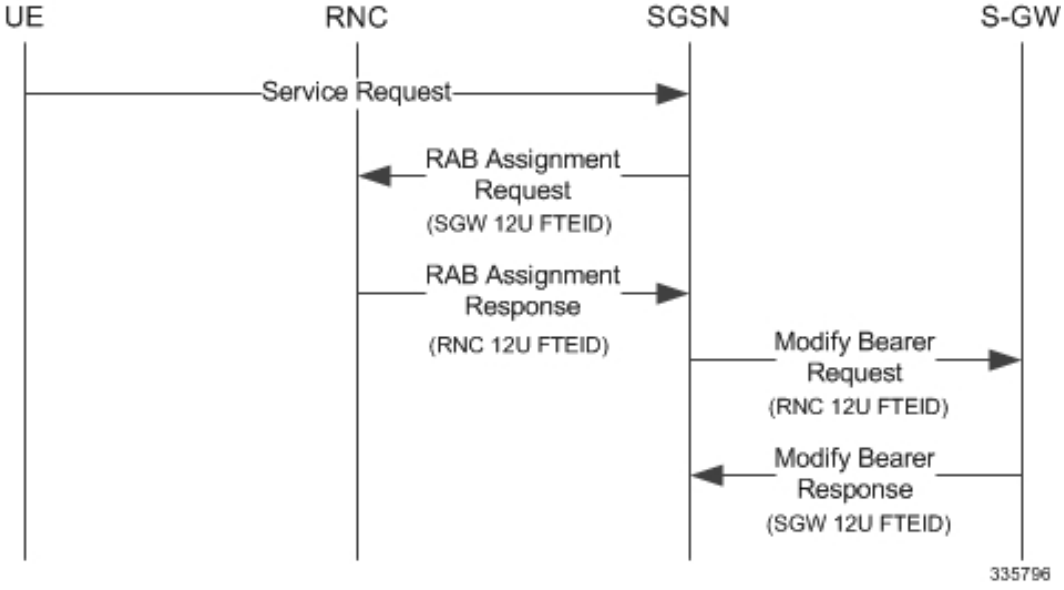


Service Request with Direct Tunnel

When a UE is Idle and wants to establish a data or signaling connection, it sends a Service Request for data. Alternatively a UE can also send a Service Request to the SGSN when it is paged by the SGSN.

Upon receiving a Service Request for data, the SGSN establishes RABs and sends a Modify Bearer Request to the S-GW with the 12U FTEID received from the RNC.

Figure 32: Service Request Procedure with Direct Tunnel



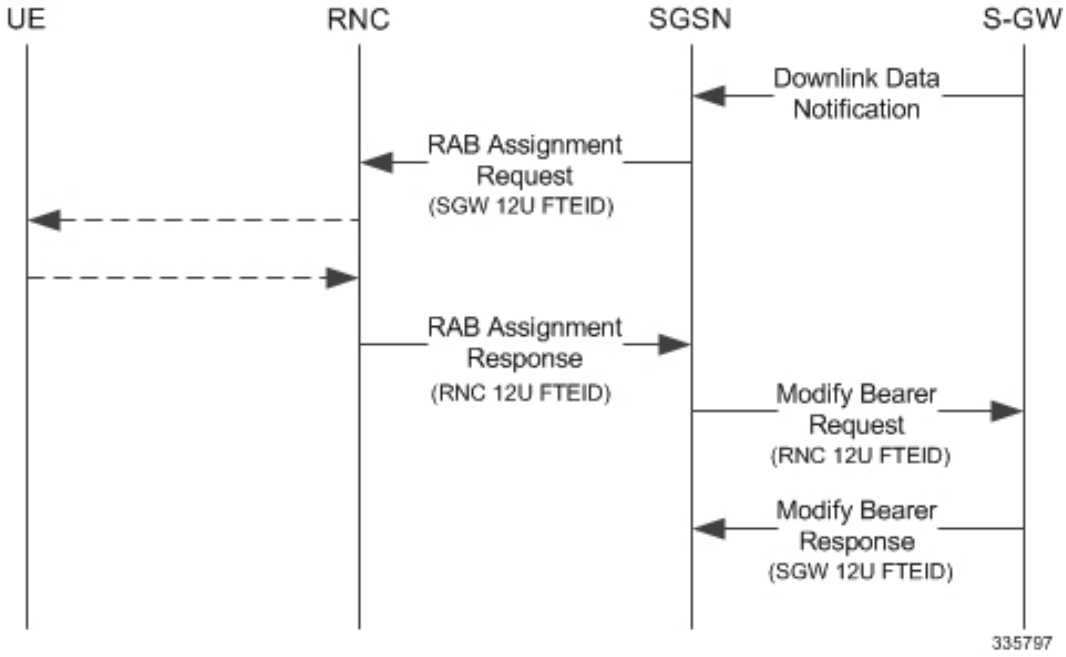
Downlink Data Notification with Direct Tunnel when UE in Connected State

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

If the S-GW receives any downlink GTPU data from the P-GW after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification message from the S-GW.

If the Downlink Data Notification is received from the S-GW, all of the missing RABs are established and a Modify Bearer Request is sent to the S-GW with the RNC S12U FTEID

Figure 33: Downlink Data Notification with Direct Tunnel

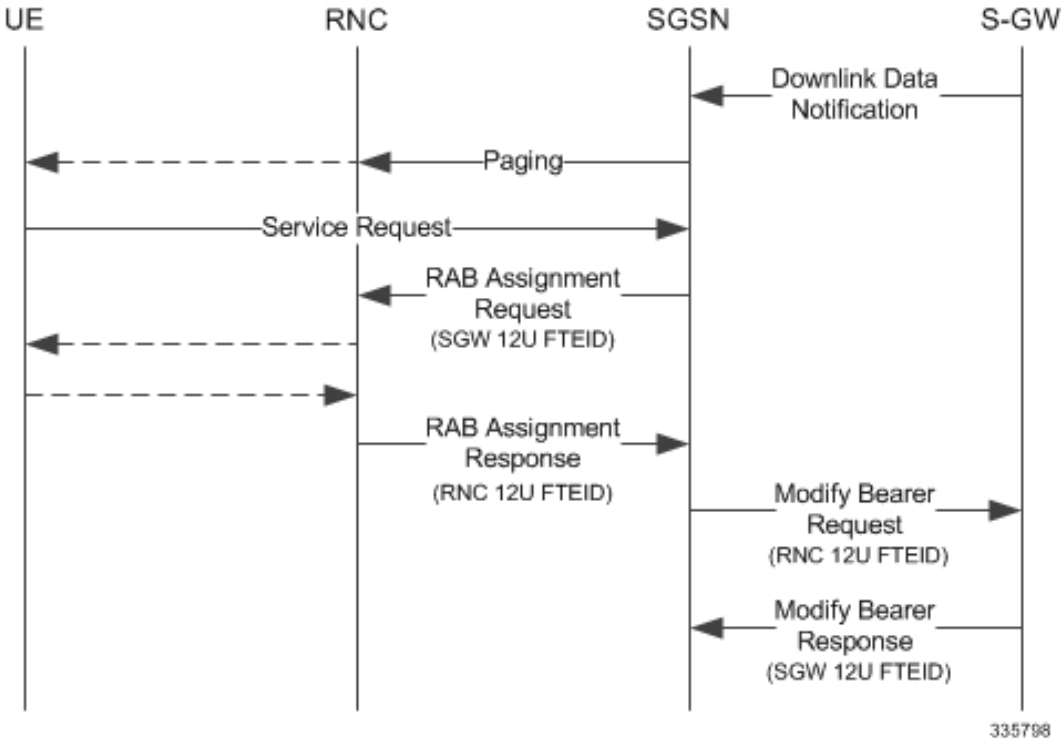


Downlink Data Notification with Direct Tunnel when UE in Idle State

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

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

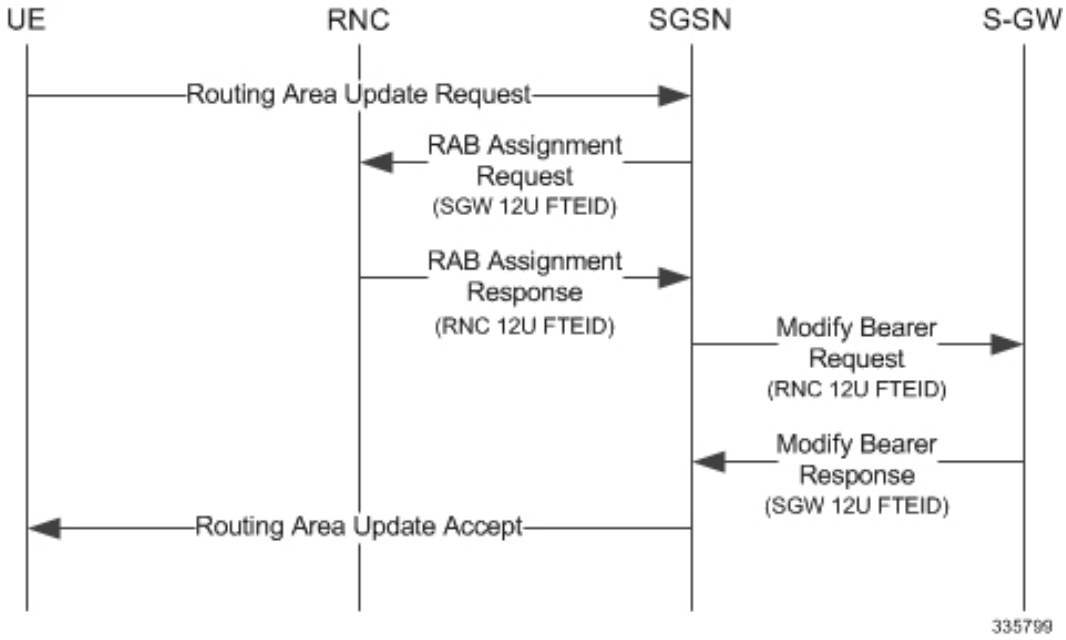
Figure 34: Downlink Data Notification when UE in Idle State



Intra SGSN Routing Area Update without SGW Change

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

Figure 35: Routing Area Update Procedure without SGW Change



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

Table 14: Routing Area Update without S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs that are be modified and the rest released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	Yes	Supported	No	No RAB establishmen with new RNC. MBR is sent with only PLMN change. Beare Context will not carry any TEID.
Intra RAU	Present	No RAB	Supported	Yes	Supported	No	Same as above.
Intra RAU	Not Present	No RAB	Not Supported	No	Supported	No	No RAB establishmen with new RNC. Modify Bearer Request to S-GW witl DTF set and no user FTEID.
Intra RAU	Present	No RAB	Not Supported	No	Supported	No	Same as above.
Intra RAU	Present	Some RABs	Not Supported	Do not care	Supported	No	Only the present RAB are established. MBR sent to S-GW with the bearers with RABs to be modified and the rest to be released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.Modify Bearer.
Intra RAU	Not Present	No RAB	Not Supported	Yes	Supported	No	No RAB establishmen with new RNC. MBR is sent with only PLMN change. SGSN will page / Service rec / establish RABs when a downlink data notification is received.
Intra RAU	Present	No RAB	Not Supported	Yes	Supported	No	Same as above.
Intra RAU: New RNC does not support Direct Tunnel. No SGW relocation							

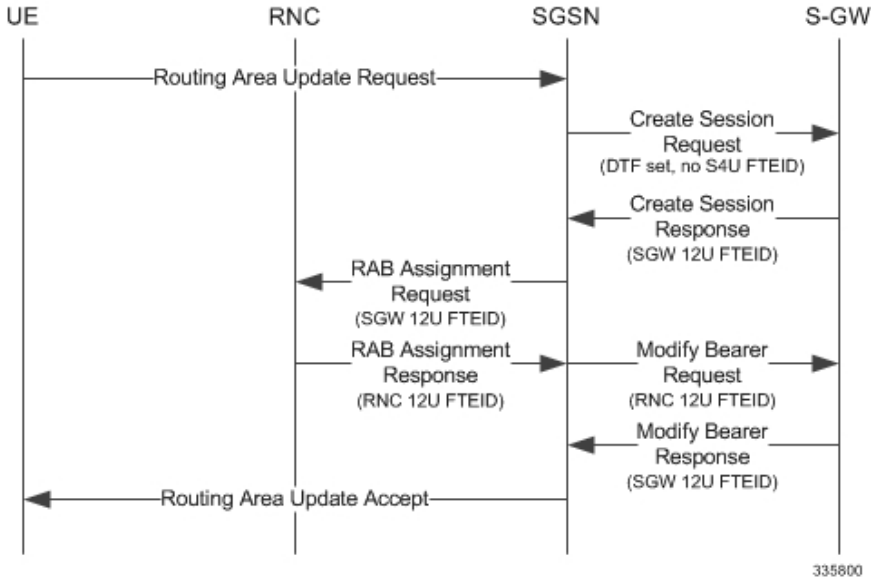
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	No	No RAB establishment with new RNC. SGSN sends Modify Bearer Request to S-GW with S4U TEID. If there is change in PLMN ID, then new PLMN ID will be carried.
Intra RAU	Present	No RAB	Supported	Do not care	No Supported	No	Same as above.
Intra RAU	Present	Some RABs	Supported	Do not care	Not supported	No	Only the present RABs are established. MBR sent to S-GW with all bearers having S4U TEID. If there is change in PLMN ID, the new PLMN ID will be carried.

Routing Area Update with S-GW Change

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

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

Figure 36: Routing Area Update Procedure with SGW Change



The table below includes detailed behaviors for a Routing Area Update with S-GW change.

Table 15: Routing Area Update with S-GW Change Behavior Table

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

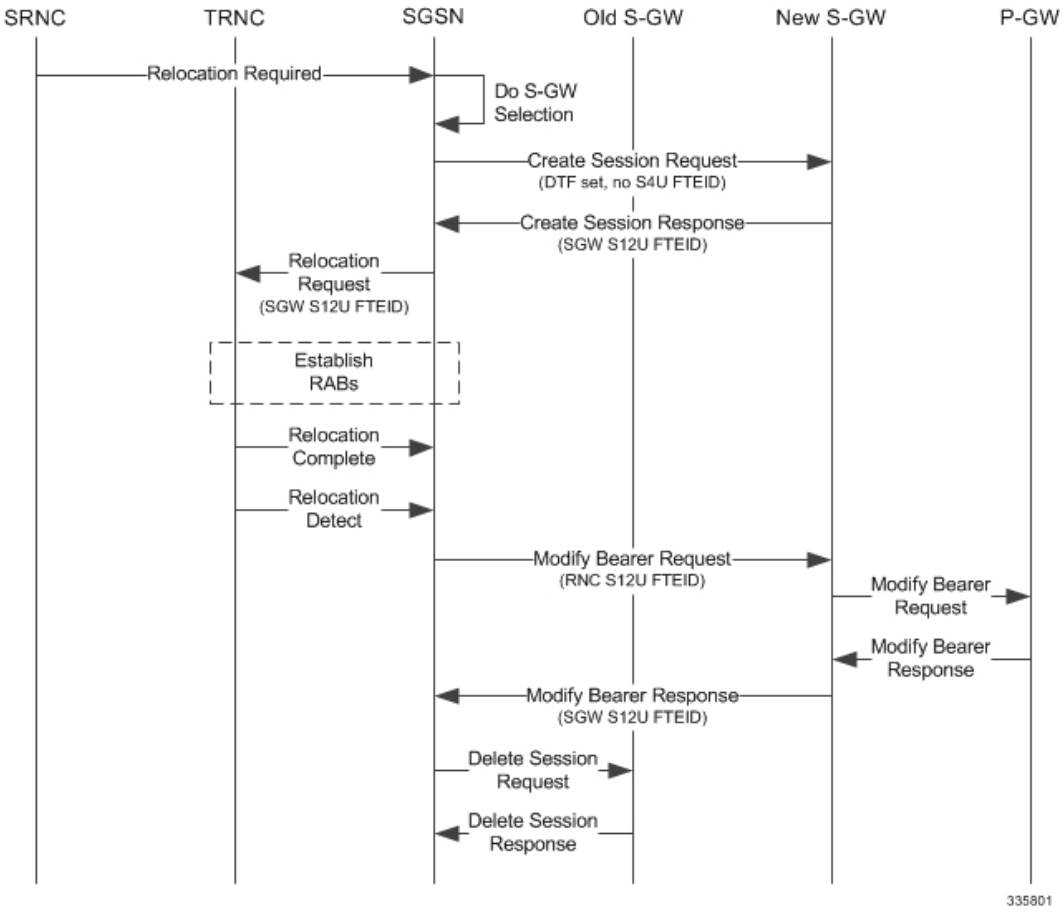
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID that SGSN stores as part of our DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN gets DDN and establishes RABs and sends MBR.
Intra RAU	present	No RAB	Not Supported	Do not care	Supported	Yes	Same as above.
Intra RAU	Present	Some RABs	Not SUpported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC and MBR will be initiated only with those RABs that are present and the rest as bearers to be removed.
Intra RAU: New RNC does not support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	Some rABs	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID. No deactivation of PDPs.

Intra SRNS with S-GW Change

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

The SGSN sends the RNC S12U FTEID to the new S-GW in a Modify Bearer Request.

Figure 37: Intra SRNS with S-GW Change

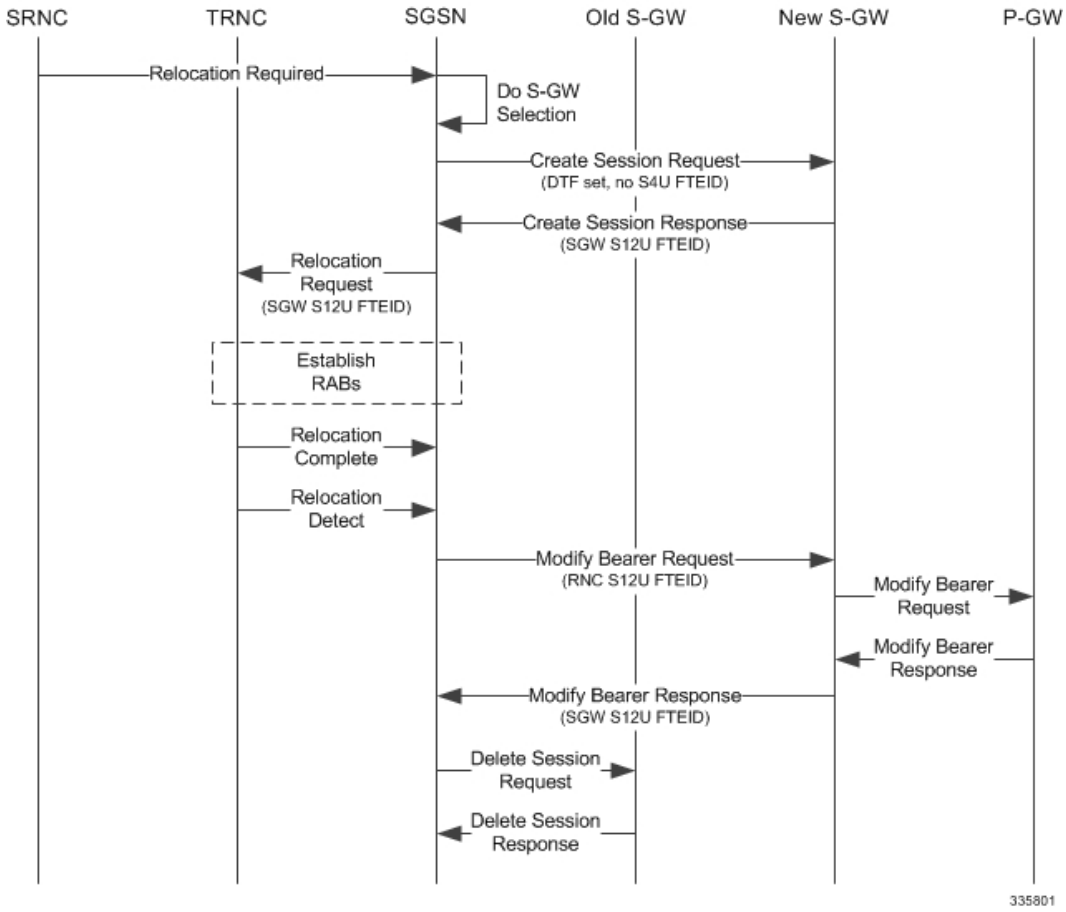


The table below includes detailed behaviors for intra SRNS scenarios.

Intra SRNS without S-GW Change

In Intra SRNS without S-GW change, a Relocation Request is sent with SGW S12U FTEID. The RNC S12U FTEID received is forwarded to the S-GW in a Modify Bearer Request.

Figure 38: Intra SRNS without S-GW Change



The table below includes detailed behaviors for intra SRNS scenarios.

Table 16: Intra SRNS Behaviors

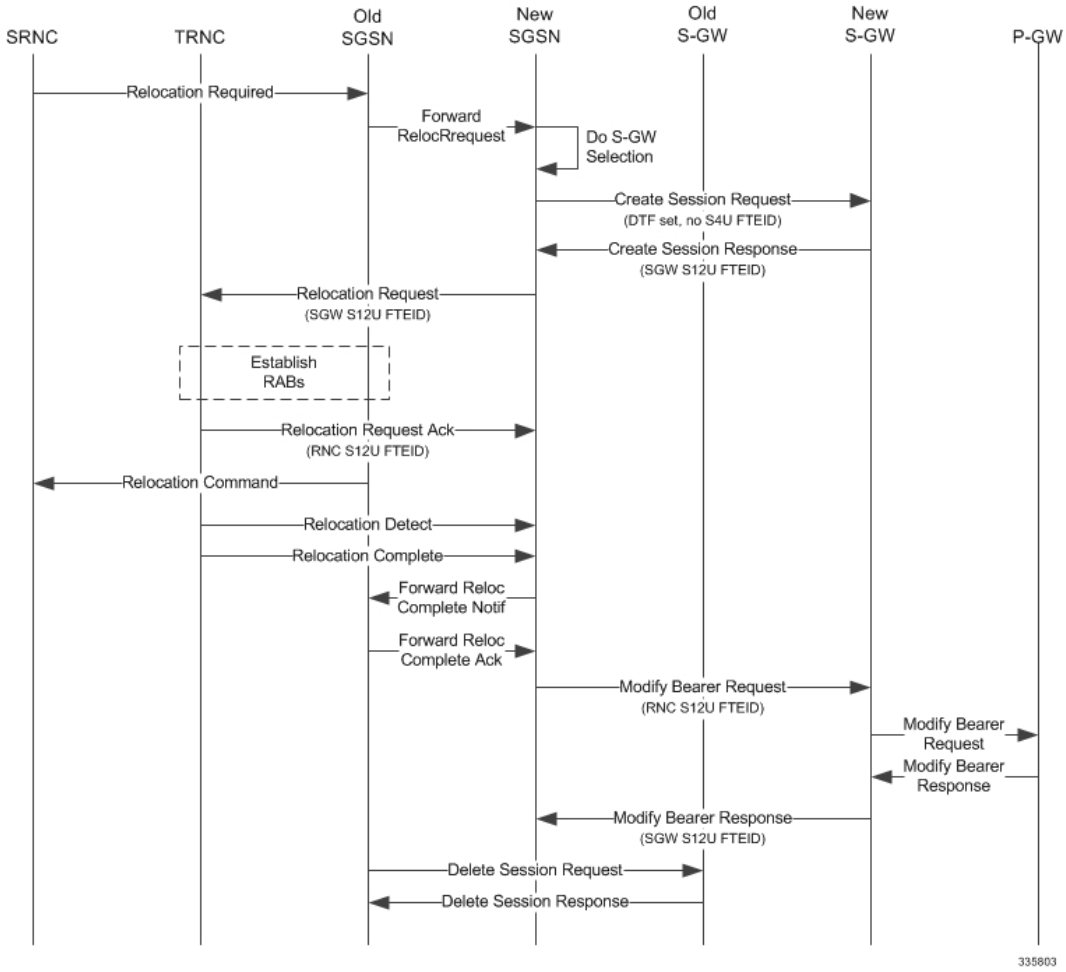
Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12 U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Supported	Not Supported	No	Relocation Request to Target RNC is sent with SGSN S4 U FTEID. Modify Bearer Request to S-GW is sent with SGSN S4 U FTEID
Not Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.

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

New SRNS with S-GW Change and Direct Data Transfer

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

Figure 39: New SRNS with S-GW Change with Data Transfer

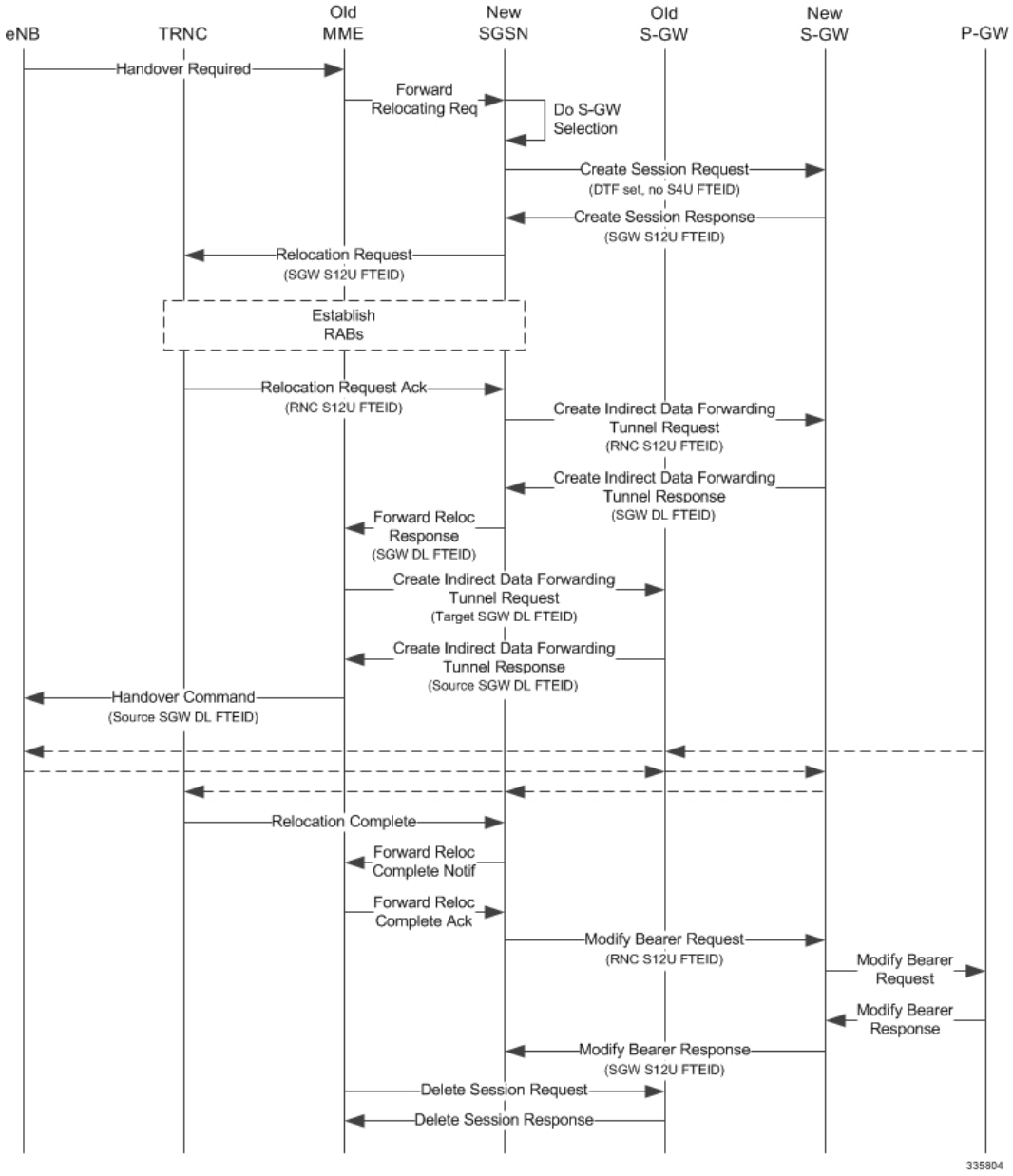


The table below includes detailed behaviors for New SRNS scenarios.

New SRNS with S-GW Change and Indirect Data Transfer

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

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



The table below includes detailed behaviors for New SRNS scenarios.

Table 17: New SRNS Behaviors

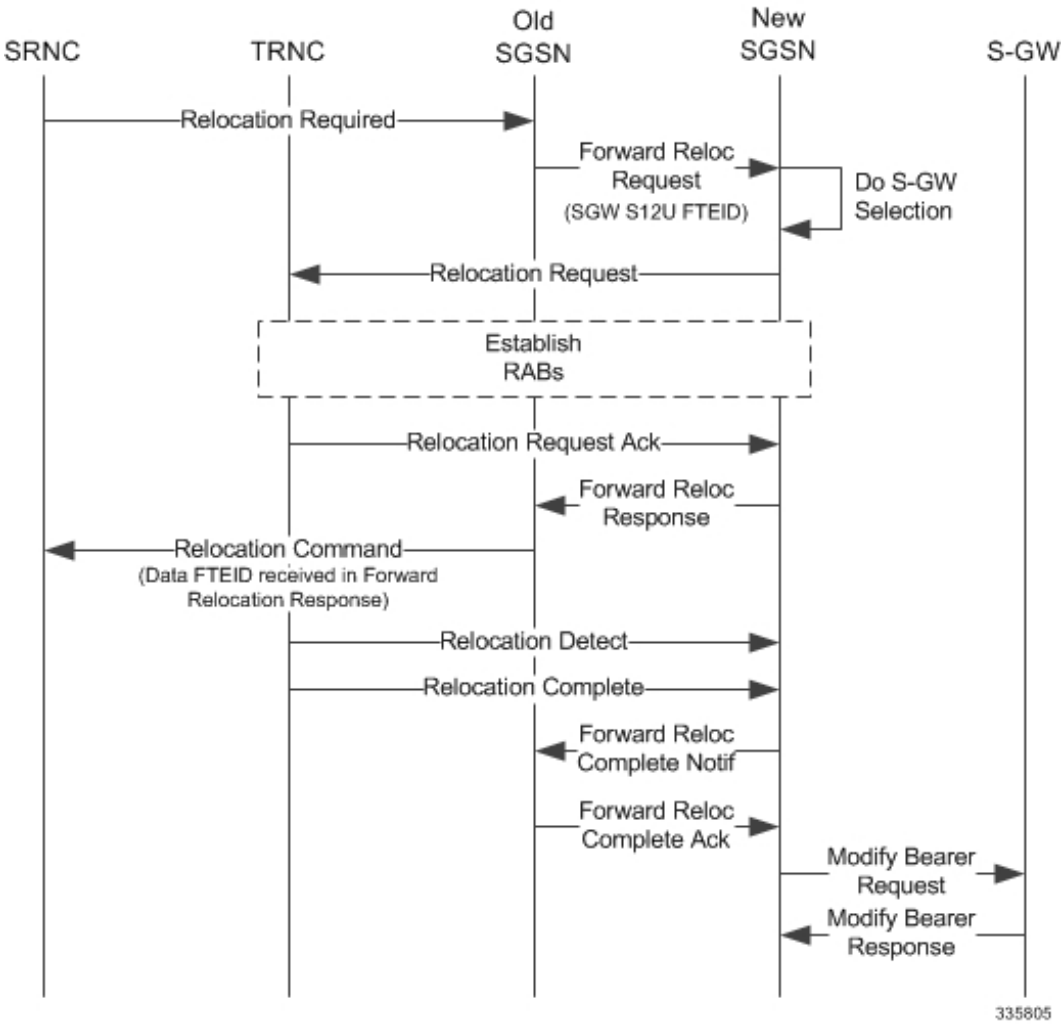
Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. SGSN includes RNC U FTEID in Forward Relocation Response. RNC U FTEID is also sen in Modify Bearer Request with DTF flag set.

Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	Yes	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. In Forward Relocation Response RNC U FTEID is included. And in Modify Bearer Request RNC U FTEID is sent and DTF flag is set.
Supported	No	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent is SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. Create Indirect Data Forwarding Tunnel Request is sent with RNC FTEID received in Relocation Request Acknowledge.In Forward Relocation Response SGW DL U FTEID received in Create IDFT response is sent. Modify Bearer Request is send with DTF set and RNC U FTEID.
Supported	Yes	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. In Forward Relocation Response RNC FTEID is sent and Modify Bearer Request is sent with DTF flag set and RNC U FTEID

Old SRNS with Direct Data Transfer

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

Figure 41: Old SRNS with Direct Data Transfer



The table below includes detailed behaviors for Old SRNS.

Old SRNS with Indirect Data Transfer

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

Figure 42: Old SRNS with Indirect Data Transfer 4

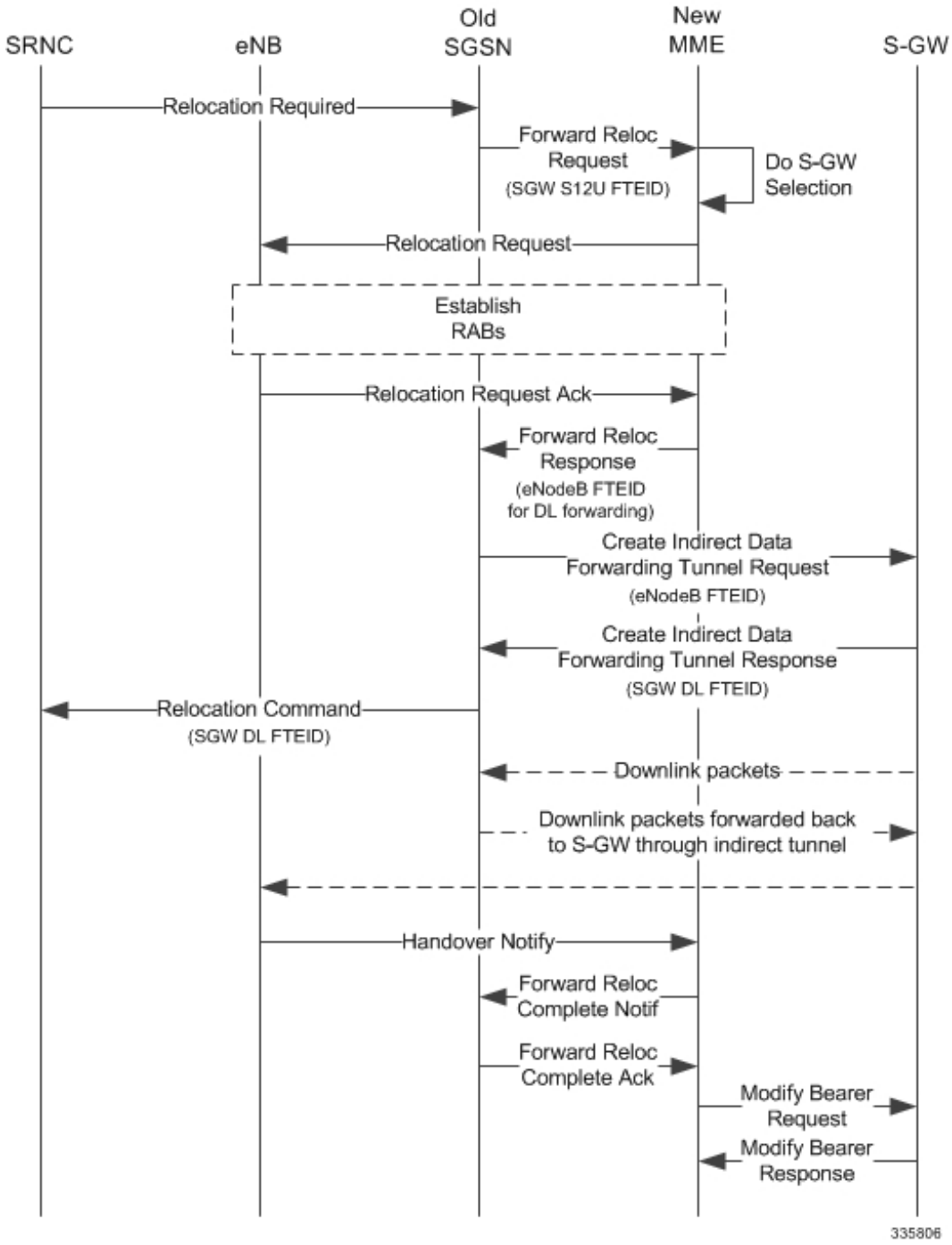


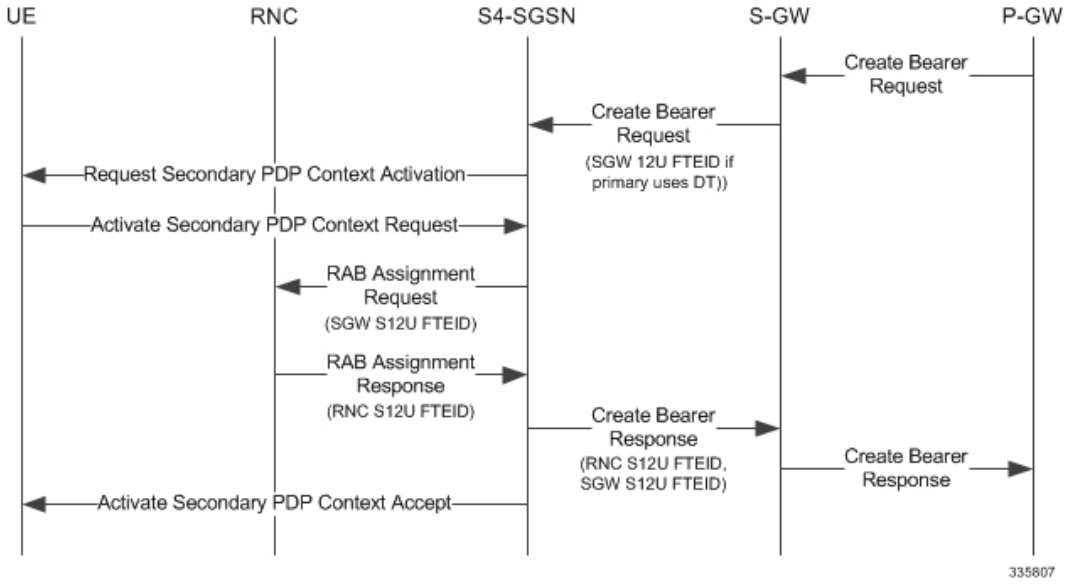
Table 18: Old SRNS Behaviors

Source RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Forward Relocation Request is send with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then a Create Indirect Data Forwarding Tunnel Request is sent with Use plane FTEID received in the Forward Relocation Response This will be the eNB user plane FTEID. The SGW DL forwarding user plane FTEID received in the Create Indirec Data Forwarding Tunnel Response is sent in the Relocatio Command.
Supported	Yes	No	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC user plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.
Supported	No	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then Create Indirect Data Forwarding Tunnel Request is sent with eNI User plane FTEID received in the Forward Relocation Response. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.
Supported	Yes	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC use plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.

Network Initiated Secondary PDP Context Activation

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

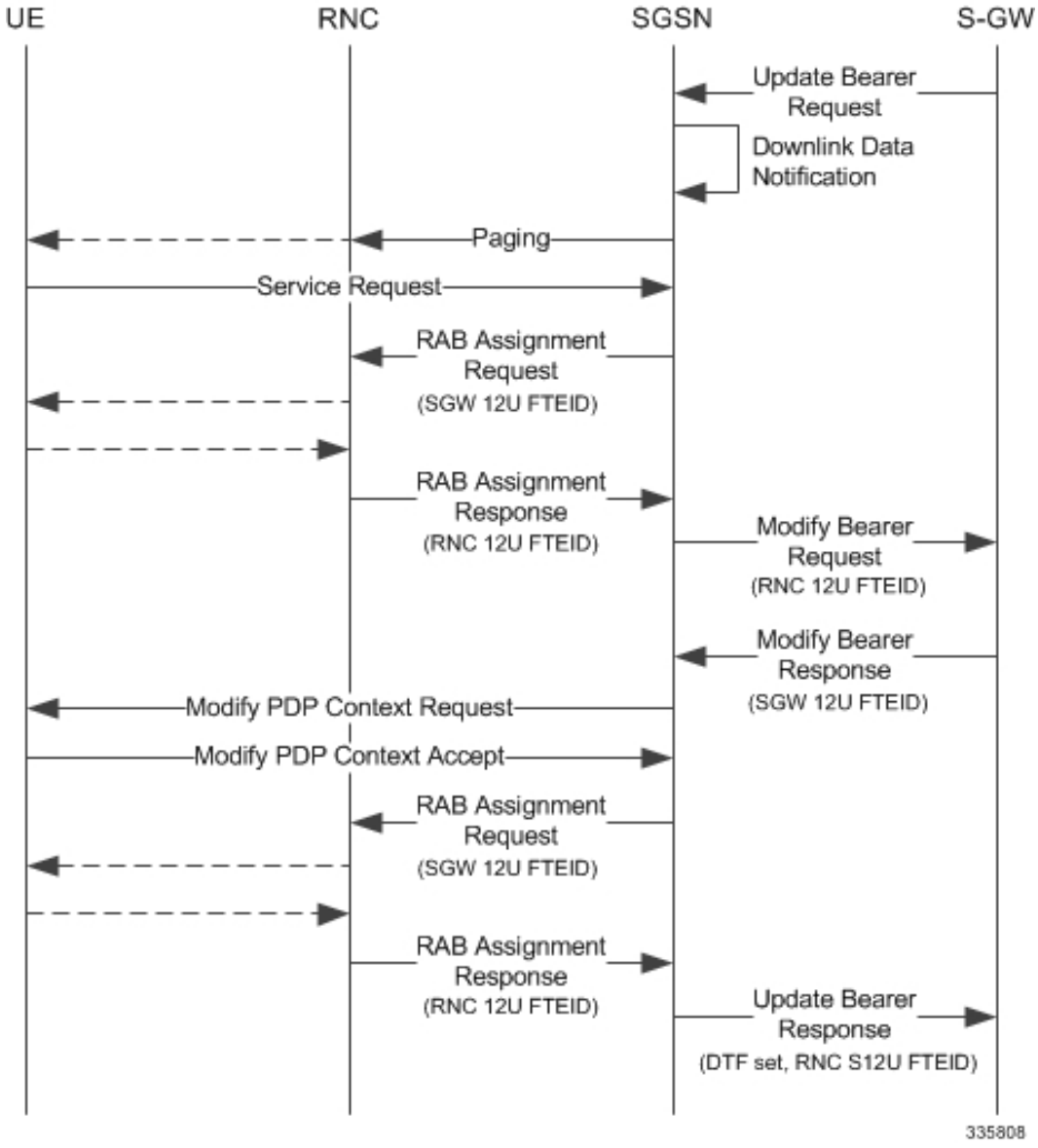
Figure 43: Network Initiated Secondary PDP Context Activation 5



PGW Init Modification when UE is Idle

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

Figure 44: PGW Init Modification when UE in Idle State



Limitations

During an intra RAU, intra SRNS or Service Request triggered by RAB establishment, if a few RABs fail the Modify Bearer Request the SGSN will mark those RABs as bearers to be removed. Under current specifications, it is not possible to send a Modify Bearer Request with a few bearers having S12U U-FTEIDs and a few bearers not having U-FTEIDs.

There is an ongoing CR at 3GPP to allow such Modify Bearer Requests and the S-GW should send DDN when it gets downlink data for the bearers that did not have U-FTEIDs. If this CR is approved, the SGSN will support (in a future release) sending a partial set of bearers with S12U FTEID and some bearers without any U-FTEID.

Standards Compliance

The Direct Tunnel complies with the following standards:

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

Configuring Support for Direct Tunnel

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

By default, direct tunnel support is

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

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the operator policy named ***default***. If direct tunnel is allowed in the ***default*** operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*. For more information about the purpose and uses of operator policies, refer to the section *Operator Policy*.

Configuring Direct Tunnel on an S4-SGSN

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

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

Enabling Setup of GTP-U Direct Tunnel

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

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

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.

- **to-ggsn** and **to-sgw** options are added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel to RNCs

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

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

```
config
  context ctxt_name
    iups-service service_name
      rnc id rnc_id
        default direct-tunnel
        end
```

Notes:

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

Restricting Direct Tunnels

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

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

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

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

Verifying the Call-Control Profile Configuration

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

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

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

```
Call Control Profile Name = ccprofile1
.
.
.
Re-Authentication
         : Disabled
Direct Tunnel
             : Not Restricted
GTPU Fast Path
            : Disabled
.
.
```

Verifying the RNC Configuration

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

show iups-service name *<service_name>*

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

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

Configuring S12 Direct Tunnel Support on the S-GW

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

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

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Use the following example to configure this feature.

```
configure
   context egress_context_name -noconfirm
      interface s12_interface_name
         ip address s12_ipv4_address_primary
         ip address s12_ipv4_address_secondary
         exit
      exit
   port ethernet slot_number/port_number
      no shutdown
      bind interface s12_interface_name egress_context_name
      exit
   context egress_context_name -noconfirm
      gtpu-service s12_gtpu_egress_service_name
         bind ipv4-address s12_interface_ip_address
         exit
      egtp-service s12_egtp_egress_service_name
         interface-type interface-sgw-egress
         validation-mode default
         associate gtpu-service s12_gtpu_egress_service_name
         gtpc bind address s12_interface_ip_address
         exit
      sgw-service sgw_service_name -noconfirm
         associate egress-proto gtp egress-context egress_context_name
egtp-service s12_egtp_egress_service_name
         end
```

Notes:

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

Monitoring and Troubleshooting Direct Tunnel

show subscribers sgsn-only

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

```
show subscribers sgsn-only full all
```

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

```
NSAPI: 05                                Context Type: Primary
Context initiated by: MS
Direct Tunnel : Established
```

show gmm-sm statistics sm-only

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

show gmm-sm statistics sm-only

```
Activate PDP Contexts:
 Total Actv PDP Ctx:
  3G-Actv Pdp Ctx:             1  2G-Avtv Pdp Ctx:       0
  Gn Interface:                1  Gn Interface:          0
  S4 Interface:                1  S4 Interface:          0
 Total Actv Pdp Ctx:
  with Direct Tunnel:          1
```

Direct Tunnel Bulk Statistics

Currently there are no bulk statistics available to monitor the number of PDP contexts with Direct Tunnel.

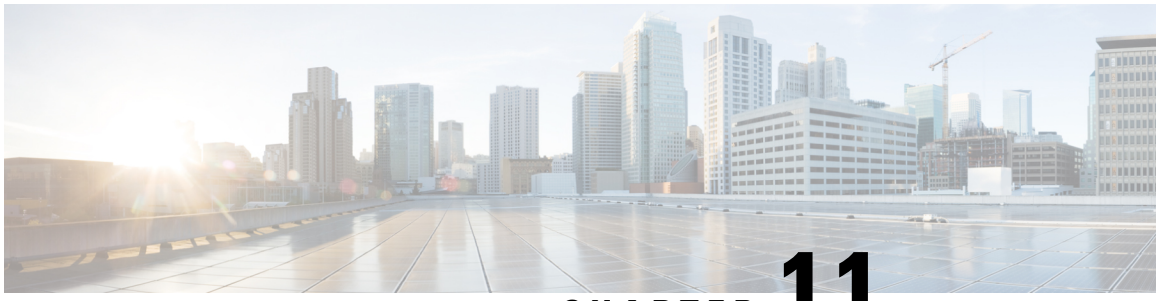
Bulk statistics under the EGTPC schema are applicable for both Direct Tunnel and Idle Mode Signalling Reduction (ISR) [3G and 2G]. The following statistics track the release access bearer request and response messages which are sent by the SGSN to the S-GW upon Iu or RAB release when either a direct tunnel or ISR is active:

- tun-sent-relaccbearreq
- tun-sent-retransrelaccbearreq
- tun-recv-relaccbearresp
- tun-recv-relaccbearrespDiscard
- tun-recv-relaccbearrespaccept
- tun-recv-relaccbearrespdenied

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

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

For complete descriptions of these variables, see the EGTPC Schema Statistics chapter in the *Statistics and Counters Reference*.



CHAPTER 11

Embed IMSI into Session Id

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW • S-GW
Applicable Platform(s)	• ASR 5500 • VPC - Di • VPC - Si
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

For troubleshooting and investigating network issues related to the Diameter interface, it is important to filter the subscriber or UE specific Diameter traffic. Any traffic associated with a particular IMSI can be easily filtered, even without knowing the Diameter session ID, if the IMSI information is embedded into the Diameter Session ID AVP. This feature allows the operator to filter the subscriber or UE specific Diameter traffic.

This feature introduces a new CLI command **session-id include imsi** under the **diameter endpoint configuration** mode to embed IMSI into Diameter session ID AVP over the Gx, Gy, and Gz (Rf) interface.

Important This feature is license controlled. Contact your Cisco account representative for information on how to obtain a license.

How It Works

A new CLI command **session-id include imsi** has been added under the **diameter endpoint configuration** mode to enable/disable inclusion of IMSI in Session-Id AVP for all Diameter sessions associated with that Diameter endpoint. Operators can enable only the required Diameter endpoints and control the inclusion of IMSI in the Session-ID AVP. IMSI information is included in the Diameter Session-ID AVP over the Gx, Gy, and Gz (Rf) interface, if the **session-id include imsi** is enabled on respective Diameter endpoints.

For emergency call with "only IMEI", IMSI information is not available for that emergency PDN. Hence, this IMSI information is not included in Diameter Session-ID at Gx, Gy, and Gz interface, when **session-id include imsi** is enabled. Configuring **session-id include imsi** impacts only new PDN connection and does not have any impact on existing PDN connection behavior (Gx, Gy, and Gz (Rf)) interface. For example, if the CLI command to include IMSI is enabled for the Gy Diameter endpoint after PDN creation. If a new dedicated bearer is created after this configuration change, then in this case Gy session established for a new dedicated bearer is not included IMSI in Gy Diameter session ID.

There is no impact of session manager recovery/ICSR on the session-ID AVP. Session-ID associated with Gx, Gy, and Gz (Rf) session is recovered transparently (which is irrespective of latest endpoint configuration). New sessions come up with session IDs as per the configuration on the newly active chassis.

Limitations

Following are the known limitations of this feature:

- Assuming IMSI information as sensitive information, operator must consider security aspects before enabling this CLI option.

- For an emergency call with "Only IMEI", IMSI information is not available for the emergency PDN, hence it is not included in the diameter Session-ID at Gx, Gy, and Gz (Rf) interface.
- During ICSR upgrade scenario, it is assumed that the new CLI option must be enabled only when the upgraded chassis is in stable state and there exists no chances of ICSR downgrade.
- If new CLI is enabled in the newer version of chassis, ICSR Downgrade is not recommended.
- As new CLI option is not available in old software versions, hence ICSR downgrade is not recommended. Performing ICSR downgrade should have the following impact on the diameter sessions, which have IMSI, included as part of Session-ID.
  - Gx and Gy: Existing diameter session (Gx, Gy) should be downgraded with old format of Session-Id. In that case, both P-GW and PCRF are out of sync leading to hanging session at P-GW or/and PCRF. Any communication from PCRF (RAR)/P-GW (CCR-U) can lead to stale session deletion.
  - Gz (Rf): However, Rf sessions should be recovered properly and any Rf signaling is sent out to Rf servers properly but responses cannot be processed as diamproxy cannot parse the new format session id which again puts Rf sessions into stale state until purged.

Configuring Diameter Accounting Interim Interval

The following CLI command has been added under the **diameter endpoint** configuration mode to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf). Configuration changes will be applicable only to new Sessions at Gx, Gy and Rf. Configuration changes will not have any impact on existing sessions behavior at Gx, Gy, and Rf. For Gy, multiple Diameter sessions can be initiated per subscriber and the session ID format setting will bind to the subscriber. The setting will be taken to effect when the first Diameter session is established and following Gy sub sessions will keep using the session ID format used in first session.

```
configure
    context context_name
       diameter endpoint endpoint_name
           [no] session-id include imsi
           end
```

Notes:

- **session-id:** Describes Diameter Session-ID format
- **include:** Includes configured information in Diameter Session-ID
- **imsi:** Includes International Mobile Subscriber Identification (IMSI) in Diameter Session-ID
- **no:** Disables this feature, that is, IMSI is not included in the Diameter Session-ID, which is the default behavior.
- By default, CLI is disabled, hence IMSI will not be populated in Diameter Session-ID.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the feature.

show configuration

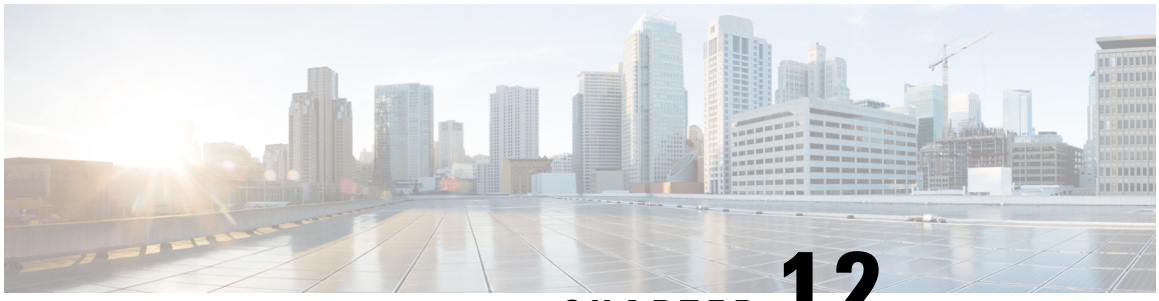
The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi

show configuration [verbose]

The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi



CHAPTER 12

Expanded Prioritization for VoLTE/Emergency Calls

This chapter describes the StarOS support for the Expanded Prioritization for VoLTE/Emergency Calls feature on the P-GW, SAE-GW, and S-GW.

Feature Description

The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

The DSCP marking of control message from P-GW and S-GW was based on associated egtpc-service configuration.

For control message belonging to eMPS session or containing Allocation and Retention Priority (ARP) associated with eMPS profile, the DSCP marking is based on eMPS profile configured DSCP value.

As part of this enhancement, support is also added for marking of certain GTP-C message at the P-GW and S-GW for priority treatment as defined in the Government Industry Requirements (GIR) NS/EP NGN.

Relationships to Other Features

Bulkstats for GTP-C Messages by ARP Value: The S-GW/P-GW will generate peg counts of the total number of received GTP-C messages containing an ARP, chosen from the set of values allocated for NS/EP NGN-PS use, for a specified interval (in minutes). This peg count is administered at the S-GW/P-GW level.

To prevent throttling of GTP-C messages corresponding to eMPS PDNs or messages containing ARP from set of configured ARP(PL) reserved for NS/EP NGN priority service, following configuration are to be considered:

1. **Load Overload control**

   In overload control profile, the set of ARPs reserved for NS/EP NGN-PS use for eMPS services should also be defined under **throttling-behavior exclude** and **self-protection-behavior exclude** CLI commands. This will ensure that incoming GTP-C messages for eMPS PDN or containing ARP from set of reserved ARP for eMPS use are not throttled. Example of configuring Load Overload configuration:

   ```
   configure
     gtpc-overload-control-profile profile_name
       throttling-behavior { earp { 1...15 } * } { exclude }
       self-protection-behavior { earp { 1...15 } * }  { exclude }
       end
   ```

2. **For Prioritized handling of calls under Congestion condition**

   ARP reserved under NS/EP NGN-PS for eMPS services is recommended to be configured under following congestion control CLI command. This will ensure that new call requests are not throttled during congestion condition defined by the **congestion-control** CLI command at context level:

   ```
   configure
     context context_name
       egtp-service service_name
         gtpc allow-on-congestion arp arp_value
         end
   ```

3. **GTP-C RLF Throttling**

   - If GTP-C RLF Throttling feature is enabled, then **gtpc overload-protection egress throttling-override-policy** CLI command should be configured with ARP(PL), reserved for NS/EP NGN-PS use, for eMPS services to bypass RLF throttling.
   - If GTP-C RLF Throttling for incoming messages is configured using **gtpc overload-protection ingress msg-rate** *message_rate* CLI command, then eMPS related messages can get throttled. Currently, there is no bypass policy for incoming RLF throttling.

Important Any existing features which works on ARP (PL) configurations will continue to work as before irrespective of whether ARP values configured are same as reserved under NS/EP NGN-PS for eMPS services. If existing features need to work with eMPS requirements, then same ARP (PL) values should be configured as reserved NS/EP NGN-PS for eMPS services.

Licensing

The DSCP marking capability requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

GIR Document References

The following table describes the requirements of this feature as per the GIR document.

Requirement No.	Description
R-127	[202] The S-GW shall transmit with priority a GTP-C “Downlink Data Notification” message or a GTP-C “Create Bearer Request” message or a GTP-C “Update Bearer Request” message, any of which contains an ARP chosen from the set allocated by the Service Provider for use by NS/EP NGN-PS.
R-130	[204] The S-GW shall mark for priority treatment the S11 “Create Session Response” message from the S-GW to the MME which contains request to establish a bearer or bearers with an ARP corresponding to an NS/EP NGN-PS call/session.
R-132	[205] The S-GW shall mark for priority treatment the S11 “Create Bearer Request” and S11 “Update Bearer Request” messages from the SGW to the MME which contains an indication that a UE currently has an established/updated bearer or bearers for NS/EP NGN-PS service.
R-134	[206] In the case where the S5/S8 Interface is GTP-based, the S-GW shall mark for priority treatment the S5/S8 “Create Session Request” message from the S-GW to the PDN-GW which contains an indication that a UE will establish a bearer or bearers for NS/EP NGN-PS.
R-137	[207] In the case where the S5/S8 Interface is GTP-based, the S-GW shall mark for priority treatment the S5/S8 “Create Bearer Response” and “Update Bearer Response” messages from the S-GW to the PDN-GW which contain an indication that a UE currently has established / updated a bearer or bearers for NS/EP NGN-PS.
R-143	[213] In the case where the S5/S8 Interface is GTP-based, the PDN-GW shall mark for priority treatment the S5/S8 “Create Session Response” message from the PDN-GW to the S-GW which contains a request to establish a bearer or bearers with an ARP corresponding to an NS/EP NGN-PS call/session.
R-146	[216] In the case where the S5/S8 Interface is GTP- based, the PDN-GW shall mark for priority treatment the S5/S8 “Create Bearer Request” and “Update Bearer Request” messages from the PDN-GW to the S-GW which contain an indication that a UE currently has an established/updated bearer or bearers for NS/EP NGN-PS.

Configuring Expanded Prioritization for VoLTE/Emergency Calls

The following section provides the configuration commands to enable the feature.

Configuring eMPS Profile and its Associated Attributes

At Configuration Mode level, CLI command option is introduced to define an eMPS profile and its associated attributes like:

- **eARP configuration**: This configuration is used for marking a bearer/PDN as an eMPS.
- **DSCP configuration**: This configuration is used at S-GW/P-GW to mark various outgoing GTP-C messages associated with an eMPS PDN with configured DSCP marking.

```
configure
   [ no ] emps-profile emps_profile_name -noconfirm
   [ no ] earp { [ 1...15 ] { [ 1...15 ] { [ 1...15 ] } } }
   [ no ] dscp-marking dscp_value
   end
```

Notes:

- **emps-profile** *emps_profile_name*: Configures eMPS profile for defining attributes of an eMPS session. The *emps_profile_name* is a string of size from 1 to 63.
- **earp**: Configures a maximum of 3 eARP priority level (PL) values so that sessions with configured eARP priority values can be marked as eMPS sessions.
- **-noconfirm**: Creates a new eMPS profile without prompting for confirmation.
- **dscp-marking** *dscp_value*: Specifies the DSCP value to be applied to eMPS sessions. The *dscp_value* is a hexadecimal number between 0x0 and 0x3F.
- Maximum of 3 eARP values can be configured under an eMPS profile. The above CLI syntax provides flexibility to configure one or more (max 3) eARP values in a single command. For example:

  earp 1 2 3

  -Or-

  earp 4

- The latest set of eARP values configured will overwrite the previous configuration. For example: Invoking below two commands in sequence will configure only eARP value 4.

  earp 1 2 3

  earp 4

- eMPS profile name should be unique and is treated case insensitive across context.
- The **no earp** command can be used to disable all configured eARP values. However, this will not delete the corresponding eMPS profile. The **no emps-profile** *emps_profile_name* CLI command will delete the profile.

- Warning message: When **no** of a non-existent eMPS profile is executed, a warning message is displayed. For example:

```
no emps-profile xyz
eMPS Profile : xyz does not exist
```

  There will be no warning message if **no** of an un-configured eARP is executed.

- There will be a warning and confirmation message when existing profile is deleted:

```
This operation will result in deletion of this eMPS Profile.
Are you sure? [Yes|No]:
```

- Maximum of 64 different eMPS profiles can be configured.

Associating an eMPS Profile with P-GW Service

The commands illustrated below associates an eMPS profile to P-GW service.

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no associate emps-profile**: Disables the feature.
- **emps-profile** *emps_profile_name*: Associates an eMPS profile with the P-GW service. The *emps_profile_name* is a string of size 1 to 63.
- The eMPS profile name in input is treated as case insensitive.
- By default, no eMPS profile is associated with pgw-service.
- For SAE-GW associated P-GW service, the eMPS profiles should be same as configured in associated S-GW service. In case of any discrepancy, it will be reported in the **show configuration error** CLI command output.

Associating an eMPS Profile with S-GW Service

The commands illustrated below associates an eMPS profile to S-GW service.

```
configure
  context context_name
    sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

Notes:

- **no associate emps-profile**: Disables the feature.
- **emps-profile** *emps_profile_name*: Associates an eMPS profile with the S-GW service. The *emps_profile_name* is a string of size 1 to 63.

- The eMPS profile name in input is treated as case insensitive.
- By default, no eMPS profile is associated with sgw-service.
- For SAE-GW associated S-GW service, the eMPS profiles should be same as configured in associated P-GW service. In case of any discrepancy, it will be reported in the **show configuration error** CLI command output.

Monitoring and Troubleshooting the Expanded Prioritization for VoLTE/Emergency Calls

This section provides information regarding show commands and/or their outputs in support of this enhancement.

Show Command(s) and/or Outputs

show emps-profile { all | name <emps_profile_name> }

The above CLI command is introduced to see a particular or all eMPS profile(s) configured with its associated attributes. Also, the output of an existing **show config [verbose]** CLI command is modified to reflect an eMPS configuration:

- **earp configured**: <earp_value>
- **dscp-marking configured**: <dscp-value>

These CLI commands can be used to verify if the configuration is appropriate.

show pgw-service { name <name> | all }

The output of this command is modified to reflect the eMPS profile associated with the P-GW service:

- **eMPS Profile Name** : <emps_profile_name>

Important Maximum of one eMPS profile can be associated with P-GW service at a time; the latest configuration will overwrite the previously associated configuration.

show sgw-service { name <name> | all }

The output of this command is modified to reflect the eMPS profile associated with the S-GW service:

- **eMPS Profile Name** : <emps_profile_name>

Important Maximum of one eMPS profile can be associated with S-GW service at a time; the latest configuration will overwrite the previously associated configuration.

show subscribers pgw-only full all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Username: 0123456789@username
 Subscriber Type   : Visitor
 Status            : Online/Active
 State             : Connected
 Connect Time      : Wed Sep  7 07:02:49 2016
 Auto Delete       : No
 Idle time         : 00h00m08s
 MS TimeZone       : n/a                    Daylight Saving Time: n/a
 Access Type: gtp-pdn-type-ipv4             Network Type: IP
 Access Tech: eUTRAN                        pgw-service-name: pgw_service
 Callid: 00004e21                           IMSI: 123456789012341
 MSISDN: 0123456789
 Interface Type: S5S8GTP                    Low Access Priority: N/A
 TWAN Mode: N/A
 eMPS Bearer: Yes
 Emergency Bearer Type: N/A
 IMS-media Bearer: No
```

show subscribers saegw-only full all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Username: 0123456789@username
 SAEGW Call mode   : Co-located
 Subscriber Type   : Home
 .
 .
 .
 MSISDN: 0123456789
 TWAN Mode: N/A
 eMPS Bearer: Yes
 MS TimeZone       :                     Daylight Saving Time: n/a
 MEI               : 1122334455667788    Accounting mode      : GTPP
```

show pgw-service statistics

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:               0    Setup:            0
   Authentic IMSI:      0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                  1       Cumulative Activated:   1
  Cumulative De-activated:         1
IPv4v6 PDN-Type Received with DAF False :         0
```

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.

- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show saegw-service statistics all function pgw

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:              0    Setup:            0
   Authentic IMSI:     0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         1
IPv4v6 PDN-Type Received with DAF False :         0
```

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.
- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show saegw-service statistics

The output of this command is modified to display the eMPS statistics for PGW-Anchored/SGW-Anchored PDNs associated with the saegw-service. For example:

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:              0    Setup:            0
  Released:      0
 .
 .
 .
eMPS PDNs:
 Colocated PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
 PGW-Anchor PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
 SGW-Anchor PDNs:
  Current Active:                  1      Cumulative Activated:   1
  Cumulative De-activated:         0
```

The above statistics information are further classified based on SAE-GW call types:

- **Colocated eMPS PDNs**: It reflects the eMPS PDN statistics information for collapsed PDNs.
- **PGW-Anchor eMPS PDNs**: It reflects the eMPS PDN statistics information for PGW-Anchor PDNs.

- **SGW-Anchor eMPS PDNs**: It reflects the eMPS PDN statistics information for SGW-Anchor PDNs.

Where:

- **Current Active**: Increments when any PDN is setup as an eMPS PDN or upgraded to eMPS PDN. Decrements when an eMPS PDN is released or when it degrades to a non-eMPS PDN.
- **Cumulative Activated**: Increments when any PDN is setup as an eMPS PDN or upgrades to an eMPS PDN.
- **Cumulative De-activated**: Increments when an eMPS PDN is released or when it degrades to a non-eMPS PDN.

show sgw-service statistics all

The output of this command is modified to reflect whether the session is eMPS or not. For example:

```
Subscribers Total:
  Active:               0    Setup:            2
  Released:             1
 .
 .
 .
eMPS PDN Statistics:
  Current Active:                   1       Cumulative Activated:    1
  Cumulative De-activated:          0
```

show saegw-service statistics all function sgw

The output of this command is modified to display the eMPS PDN statistics information. For example:

```
Subscribers Total:
  Active:               0    Setup:            0
  Released:             0
 .
 .
 .
eMPS PDN Statistics:
  Current Active:                   1       Cumulative Activated:    1
  Cumulative De-activated:          0
```

show configuration error

System will show configuration errors for following scenarios:

- When different eMPS profiles are configured under pgw-service and sgw-service associated to same sae-gw service. For example:

```
##############################################################
    Displaying SAEGW-Service system errors
##############################################################
Error   : eMPS profile of SGW <sgw-service> and PGW service <pgw_service>
is not same for SAEGW service <saegw-service> in the context <context_name>.
Total 1 error(s) in this section !
```

- When non-existent emps-profile is associated to pgw-service. For example:

```
##############################################################
    Displaying PGW-Service system errors
##############################################################
```

```
Error   : eMPS Profile <emps_profile_pgw> configured for PGW service <pgw_service>
is not present in the system
Total 1 error(s) in this section !
```

- When non-existent emps-profile is associated to sgw-service. For example:

```
##########################################################
    Displaying SGW-Service system errors
##########################################################
Error   : eMPS Profile <emps_profile_sgw> configured for SGW service <sgw_service>
is not present in the system
Total 1 error(s) in this section !
```

Bulkstats for Expanded Prioritization for VoLTE/Emergency Calls

PGW Schema

The following bulk statistics have been added to the P-GW schema as part of this enhancement:

- sessstat-pdn-emps-current-active – The total number of currently active P-GW eMPS PDNs.
- sessstat-pdn-emps-cumulative-activated – The total number of P-GW PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sessstat-pdn-emps-cumulative-deactivated – The total number of P-GW PDNs that were either released or degrades to a non-eMPS PDN.

SGW Schema

The following bulk statistics have been added to the S-GW schema as part of this enhancement:

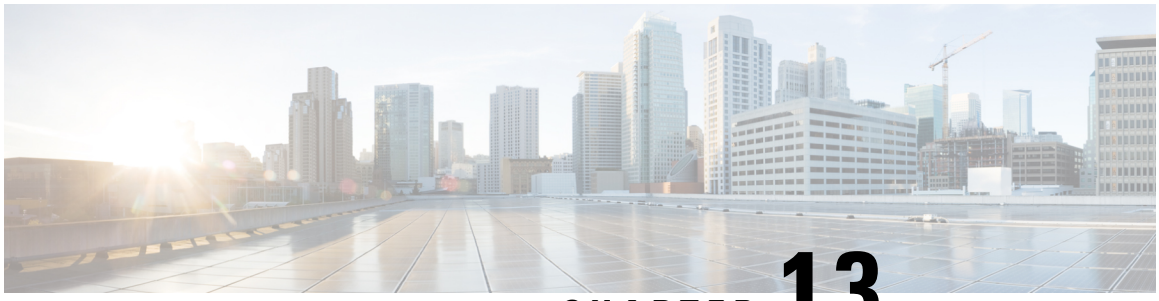
- sessstat-pdn-emps-current-active – The total number of currently active S-GW eMPS PDNs.
- sessstat-pdn-emps-cumulative-activated – The total number of S-GW PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sessstat-pdn-emps-cumulative-deactivated – The total number of S-GW PDNs that were either released or degrades to a non-eMPS PDN.

SAEGW Schema

The following bulk statistics have been added to the SAE-GW schema as part of this enhancement:

- pgw-anchor-pdns-emps-current-active – The total number of currently active P-GW anchored eMPS PDNs.
- pgw-anchor-pdns-emps-cumulative-activated – The total number of P-GW anchored PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- pgw-anchor-pdns-emps-cumulative-deactivated – The total number of P-GW anchored PDNs that were either released or degrades to a non-eMPS PDN.
- saegw-colocated-pdns-emps-current-active – The total number of currently active SAE-GW collapsed eMPS PDNs.
- saegw-colocated-pdns-emps-cumulative-activated – The total number of SAE-GW collapsed PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.

- saegw-colocated-pdns-emps-cumulative-deactivated – The total number of SAE-GW collapsed PDNs that were either released or degrades to a non-eMPS PDN.
- sgw-anchor-pdns-emps-current-active – The total number of currently active S-GW anchored eMPS PDNs.
- sgw-anchor-pdns-emps-cumulative-activated – The total number of S-GW anchored PDNs that are either setup as an eMPS PDN or upgrades to an eMPS PDN.
- sgw-anchor-pdns-emps-cumulative-deactivated – The total number of S-GW anchored PDNs that were either released or degrades to a non-eMPS PDN.



CHAPTER 13

Extended QCI Options

This chapter describes extended QCI functionality.

Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Feature Description

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

Important For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

The existing **show apn statistics name** *apn-name* and **show apn statistics** *Exec Mode* CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.

Licensing

Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring ARP Granularity for QCI Level Counters

This section describes how to configure the ARP Granularity for QCI Level Counters feature.

Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring the feature consists of the following tasks:

1. Create a Stats Profile.
2. Enable the Collection of Per QCI Packet Drop Counters.
3. Enable the Collection of QCI/ARP Level Statistics.
4. Associate a Stats Profile with an APN.
5. Verify the Configuration.

Create a Stats Profile

Use the following example to access *Global Configuration Mode* and create a Stats Profile:

```
configure
  stats-profile stats_profile_name
  end
```

Notes:

- *stats_profile_name* must be an alphanumeric string from 1 to 63 characters in length.

Enable the Collection of Packet Drop Statistics

Use the following example to access *Stats Profile Configuration Mode* and create a Stats Profile and enable the collection of packet drop statistics:

```
configure
  stats-profile stats_profile_name
    packet-drop
    end
```

To disable the collection of packet drop statistics

```
configure
  stats-profile stats_profile_name
    no packet-drop
    end
```

Notes:

- *stats_profile_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- **packet-drop**: enables the collection of packet drop statistics for the specified Stats Profile.
- **no packet-drop**: disables the collection of packet drop statistics for the specified Stats Profile.

Enable the Collection of QCI/ARP Level Statistics

Use the following example to access *Stats Profile Configuration Mode* and enable the collection of QCI/ARP level statistics for a Stats Profile:

```
configure
  stats-profile stats_profile_name
    qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
 |12 | 13 | 14 | 15 ] + } }
    end
```

To disable the collection of QCI/ARP statistics:

```
configure
  stats-profile stats_profile_name
  no qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
 |12 | 13 | 14 | 15 ] + } }
  end
```

Notes:

- *stats_proflle_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 64 characters in length.
- **qci**: configures the collection of ARP priority level statistics for the specified QCI(s).
- **non-std**: configures the collection of ARP priority level statistics for non-standard QCIs.
- **non-gbr**: configures the collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.

- **gbr**: configures the collection of ARP priority level statistics for non-standard GBR QCIs.
- **arp**: configures the collection of ARP priority level statistics for the specified ARP values.
- **no**: disables the collection of ARP priority level statistics for the specified **qci** and **arp** settings.

Associate a Stats Profile with an APN

Use the following example to access *APN Configuration Mode* and associate a Stats Profile with an APN:

```
configure
  apn apn_name
    stats-profile stats_profile_name
    end
```

To disassociate a Stats Profile from a specified APN:

```
configure
  apn apn_name
    no stats-profile
    end
```

Notes:

- *stats_profile_name*: must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- A maximum of 64 Stats Profiles can be configured per P-GW/SAEGW/GGSN service.
- **no stats-profile**: disassociates the Stats Profile from the APN.

Important If a Stats Profile is associated with more than 12 APNs, the following memory and performance impact warning is provided:

```
[WARNING] Configuring QCI/ ARP level statistics for more then 12 APNs will have
memory and performance impact. Do you want to continue [Y/N]
```

Verify the Configuration

Use the following procedure to verify the configuration:

First, verify that the Stats Profile is associated with the correct APN. In *Exec Mode*, enter the following command:

```
show apn name apn_name
```

Notes:

- In the command output, look for the **stats profile** field. It should contain the name of the Stats Profile which is associated with this APN.

Next, verify that the Stats Profile configuration settings are correct. In *Exec Mode*, enter the following command:

```
show stats-profile name stats_profile_name
```

Notes:

- Where *stats_profile_name* is the name of the Stats Profile for which you want to view settings.
- The command output includes the following information:
  - Stats Profile name
  - Packet-drop configuration settings for both QCI and ARP
  - QCI ARP combinations for which the StarOS will collect granular ARP statistics

If any of the above settings are incorrect, perform the configuration procedure again to reconfigure the Stats Profile with the proper settings.

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes how to monitor the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Bulk Statistics

This section provides the bulk statistics that have been added to support the ARP Granularity and per QCI Packet Drop Counters feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
```

```
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

Show Commands

This section provides the Exec Mode show commands that are available to support the Per Packet QCI Drop Counters and ARP Granularity for QCI Level Counters feature.

show apn statistics

The **qci** and **arp** keywords have been added to this command. The new keywords enable operators to view output for four basic scenarios that apply to the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Scenario 1

View packet drop counters with granularity at the QCI/ARP level for a single APN. The output of this command is useful for isolating network issues that may be affecting packet drops.

show apn statistics name *apn_name* **qci { all | 1-9 | non-std { gbr | non-gbr } } arp { all | 1-15 }**

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.

- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 2

View packet drop counters with granularity at the QCI/ARP level for all APNs.

```
show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } } arp {
all | 1-15 }
```

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 3

View the new packet drop counters at granularity of QCI level, and pre-existing QCI level counters for the specified APN.

```
show apn statistics name apn_name qci { all | 1-9 | non-std { gbr | non-gbr
 } }
```

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).

- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 4

View the packet drop counters at the granularity of the QCI level, and view pre-existing QCI counters consolidated for all APNs.

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } }

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

The output of the **show apn statistics name** *apn_name* **qci all arp all** command has been enhanced to display the following new statistics:

```
Data Statistics:

    Uplink Bytes:                0   Downlink Bytes:                          0
    Uplink Pkts:                 0   Downlink Pkts:                           0
    Uplink Bytes dropped:        0   Downlink Bytes dropped:                  0
    Uplink Pkts dropped:         0   Downnlink Pkts dropped:                  0

  Uplink Dropped:                          Downlink Dropped:
    MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                  0
    MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                   0
    AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):                 0
    AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                  0
    Miscellaneous(Bytes):                0  Miscellaneous(Bytes):                 0
    Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                  0
    Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):             0
    Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):              0
    SGW Restoration(Bytes):              0  SGW Restoration(Bytes):               0
```

```
    SGW Restoration(Pkts):                  0  SGW Restoration(Pkts):                  0
    SDF Gate(Bytes):                        0  SDF Gate(Bytes):                        0
    SDF Gate(Pkts):                         0  SDF Gate(Pkts):                         0
    ITC Gate(Bytes):                        0  ITC Gate(Bytes):                        0
    ITC Gate(Pkts):                         0  ITC Gate(Pkts):                         0
    Flow Terminated(Bytes):                 0  Flow Terminated(Bytes):                 0
    Flow Terminated(Pkts):                  0  Flow Terminated(Pkts):                  0
    Subsession Terminated(Bytes):           0  Subsession Terminated(Bytes):           0
    Subsession Terminated(Pkts):            0  Subsession Terminated(Pkts):            0
    Call Terminated(Bytes):                 0  Call Terminated(Bytes):                 0
    Call Terminated(Pkts):                  0  Call Terminated(Pkts):                  0
    DCCA Discard(Bytes):                    0  DCCA Discard(Bytes):                    0
    DCCA Discard(Pkts):                     0  DCCA Discard(Pkts):                     0
    No Rule Match(Bytes):                   0  No Rule Match(Bytes):                   0
    No Rule Match(Pkts):                    0  No Rule Match(Pkts):                    0
    ICAP(Bytes):                            0  ICAP(Bytes):                          N/A
    ICAP(Pkts):                             0  ICAP(Pkts):                           N/A
    SFW(Bytes):                             0  SFW(Bytes):                             0
    SFW(Pkts):                              0  SFW(Pkts):                              0
    Hierarchical ENF(Bytes):                0  Hierarchical ENF(Bytes):                0
    Hierarchical ENF(Pkts):                 0  Hierarchical ENF(Pkts):                 0
    Dynamic CA Gate(Bytes):                 0  Dynamic CA Gate(Bytes):    :            0
    Dynamic CA Gate(Pkts):                  0  Dynamic CA Gate(Pkts):                  0
    NAT64 Cancel(Bytes):                    0  NAT64 Cancel(Bytes):                    0
    NAT64 Cancel(Pkts):                     0  NAT64 Cancel(Pkts):                     0
    Bearer Not Found(Bytes):                0  Bearer Not Found(Bytes):                0
    Bearer Not Found(Pkts):                 0  Bearer Not Found(Pkts):                 0


4G Bearers Released By Reasons:
                 QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
```

```
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0


Subscriber QoS Statistics:


4G Bearers Released By Reasons:
                QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0

  QCI 1:
```

```
 ARP 1:
  Bearer Active:                0   Bearer setup:                                2
  Bearer Released:              2   Bearer Rejected:                             0

  Uplink Bytes forwarded:       0   Downlink Bytes forwarded:                    0
  Uplink Pkts forwarded:        0   Downlink Pkts forwarded:                     0
  Uplink Bytes dropped:         0   Downlink Bytes dropped:                      0
  Uplink Pkts dropped:          0   Downlink Pkts dropped:                       0
 Uplink Dropped:                          Downlink Dropped:
  MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                  0
  MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                   0
  AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):                 0
  AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                  0
  Miscellaneous(Bytes):                0  Miscellaneous(Bytes):                 0
  Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                  0
  Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):             0
  Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):              0
  SGW Restoration(Bytes):              0  SGW Restoration(Bytes):               0
  SGW Restoration(Pkts):               0  SGW Restoration(Pkts):                0
  SDF Gate(Bytes):                     0  SDF Gate(Bytes):                      0
  SDF Gate(Pkts):                      0  SDF Gate(Pkts):                       0
  ITC Gate(Bytes):                     0  ITC Gate(Bytes):                      0
  ITC Gate(Pkts):                      0  ITC Gate(Pkts):                       0
  Flow Terminated(Bytes):              0  Flow Terminated(Bytes):               0
  Flow Terminated(Pkts):               0  Flow Terminated(Pkts):                0
  Subsession Terminated(Bytes):        0  Subsession Terminated(Bytes):         0
  Subsession Terminated(Pkts):         0  Subsession Terminated(Pkts):          0
  Call Terminated(Bytes):              0  Call Terminated(Bytes):               0
  Call Terminated(Pkts):               0  Call Terminated(Pkts):                0
  DCCA Discard(Bytes):                 0  DCCA Discard(Bytes):                  0
  DCCA Discard(Pkts):                  0  DCCA Discard(Pkts):                   0
  No Rule Match(Bytes):                0  No Rule Match(Bytes):                0
  No Rule Match(Pkts):                 0  No Rule Match(Pkts):                 0
  ICAP(Bytes):                         0  ICAP(Bytes):                        N/A
  ICAP(Pkts):                          0  ICAP(Pkts):                         N/A
  SFW(Bytes):                          0  SFW(Bytes):                           0
  SFW(Pkts):                           0  SFW(Pkts):                            0
  Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):              0
  Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):               0
  Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :          0
  Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):                0
  NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                  0
  NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                   0
  Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):              0
  Bearer Not Found(Pkts):              0  Bearer Not Found(Pkts):               0
QCI 1:
 ARP 2:
  Bearer Active:                0   Bearer setup:                                2
  Bearer Released:              2   Bearer Rejected:                             0

  Uplink Bytes forwarded:       0   Downlink Bytes forwarded:                    0
  Uplink Pkts forwarded:        0   Downlink Pkts forwarded:                     0
  Uplink Bytes dropped:         0   Downlink Bytes dropped:                      0
  Uplink Pkts dropped:          0   Downlink Pkts dropped:                       0
 Uplink Dropped:                          Downlink Dropped:
  MBR Exceeded(Bytes):          0  MBR Exceeded(Bytes):                  0
  MBR Exceeded(Pkts):           0  MBR Exceeded(Pkts):                   0
  AMBR Exceeded(Bytes):         0  AMBR Exceeded(Bytes):                 0
  AMBR Exceeded(Pkts):          0  AMBR Exceeded(Pkts):                  0
  Miscellaneous(Bytes):         0  Miscellaneous(Bytes):                 0
  Miscellaneous(Pkts):          0  Miscellaneous(Pkts):                  0
  Overcharge Prtctn(Bytes)      0  Overcharge Prtctn(Bytes):             0
  Overcharge Prtctn(Pkts):      0  Overcharge Prtctn(Pkts):              0
  SGW Restoration(Bytes):       0  SGW Restoration(Bytes):               0
```

```
    SGW Restoration(Pkts):          0  SGW Restoration(Pkts):                0
    SDF Gate(Bytes):                0  SDF Gate(Bytes):                      0
    SDF Gate(Pkts):                 0  SDF Gate(Pkts):                       0
    ITC Gate(Bytes):                0  ITC Gate(Bytes):                      0
    ITC Gate(Pkts):                 0  ITC Gate(Pkts):                       0
    Flow Terminated(Bytes):         0  Flow Terminated(Bytes):               0
    Flow Terminated(Pkts):          0  Flow Terminated(Pkts):                0
    Subsession Terminated(Bytes):   0  Subsession Terminated(Bytes):          0
    Subsession Terminated(Pkts):    0  Subsession Terminated(Pkts):           0
    Call Terminated(Bytes):         0  Call Terminated(Bytes):               0
    Call Terminated(Pkts):          0  Call Terminated(Pkts):                0
    DCCA Discard(Bytes):            0  DCCA Discard(Bytes):                  0
    DCCA Discard(Pkts):             0  DCCA Discard(Pkts):                   0
    No Rule Match(Bytes):           0  No Rule Match(Bytes):                 0
    No Rule Match(Pkts):            0  No Rule Match(Pkts):                  0
    ICAP(Bytes):                    0  ICAP(Bytes):                        N/A
    ICAP(Pkts):                     0  ICAP(Pkts):                         N/A
    SFW(Bytes):                     0  SFW(Bytes):                           0
    SFW(Pkts):                      0  SFW(Pkts):                            0
    Hierarchical ENF(Bytes):        0  Hierarchical ENF(Bytes):              0
    Hierarchical ENF(Pkts):         0  Hierarchical ENF(Pkts):               0
    Dynamic CA Gate(Bytes):         0  Dynamic CA Gate(Bytes):    :          0
    Dynamic CA Gate(Pkts):          0  Dynamic CA Gate(Pkts):                0
    NAT64 Cancel(Bytes):            0  NAT64 Cancel(Bytes):                  0
    NAT64 Cancel(Pkts):             0  NAT64 Cancel(Pkts):                   0
    Bearer Not Found(Bytes):        0  Bearer Not Found(Bytes):              0
    Bearer Not Found(Pkts):         0  Bearer Not Found(Pkts):               0
```

The output of the **show apn statistics name** *apn_name* **qci all** command has been enhanced to display the following new statistics:

```
Data Statistics:

    Uplink Bytes:                   0   Downlink Bytes:                       0
    Uplink Pkts:                    0   Downlink Pkts:                        0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:               0
    Uplink Pkts dropped:            0   Downnlink Pkts dropped:               0

  Uplink Dropped:                         Downlink Dropped:
    MBR Exceeded(Bytes):              0   MBR Exceeded(Bytes):                0
    MBR Exceeded(Pkts):               0   MBR Exceeded(Pkts):                 0
    AMBR Exceeded(Bytes):             0   AMBR Exceeded(Bytes):               0
    AMBR Exceeded(Pkts):              0   AMBR Exceeded(Pkts):                0
    Miscellaneous(Bytes):             0   Miscellaneous(Bytes):               0
    Miscellaneous(Pkts):              0   Miscellaneous(Pkts):                0
    Overcharge Prtctn(Bytes)          0   Overcharge Prtctn(Bytes):           0
    Overcharge Prtctn(Pkts):          0   Overcharge Prtctn(Pkts):            0
    SGW Restoration(Bytes):           0   SGW Restoration(Bytes):             0
    SGW Restoration(Pkts):            0   SGW Restoration(Pkts):              0
    SDF Gate(Bytes):                  0   SDF Gate(Bytes):                    0
    SDF Gate(Pkts):                   0   SDF Gate(Pkts):                     0
    ITC Gate(Bytes):                  0   ITC Gate(Bytes):                    0
    ITC Gate(Pkts):                   0   ITC Gate(Pkts):                     0
    Flow Terminated(Bytes):           0   Flow Terminated(Bytes):             0
    Flow Terminated(Pkts):            0   Flow Terminated(Pkts):              0
    Subsession Terminated(Bytes):     0   Subsession Terminated(Bytes):       0
    Subsession Terminated(Pkts):      0   Subsession Terminated(Pkts):        0
    Call Terminated(Bytes):           0   Call Terminated(Bytes):             0
    Call Terminated(Pkts):            0   Call Terminated(Pkts):              0
    DCCA Discard(Bytes):              0   DCCA Discard(Bytes):                0
    DCCA Discard(Pkts):               0   DCCA Discard(Pkts):                 0
    No Rule Match(Bytes):             0   No Rule Match(Bytes):               0
    No Rule Match(Pkts):              0   No Rule Match(Pkts):                0
    ICAP(Bytes):                      0   ICAP(Bytes):                      N/A
    ICAP(Pkts):                       0   ICAP(Pkts):                       N/A
```

```
    SFW(Bytes):                          0  SFW(Bytes):                          0
    SFW(Pkts):                           0  SFW(Pkts):                           0
    Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):             0
    Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):              0
    Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :          0
    Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):              0
    NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                 0
    NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                  0
    Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):             0
    Bearer Not Found(Pkts):              0  Bearer Not Found(Pkts):              0

4G Bearers Released By Reasons:

                      QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8    QCI9
   Admin disconnect:     0     0     0     0     0     0     0     0       0


Subscriber QoS Statistics:

  QCI 1:
    Bearer Active:                   0   Bearer setup:                          0
    Bearer Released:                 0   Bearer Rejected:                       0

    Uplink Bytes forwarded:          0   Downlink Bytes forwarded:              0
    Uplink Pkts forwarded:           0   Downlink Pkts forwarded:               0
    Uplink Bytes dropped:            0   Downlink Bytes dropped:                0
    Uplink Pkts dropped:             0   Downlink Pkts dropped:                 0
  Uplink Dropped:                          Downlink Dropped:
    MBR Exceeded(Bytes):                 0  MBR Exceeded(Bytes):                0
    MBR Exceeded(Pkts):                  0  MBR Exceeded(Pkts):                 0
    AMBR Exceeded(Bytes):                0  AMBR Exceeded(Bytes):               0
    AMBR Exceeded(Pkts):                 0  AMBR Exceeded(Pkts):                0
    Miscellaneous(Bytes):                0  Miscellaneous(Bytes):               0
    Miscellaneous(Pkts):                 0  Miscellaneous(Pkts):                0
    Overcharge Prtctn(Bytes)             0  Overcharge Prtctn(Bytes):           0
    Overcharge Prtctn(Pkts):             0  Overcharge Prtctn(Pkts):            0
    SGW Restoration(Bytes):              0  SGW Restoration(Bytes):             0
    SGW Restoration(Pkts):               0  SGW Restoration(Pkts):              0
    SDF Gate(Bytes):                     0  SDF Gate(Bytes):                    0
    SDF Gate(Pkts):                      0  SDF Gate(Pkts):                     0
    ITC Gate(Bytes):                     0  ITC Gate(Bytes):                    0
    ITC Gate(Pkts):                      0  ITC Gate(Pkts):                     0
    Flow Terminated(Bytes):              0  Flow Terminated(Bytes):             0
    Flow Terminated(Pkts):               0  Flow Terminated(Pkts):              0
    Subsession Terminated(Bytes):        0  Subsession Terminated(Bytes):       0
    Subsession Terminated(Pkts):         0  Subsession Terminated(Pkts):        0
    Call Terminated(Bytes):              0  Call Terminated(Bytes):             0
    Call Terminated(Pkts):               0  Call Terminated(Pkts):              0
    DCCA Discard(Bytes):                 0  DCCA Discard(Bytes):                0
    DCCA Discard(Pkts):                  0  DCCA Discard(Pkts):                 0
    No Rule Match(Bytes):                0  No Rule Match(Bytes):               0
    No Rule Match(Pkts):                 0  No Rule Match(Pkts):                0
    ICAP(Bytes):                         0  ICAP(Bytes):                      N/A
    ICAP(Pkts):                          0  ICAP(Pkts):                       N/A
    SFW(Bytes):                          0  SFW(Bytes):                         0
    SFW(Pkts):                           0  SFW(Pkts):                          0
    Hierarchical ENF(Bytes):             0  Hierarchical ENF(Bytes):            0
    Hierarchical ENF(Pkts):              0  Hierarchical ENF(Pkts):             0
    Dynamic CA Gate(Bytes):              0  Dynamic CA Gate(Bytes):    :        0
    Dynamic CA Gate(Pkts):               0  Dynamic CA Gate(Pkts):              0
    NAT64 Cancel(Bytes):                 0  NAT64 Cancel(Bytes):                0
    NAT64 Cancel(Pkts):                  0  NAT64 Cancel(Pkts):                 0
    Bearer Not Found(Bytes):             0  Bearer Not Found(Bytes):            0
```

```
    Bearer Not Found(Pkts):                0  Bearer Not Found(Pkts):                0

.
.
.
QCI 9:
    Bearer Active:                 0   Bearer setup:                              0
    Bearer Released:               0   Bearer Rejected:                           0

    Uplink Bytes forwarded:        0   Downlink Bytes forwarded:                  0
    Uplink Pkts forwarded:         0   Downlink Pkts forwarded:                   0
    Uplink Bytes dropped:          0   Downlink Bytes dropped:                    0
    Uplink Pkts dropped:           0   Downlink Pkts dropped:
```

show configuration

The output of this command has been enhanced to show the Stats Profile configuration settings.

- stats-profile <*stats_profile_name*>
- qci <*qci number*> arp <*arp number*>
- packet-drop (*if packet-drop is enabled*)

show stats-profile name

This new command in *Exec Mode* shows the configuration settings for the specified Stats Profile.

- Stats Profile Name: <*stats_profile_name*>
- qci <*qci number*> arp <*arp_number(s)*>
- packet-drop <*if packet drop is enabled*>

DSCP Marking Based on Both QCI and ARP Values

Feature Description

P-GW allows users to perform DSCP marking based on QoS Class Identifier (QCI) values. This functionality has been expanded to include the Priority Level (PL) values 1-15 of Allocation and Retention Priority (ARP), which allows users to assign different DSCP values for bearers with the same QCI but different ARP priority values. For example, the ability to assign DSCP values based on QCI+ARP could be used to meet compliance on priority and emergency calling via VoLTE.

Applies to the P-GW for the following interfaces:

- S5
- S8
- SGi
- S2b

Applies to the S-GW for the following interfaces:

- S1-U
- S5
- S8
- S11
- S4

Relationships to Other Features

ECS populates the DSCP values in inner IP header. These values are fetched from the DSCP table by means of a sessmanager API. Since DSCP values are now available for QCI-ARP combination, the API is replaced by a wrapper API that will accept both QCI and ARP and provide the DSCP values to ECS in a new data structure.

The API will return correct values in the following scenarios:

1. QCI-DSCP table is not configured, or it is not associated for this session.

   API will return an indication to ECS that table was not found.

2. Table is configured, but entry for the given QCI value is not present in the table.

   API will not populate the structure and keep the same unaltered.

3. Entry for given QCI is present, but it is not available for the given QCI-ARP pair.

   The default DSCP values for that particular QCI will be populated in the return structure.

4. Entry for given QCI-ARP combination is present.

   The DSCP values for given QCI-ARP combination will be populated in the return structure.

Once values are received from SM, ECS caches these values and uses the cached values for marking the further packets. Another lookup into the table is done only when there is a mismatch between the currently cached QCI-ARP value and the current packet's QCI-ARP value. Therefore, any change in the QCI-ARP table would be affected for inner DSCP marking on existing flows only in case of QCI or ARP change.

Licensing

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

How It Works

The expansion of functionality to allow assigning different DSCP values for bearers with the same QCI, but different APR values, works as follows.

- DSCP marking of packets based on QCI+ARP combination allowed
- QCI + ARP configuration will override any DSCP entry for that QCI+ARP combination
- QCI only DSCP entry will override all existing QCI+ARP configuration
- Applying associated DSCP marking for QCI+ARP for Uplink and Downlink functionality is also allowed

Configuring DSCP Marking Based on Both QCI and ARP Values

This section describes how to configure DSCP marking based on both QCI and ARP values.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI and ARP values to enforceable Quality of Service (QoS) parameters:

```
configure
   qci-qos-mapping name
      qci num [ arp-priority-level arp_value ] [ downlink [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ] [ internal-qos priority priority ] [ user-datagram dscp-marking dscp-marking-value  ] ] [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ]  [ internal-qos priority priority ]  [ user-datagram dscp-marking dscp-marking-value  ] ]
      end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values. In addition, QCI values 65, 66, 69, and 70 can be used in StarOS release 21.0 and later.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs are supported and carriers can define QCI 128- 254.

- **arp-priority-level** *arp_value*: Specifies the address retention priority (ARP) priority level.

  arp_value must be an integer from 1 through 15.

- 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.

Use the following example to disable QCI and ARP values:

```
configure
   qci-qos-mapping name
      no qci num [ arp-priority-level arp_value ]
      end
```

Associating QCI-QoS Mapping Configuration

Use the following example to specify that the P-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
   contextcontext_name
      pgw-service pgw_service_name
         associate qci-qos-mapping name
         end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Use the following example to specify that the S-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
  context context_name
    sgw-service sgw_service_name
      associate qci-qos-mapping name
      end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Configuring CS5 Marking for GTP-C

Use the following example to mark DSCP precedence CS5 on control packets:

```
configure
  context context_name
    ggsn-service ggsn_service_name
      ip qos-dscp gtpc cs5
      end
```

Notes:

- Designates Class Selector 5 DSCP precedence for GTP-C packets.

Verifying the Configuration

Use the following command in Exec mode to display/verify the configuration.

```
show configuration
```

Monitoring DSCP Marking Based on Both QCI and ARP Values

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of DSCP marking based on both QCI and ARP values.

show qci-qos-mapping table all

The output of this command has been enhanced to show the ARP value:

- arp-priority-level

New Standard QCI Support

CDETS: CSCuy20910 - Support of new standard QCIs (65, 66, 69, 70)

Applicable Products: P-GW, SAEGW, S-GW

Feature Description

The P-GW/SAEGW/S-GW support additional new 3GPP-defined standard QCIs. QCIs 65, 66, 69, and 70 are now supported for Mission Critical and Push-to-Talk (MCPTT) applications. These new standard QCIs are supported in addition to the previously supported QCIs of 1 through 9, and operator-defined QCIs 128 through 254.

The StarOS will continue to reject QCIs 10 through 127 sent by the PCRF.

Licensing

Important New Standard QCI Support is a licensed feature. Contact your Cisco account or support representative for licensing details.

How it Works

Although the 3GPP specification mentions that only QCIs 65 and 69 can co-exist, there is no hard restriction on the QCIs in the StarOS implementation of this feature, as that is applicable to the PCRF. The P-GW acts as a pass-through node and allows QCIs 65 and 69 if a different QCI combination is requested from PCRF.

With support for standard QCIs 65, 66, 69, and 70 present, the implementation has also added support across the following StarOS interfaces:

- **Gx**: Gx processes Default Bearer QoS and Rule Validation allowing the new Mission Critical (MC)/Push to Talk (PTT) QCIs. When the MC/PTT bit is not negotiated with the PCRF, the PCEF will reject the creation of a bearer or reject call setup.
- **sessmgr**: The P-GW sessmgr now processes the updating and modification of QoS. The P-GW rejects all UE initiated BRC creation for the new standard QCIs.
- **ECS**: ECS accepts the new standard QCIs when received from the PCRF and will reject them when either the license is not configured or the same is received in 3G. The ECS is able to update a Default bearer with this QoS change or create a Dedicated Bearer for the new standard QCIs.

Handoff Behavior

For Gn/Gp handoffs, local mapping via the CLI is supported so that the P-GW/SAEGW/S-GW is in sync with the MME-to-SGSN context transfer. The following scenarios are supported:

No Local QoS Mapping Present: When no local mapping is present for the new QCIs, a call handoff from 4G to 3G will be rejected.

Local QoS Mapping Present: Three scenarios are supported when local mapping is present:

- **Local Mapping present for MME-SGSN and PCRF Out of Synchronization**: When local mapping is present it is assumed that the QoS mapping in the P-GW is in sync with the mapping from the MME to SGSN. Even if the QoS mapping for one of the transferred PDPs during a Gn/Gp handoff is not in sync with MME-SGSN mapping, the P-GW/SAEGW/S-GW still continues with the handoff with the local mapping present. However, the CDR generated while waiting for the PCRF response during the handoff would be out of sync with the CDR's received after the handoff.

- **Mapping present for MME-SGSN and PCRF in Synchronization**: When local mapping is in sync with the MME-SGSN there is no difference in the CDR generated after the handoff.
- **Partial Mapping Present**: Partial mapping occurs when some MC/PTT QCI(s) have mapping and the remainder of the MC/PTT QCI(s) do not have mapping. In this case the call is dropped.

Expected Call Flow Output

This section provides detailed information on the expected call flow output for various scenarios with the New Standard QCI support feature:

- New Call Procedure
- Handoff Procedures
- UE Initiated Bearer Creation
- Bearer Creation
- Bearer Update

These sections describe new behaviors and provide behavior clarification for this feature. Behavior not described is similar to that for Standard QCIs.

New Call Procedure

This section provides detailed information on the expected call flow output for various new call procedure scenarios with the New Standard QCI Support feature.

Table 19: Expected Call Flow Output: New Call Procedure

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Setup 3G (GGSN)	N/A	N/A	Create PDP Req	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call rejected by application
Setup eHRPD	N/A	N/A	PBU	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call accepted and created with this rule
Setup 4G (RAT: S4-SGSN)	N/A	N/A	Create Session Req	Std QCI	Enabled	MC/PTT-Std QCI	N/A	N/A	Call accepted and created with this rule

Handoff Procedures

This section provides detailed information on expected call flow output for various handoff procedure scenarios with the New Standard QCI Support feature.

Table 20: Expected Call Flow Output: Handoff Procedures

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Default bearer existing for WiFi	Call existing with MC/PTT-QCI requested to handoff to MC/PTT-QCI	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT-Std QCI received for default bearer	N/A	Handoff accepted and dowlnadd MC/PTT Std QCI applied	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GnGp Handoff (4G (LTE) to 3G (GGSN))	Update PDP request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI where mapping not received for few MC/PTT-QCI bearers	Update PDP Req	Partial mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	Partial mapped Std QCI for MC/PTT-QCIs received. Here mapping is not Received for some PDP bearers .	N/A	Handoff rejected and call drop Initiated
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI where no mapping received for few MC/PTT-QCI bearers	Update PDP Req	No mapping Received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	No mapping received	N/A	Handoff rejected and call drop initiated
	Update PDP request received for primary PDP and pending response (No-Local Mapping Present)	Call existing with Std primary PDP & MC/PTT-QCI requested to Std-QCI	Update PDP Req	N/A	Enabled	N/A	MC/PTT update rules received for Std QCI dedicated bearers	N/A	MC/PTT QCI mapped rule associated dedicated bearer purged and handoff accepted
		Call existing with MC/PTT primary PDP	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response (No-local mapping present)								Handoff rejected and call drop Initiated (dropped before Initiating CCA-U for handoff)
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	PCRF Timeout No Response received	Enabled	N/A	No response from PCRF / CCA-U timeout	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and same as what QCI values comes in UPC during HO)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
			Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and not same as what QCI values comes in UPC during HO).	Call existing with MC/PTT-QCI requested to Std-QCI							
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and same as what QCI values come in UPC during HO)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
		Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and not same as what QCI values come in UPC during HO.)								
	Update PDP Request received for primary PDP and pending response (Local mapping present/not present)	Call existing with MC/PTT-QCI requested to Std-QCI. Also suppress-NRUPC UPC is configured at the GGSN service level.	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and response sent (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers	Update PDP Req	Complete mapping Received from PCRF for MC/PTT- QCI to Std-QCI (as per Local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT-QCI	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and response sent (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers	Update PDP Req	Complete mapping received from PCRF for MC/PTT- QCI to Std-QCI (different from local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT-QCI	N/A	Handoff accepted and Update PDP Response sent for all bearers
eHRPD -> LTE	Create Session Req received with ho_ind = 1	Only one bearer existing with the call	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT-Std QCI received with rules	N/A	Handoff accepted and dedicated bearer are created with the MC/PTT-Std QCI received.
LTE -> eHRPD	Default + dedicated bearer existing for LTE	Call existing with MC/PTT-QCI	PBU	N/A	Enabled	N/A	N/A	N/A	Handoff accepted and PBA is sent and dedicated bearer rules are added under single bearer

UE Initiated Bearer Creation

This section provides detailed information on the expected call flow output for various UE initiated bearer creation scenarios with the New Standard QCI Support feature.

Table 21: Expected Call Flow Output: UE Initiated Bearer Creation

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
LTE UE Initiated Bearer	Default bearer existing for LTE	N/A	Bearer Resource Command	MC/PTT- Std QCI	N/A	N/A	N/A	N/A	BRC rejected by application
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Disabled	N/A	MC/PTT-Std dedicated QCI	N/A	BRC rejected / rule rejected with resource allocation failure
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Enabled	N/A	MC/PTT-Std dedicated QCI	N/A	BRC rejected /CBReq initiated with MC/PTT- Std QCI

Bearer Creation

This section provides detailed information on the expected call flow output for Bearer Creation scenarios with the New Standard QCI Support feature.

Table 22: Expected Call Flow Output: Bearer Creation

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN secondary PDP creation	Primary PDP existing for GGSN	New secondary PDP requested with MC/PTT-Std-QCI	RAR Procedure	N/A	Enabled	N/A	N/A	Rules received with MC/PTT-Std QCI	CCR-I resource allocation failure for secondary PDP sent to PCRF

Bearer Update

This section provides detailed information on the expected call flow output for Bearer Update scenarios with the New Standard QCI Support feature.

Table 23: Expected Call Flow Output: Bearer Update

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN Primary PDP QoS modification	Primary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT-Std QCI modification	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MC/PTT-Std QCI for primary PDP received	CCR-I QoS modification failure for primary PDP QoS modification rejected
GGSN Secondary PDP Qos Modification	Primary PDP & secondary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT-Std QCI modification for secondary PDP	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MC/PTT-Std QCI for secondary PDP with rules received	CCR-I resource allocation failure for secondary PDP QoS modification sent

Configuring New Standard QCIs

Configuring New Standard QCIs consists of the following tasks:

- Configuring QCI-QoS Mapping
- Configuring Local Mapping for Gn/Gp Support
- Configuring Transaction Rate Network Initiated Setup/Teardown Events
- Enable Mission Critical QCIs

Configuring QCI-QoS Mapping

Standard QCI options **65**, **66**, **69**, and **70** have been added to the **qci** command in *QCI-QoS Mapping Configuration Mode*.

To configure QCI-QoS Mapping for new standard QCIs:

```
configure
  qci-qos-mapping qci_qos_map_name
    qci { 1-9 | 65 | 66 | 69 | 70 }
    end
```

To disable new QCI-QoS mapping for new standard QCIs:

```
configure
  qci-qos-mapping qci_qos_map_name
```

```
no qci { 1-9 | 65 | 66 | 69 | 70 }
end
```

Notes:

- **qci** options 65 and 66 are available for guaranteed bit rate (GBR) network initiated QCI values only.

  qci options 69 and 70 are available for non-GBR network initiated QCI values only.

- **no** disables the specified standard **qci** value.

Configuring Local QCI Mapping for Gn/Gp QoS Support

Use the following example to configure local QCI mapping for Gn/Gp support:

```
configure
  qci-qos-mapping mapping_name
    qci  { 1-9 | 65 | 66 | 69 | 70 } pre-rel8-qos-mapping qci_value
    end
```

Notes:

- **qci**: When the MPS license is disabled, this value must be a Standard QoS Class Identifier (QCI) from 1 to 9. When the MPS license is enabled, this value must be a Standard QCI from 1 to 9, or 65, 66, 69, 70.
- **qci** 65 and 66 are Mission Critical/Push to Talk (MC/PTT) GBR values and values 69 and 70 are MC/PTT Non-GBR values.
- **qci** values 65 and 66 can only be mapped to QCI values 1 through 4, and QCI values 69 and 70 can only be mapped to QCI values 5 through 9.

Configuring Transaction Rate Network Initiated Setup/Teardown Events

To configure transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
  transaction-rate nw-initiated-setup-teardown-events qci { 1-9 | 65 |
66 | 69 | 70 | 128-254 }
  end
```

To disable transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
  no transaction-rate nw-initiated-setup-teardown-events qci qci_value
  end
```

Notes:

- **65** and **66** are available options for GBR network-initiated QCI values.
- **69** and **70** are available options for non-GBR network-initiated QCI values.
- **no** disables transaction rate network initiated setup/teardown events for the specified new standard QCI value.

Enable Mission Critical QCIs

The **mission-critical-qcis** keyword in the **diameter encode-supported-features** command is required for support between the PCEF and PCRF for new standard QCI support. Use the following example to enable mission critical QCIs in *Policy Control Configuration Mode*:

```
configure
  context context_name
    ims-auth-service ims-ggsn-auth
      policy-control
        diameter encode-supported-features mission-critical-qcis
        end
```

To disable this feature, enter the following commands:

```
configure
  context context_name
    ims-auth-service ims-ggsn-auth
      policy-control
        no diameter encode-supported-features
        end
```

Notes:

Important The LTE Wireless Priority Feature Set must be enabled to configure the **mission-critical-qcis** option. The LTE Wireless Priority Feature Set is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

Verifying the Configuration

Use the following example to verify the new standard QCI configuration:

```
show qci-qos-mapping table name qci_qos_mapping_table_name
```

Notes:

- The command output provides all qci-qos mapping attributes, including the new standard qci number. If any of the attributes are incorrect, repeat the configuration procedure in this chapter to correct the settings.

Monitoring the Feature

This section describes how to monitor the New Standard QCI Support feature.

Bulk Statistics

This section lists the bulk statistics that have been added to support the New Standard QCIs feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
```

```
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

GTPU Schema

The following bulk statistics have been added to the GTPU Schema to support the New Standard QCIs feature.

```
qci65-uplink-pkts
qci65-uplink-bytes
qci65-dwlink-pkts
qci65-dwlink-byte
qci65-pkts-discard
qci65-bytes-discard
qci66-uplink-pkts
qci66-uplink-bytes
qci66-dwlink-pkts
qci66-dwlink-byte
qci66-pkts-discard
qci66-bytes-discard
qci69-uplink-pkts
qci69-uplink-bytes
qci69-dwlink-pkts
qci69-dwlink-byte
qci69-pkts-discard
qci69-bytes-discard
qci70-uplink-pkts
qci70-uplink-bytes
qci70-dwlink-pkts
qci70-dwlink-byte
qci70-pkts-discard
qci70-bytes-discard
```

P-GW Schema

The following bulk statistics have been added to the P-GW schema to support the New Standard QCIs feature.

```
subqosstat-bearact-qci65
subqosstat-bearact-qci66
subqosstat-bearact-qci69
subqosstat-bearact-qci70
subqosstat-bearsetup-qci65
subqosstat-bearsetup-qci66
subqosstat-bearsetup-qci69
subqosstat-bearsetup-qci70
subqosstat-bearrel-qci65
subqosstat-bearrel-qci66
subqosstat-bearrel-qci69
subqosstat-bearrel-qci70
subdatastat-uppktfwd-qci65
subdatastat-uppktfwd-qci66
subdatastat-uppktfwd-qci69
subdatastat-uppktfwd-qci70
subdatastat-upbytefwd-qci65
subdatastat-upbytefwd-qci66
subdatastat-upbytefwd-qci69
subdatastat-upbytefwd-qci70
subdatastat-downpktfwd-qci65
subdatastat-downpktfwd-qci66
subdatastat-downpktfwd-qci69
subdatastat-downpktfwd-qci70
subdatastat-downbytefwd-qci65
subdatastat-downbytefwd-qci66
```

```
subdatastat-downbytefwd-qci69
subdatastat-downbytefwd-qci70
subdatastat-uppktdrop-qci65
subdatastat-uppktdrop-qci66
subdatastat-uppktdrop-qci69
subdatastat-uppktdrop-qci70
subdatastat-upbytedrop-qci65
subdatastat-upbytedrop-qci66
subdatastat-upbytedrop-qci69
subdatastat-upbytedrop-qci70
subdatastat-downpktdrop-qci65
subdatastat-downpktdrop-qci66
subdatastat-downpktdrop-qci69
subdatastat-downpktdrop-qci70
subdatastat-downbytedrop-qci65
subdatastat-downbytedrop-qci66
subdatastat-downbytedrop-qci69
subdatastat-downbytedrop-qci70
subdatastat-uppktdropmbrexc-qci65
subdatastat-uppktdropmbrexc-qci66
subdatastat-uppktdropmbrexc-qci69
subdatastat-uppktdropmbrexc-qci70
subdatastat-upbytedropmbrexc-qci65
subdatastat-upbytedropmbrexc-qci66
subdatastat-upbytedropmbrexc-qci69
subdatastat-upbytedropmbrexc-qci70
subdatastat-downpktdropmbrexc-qci65
subdatastat-downpktdropmbrexc-qci66
subdatastat-downpktdropmbrexc-qci69
subdatastat-downpktdropmbrexc-qci70
subdatastat-downbytedropmbrexc-qci65
subdatastat-downbytedropmbrexc-qci66
subdatastat-downbytedropmbrexc-qci69
subdatastat-downbytedropmbrexc-qci70
```

SAEGW Schema

The following bulk statistics have been added to the SAEGW Schema to support the New Standard QCIs feature.

```
sgw-totepsbearact-qci65
sgw-totepsbearact-qci66
sgw-totepsbearact-qci69
sgw-totepsbearact-qci70
sgw-totepsbearset-qci65
sgw-totepsbearset-qci66
sgw-totepsbearset-qci69
sgw-totepsbearset-qci70
sgw-totepsbearrel-qci65
sgw-totepsbearrel-qci66
sgw-totepsbearrel-qci69
sgw-totepsbearrel-qci70
sgw-totepsbearmod-qci65
sgw-totepsbearmod-qci66
sgw-totepsbearmod-qci69
sgw-totepsbearmod-qci70
sgw-totepsbearrel-dedrsn-pgw-qci65
sgw-totepsbearrel-dedrsn-pgw-qci66
sgw-totepsbearrel-dedrsn-pgw-qci69
sgw-totepsbearrel-dedrsn-pgw-qci70
sgw-totepsbearrel-dedrsn-s1err-qci65
sgw-totepsbearrel-dedrsn-s1err-qci66
sgw-totepsbearrel-dedrsn-s1err-qci69
sgw-totepsbearrel-dedrsn-s1err-qci70
```

```
sgw-totepsbearrel-dedrsn-s5err-qci65
sgw-totepsbearrel-dedrsn-s5err-qci66
sgw-totepsbearrel-dedrsn-s5err-qci69
sgw-totepsbearrel-dedrsn-s5err-qci70
sgw-totepsbearrel-dedrsn-s4err-qci65
sgw-totepsbearrel-dedrsn-s4err-qci66
sgw-totepsbearrel-dedrsn-s4err-qci69
sgw-totepsbearrel-dedrsn-s4err-qci70
sgw-totepsbearrel-dedrsn-s12err-qci65
sgw-totepsbearrel-dedrsn-s12err-qci66
sgw-totepsbearrel-dedrsn-s12err-qci69
sgw-totepsbearrel-dedrsn-s12err-qci70
sgw-totepsbearrel-dedrsn-local-qci65
sgw-totepsbearrel-dedrsn-local-qci66
sgw-totepsbearrel-dedrsn-local-qci69
sgw-totepsbearrel-dedrsn-local-qci70
sgw-totepsbearrel-dedrsn-pdn-qci65
sgw-totepsbearrel-dedrsn-pdn-qci66
sgw-totepsbearrel-dedrsn-pdn-qci69
sgw-totepsbearrel-dedrsn-pdn-qci70
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-qci70
sgw-totepsbearrel-dedrsn-pathfail-s11-qci65
sgw-totepsbearrel-dedrsn-pathfail-s11-qci66
sgw-totepsbearrel-dedrsn-pathfail-s11-qci69
sgw-totepsbearrel-dedrsn-pathfail-s11-qci70
sgw-totepsbearrel-dedrsn-pathfail-s12-qci65
sgw-totepsbearrel-dedrsn-pathfail-s12-qci66
sgw-totepsbearrel-dedrsn-pathfail-s12-qci69
sgw-totepsbearrel-dedrsn-pathfail-s12-qci70
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci70
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci65
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci66
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci69
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci70
sgw-totepsbearrel-dedrsn-other-qci65
sgw-totepsbearrel-dedrsn-other-qci66
sgw-totepsbearrel-dedrsn-other-qci69
sgw-totepsbearrel-dedrsn-other-qci70
sgw-datastat-ul-qci65totbyte
sgw-datastat-ul-qci65totpkt
sgw-datastat-ul-qci66totbyte
sgw-datastat-ul-qci66totpkt
sgw-datastat-ul-qci69totbyte
sgw-datastat-ul-qci69totpkt
sgw-datastat-ul-qci70totbyte
sgw-datastat-ul-qci70totpkt
sgw-datastat-ul-dropstat-qci65totbyte
sgw-datastat-ul-dropstat-qci65totpkt
sgw-datastat-ul-dropstat-qci66totbyte
sgw-datastat-ul-dropstat-qci66totpkt
```

```
sgw-datastat-ul-dropstat-qci69totbyte
sgw-datastat-ul-dropstat-qci69totpkt
sgw-datastat-ul-dropstat-qci70totbyte
sgw-datastat-ul-dropstat-qci70totpkt
sgw-datastat-dl-qci65totbyte
sgw-datastat-dl-qci65totpkt
sgw-datastat-dl-qci66totbyte
sgw-datastat-dl-qci66totpkt
sgw-datastat-dl-qci69totbyte
sgw-datastat-dl-qci69totpkt
sgw-datastat-dl-qci70totbyte
sgw-datastat-dl-qci70totpkt
sgw-datastat-dl-dropstat-qci65totbyte
sgw-datastat-dl-dropstat-qci65totpkt
sgw-datastat-dl-dropstat-qci66totbyte
sgw-datastat-dl-dropstat-qci66totpkt
sgw-datastat-dl-dropstat-qci69totbyte
sgw-datastat-dl-dropstat-qci69totpkt
sgw-datastat-dl-dropstat-qci70totbyte
sgw-datastat-dl-dropstat-qci70totpkt
sgw-s1u-ul-qci65totbyte
sgw-s1u-ul-qci65totpkt
sgw-s1u-ul-qci66totbyte
sgw-s1u-ul-qci66totpkt
sgw-s1u-ul-qci69totbyte
sgw-s1u-ul-qci69totpkt
sgw-s1u-ul-qci70totbyte
sgw-s1u-ul-qci70totpkt
sgw-s1u-ul-drop-qci65totbyte
sgw-s1u-ul-drop-qci65totpkt
sgw-s1u-ul-drop-qci66totbyte
sgw-s1u-ul-drop-qci66totpkt
sgw-s1u-ul-drop-qci69totbyte
sgw-s1u-ul-drop-qci69totpkt
sgw-s1u-ul-drop-qci70totbyte
sgw-s1u-ul-drop-qci70totpkt
sgw-s1u-dl-qci65totbyte
sgw-s1u-dl-qci65totpkt
sgw-s1u-dl-qci66totbyte
sgw-s1u-dl-qci66totpkt
sgw-s1u-dl-qci69totbyte
sgw-s1u-dl-qci69totpkt
sgw-s1u-dl-qci70totbyte
sgw-s1u-dl-qci70totpkt
sgw-s1u-dl-drop-qci65totbyte
sgw-s1u-dl-drop-qci65totpkt
sgw-s1u-dl-drop-qci66totbyte
sgw-s1u-dl-drop-qci66totpkt
sgw-s1u-dl-drop-qci69totbyte
sgw-s1u-dl-drop-qci69totpkt
sgw-s1u-dl-drop-qci70totbyte
sgw-s1u-dl-drop-qci70totpkt
sgw-s4u-ul-qci65totbyte
sgw-s4u-ul-qci65totpkt
sgw-s4u-ul-qci66totbyte
sgw-s4u-ul-qci66totpkt
sgw-s4u-ul-qci69totbyte
sgw-s4u-ul-qci69totpkt
sgw-s4u-ul-qci70totbyte
sgw-s4u-ul-qci70totpkt
sgw-s4u-ul-drop-qci65totbyte
sgw-s4u-ul-drop-qci65totpkt
sgw-s4u-ul-drop-qci66totbyte
sgw-s4u-ul-drop-qci66totpkt
```

```
sgw-s4u-ul-drop-qci69totbyte
sgw-s4u-ul-drop-qci69totpkt
sgw-s4u-ul-drop-qci70totbyte
sgw-s4u-ul-drop-qci70totpkt
sgw-s4u-dl-qci65totbyte
sgw-s4u-dl-qci65totpkt
sgw-s4u-dl-qci66totbyte
sgw-s4u-dl-qci66totpkt
sgw-s4u-dl-qci69totbyte
sgw-s4u-dl-qci69totpkt
sgw-s4u-dl-qci70totbyte
sgw-s4u-dl-qci70totpkt
sgw-s4u-dl-drop-qci65totbyte
sgw-s4u-dl-drop-qci65totpkt
sgw-s4u-dl-drop-qci66totbyte
sgw-s4u-dl-drop-qci66totpkt
sgw-s4u-dl-drop-qci69totbyte
sgw-s4u-dl-drop-qci69totpkt
sgw-s4u-dl-drop-qci70totbyte
sgw-s4u-dl-drop-qci70totpkt
sgw-s12-ul-qci65totbyte
sgw-s12-ul-qci65totpkt
sgw-s12-ul-qci66totbyte
sgw-s12-ul-qci66totpkt
sgw-s12-ul-qci69totbyte
sgw-s12-ul-qci69totpkt
sgw-s12-ul-qci70totbyte
sgw-s12-ul-qci70totpkt
sgw-s12-ul-drop-qci65totbyte
sgw-s12-ul-drop-qci65totpkt
sgw-s12-ul-drop-qci66totbyte
sgw-s12-ul-drop-qci66totpkt
sgw-s12-ul-drop-qci69totbyte
sgw-s12-ul-drop-qci69totpkt
sgw-s12-ul-drop-qci70totbyte
sgw-s12-ul-drop-qci70totpkt
sgw-s12-dl-qci65totbyte
sgw-s12-dl-qci65totpkt
sgw-s12-dl-qci66totbyte
sgw-s12-dl-qci66totpkt
sgw-s12-dl-qci69totbyte
sgw-s12-dl-qci69totpkt
sgw-s12-dl-qci70totbyte
sgw-s12-dl-qci70totpkt
sgw-s12-dl-drop-qci65totbyte
sgw-s12-dl-drop-qci65totpkt
sgw-s12-dl-drop-qci66totbyte
sgw-s12-dl-drop-qci66totpkt
sgw-s12-dl-drop-qci69totbyte
sgw-s12-dl-drop-qci69totpkt
sgw-s12-dl-drop-qci70totbyte
sgw-s12-dl-drop-qci70totpkt
sgw-s5-ul-qci65totbyte
sgw-s5-ul-qci65totpkt
sgw-s5-ul-qci66totbyte
sgw-s5-ul-qci66totpkt
sgw-s5-ul-qci69totbyte
sgw-s5-ul-qci69totpkt
sgw-s5-ul-qci70totbyte
sgw-s5-ul-qci70totpkt
sgw-s5-ul-drop-qci65totbyte
sgw-s5-ul-drop-qci65totpkt
sgw-s5-ul-drop-qci66totbyte
sgw-s5-ul-drop-qci66totpkt
```

```
sgw-s5-ul-drop-qci69totbyte
sgw-s5-ul-drop-qci69totpkt
sgw-s5-ul-drop-qci70totbyte
sgw-s5-ul-drop-qci70totpkt
sgw-s5-dl-qci65totbyte
sgw-s5-dl-qci65totpkt
sgw-s5-dl-qci66totbyte
sgw-s5-dl-qci66totpkt
sgw-s5-dl-qci69totbyte
sgw-s5-dl-qci69totpkt
sgw-s5-dl-qci70totbyte
sgw-s5-dl-qci70totpkt
sgw-s5-dl-drop-qci65totbyte
sgw-s5-dl-drop-qci65totpkt
sgw-s5-dl-drop-qci66totbyte
sgw-s5-dl-drop-qci66totpkt
sgw-s5-dl-drop-qci69totbyte
sgw-s5-dl-drop-qci69totpkt
sgw-s5-dl-drop-qci70totbyte
sgw-s5-dl-drop-qci70totpkt
sgw-s8-ul-qci65totbyte
sgw-s8-ul-qci65totpkt
sgw-s8-ul-qci66totbyte
sgw-s8-ul-qci66totpkt
sgw-s8-ul-qci69totbyte
sgw-s8-ul-qci69totpkt
sgw-s8-ul-qci70totbyte
sgw-s8-ul-qci70totpkt
sgw-s8-ul-drop-qci65totbyte
sgw-s8-ul-drop-qci65totpkt
sgw-s8-ul-drop-qci66totbyte
sgw-s8-ul-drop-qci66totpkt
sgw-s8-ul-drop-qci69totbyte
sgw-s8-ul-drop-qci69totpkt
sgw-s8-ul-drop-qci70totbyte
sgw-s8-ul-drop-qci70totpkt
sgw-s8-dl-qci65totbyte
sgw-s8-dl-qci65totpkt
sgw-s8-dl-qci66totbyte
sgw-s8-dl-qci66totpkt
sgw-s8-dl-qci69totbyte
sgw-s8-dl-qci69totpkt
sgw-s8-dl-qci70totbyte
sgw-s8-dl-qci70totpkt
sgw-s8-dl-drop-qci65totbyte
sgw-s8-dl-drop-qci65totpkt
sgw-s8-dl-drop-qci66totbyte
sgw-s8-dl-drop-qci66totpkt
sgw-s8-dl-drop-qci69totbyte
sgw-s8-dl-drop-qci69totpkt
sgw-s8-dl-drop-qci70totbyte
sgw-s8-dl-drop-qci70totpkt
sgw-s5s8-ul-qci65totbyte
sgw-s5s8-ul-qci65totpkt
sgw-s5s8-ul-qci66totbyte
sgw-s5s8-ul-qci66totpkt
sgw-s5s8-ul-qci69totbyte
sgw-s5s8-ul-qci69totpkt
sgw-s5s8-ul-qci70totbyte
sgw-s5s8-ul-qci70totpkt
sgw-s5s8-ul-drop-qci65totbyte
sgw-s5s8-ul-drop-qci65totpkt
sgw-s5s8-ul-drop-qci66totbyte
sgw-s5s8-ul-drop-qci66totpkt
```

```
sgw-s5s8-ul-drop-qci69totbyte
sgw-s5s8-ul-drop-qci69totpkt
sgw-s5s8-ul-drop-qci70totbyte
sgw-s5s8-ul-drop-qci70totpkt
sgw-s5s8-dl-qci65totbyte
sgw-s5s8-dl-qci65totpkt
sgw-s5s8-dl-qci66totbyte
sgw-s5s8-dl-qci66totpkt
sgw-s5s8-dl-qci69totbyte
sgw-s5s8-dl-qci69totpkt
sgw-s5s8-dl-qci70totbyte
sgw-s5s8-dl-qci70totpkt
sgw-s5s8-dl-drop-qci65totbyte
sgw-s5s8-dl-drop-qci65totpkt
sgw-s5s8-dl-drop-qci66totbyte
sgw-s5s8-dl-drop-qci66totpkt
sgw-s5s8-dl-drop-qci69totbyte
sgw-s5s8-dl-drop-qci69totpkt
sgw-s5s8-dl-drop-qci70totbyte
sgw-s5s8-dl-drop-qci70totpkt
pgw-subqosstat-bearact-qci65
pgw-subqosstat-bearact-qci66
pgw-subqosstat-bearact-qci69
pgw-subqosstat-bearact-qci70
pgw-subqosstat-bearset-qci65
pgw-subqosstat-bearset-qci66
pgw-subqosstat-bearset-qci69
pgw-subqosstat-bearset-qci70
pgw-subqosstat-bearrel-qci65
pgw-subqosstat-bearrel-qci66
pgw-subqosstat-bearrel-qci69
pgw-subqosstat-bearrel-qci70
pgw-subdatastat-ulpktfwd-qci65
pgw-subdatastat-ulpktfwd-qci66
pgw-subdatastat-ulpktfwd-qci69
pgw-subdatastat-ulpktfwd-qci70
pgw-subdatastat-ulbytefwd-qci65
pgw-subdatastat-ulbytefwd-qci66
pgw-subdatastat-ulbytefwd-qci69
pgw-subdatastat-ulbytefwd-qci70
pgw-subdatastat-dlpktfwd-qci65
pgw-subdatastat-dlpktfwd-qci66
pgw-subdatastat-dlpktfwd-qci69
pgw-subdatastat-dlpktfwd-qci70
pgw-subdatastat-dlbytefwd-qci65
pgw-subdatastat-dlbytefwd-qci66
pgw-subdatastat-dlbytefwd-qci69
pgw-subdatastat-dlbytefwd-qci70
pgw-subdatastat-ulpktdrop-qci65
pgw-subdatastat-ulpktdrop-qci66
pgw-subdatastat-ulpktdrop-qci69
pgw-subdatastat-ulpktdrop-qci70
pgw-subdatastat-ulbytedrop-qci65
pgw-subdatastat-ulbytedrop-qci66
pgw-subdatastat-ulbytedrop-qci69
pgw-subdatastat-ulbytedrop-qci70
pgw-subdatastat-dlpktdrop-qci65
pgw-subdatastat-dlpktdrop-qci66
pgw-subdatastat-dlpktdrop-qci69
pgw-subdatastat-dlpktdrop-qci70
pgw-subdatastat-dlbytedrop-qci65
pgw-subdatastat-dlbytedrop-qci66
pgw-subdatastat-dlbytedrop-qci69
pgw-subdatastat-dlbytedrop-qci70
```

pgw-subdatastat-ulpktdropmbrexc-qci65
pgw-subdatastat-ulpktdropmbrexc-qci66
pgw-subdatastat-ulpktdropmbrexc-qci69
pgw-subdatastat-ulpktdropmbrexc-qci70
pgw-subdatastat-ulbytedropmbrexc-qci65
pgw-subdatastat-ulbytedropmbrexc-qci66
pgw-subdatastat-ulbytedropmbrexc-qci69
pgw-subdatastat-ulbytedropmbrexc-qci70
pgw-subdatastat-dlpktdropmbrexc-qci65
pgw-subdatastat-dlpktdropmbrexc-qci66
pgw-subdatastat-dlpktdropmbrexc-qci69
pgw-subdatastat-dlpktdropmbrexc-qci70
pgw-subdatastat-dlbytedropmbrexc-qci65
pgw-subdatastat-dlbytedropmbrexc-qci66
pgw-subdatastat-dlbytedropmbrexc-qci69
pgw-subdatastat-dlbytedropmbrexc-qci70
collapsed-subdatastat-ulpktfwd-qci65
collapsed-subdatastat-ulpktfwd-qci66
collapsed-subdatastat-ulpktfwd-qci69
collapsed-subdatastat-ulpktfwd-qci70
collapsed-subdatastat-ulbytefwd-qci65
collapsed-subdatastat-ulbytefwd-qci66
collapsed-subdatastat-ulbytefwd-qci69
collapsed-subdatastat-ulbytefwd-qci70
collapsed-subdatastat-dlpktfwd-qci65
collapsed-subdatastat-dlpktfwd-qci66
collapsed-subdatastat-dlpktfwd-qci69
collapsed-subdatastat-dlpktfwd-qci70
collapsed-subdatastat-dlbytefwd-qci65
collapsed-subdatastat-dlbytefwd-qci66
collapsed-subdatastat-dlbytefwd-qci69
collapsed-subdatastat-dlbytefwd-qci70
collapsed-subdatastat-ulpktdrop-qci65
collapsed-subdatastat-ulpktdrop-qci66
collapsed-subdatastat-ulpktdrop-qci69
collapsed-subdatastat-ulpktdrop-qci70
collapsed-subdatastat-ulbytedrop-qci65
collapsed-subdatastat-ulbytedrop-qci66
collapsed-subdatastat-ulbytedrop-qci69
collapsed-subdatastat-ulbytedrop-qci70
collapsed-subdatastat-dlpktdrop-qci65
collapsed-subdatastat-dlpktdrop-qci66
collapsed-subdatastat-dlpktdrop-qci69
collapsed-subdatastat-dlpktdrop-qci70
collapsed-subdatastat-dlbytedrop-qci65
collapsed-subdatastat-dlbytedrop-qci66
collapsed-subdatastat-dlbytedrop-qci69
collapsed-subdatastat-dlbytedrop-qci70
collapsed-subqosstat-bearact-qci65
collapsed-subqosstat-bearact-qci66
collapsed-subqosstat-bearact-qci69
collapsed-subqosstat-bearact-qci70
collapsed-subqosstat-bearset-qci65
collapsed-subqosstat-bearset-qci66
collapsed-subqosstat-bearset-qci69
collapsed-subqosstat-bearset-qci70
collapsed-subqosstat-bearrel-qci65
collapsed-subqosstat-bearrel-qci66
collapsed-subqosstat-bearrel-qci69
collapsed-subqosstat-bearrel-qci70
saegw-ggsn-subqosstat-bearact-qci65
saegw-ggsn-subqosstat-bearact-qci66
saegw-ggsn-subqosstat-bearact-qci69
saegw-ggsn-subqosstat-bearact-qci70

```
saegw-ggsn-subqosstat-bearset-qci65
saegw-ggsn-subqosstat-bearset-qci66
saegw-ggsn-subqosstat-bearset-qci69
saegw-ggsn-subqosstat-bearset-qci70
saegw-ggsn-subqosstat-bearrel-qci65
saegw-ggsn-subqosstat-bearrel-qci66
saegw-ggsn-subqosstat-bearrel-qci69
saegw-ggsn-subqosstat-bearrel-qci70
saegw-ggsn-subdatastat-ulpktfwd-qci65
saegw-ggsn-subdatastat-ulpktfwd-qci66
saegw-ggsn-subdatastat-ulpktfwd-qci69
saegw-ggsn-subdatastat-ulpktfwd-qci70
saegw-ggsn-subdatastat-ulbytefwd-qci65
saegw-ggsn-subdatastat-ulbytefwd-qci66
saegw-ggsn-subdatastat-ulbytefwd-qci69
saegw-ggsn-subdatastat-ulbytefwd-qci70
saegw-ggsn-subdatastat-dlpktfwd-qci65
saegw-ggsn-subdatastat-dlpktfwd-qci66
saegw-ggsn-subdatastat-dlpktfwd-qci69
saegw-ggsn-subdatastat-dlpktfwd-qci70
saegw-ggsn-subdatastat-dlbytefwd-qci65
saegw-ggsn-subdatastat-dlbytefwd-qci66
saegw-ggsn-subdatastat-dlbytefwd-qci69
saegw-ggsn-subdatastat-dlbytefwd-qci70
saegw-ggsn-subdatastat-ulpktdrop-qci65
saegw-ggsn-subdatastat-ulpktdrop-qci66
saegw-ggsn-subdatastat-ulpktdrop-qci69
saegw-ggsn-subdatastat-ulpktdrop-qci70
saegw-ggsn-subdatastat-ulbytedrop-qci65
saegw-ggsn-subdatastat-ulbytedrop-qci66
saegw-ggsn-subdatastat-ulbytedrop-qci69
saegw-ggsn-subdatastat-ulbytedrop-qci70
saegw-ggsn-subdatastat-dlpktdrop-qci65
saegw-ggsn-subdatastat-dlpktdrop-qci66
saegw-ggsn-subdatastat-dlpktdrop-qci69
saegw-ggsn-subdatastat-dlpktdrop-qci70
saegw-ggsn-subdatastat-dlbytedrop-qci65
saegw-ggsn-subdatastat-dlbytedrop-qci66
saegw-ggsn-subdatastat-dlbytedrop-qci69
saegw-ggsn-subdatastat-dlbytedrop-qci70
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci65
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci66
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci69
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci70
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci65
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci66
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci69
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci70
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci65
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci66
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci69
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci70
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci65
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci66
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci69
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci70
```

S-GW Schema

The following bulk statistics have been added to the S-GW schema to support the New Standard QCIs feature.

```
totepsbearactive-qci65
totepsbearactive-qci66
totepsbearactive-qci69
```

```
totepsbearactive-qci70
totepsbearsetup-qci65
totepsbearsetup-qci66
totepsbearsetup-qci69
totepsbearsetup-qci70
totepsbearrel-qci65
totepsbearrel-qci66
totepsbearrel-qci69
totepsbearrel-qci70
totepsbearmod-qci65
totepsbearmod-qci66
totepsbearmod-qci69
totepsbearmod-qci70
totepsbearrel-dedrsn-pgw-qci65
totepsbearrel-dedrsn-pgw-qci66
totepsbearrel-dedrsn-pgw-qci69
totepsbearrel-dedrsn-pgw-qci70
totepsbearrel-dedrsn-s1err-qci65
totepsbearrel-dedrsn-s1err-qci66
totepsbearrel-dedrsn-s1err-qci69
totepsbearrel-dedrsn-s1err-qci70
totepsbearrel-dedrsn-s5err-qci65
totepsbearrel-dedrsn-s5err-qci66
totepsbearrel-dedrsn-s5err-qci69
totepsbearrel-dedrsn-s5err-qci70
totepsbearrel-dedrsn-s4err-qci65
totepsbearrel-dedrsn-s4err-qci66
totepsbearrel-dedrsn-s4err-qci69
totepsbearrel-dedrsn-s4err-qci70
totepsbearrel-dedrsn-s12err-qci65
totepsbearrel-dedrsn-s12err-qci66
totepsbearrel-dedrsn-s12err-qci69
totepsbearrel-dedrsn-s12err-qci70
totepsbearrel-dedrsn-local-qci65
totepsbearrel-dedrsn-local-qci66
totepsbearrel-dedrsn-local-qci69
totepsbearrel-dedrsn-local-qci70
totepsbearrel-dedrsn-pdn-qci65
totepsbearrel-dedrsn-pdn-qci66
totepsbearrel-dedrsn-pdn-qci69
totepsbearrel-dedrsn-pdn-qci70
totepsbearrel-dedrsn-pathfail-s1-u-qci65
totepsbearrel-dedrsn-pathfail-s1-u-qci66
totepsbearrel-dedrsn-pathfail-s1-u-qci69
totepsbearrel-dedrsn-pathfail-s1-u-qci70
totepsbearrel-dedrsn-pathfail-s5-u-qci65
totepsbearrel-dedrsn-pathfail-s5-u-qci66
totepsbearrel-dedrsn-pathfail-s5-u-qci69
totepsbearrel-dedrsn-pathfail-s5-u-qci70
totepsbearrel-dedrsn-pathfail-s5-qci65
totepsbearrel-dedrsn-pathfail-s5-qci66
totepsbearrel-dedrsn-pathfail-s5-qci69
totepsbearrel-dedrsn-pathfail-s5-qci70
totepsbearrel-dedrsn-pathfail-s11-qci65
totepsbearrel-dedrsn-pathfail-s11-qci66
totepsbearrel-dedrsn-pathfail-s11-qci69
totepsbearrel-dedrsn-pathfail-s11-qci70
totepsbearrel-dedrsn-pathfail-s12-qci65
totepsbearrel-dedrsn-pathfail-s12-qci66
totepsbearrel-dedrsn-pathfail-s12-qci69
totepsbearrel-dedrsn-pathfail-s12-qci70
totepsbearrel-dedrsn-pathfail-s4-u-qci65
totepsbearrel-dedrsn-pathfail-s4-u-qci66
totepsbearrel-dedrsn-pathfail-s4-u-qci69
```

```
totepsbearrel-dedrsn-pathfail-s4-u-qci70
totepsbearrel-dedrsn-inactivity-timeout-qci65
totepsbearrel-dedrsn-inactivity-timeout-qci66
totepsbearrel-dedrsn-inactivity-timeout-qci69
totepsbearrel-dedrsn-inactivity-timeout-qci70
totepsbearrel-dedrsn-other-qci65
totepsbearrel-dedrsn-other-qci66
totepsbearrel-dedrsn-other-qci69
totepsbearrel-dedrsn-other-qci70
datastat-uplink-qci65totbyte
datastat-uplink-qci65totpkt
datastat-uplink-qci66totbyte
datastat-uplink-qci66totpkt
datastat-uplink-qci69totbyte
datastat-uplink-qci69totpkt
datastat-uplink-qci70totbyte
datastat-uplink-qci70totpkt
datastat-uplink-dropstat-qci65totbyte
datastat-uplink-dropstat-qci65totpkt
datastat-uplink-dropstat-qci66totbyte
datastat-uplink-dropstat-qci66totpkt
datastat-uplink-dropstat-qci69totbyte
datastat-uplink-dropstat-qci69totpkt
datastat-uplink-dropstat-qci70totbyte
datastat-uplink-dropstat-qci70totpkt
datastat-downlink-qci65totbyte
datastat-downlink-qci65totpkt
datastat-downlink-qci66totbyte
datastat-downlink-qci66totpkt
datastat-downlink-qci69totbyte
datastat-downlink-qci69totpkt
datastat-downlink-qci70totbyte
datastat-downlink-qci70totpkt
datastat-downlink-dropstat-qci65totbyte
datastat-downlink-dropstat-qci65totpkt
datastat-downlink-dropstat-qci66totbyte
datastat-downlink-dropstat-qci66totpkt
datastat-downlink-dropstat-qci69totbyte
datastat-downlink-dropstat-qci69totpkt
datastat-downlink-dropstat-qci70totbyte
datastat-downlink-dropstat-qci70totpkt
s1u-uplnk-qci65totbyte
s1u-uplnk-qci65totpkt
s1u-uplnk-qci66totbyte
s1u-uplnk-qci66totpkt
s1u-uplnk-qci69totbyte
s1u-uplnk-qci69totpkt
s1u-uplnk-qci70totbyte
s1u-uplnk-qci70totpkt
s1u-uplnk-drop-qci65totbyte
s1u-uplnk-drop-qci65totpkt
s1u-uplnk-drop-qci66totbyte
s1u-uplnk-drop-qci66totpkt
s1u-uplnk-drop-qci69totbyte
s1u-uplnk-drop-qci69totpkt
s1u-uplnk-drop-qci70totbyte
s1u-uplnk-drop-qci70totpkt
s1u-downlnk-qci65totbyte
s1u-downlnk-qci65totpkt
s1u-downlnk-qci66totbyte
s1u-downlnk-qci66totpkt
s1u-downlnk-qci69totbyte
s1u-downlnk-qci69totpkt
s1u-downlnk-qci70totbyte
```

```
s1u-downlnk-qci70totpkt
s1u-downlnk-drop-qci65totbyte
s1u-downlnk-drop-qci65totpkt
s1u-downlnk-drop-qci66totbyte
s1u-downlnk-drop-qci66totpkt
s1u-downlnk-drop-qci69totbyte
s1u-downlnk-drop-qci69totpkt
s1u-downlnk-drop-qci70totbyte
s1u-downlnk-drop-qci70totpkt
s4u-uplnk-qci65totbyte
s4u-uplnk-qci65totpkt
s4u-uplnk-qci66totbyte
s4u-uplnk-qci66totpkt
s4u-uplnk-qci69totbyte
s4u-uplnk-qci69totpkt
s4u-uplnk-qci70totbyte
s4u-uplnk-qci70totpkt
s4u-uplnk-drop-qci65totbyte
s4u-uplnk-drop-qci65totpkt
s4u-uplnk-drop-qci66totbyte
s4u-uplnk-drop-qci66totpkt
s4u-uplnk-drop-qci69totbyte
s4u-uplnk-drop-qci69totpkt
s4u-uplnk-drop-qci70totbyte
s4u-uplnk-drop-qci70totpkt
s4u-downlnk-qci65totbyte
s4u-downlnk-qci65totpkt
s4u-downlnk-qci66totbyte
s4u-downlnk-qci66totpkt
s4u-downlnk-qci69totbyte
s4u-downlnk-qci69totpkt
s4u-downlnk-qci70totbyte
s4u-downlnk-qci70totpkt
s4u-downlnk-drop-qci65totbyte
s4u-downlnk-drop-qci65totpkt
s4u-downlnk-drop-qci66totbyte
s4u-downlnk-drop-qci66totpkt
s4u-downlnk-drop-qci69totbyte
s4u-downlnk-drop-qci69totpkt
s4u-downlnk-drop-qci70totbyte
s4u-downlnk-drop-qci70totpkt
s12-uplnk-qci65totbyte
s12-uplnk-qci65totpkt
s12-uplnk-qci66totbyte
s12-uplnk-qci66totpkt
s12-uplnk-qci69totbyte
s12-uplnk-qci69totpkt
s12-uplnk-qci70totbyte
s12-uplnk-qci70totpkt
s12-uplnk-drop-qci65totbyte
s12-uplnk-drop-qci65totpkt
s12-uplnk-drop-qci66totbyte
s12-uplnk-drop-qci66totpkt
s12-uplnk-drop-qci69totbyte
s12-uplnk-drop-qci69totpkt
s12-uplnk-drop-qci70totbyte
s12-uplnk-drop-qci70totpkt
s12-downlnk-qci65totbyte
s12-downlnk-qci65totpkt
s12-downlnk-qci66totbyte
s12-downlnk-qci66totpkt
s12-downlnk-qci69totbyte
s12-downlnk-qci69totpkt
s12-downlnk-qci70totbyte
```

```
s12-downlnk-qci70totpkt
s12-downlnk-drop-qci65totbyte
s12-downlnk-drop-qci65totpkt
s12-downlnk-drop-qci66totbyte
s12-downlnk-drop-qci66totpkt
s12-downlnk-drop-qci69totbyte
s12-downlnk-drop-qci69totpkt
s12-downlnk-drop-qci70totbyte
s12-downlnk-drop-qci70totpkt
s5-uplnk-qci65totbyte
s5-uplnk-qci65totpkt
s5-uplnk-qci66totbyte
s5-uplnk-qci66totpkt
s5-uplnk-qci69totbyte
s5-uplnk-qci69totpkt
s5-uplnk-qci70totbyte
s5-uplnk-qci70totpkt
s5-uplnk-drop-qci65totbyte
s5-uplnk-drop-qci65totpkt
s5-uplnk-drop-qci66totbyte
s5-uplnk-drop-qci66totpkt
s5-uplnk-drop-qci69totbyte
s5-uplnk-drop-qci69totpkt
s5-uplnk-drop-qci70totbyte
s5-uplnk-drop-qci70totpkt
s5-downlnk-qci65totbyte
s5-downlnk-qci65totpkt
s5-downlnk-qci66totbyte
s5-downlnk-qci66totpkt
s5-downlnk-qci69totbyte
s5-downlnk-qci69totpkt
s5-downlnk-qci70totbyte
s5-downlnk-qci70totpkt
s5-downlnk-drop-qci65totbyte
s5-downlnk-drop-qci65totpkt
s5-downlnk-drop-qci66totbyte
s5-downlnk-drop-qci66totpkt
s5-downlnk-drop-qci69totbyte
s5-downlnk-drop-qci69totpkt
s5-downlnk-drop-qci70totbyte
s5-downlnk-drop-qci70totpkt
s8-uplnk-qci65totbyte
s8-uplnk-qci65totpkt
s8-uplnk-qci66totbyte
s8-uplnk-qci66totpkt
s8-uplnk-qci69totbyte
s8-uplnk-qci69totpkt
s8-uplnk-qci70totbyte
s8-uplnk-qci70totpkt
s8-uplnk-drop-qci65totbyte
s8-uplnk-drop-qci65totpkt
s8-uplnk-drop-qci66totbyte
s8-uplnk-drop-qci66totpkt
s8-uplnk-drop-qci69totbyte
s8-uplnk-drop-qci69totpkt
s8-uplnk-drop-qci70totbyte
s8-uplnk-drop-qci70totpkt
s8-downlnk-qci65totbyte
s8-downlnk-qci65totpkt
s8-downlnk-qci66totbyte
s8-downlnk-qci66totpkt
s8-downlnk-qci69totbyte
s8-downlnk-qci69totpkt
s8-downlnk-qci70totbyte
```

```
s8-downlnk-qci70totpkt
s8-downlnk-drop-qci65totbyte
s8-downlnk-drop-qci65totpkt
s8-downlnk-drop-qci66totbyte
s8-downlnk-drop-qci66totpkt
s8-downlnk-drop-qci69totbyte
s8-downlnk-drop-qci69totpkt
s8-downlnk-drop-qci70totbyte
s8-downlnk-drop-qci70totpkt
s5s8-uplnk-qci65totbyte
s5s8-uplnk-qci65totpkt
s5s8-uplnk-qci66totbyte
s5s8-uplnk-qci66totpkt
s5s8-uplnk-qci69totbyte
s5s8-uplnk-qci69totpkt
s5s8-uplnk-qci70totbyte
s5s8-uplnk-qci70totpkt
s5s8-uplnk-drop-qci65totbyte
s5s8-uplnk-drop-qci65totpkt
s5s8-uplnk-drop-qci66totbyte
s5s8-uplnk-drop-qci66totpkt
s5s8-uplnk-drop-qci69totbyte
s5s8-uplnk-drop-qci69totpkt
s5s8-uplnk-drop-qci70totbyte
s5s8-uplnk-drop-qci70totpkt
s5s8-downlnk-qci65totbyte
s5s8-downlnk-qci65totpkt
s5s8-downlnk-qci66totbyte
s5s8-downlnk-qci66totpkt
s5s8-downlnk-qci69totbyte
s5s8-downlnk-qci69totpkt
s5s8-downlnk-qci70totbyte
s5s8-downlnk-qci70totpkt
s5s8-downlnk-drop-qci65totbyte
s5s8-downlnk-drop-qci65totpkt
s5s8-downlnk-drop-qci66totbyte
s5s8-downlnk-drop-qci66totpkt
s5s8-downlnk-drop-qci69totbyte
s5s8-downlnk-drop-qci69totpkt
s5s8-downlnk-drop-qci70totbyte
s5s8-downlnk-drop-qci70totpkt
```

System Schema

The following bulk statistics have been added to the System Schema to support the New Standard QCIs feature.

```
sess-bearerdur-5sec-qci65
sess-bearerdur-10sec-qci65
sess-bearerdur-30sec-qci65
sess-bearerdur-1min-qci65
sess-bearerdur-2min-qci65
sess-bearerdur-5min-qci65
sess-bearerdur-15min-qci65
sess-bearerdur-30min-qci65
sess-bearerdur-1hr-qci65
sess-bearerdur-4hr-qci65
sess-bearerdur-12hr-qci65
sess-bearerdur-24hr-qci65
sess-bearerdur-over24hr-qci65
sess-bearerdur-2day-qci65
sess-bearerdur-4day-qci65
sess-bearerdur-5day-qci65
sess-bearerdur-5sec-qci66
```

```
sess-bearerdur-10sec-qci66
sess-bearerdur-30sec-qci66
sess-bearerdur-1min-qci66
sess-bearerdur-2min-qci66
sess-bearerdur-5min-qci66
sess-bearerdur-15min-qci66
sess-bearerdur-30min-qci66
sess-bearerdur-1hr-qci66
sess-bearerdur-4hr-qci66
sess-bearerdur-12hr-qci66
sess-bearerdur-24hr-qci66
sess-bearerdur-over24hr-qci66
sess-bearerdur-2day-qci66
sess-bearerdur-4day-qci66
sess-bearerdur-5day-qci66
sess-bearerdur-5sec-qci69
sess-bearerdur-10sec-qci69
sess-bearerdur-30sec-qci69
sess-bearerdur-1min-qci69
sess-bearerdur-2min-qci69
sess-bearerdur-5min-qci69
sess-bearerdur-15min-qci69
sess-bearerdur-30min-qci69
sess-bearerdur-1hr-qci69
sess-bearerdur-4hr-qci69
sess-bearerdur-12hr-qci69
sess-bearerdur-24hr-qci69
sess-bearerdur-over24hr-qci69
sess-bearerdur-2day-qci69
sess-bearerdur-4day-qci69
sess-bearerdur-5day-qci69
sess-bearerdur-5sec-qci70
sess-bearerdur-10sec-qci70
sess-bearerdur-30sec-qci70
sess-bearerdur-1min-qci70
sess-bearerdur-2min-qci70
sess-bearerdur-5min-qci70
sess-bearerdur-15min-qci70
sess-bearerdur-30min-qci70
sess-bearerdur-1hr-qci70
sess-bearerdur-4hr-qci70
sess-bearerdur-12hr-qci70
sess-bearerdur-24hr-qci70
sess-bearerdur-over24hr-qci70
sess-bearerdur-2day-qci70
sess-bearerdur-4day-qci70
sess-bearerdur-5day-qci70
```

Show Commands

This section describes the show commands available to monitor the New Standard QCIs feature.

show apn statistics all

The output of this command has been enhanced to show administrative disconnects and bearer statistics for the new standard QCIs 65, 66, 69, and 70. New statistics are highlighted in *italics*.

```
...

4G Bearers Released By Reasons:

                     QCI1   QCI2   QCI3   QCI4   QCI5   QCI6   QCI7   QCI8   QCI9
   Admin disconnect:  0          0          0      0      0      0      0      0
```

```
                     QCI65      QCI66      QCI69      QCI70
  Admin disconnect:         0          0          0          0
...

  QCI 65:
    Bearer Active:                  0   Bearer setup:                          0
    Bearer Released:                0   Bearer Rejected:                       0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:              0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:               0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                0
    Uplink pkts dropped:            0   Downlink pkts dropped:                 0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 66:
    Bearer Active:                  0   Bearer setup:                          0
    Bearer Released:                0   Bearer Rejected:                       0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:              0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:               0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                0
    Uplink pkts dropped:            0   Downlink pkts dropped:                 0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 69:
    Bearer Active:                  0   Bearer setup:                          0
    Bearer Released:                0   Bearer Rejected:                       0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:              0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:               0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                0
    Uplink pkts dropped:            0   Downlink pkts dropped:                 0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0

  QCI 70:
    Bearer Active:                  0   Bearer setup:                          0
    Bearer Released:                0   Bearer Rejected:                       0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:              0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:               0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                0
    Uplink pkts dropped:            0   Downlink pkts dropped:                 0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):       0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):        0
                      0
...
```

show gtpu statistics

The output of this command has been enhanced to provide packet and byte information for QCI values 65, 66, 69, and 70. New statistics are in *italics*.

```
...
    QCI 9:
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0

    QCI 65:
         Uplink Packets:              0  Uplink Bytes:                0
```

```
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0

    QCI 66:
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0


    QCI 69:
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0

    QCI 70:
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0

    Non-Std QCI(Non-GBR):
         Uplink Packets:              0  Uplink Bytes:                0
         Downlink Packets:            0  Downlink Bytes:              0
         Packets Discarded:           0  Bytes Discarded:             0
...
```

show pgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information by QoS characteristics and IPv4v6 PDN Data statistics. New statistics are in *italics*.

```
Bearers By QoS characteristics:
  Active:                                    Setup:
    QCI 1:                              0      QCI 1:                           0
...
    QCI 65:                          0      QCI 65:                          0
    QCI 66:                             0      QCI 66:                          0
    QCI 69:                             0      QCI 69:                          0
    QCI 70:                             0      QCI 70:                          0
...

  Released:
    QCI 1:                              0
...
    QCI 65:                             0
    QCI 66:                             0
    QCI 69:                             0
    QCI 70:                             0
...

  IPv4v6 PDN Data Statistics:
    Uplink :                                 Downlink :
...
      Packets:                                 Packets:
        QCI 1:                          0        QCI 1:                           0
...
        QCI 65:                      0        QCI 65:                          0
        QCI 66:                             0        QCI 66:                          0
        QCI 69:                             0        QCI 69:                          0
        QCI 70:                             0        QCI 70:                          0
```

show saegw-service statistics all verbose

The output of this command has been enhanced to provide information related to the new standard QCIs. New statistics are in *italics*.

```
...

Bearers By QoS characteristics:
  Active:                                  Setup:
    QCI  1:                          0      QCI  1:                          0
    ...
    QCI  9:                          0      QCI  9:                          0
    QCI 65:                          0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0
  Released:
    QCI  1:                          0
   ...
    QCI  9:                          0
    QCI 65:                          0
    QCI 66:                          0
    QCI 69:                          0
    QCI 70:                          0
    Non-Std QCI:                     0

…
      Std QCI(Non-GBR):              0      Std QCI(Non-GBR):              0
      Std QCI(GBR):                  0      Std QCI(GBR):                  0

    Uplink :                                 Downlink :
      Packets:                                 Packets:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Bytes:                                   Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Dropped Packets:                         Dropped Packets:
        QCI 1:                       0          QCI 1:                       0\
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
        QCI 69:                      0          QCI 69:                      0
        QCI 70:                      0          QCI 70:                      0
        Non-Std QCI:                 0          Non-Std QCI:                 0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                      0          QCI 66:                      0
```

```
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0
Setup Guard Timer Expired:        0
```

show sgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information. New statistics are highlighted in *italics*.

```
...

Bearers By QoS characteristics:
  Active:                                 Setup:
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                     0       QCI 65:                         0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
...

  Released:                               Modified:
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                     0       QCI 65:                         0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
...

Dedicated Bearers Released By Reason:
  PGW Ini:                          0     PCRF Ini:                         0
    QCI 1:                          0
...
    QCI 65:                     0
    QCI 66:                         0
    QCI 69:                         0
    QCI 70:                         0
    Non-Std QCI:                    0
...
  S1 Error Ind:                     0     S5 Error Ind:                     0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                     0       QCI 65:                         0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
    Non-Std QCI:                    0       Non-Std QCI:                    0

  S4 Error Ind:                     0     S12 Error Ind:                    0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                     0       QCI 65:                         0
    QCI 66:                         0       QCI 66:                         0
    QCI 69:                         0       QCI 69:                         0
    QCI 70:                         0       QCI 70:                         0
    Non-Std QCI:                    0       Non-Std QCI:                    0

  Local:                            0     PDN Down:                         0
    QCI 1:                          0       QCI 1:                          0
...
    QCI 65:                     0       QCI 65:                         0
    QCI 66:                         0       QCI 66:                         0
```

```
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S1-U:                 0    Path Failure S5-U:                 0
    QCI 1:                           0      QCI 1:                           0
    ...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S5:                   0    Path Failure S11:                  0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Path Failure S4-U:                 0    Path Failure S12:                  0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Inactivity Timeout:                0    Other:                             0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                    0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

 ...
 Data Statistics Per Interface:
  S1-U Total Data Statistics:
    Uplink :                           Downlink :
...
      Packets:                           Packets:
        QCI 1:                       0      QCI 1:                           0
...
        QCI 65:                    0      QCI 65:                          0
        QCI 66:                          0      QCI 66:                          0
        QCI 69:                          0      QCI 69:                          0
        QCI 70:                          0      QCI 70:                          0
        Non-Std QCI:                     0      Non-Std QCI:                     0

      Bytes:                             Bytes:
        QCI 1:                       0      QCI 1:                           0
...
        QCI 65:                    0      QCI 65:                          0
        QCI 66:                          0      QCI 66:                          0
        QCI 69:                          0      QCI 69:                          0
        QCI 70:                          0      QCI 70:                          0
        Non-Std QCI:                     0      Non-Std QCI:                     0

      Dropped Packets:                   Dropped Packets:
```

```
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S4-U Total Data Statistics:
    Uplink :                              Downlink :
      Total Pkts:                     0      Total Pkts:                     0
      Total Bytes:                    0      Total Bytes:                    0
      Dropped Pkts:                   0      Dropped Pkts:                   0
      Dropped Bytes:                  0      Dropped Bytes:                  0

      Packets:                                Packets:
        QCI 1:                        0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Bytes:                                  Bytes:
        QCI 1:                        0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Packets:                        Dropped Packets:
        QCI 1:                        0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                        0        QCI 1:                          0
...
        QCI 65:                     0        QCI 65:                         0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S12 Total Data Statistics:
    Uplink :                              Downlink :
      Total Pkts:                     0      Total Pkts:                     0
      Total Bytes:                    0      Total Bytes:                    0
```

```
      Dropped Pkts:                    0      Dropped Pkts:                    0
      Dropped Bytes:                   0      Dropped Bytes:                   0

      Packets:                                Packets:
        QCI 1:                         0        QCI 1:                         0
...
        QCI 65:                    0         QCI 65:                    0
        QCI 66:                        0         QCI 66:                        0
        QCI 69:                        0         QCI 69:                        0
        QCI 70:                        0         QCI 70:                        0
        Non-Std QCI:                   0         Non-Std QCI:                   0

      Bytes:                                  Bytes:
        QCI 1:                         0        QCI 1:                         0
...
        QCI 65:                    0         QCI 65:                    0
        QCI 66:                        0         QCI 66:                        0
        QCI 69:                        0         QCI 69:                        0
        QCI 70:                        0         QCI 70:                        0
        Non-Std QCI:                   0         Non-Std QCI:                   0

      Dropped Packets:                        Dropped Packets:
        QCI 1:                         0        QCI 1:                         0
...
        QCI 65:                    0         QCI 65:                    0
        QCI 66:                        0         QCI 66:                        0
        QCI 69:                        0         QCI 69:                        0
        QCI 70:                        0         QCI 70:                        0
        Non-Std QCI:                   0         Non-Std QCI:                   0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                         0        QCI 1:                         0
...
        QCI 65:                    0         QCI 65:                    0
        QCI 66:                        0         QCI 66:                        0
        QCI 69:                        0         QCI 69:                        0
        QCI 70:                        0         QCI 70:                        0
        Non-Std QCI:                   0         Non-Std QCI:                   0

    S5-U Total Data Statistics:
      Uplink :                                Downlink :
        Total Pkts:                    0        Total Pkts:                    0
        Total Bytes:                   0        Total Bytes:                   0
        Dropped Pkts:                  0        Dropped Pkts:                  0
        Dropped Bytes:                 0        Dropped Bytes:                 0

        Packets:                                Packets:
          QCI 1:                       0          QCI 1:                       0
...
          QCI 65:                  0           QCI 65:                  0
          QCI 66:                      0           QCI 66:                      0
          QCI 69:                      0           QCI 69:                      0
          QCI 70:                      0           QCI 70:                      0
          Non-Std QCI:                 0           Non-Std QCI:                 0

        Bytes:                                  Bytes:
          QCI 1:                       0          QCI 1:                       0
...
          QCI 65:                  0           QCI 65:                  0
          QCI 66:                      0           QCI 66:                      0
          QCI 69:                      0           QCI 69:                      0
          QCI 70:                      0           QCI 70:                      0
          Non-Std QCI:                 0           Non-Std QCI:                 0
```

```
      Dropped Packets:                          Dropped Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0

      Dropped Bytes:                            Dropped Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0

  S8-U Total Data Statistics:
    Uplink :                                Downlink :
      Total Pkts:                       0     Total Pkts:                       0
      Total Bytes:                      0     Total Bytes:                      0
      Dropped Pkts:                     0     Dropped Pkts:                     0
      Dropped Bytes:                    0     Dropped Bytes:                    0

      Packets:                                  Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0

      Bytes:                                    Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0

      Dropped Packets:                          Dropped Packets:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0

      Dropped Bytes:                            Dropped Bytes:
        QCI 1:                          0         QCI 1:                          0
...
        QCI 65:                         0       QCI 65:                           0
        QCI 66:                             0       QCI 66:                           0
        QCI 69:                             0       QCI 69:                           0
        QCI 70:                             0       QCI 70:                           0
        Non-Std QCI:                        0       Non-Std QCI:                      0
```

Non-standard QCI Support

This section describes the Non-standard QCI Support feature.

Feature Description

Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. A license, however, allows non-standard QCIs (128-254) to be used on P-GW/GGSN (not standalone GGSN).

Licensing

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128-254. QCI values 0 and 10 to 255 are defined as follows:

- 0: Reserved
- 10-127: Reserved
- 128-254: Operator-specific/Non-standard QCI
- 255: Reserved

Unique operator-specific QCIs (128-254) can be used to differentiate between various services/applications carriers provide to the end users in their network.

Limitations

- Non-standard QCIs can only be supported with S5/S8/S2a/S2b interfaces.
- The Gn interface is not supported.

Standards Compliance

- 3GPP Specification TS 23.203: Policy and charging control architecture
- 3GPP Specification TS 29.212: Policy and Charging Control over Gx reference point

Configuring Non-standard QCI Support

The **operator-defined-qci** command in the QCI-QoS Mapping Configuration Mode configures the non-standard QCIs in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF. Unique DSCP parameters (uplink and downlink) and GBR or Non-GBR can also be configured.

As non-standard QCIs are not supported in GGSN, **pre-rel8-qos-mapping** is used as a reference for mapping the non-standard QCI values to pre-rel8 QoS values during 3G calls or GnGp handovers.

Configuring Non-standard QCI Support in P-GW

Use the following command to configure non-standard QCI support in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF.

```
configure
    qci-qos-mapping name
         operator-defined-qci num { gbr | non-gbr } [ { downlink |
uplink } [ encaps-header { copy-inner | copy-outer | dscp-marking
dscp-marking-value } [ internal-qos priority priority ] | internal-qos priority
 priority | user-datagram dscp-marking dscp-marking-value [ encaps-header {
copy-inner | copy-outer | dscp-marking dscp-marking-value } [ internal-qos
priority priority ] ] | pre-rel8-qos-mapping num ]
         no operator-defined-qci num
         end
```

Notes:

- This command is only visible if the license key supporting non-standard QCIs is installed. Contact your Cisco Account or Support representative for information on how to obtain a license.
- **operator-defined-qci** *num*: Specifies the operator-defined QCI value to be enabled.

  num must be an integer from 128 through 254.

  Standards-based QCI values 1 through 9 are configured through the **qci** command.
- **pre-rel8-qos-mapping** *num*: Maps non-standard QCI to a standard QCI that has the characteristics (TC, THP, SI, TD, SSD) similar to desired pre-rel8 standard QoS values during 3G call or GnGp handover.

  num must be an integer from 1 through 4 for GBR and 5 through 9 for non-GBR. QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

  3G GGSN Call

  If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI under P-GW which is associated with a GGSN, then the 3G call would be rejected.

  GnGp Handoff

  1. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for default bearer, then the handoff would be rejected.
  2. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for dedicated bearer, then only that bearer would be rejected during handoff.
  3. In the following scenario:
     - default bearer with standard QCI or non-standard QCI (with **pre-rel8-qos-mapping** configured)
     - more than one dedicated bearer (some with standard QCI, some with non-standard QCI with **pre-rel8-qos-mapping** configured, and some with non-standard QCI with no mapping)

     During LTE-to-GnGp handoff:

     - UPC Request for all the dedicated bearers with non-standard QCI with no mapping would be rejected
     - handoff will be successful for the remaining bearers

Monitoring Non-standard QCI Support

Bulk Statistics

This section provides information regarding bulk statistics in support of non-standard QCI support.

APN Schema

The following counters have been added in support of non-standard QCIs (GBR and Non-GBR):

- nonstdqci-nongbr-uplinkpkt-drop-mbrexcd
- nonstdqci-nongbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-nongbr-uplinkbyte-drop-mbrexcd
- nonstdqci-nongbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-nongbr-rejbearer
- nonstdqci-gbr-uplinkpkt-drop-mbrexcd
- nonstdqci-gbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-gbr-uplinkbyte-drop-mbrexcd
- nonstdqci-gbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-gbr-rejbearer

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of non-standard QCI support.

show apn statistics

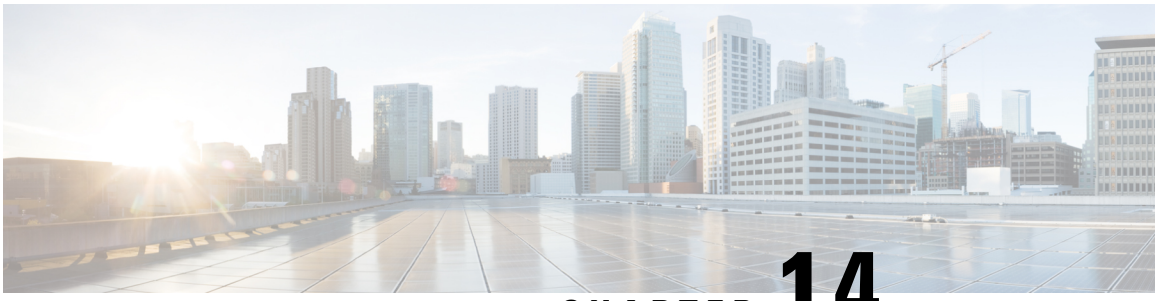
The output of this command has been enhanced to show the following non-standard QCI counters (GBR and Non-GBR):

- Non-Std QCI(Non-GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)
- Non-Std QCI(GBR)
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)

show qci-qos-mapping table all

The output of this command has been enhanced to show when non-standard QCI are configured:

- Operator-defined-qci
- pre-rel8-qos-mapping



CHAPTER 14

GGSN UPC Collision Handling

GGSN UPC Collision Handling

Feature Description

During collision between SGSN-initiated UPC request and GGSN-initiated UPC Request, SGSN-initiated UPC request gets higher priority over Network Operated (NRUPC). With the UPC Collision Handling feature, there is no call or data loss during call establishment or during mid-call phase. This feature can be enabled or disabled using a CLI and is enabled by default.

- When GGSN detects collision between SGSN initiated UPC request and NRUPC on primary PDP context, NRUPC is retried (with different sequence number) after sending UPC Response.
- When GGSN detects collision between SGSN initiated UPC request for Inter-SGSN handoff and NRUPC with TFT and after handoff BCM mode is changed from Mixed mode to MS-Only mode, NRUPC is retried (with different sequence number) after sending UPC Response, but without TFT.
- When GGSN detects collision between an SGSN initiated UPC and a NRUPC on secondary PDP context, NRUPC is aborted and PCRF is notified. When multiple CCR-U support is not enabled on GGSN, CCR-U for aborted NRUPC (on secondary PDP context) is not informed to PCRF. In this case, PCRF will not be aware of this aborted transaction (rule failure).

Note During S2bGTP to LTE handoff procedure, when there is already a pending transaction and a Handoff request is received by SAE-GW, Handoff is rejected with a following message:

```
Rejecting S2b/LTE Handoff as only one pending transaction is supported
```

Limitations

- Behavior for GnGp GGSN has been modified for this feature, in this release. Behavior for GGSN remains unaltered.

- When NRUPC received from Direct Tunnel (due to "Direct Tunnel Error Indication") collides with SGSN initiated UPC request, NRUPC is aborted and not retried. This does not affect the functionality as, when "Direct Tunnel Error Indication" is received from access side, NRUPC is triggered again.
- When a request for handoff to LTE is received before receiving NRUPC response, the behavior remains unchanged. In this case, the pending NRUPC request is aborted. If the NRUPC request received is for rule installation, the request remains in the pending state and the rule is not installed. As there is no static rule and the rule installation request is in pending state, the PDP context stays up without an installed rule.

Configuring GGSN UPC Collision Handling

Operators can use the Command Line Interface (CLI) to configure the collision between SGSN initiated UPC request and network initiated UPC Request.

gtpc handle-collision

This command in the service configuration mode can be used to the collision between SGSN initiated UPC request and network initiated UPC Request.

GGSN Service

```
configure
     context context_name
       ggsn-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

P-GW Service

```
configure
     context context_name
       pgw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

S-GW Service

```
configure
     context context_name
       sgw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

SAEGW Service

```
configure
     context context_name
       saegw-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

Notes:

- **no:** Disables collision handling between SGSN initiated UPC and NRUPC request.

- **default:** Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.
- **handle-collision upc nrupc:** Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show configuration verbose**

Please see the *Monitoring and Troubleshooting GGSN UPC Collision Handling* section for the command output.

Monitoring and Troubleshooting GGSN UPC Collision Handling

The following section describes commands available to monitor GGSN UPC Collision Handling.

Show Commands for GGSN UPC Collision Handling

show configuration

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show configuration verbose

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show ggsn-service name *service_name*

This command displays the following output:

```
Service name:                       ggsn-service
Context:                            ingress
…
Suppress NRUPC triggered by UPC:    Disabled
```

```
Collision handling for UPC-NRUPC:  Enabled/Disabled
```

show gtpc statistics

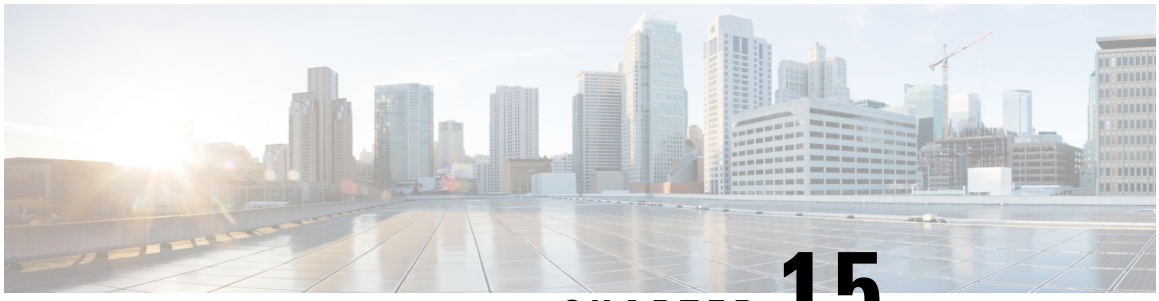
This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:                        1
  2G:                           0
  3G:                           1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:       0   Accepted:                     0
  Denied:                       0   Discarded:                    0

NRUPC UPC Collision:
  Primary PDP ctxt:             3   Secondary PDP ctxt:           0

QoS negotiation:
  CPC QoS Accepted:             3   CPC QoS Downgraded:           0
  UPC QoS Accepted:             3   UPC QoS Downgraded:           0
```

show gtpc statistics [format1 | ggsn-service *service_name* | verbose]

This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:                        1
  2G:                           0
  3G:                           1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:       0   Accepted:                     0
  Denied:                       0   Discarded:                    0

NRUPC UPC Collision:
  Primary PDP ctxt:             3   Secondary PDP ctxt:           0

QoS negotiation:
  CPC QoS Accepted:             3   CPC QoS Downgraded:           0
  UPC QoS Accepted:             3   UPC QoS Downgraded:           0
```



CHAPTER 15

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

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

Feature Description

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

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

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

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

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

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

- **Load Control**: Load control enables a GTP-C entity (for example, an P-GW/SAEGW/S-GW) to send its load information to a GTP-C peer (for example, an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- **Overload Control**: Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signaling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Load and Overload Factor Calculation Enhancement

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

A new CLI command, **gtpc-system-param-poll interval**, is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.

Relationships to Other Features

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

- One of the following services must be configured on the node before GTP-C Load and Overload Control can be configured.
  - P-GW
  - SAEGW
  - S-GW
- Once configured, the GTP-C Load and Overload Control profiles must be associated with a P-GW, SAEGW, or S-GW service to function properly in the network.

How It Works

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

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

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

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

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

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

Configuration Overview

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

Step 1 Create a load control profile. Refer to Creating the GTPP R12 Load Control Profile, on page 247.

Step 2 Configure the load control weightage settings. Refer to Configuring the 3GPP R12 Load Control Profile Weightage Settings, on page 248.

Step 3 Configure the load control inclusion frequency. Refer to Configuring the 3GPP R12 Load Control Profile Inclusion Frequency, on page 248.

Step 4 P-GW Only. Configure the load control threshold. Refer to Configuring the 3GPP R12 Load Control Threshold, on page 249.

Step 5 Configure load control information handling. Refer to Configuring 3GPP R12 Load Control Information Handling, on page 249.

Step 6 Configure load control information publishing. Refer to Configuring 3GPP R12 Load Control Information Publishing, on page 249.

Step 7 Configure the 3GPP R12 GTP-C Polling Parameter Interval. Refer to Configuring the 3GPP R12 GTP-C Polling Parameter Interval, on page 250

Step 8 Associate the load control profile with a P-GW, SAEGW, or S-GW service. Refer to Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service., on page 250.

Step 9 Verify the configuration settings. Refer to Verifying the 3GPP R12 Load Control Configuration , on page 251.

Step 10 Save the configuration. Refer to Saving the Configuration, on page 252.

Creating the GTPP R12 Load Control Profile

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

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

Notes:

- The profile name must be an alphanumeric string from 1 to 64 characters in length.

- Once you have created the load control profile, you will enter *GTP-C Load Control Profile Configuration Mode*.

Configuring the 3GPP R12 Load Control Profile Weightage Settings

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

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

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

Notes:

- **system-cpu-utilization** *percentage*: Configures system CPU utilization weightage as a percentage of 100.

  percentage must be an integer from 0 to 100. The default is 40.

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

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

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

Configuring the 3GPP R12 Load Control Profile Inclusion Frequency

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

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

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

Notes:

- **inclusion frequency**: Configures parameters to determine the inclusion frequency of the LCI.
- **advertisement-interval** *interval_in_seconds*: Configures advertisement-interval for the LCI in seconds. This specifies how often load control information should be sent to the peers. If configured to 0, the node will send load control information in each and every outgoing message to the peers. *interval_in_seconds* must be an integer from 0 to 3600. The default is 300.
- **change-factor** *change_factor*: Configures the change factor for the load control profile. If the load control change factor changes by the configured factor, whether it is an increase or decrease in load, the load control information is sent to the peers. This information is only sent to the peers when the load factor changes by the factor configured. *change_factor* must be an integer from 1 to 20. The default is 5.

Configuring the 3GPP R12 Load Control Threshold

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

Use the following example to configure Load Control Profile threshold on the P-GW.

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

Notes:

- The default threshold value is 50.

Configuring 3GPP R12 Load Control Information Handling

The handling of load control information for the home or visited PLMN can be enabled/disabled via this procedure.

Use the following example to enable/disable load control profile information handling on the SAEGW/S-GW/P-GW.

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

Notes:

- **no** disables load-control-handling for the specified option.

Configuring 3GPP R12 Load Control Information Publishing

The publishing of load control information can be enabled/disabled for the home or visited PLMN.

Use the following example to enable/disable load control profile information publishing on the P-GW/SAEGW/S-GW.

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

Notes:

- **no** disables load control profile information publishing for the specified option.

Configuring the 3GPP R12 GTP-C Polling Parameter Interval

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

Beginning with StarOS release 21, a new CLI command, **gtpc-system-param-poll interval**, is introduced in *Context Configuration Mode* to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements. This command sets the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager.

To configure the GTP-C polling parameter interval:

```
config
   context context_name
      gtpc-system-param-poll interval seconds
      default gtpc-system-param-poll interval
      end
```

- Where *seconds* is the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager. Valid entries are from 15 to 300 seconds. The default setting is 30 seconds.
- **default** returns the setting to its default value of 30 seconds.

⚠

Caution Setting the time interval to a low value may impact system performance.

Associating the 3GPP R12 Load Control Profile with a P-GW, SAEGW, or S-GW Service.

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

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

P-GW Service Association:

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

Notes:

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

S-GW Service Association:

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

Notes:

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

SAEGW Service Association::

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

Verifying the 3GPP R12 Load Control Configuration

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

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

The output of this command provides the configuration settings of all load control parameters, including:

- Weightage
- Inclusion Frequency
- Load control information handling
- Load control information publishing
- Load threshold

Saving the Configuration

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

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

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

Configuration Overview

Step 1 Create the GTP-C overload control profile. Refer to Creating the GTPP R12 Overload Control Profile, on page 252.

Step 2 Configure the weightage settings. Refer to Configuring 3GPP R12 Overload Control Weightage Settings, on page 253.

Step 3 Configure the inclusion frequency. Refer to Configuring the 3GPP R12 Overload Control Inclusion Frequency, on page 253.

Step 4 Configure the validity period. Refer to Configuring the 3GPP R12 Overload Control Validity Period, on page 254.

Step 5 Configure the tolerance settings. Refer to Configuring 3GPP R12 Overload Control Tolerance Limits, on page 254.

Step 6 Configure the throttling behavior for the node. Refer to Configuring 3GPP R12 Overload Control Throttling Behavior, on page 255.

Step 7 Configure the message prioritization. Refer to Configuring 3GPP R12 Overload Control Message Prioritization, on page 256.

Step 8 Configure self-protection behavior for the node. Refer to Configuring 3GPP R12 Overload Control Self-Protection Behavior, on page 256.

Step 9 Configure overload control information handling. Refer to Configuring 3GPP R12 Overload Control Information Handling, on page 257.

Step 10 Configure overload control information publishing. Refer to Configuring 3GPP R12 Overload Control Information Publishing, on page 257.

Step 11 Configure the GTP-C polling parameter interval . Refer to Configuring the 3GPP R12 GTP-C Polling Parameter Interval, on page 250.

Step 12 Associate the overload control configuration with an existing P-GW/SAEGW/S-GW service. Refer to Associating the 3GPP R12 Overload Control Configuration with a P-GW, SAEGW, or S-GW Service, on page 258.

Step 13 Verify the overload control configuration. Refer to Verifying the 3GPP R12 Overload Control Configuration , on page 259.

Step 14 Save the configuration. Refer to Saving the 3GPP R12 Overload Control Configuration, on page 259.

Creating the GTPP R12 Overload Control Profile

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

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

Notes:

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

Configuring 3GPP R12 Overload Control Weightage Settings

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

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

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

Notes:

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

Configuring the 3GPP R12 Overload Control Inclusion Frequency

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

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

```
configure
   gtpc-overload-control-profile  profile_name
```

```
      inclusion-frequency { advertisement-interval interval_in_seconds |
change-factor change_factor }
     default inclusion-frequency { advertisement-interval | change-factor
 }
      end
```

Notes:

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

Configuring the 3GPP R12 Overload Control Validity Period

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

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

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

Notes:

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

Configuring 3GPP R12 Overload Control Tolerance Limits

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

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

Notes:

- **initial-reduction-metric** *percentage*: Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit. When reaching the configured minimum threshold, this parameter specifies how much the node wants the peers to reduce incoming traffic.*percentage* must be an integer from 1 to 100. The default is 10.
- **threshold report-reduction-metric** *percentage*: Configures the minimum overload tolerance threshold for advertising overload reduction metric to the peer. When the minimum threshold is reached, the node will report this information to peers. When the maximum limit is reached, the node will go into self-protection mode. *percentage* must be an integer from 1 to 100. The default is 80.
- The **threshold report-reduction-metric** should always be lower than the **self-protection-limit**.
- **self-protection-limit** *percentage*: Configures the maximum overload tolerance threshold after which node will move to self protection mode. When the maximum limit is reached, the node will start rejecting all incoming messages, except for delete messages. The node will not initiate any new messages to the peers. This is to mitigate the overload condition.*percentage* must be an integer from 1 to 100. The default is 95.

Configuring 3GPP R12 Overload Control Throttling Behavior

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

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

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

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

Notes:

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

Configuring 3GPP R12 Overload Control Message Prioritization

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

Use the following example to configure message prioritization.

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

Notes:

- **group1** specifies the message priority percentage for the following messages:
  - Update Bearer Request message for default bearer generated from P-GW ingress
  - Update Bearer Request message for dedicated bearer generated from P-GW ingress
  - Handoff Create Session Request message generated from ePDG egress.
- **group2** specifies the message priority percentage for the following messages:
  - Create Bearer Request message for default bearer generated from P-GW ingress
  - PDN connection requested Create Session Request message from ePDG egress
- The total percentage for the message groups should equal 100.
- **group1** messages will have the highest priority (1) and are dropped last. **group2** messages will have the lowest priority (2) and are dropped first.
- **default** returns the group message priority settings to their default value. The default for each group is 50.
- The default behavior for this command is enabled. To disable the command use the **no** option.

Configuring 3GPP R12 Overload Control Self-Protection Behavior

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

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

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

Notes:

- **apn** configures up to three APN names to be allowed under self-protection behavior.

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

Configuring 3GPP R12 Overload Control Information Handling

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

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

Notes:

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

Configuring 3GPP R12 Overload Control Information Publishing

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

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

Notes:

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

Configuring the 3GPP R12 GTP-C Polling Parameter Interval

In capacity testing and also in customer deployments it was observed that the chassis load factor for the 3GPP R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

The 3GPP R12 Load/Overload Control Profile feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

Beginning with StarOS release 21, a new CLI command, **gtpc-system-param-poll interval**, is introduced in *Context Configuration Mode* to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements. This command sets the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager.

To configure the GTP-C polling parameter interval:

```
config
  context context_name
    gtpc-system-param-poll interval seconds
    default gtpc-system-param-poll interval
    end
```

- Where *seconds* is the time period over which to monitor the chassis level CPU, Memory, and Session count information from the resource manager. Valid entries are from 15 to 300 seconds. The default setting is 30 seconds.
- **default** returns the setting to its default value of 30 seconds.

Caution Setting the time interval to a low value may impact system performance.

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

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

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

P-GW Service Association:

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

Notes:

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

S-GW Service Association:

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

Notes:

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

SAEGW Service Association::

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

Verifying the 3GPP R12 Overload Control Configuration

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

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

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

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

Saving the 3GPP R12 Overload Control Configuration

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

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

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

3GPP R12 GTP-C Load and Overload Show Commands

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

show egtpc statistics egtp-service <egtp-service name>

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

show gtpc-load-control-profile full all

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

show gtpc-load-control-profile full name <name>

Use this command to view all configuration settings for the specified 3GPP R12 load control profile.

show gtpc-overload-control-profile full all

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

show gtpc-overload-control full name <name>

The output of this command provides all configuration settings for all 3GPP R12 Overload Control Profiles configured on the node. Use this command to determine if the Overload Control Profile is configured as intended.

show pgw-service all

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

show sgw-service all

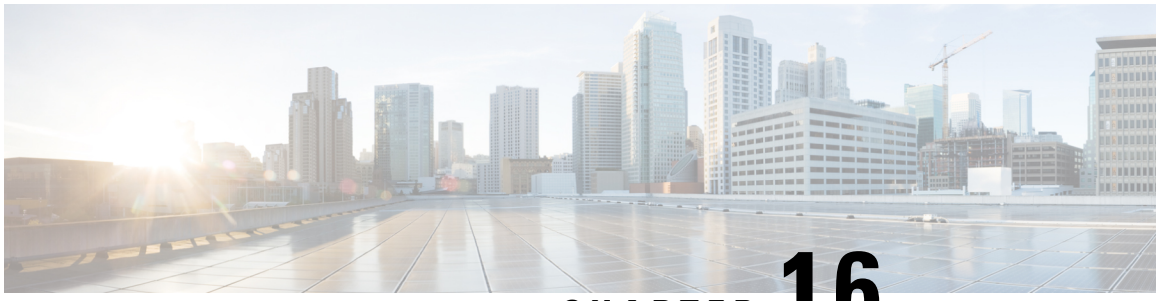
Use this command to obtain the names of all 3GPP R12 Load Control and Overload Control profiles configured on the S-GW.

eGTP-C Bulk Statistics

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

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

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



CHAPTER 16

Intelligent RAT Paging for ISR on the S-GW

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

Feature Description

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

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

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

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

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

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

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

Relationships to Other Features

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

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

How it Works

Intelligent RAT Paging for ISR on the S-GW

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

- **Sequential Paging** (pages both nodes one after the other). This method optimizes radio resource utilization. If quick call setup time is not indicated, the S-GW will perform sequential paging and it will page the S4-SGSN and MME one after the other. It first will page to the node of the last known RAT type of the UE.
- **Parallel Paging** (pages both the nodes in parallel). This method results in quick paging response time and faster call setup time. If the DDN is initiated for an APN that requires the quick call setup time (for example, VoLTE APN) then the S-GW performs parallel paging.

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

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

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

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

Licenses

Intelligent RAT Paging for ISR is a licensed-controlled Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations

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

1. The S-GW performs sequential paging (if configured) only for Downlink data triggered Downlink Data Notification (DDN) messages. All control event triggered DDN messages are treated as high priority

DDN messages and the S-GW always performs parallel paging for control event triggered DDN messages. No DDN-Throttling and DDN-Delay shall be applicable only to Downlink data triggered DDN messages.

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

Flows

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

Figure 45: Intelligent RAT Paging for ISR: Sequential Paging Procedure

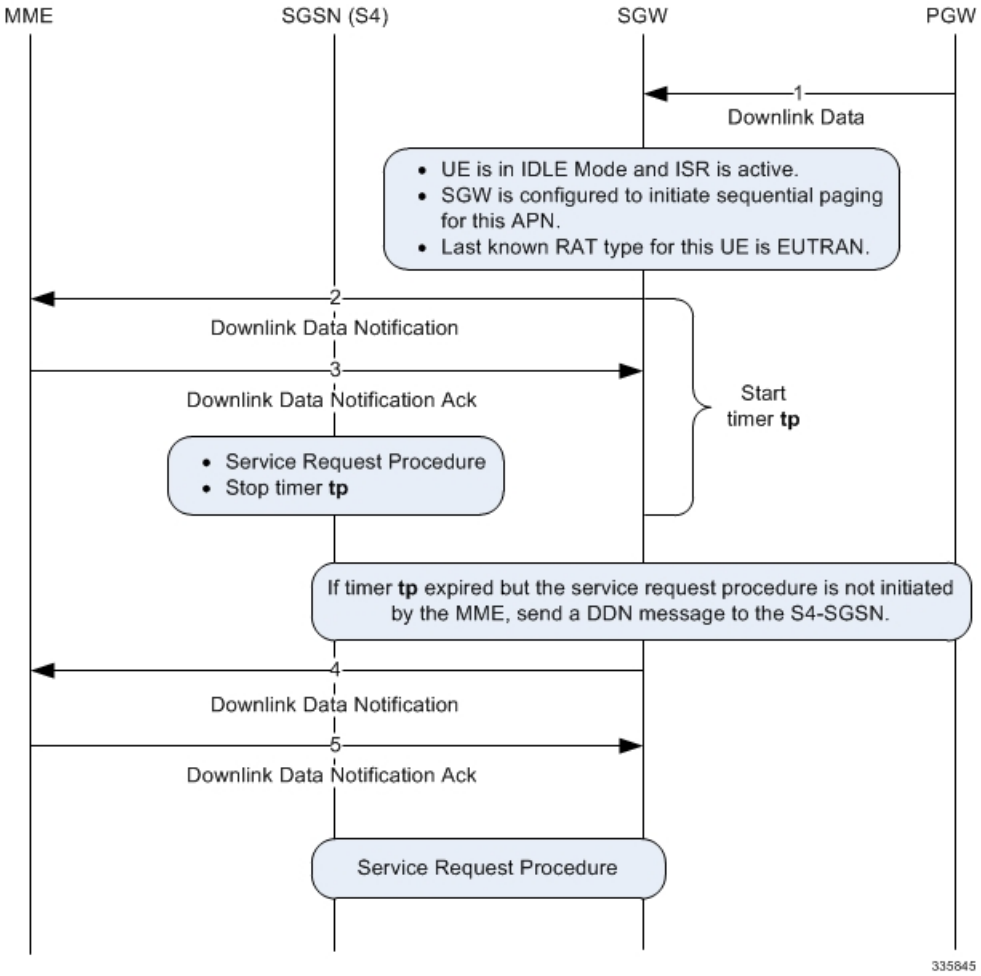


Table 24: Intelligent RAT Paging for ISR: Sequential Paging Procedure Description

Step	Description
1	The S-GW receives the downlink data packet for an idle UE which has ISR active and the S-GW is configured to initiate sequential paging for this APN. The Last known RAT Type for this UE is E-UTRAN.
2	The S-GW initiates Downlink Data Notification towards the MME and starts the timer **tp**.

Step	Description
3	The MME replies with a Downlink Data Notification Ack message. If the MME initiates the service request procedure for this UE within time **tp**, then the S-GW will stop the timer **tp** and process the service request procedure. The S-GW will not initiate the Downlink Data Notification towards S4-SGSN (in a different RAT). Therefore, the system saves the paging attempt and the radio resource of the S4-SGSN.
4	If the MME does not initiates the service request procedure for this UE within time **tp** then upon expiry of timer **tp**, the S-GW will initiate the Downlink Data Notification towards the S4-SGSN.
5	The S4-SGSN replies with a Downlink Data Notification Ack message. The S4-SGSN attempts to page the UE. The S-GW will receive the service request procedure from S4-SGSN.

Figure 46: Intelligent RAT Paging for ISR: Parallel Paging Procedure

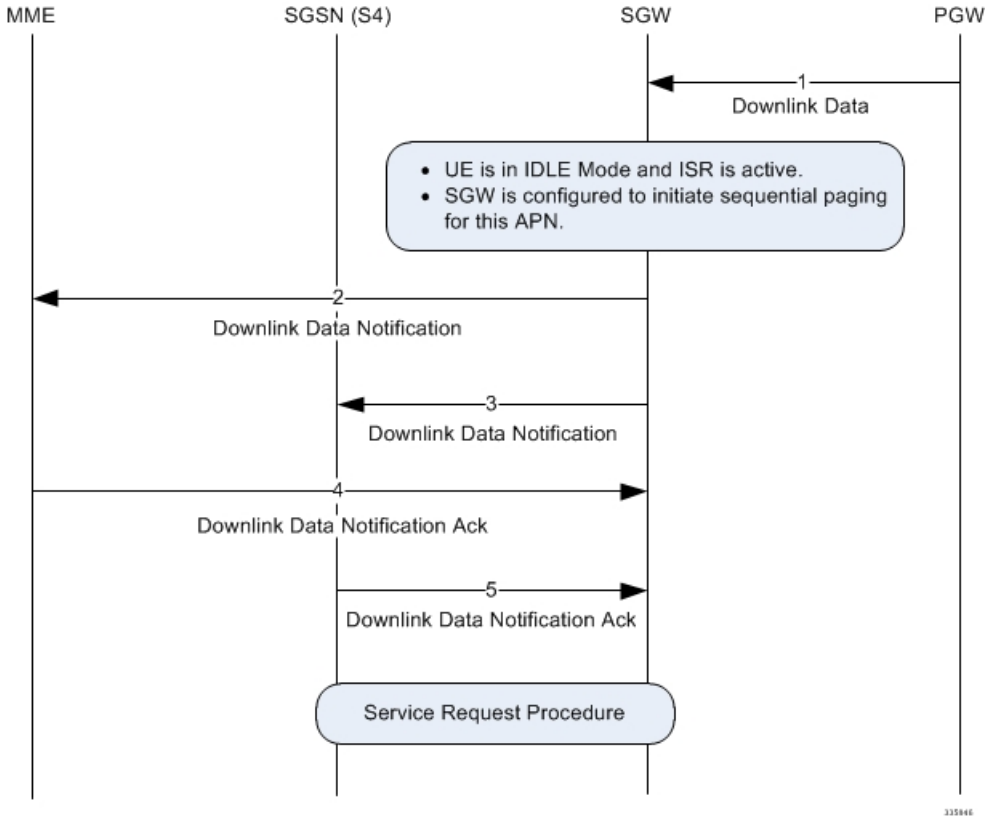


Table 25: Intelligent RAT Paging for ISR: Parallel Paging Procedure 1

Step	Description
1	The S-GW receives the downlink data packet for an ISR active, Idle UE. The S-GW is configured to initiate parallel paging for this APN.
2	The S-GW initiates Downlink Data Notification towards the MME.

Step	Description
3	The S-GW initiates Downlink Data Notification towards the S4-SGSN.
4	The MME replies with a Downlink Data Notification Ack message.
5	The S4-SGSN replies with a Downlink Data Notification Ack message.
6	The MME and S4-SGSN attempt to page the UE. The S-GW will receive the service request procedure from either the MME or S4-SGSN.

Configuring Intelligent RAT Paging for ISR on the S-GW

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

Configuring the Intelligent RAT Paging for ISR Feature

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

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

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

Notes:

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

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

Notes:

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

Verifying the Intelligent RAT Paging for ISR Configuration

This section describes how to verify the Intelligent RAT Paging for ISR configuration settings.

To verify that Intelligent RAT Paging for ISR is enabled in the APN profile for this S-GW, enter the following command from Exec Mode:

```
show apn-profile full name apn_profile_name
...
LIPA-APN                                :Disabled
ISR-SEQUENTIAL-PAGING                  :Enabled
Local Offload                           :Disabled
Overcharging protection                 :Disabled
...
```

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

```
show sgw-service name sgw_service_name
...
Service name
...
   GTPU Error Indication Handling:
...
      S4U-Interface: local-purge
      ddn failure-action pkt-drop-time:   300
      ddn isr-sequential-paging delay-time:  1
      Idle timeout                           :n/a
...
```

CHAPTER 17

LTE-M RAT Type Support on SAEGW, P-GW, and S-GW Services

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Default Setting	Enabled-Always-On
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administartion Guide*

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

LTE-M (LTE-MTC low-power-wide area (LPWA)) is a new cellular radio access technology specified by 3GPP that addresses low power-wide area connectivity solutions. It specifically refers to a specific category of LTE UEs that are suitable for IoT LTE-M, which supports IoT through lower device complexity and provides extended coverage, while allowing the reuse of the LTE installed base.

The RAT type IE is present in various call flows across many interfaces. When a Create Session Request is received with an unknown RAT Type, as the RAT Type is a Mandatory IE in this message, S-GW or P-GW may reject a create session request. In this StarOS 21.24 release, LTE-M RAT (Radio Access Technology) type for S-GW, P-GW, and SAEGW products are supported.

The RAT type is present either as an IE (for example, in GTPv2-C, GTPP), AVP (on Diameter-based interfaces) or as an attribute (for example in EDRs) across many interfaces.

The LTE-M solution for S-GW, P-GW, and SAEGW supports the following new LTE-M RAT type attribute value in the following Interfaces protocols and dictionaries:

- GX-interface: Diameter Protocol
- GY-interface: Diameter Protocol
- GZ/RF- interface: GTPP/Diameter/Radius
- S6B- Interface: Diameter Protocol
- S11/ S5/S8-Interface: GTPv2-C
- Dictionaries Radius AVPs, and dictionaries.
- Rf interface for CDR generation
- Attributes in EDRs

Enhancements to the Existing Features

The following existing features are enhanced to support the new RAT-TYPE LTE-M.

- **Virtual APN Selection Based on RAT Type**: 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 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, where different policies imply different APNs.

  You can select the virtual APN by configuring directly under the base APN. This APN selection is done based on RAT Types. In this release, support is added through CLI to select the virtual APN for the LTE-M RAT type.

- **Qci and Qos Mapping**: P-GW supports QCI and QoS mapping association with APN based on RAT type LTE-M. This QCI and QoS mapping allow you to perform quick actions on the QoS Class Index (QCI) to QoS Mapping Configuration Mode, which is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur in Serving Gateway (S-GW), and/or the PDN Gateway (P-GW) in an LTE network.
- **PCRF-based Handling**: P-GW informs the RAT type changes to PCRF through Credit Control Request -Initial and Updated messages, and PCRF provides a new PCC rule. Allows you to create a Bearer by enforcing a new Policy and Charging Control (PCC) rule from Policy and Charging Rules Function (PCRF).

How it Works

Architecture

The following table specifies the field and its value for various interfaces with support of LTE-M RAT type. Only Standard dictionaries and customized dictionaries are modified.

Table 26:

		P-GW Product		
x	RAT-Type (1032) Diameter	M -)	E T 7 0 0 1 (	• Credit Control Request-Initial • Credit Control Request - Updated
y	3GPP-RAT-Type (21) Diameter	M -)	E T 9 (	• Credit Control Request-Initial • Credit Control Request - Updated
SU3	3GPP-RAT-Type (21)	M -)	E T 9 (	• Accounting Request -Start • Accounting Request- Stop • Account request -Interim
f	3GPP-RAT-Type (21) Diameter	M -)	E T 9 (	• Accounting Request -Start • Accounting Request- Stop • Account request -Interim
b	3GPP-RAT-Type (1032) Diameter	M -)	E T 9 (	• Authentication • Authorisation • Request

ea	Fie	l	P et	M ubi	ess r t	Ages A
s	RA	-Type	M)	-	E T 9	L (
W S	G R_ GTPP	-Type (30)	M)	-	E T 9	Gtpp Data Record (• Transfer Request
	S-GW Product					
s	R G	-Type (30)	M)	-	E T 9	Gtpp Data Record (• Transfer Request

Limitations

Following are the known limitations for new LTE-M RAT type feature:

- Rule matching at ECS
- Ruledef matching at Local-Policy

Supported Standards

Cisco's implementation of the LTE RAT type complies with the following standards:

- 3GPP 23.401 – eGPTC Interface
- 3GPP 29.274 Release 15.4.0 – 3GPP GTPv2 Protocol Specification Reference table for LTE-M Rat type support; RAT Type IE details are given in the following table for egtpc IEs encoding and decoding :
  - Table 7.2.1-1: Information Elements in a Create Session Request
  - Table 7.2.7-1: Information Elements in a Modify Bearer Request
  - Table 7.2.7-1: Information Elements in a Modify Bearer Request
- 3GPP 23.401 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 32.299 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).
- 3GPP 29.060 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface.
- 3GPP 29.061 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)

- 3GPP 32.298 – 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP 29.212 Release 15.4.0 – 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC).

Configuring Virtual-APN

Use the following configuration to display an additional option (LTE-M) “RAT-Type” based Virtual-APN selection .

```
configure
  context context_name
    apn apn_name
       virtual-apn preference value apn apn_name rat-type lte-m
       end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **virtual-apn preference** *value* **apn** *apn_name* : Configures the virtual-apn (virtual.ipv4).
- **rat-type lte-m**: Enables LTE-M as an additional RAT-type.

Configuring qci-qos-mapping

Use the following configuration to configure QCI-QOS mapping in the APN Configuration mode and associate additional RAT type (LTE-M).

```
configure
  context context_name
    apn apn_name
      qci table
       qci-qos-mapping
           qci qci_val non-gbr { downlink user-datagram dscp-marking value
 }
           end
```

NOTES:

- **apn** *apn_name*: Allows to specify the APN name as a condition. *apn_name* must be an alphanumeric string of 1 through 63 characters.
- **qci-qos-mapping**: Configures the qci-qos-mapping for APN.
- **qci** *qci_val*: Specifies the QoS Class Identifier. *qci_val* must be an integer between 1 to 9, 80, 82, and 83.
    - **downlink**: Specifies the direction of traffic on which this QoS configuration needs to be applied.

Associate Qci-Qos-Mapping

Use the configuration to select the qci-qos-mapping RAT Type.

```
configure
  context context_name
    apn apn_name
      associate  qci-qos-mapping table rat-type lte-m
      end
```

NOTES:

- **associate qci-qos-mapping table rat-type lte-m** : Associates apn qci-qos-mapping based on the RAT type.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the LTE-M RAT Type support on the SAEGW, P-GW and S-GW Services.

Show Commands and Output

This section provides information on show commands and their corresponding outputs for the LTE-M RAT type feature.

show apn name

The following output is displayed if the Virtual-APN is selected based on the RAT-Type, during the Session-Setup.

Output:

```
show apn name <>
Virtual APN Configuration:
  Preference  Selected-APN           Rule-Definition
  10          verizon.ipv4           CC Profile Index = 3
   RAT Type = lte-m [local]qvpc-si# show configuration
```

show apn all

The output of **show apn all** and **show apn name** *apn_name* **all** commands has been enhanced to monitor the APN configuration for qci-qos-mapping on RAT type **lte-m**:

Example:

```
show apn name <>
qci-qos-mapping Name for RAT-Type:
GERAN :N/A             UTRAN :N/A
EUTRAN : N/A           LTE-M : table
Stats Profile Name : N/A
```

show qci-qos-mapping table all

Following example is the sample output before associating the qci-qos-mapping table based on additional RAT Type (LTE-M).

```
QCI-QOS Table Name: table

 Qci:  1
  uplink: n/a
  downlink: user-datagram            dscp-marking 0x3e
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:  n/a            precedence class:     n/a
  reliability class:  n/a            qci type:   non-gbr
  volte:   n/a                       traffic policing interval:  n/a

 Qci:  2
  uplink: n/a
  downlink: internal-qos priority 1
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:     n/a               precedence class:  n/a
  reliability class:     n/a         qci type:   gbr
  volte:     n/a                     traffic policing interval:  n/a
```

show configuration

The **virtual-apn preference** *value* **apn** *apn_name* **rat-type lte-m** output is displayed when the Virtual APN is configured with the LTE-M RAT type. Following is the sample output:

```
[local]qvpc-si# show configuration
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      accounting-mode radius
      ims-auth-service ims-ggsn-auth
      ip access-group acl4-1 in
      ip access-group acl4-1 out
      authentication pap 1 chap 2 allow-noauth
      ip context-name egress
      virtual-apn preference 10 apn verizon.ipv4 rat-type lte-m
      ipv6 access-group acl6-1 in
      ipv6 access-group acl6-1 out
      active-charging rulebase prepaid
    exit
```

Similarly, the **associate qci-qos-mapping table rat-type lte-m** output is displayed for the qci-qos association changes based on RAT type. Following is the sample output

```
 [local]laas-setup# show configuration
                apn intershat
                context ingress
               subscriber default
                nexthop-forwarding-address
                exit
                apn intershat
                associate qci-qos-mapping table rat-type lte-m
                exit
```

show subscribers full

The output of this show command is used for monitoring the subscriber call. The RAT type of the call is displayed as LTE-M. A new field **LTE-M** is added under Access Technology. Following is the sample output:

```
[local]laas-setup# show subscribers all
Access  (X) - CDMA 1xRTT               (E) - GPRS GERAN    (I) - IP
||    Tech:       (D) - CDMA EV-DO     (U) - WCDMA UTRAN   (W) - Wireless LAN
||                (A) - CDMA EV-DO REVA (G) - GPRS Other    (M) - WiMax
```

```
||                (C) - CDMA Other      (J) - GAN           (O) - Femto IPSec
||                (P) - PDIF            (S) - HSPA          (L) - eHRPD
||                (T) - eUTRAN          (B) - PPPoE         (F) - FEMTO UTRAN
||                (N) - NB-IoT          (Q) - WSG           (R)- LTE-M
                  (.) - Other/Unknown
```

show subcscribers full all

The output of the following show commands are used for monitoring the subscriber call. The Access Technology of the call is displayed as LTE-M.

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Tue Mar 23 04:33:55 2021 call duration: 00h00m46s
  idle time: 00h00m40s                idle time left:  n/a
```

show subs pgw-only full / show subs pgw-only full all

The **show subs pgw-only full** / **show subs pgw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
Access Type: gtp-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                   pgw-service-name: PGW21
  Callid: 02fb3ea2                     IMSI: 404005123456789
  MSISDN: 9890098900                   External ID: n/a
  Interface Type: S5S8GTP              Low Access Priority: N/A
  TWAN Mode: N/A
  eMPS Bearer: No
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
```

show subs sgw-only full / show subs sgw-only full all

The **show subs sgw-only full** / **show subs sgw-only full all** scommands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Card/Cpu        : 1/0         Sessmgr Instance : 11
  Idle time       : 00h05m47s
  MS TimeZone     : n/a                  Daylight Saving Time: n/a

  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                           sgw-service-name: SGW21
  Callid: 02fb3ea1                       IMSI: 404005123456789
  MSISDN: 9890098900
  eMPS Bearer: No
```

show subs saegw-only full / show subs saegw-only full all

The **show subs saegw-only full** / **show subs saegw-only full all** commands display the Access Technology of the call as LTE-M. Following is the sample output:

```
 Callid   : 02fb3ea3                    IMSI                : 404005123456789
  Card/Cpu          : 1/0                          Sessmgr Instance    : 11
  Source context    : EPC2                         Destination context : ISP1
  Bearer Type       : Default                      Bearer-Id           : 5
  Access Type       : gtp-pdn-type-ipv4-ipv6       Network Type        : IPV4+IPv6
```

```
  Access Tech       : LTE-M                       saegw-service-name  : SAEGW21
  MSISDN            : 9890098900                  External ID         : n/a
  TWAN Mode         : N/A
  eMPS Bearer       : No
  WPS Bearer        : No
```

show subs pgw-only all

The **show subs pgw-only all** command displays the following output:.

```
|+------Access     (U) - UTRAN     (G) - GERAN
||      Tech:      (W) - WLAN                (J) - GAN
||                 (U) - HSPA Evolution      (E) - eUTRAN
||                 (H) - eHRPD               (.) - Unknown
||                 (N) - NB-IoT              (R) - LTE-M
```

show subs sgw-only all

The **show subs sgw-only all** command displays the following output:

```
|+----Access    (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:     (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||              (.) - Unknown          (N) - NB-IoT          (R) - LTE-M

||
```

show subs saegw-only all

The **show subs saegw-only all** command displays the following output:

```
|+----Access    (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:     (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||              (H) - eHRPD            (.) - Unknown         (N) - NB-IoT
||              (R) - LTE-M
```

show subscribers callid

The **show subscribers callid** *callid*command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
|+----Access  (X) - CDMA 1xRTT(E) - GPRS GERAN      (I) - IP
||    Tech:   (D) - CDMA EV-DO          (U) - WCDMA UTRAN     (W) - Wireless LAN
||            (A) - CDMA EV-DO REVA     (G) - GPRS Other      (M) - WiMax
||            (C) - CDMA Other          (J) - GAN             (O) - Femto IPSec
||            (P) - PDIF                (S) - HSPA            (L) - eHRPD
||            (T) - eUTRAN              (B) - PPPoE           (F) - FEMTO UTRAN
||            (N) - NB-IoT              (Q) - WSG             (R) - LTE-M

||            (.) - Other/Unknown
```

show session subsystem

The following output displays the session related statistics:

```
LTE-M Data Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
LTE-M Connection Statistics
```

```
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

Similarly, the **show session subsystem full** is enhanced to display the Data packets and subscribers count per RAT type.

show session subsystem verbose

The **show session subsystem verbose** command displays the following output:

```
NB-IoT Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

LTE-M Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

 NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
 LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

show session summary

The **show session summary** command displays the following output:

```
4G LTE (EUTRAN): 0
2G (GERAN): 0
3G (UTRAN): 0
WiFi (WIRELSS LAN): 0
eHRPD: 0
3G HA: 0
NB-IoT: 2
LTE-M: 0
Others: 0
```

show subscribers subscription full

The **show subscribers subscription full** command displays the following output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Wed Mar 17 09:59:47 2021 call duration: 00h01m19s
  idle time: 00h01m13s                idle time left:  n/a
  session time left:  n/a
```

show subscribers activity all

The **show subscribers activity all** command displays the Access Technology of the call as LTE-M. Following is the sample output:

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
```

```
  Access Tech: LTE-M                    Access Network Peer ID: n/a
  callid: 02fb3ea1                      msid: 404005123456789
```

show apn statistics all-name

The show output command displays the statistics per APN and also displays number of initiated sessions and active sessions with LTE-M RAT Type per APN. Following is the sample output:

```
Initiated Sessions per RAT Type:
    EUTRAN:  0    UTRAN:   0
    GERAN:   0    EHRPD:   0
    S2A GTP: 0    S2B GTP: 0
    S2B PMIP:0    NB-IoT:  0
    LTE-M :  0

  Active Sessions per RAT Type:
   EUTRAN: 0   UTRAN: 0
   GERAN:  0   WLAN:  0
   HSPA:   0   NB-IoT:0
   LTE-M:  0   OTHER: 0
```

show saegw-service statistics all-name

The show output command displays the statistics per SAEGW service and also displays Current subscribers, the Current PDNs with NB-IoT RAT Type per SAEGW Service. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    NB-IoT:                         0
  LTE-M:                            0    OTHER:                          0

Current PDNs By RAT-Type:
    EUTRAN:                         0    UTRAN:                        0
    GERAN:                          0    NB-IoT:                       0
    LTE-M:                          0    OTHER:                        0
```

show pgw-service statistics all-name

The show output command displays statistics for each P-GW Services, the number of initiated PDNs, and current PDNs with NB-IoT RAT Type for each P-GW Services. Following is the sample output:

```
Initiated PDNs By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    EHRPD:                          0
  S2A GTP:                          0    S2B GTP:                        0
  S2B PMIP:                         0    NB-IoT:                         0
  LTE-M                         0

Current PDNs By RAT-Type:
  EUTRAN:                           0    UTRAN:                          0
  GERAN:                            0    WLAN:                           0
  NB-IoT:                           0    LTE-M                           0
  OTHER:                            0
```

show sgw-service statistics

This show command displays statistics for each S-GW Services. This CLI is enhanced to display Current Subscribers and Current PDNs with NB-IoT RAT type for each S-GW Services. Following is the sample output:

```
Current Subscribers By RAT-Type:
  EUTRAN:                           0    UTRAN:                           0
  GERAN:                            0    NB-IoT:                          0
  LTE-M:                            0    OTHER:                           0
Current PDNs By RAT-Type:
    EUTRAN:                         0    UTRAN:                           0
    GERAN:                          0    NB-IoT:                          0
    LTE-M:                          0    OTHER:                           0
```

Bulk Statistics

The following statistics are added in support of the LTE-M RAT type feature

APN Schema

The following LTE-M RAT type feature-related bulk statistics are available in the APN schema.

Bulk Statistics	Description
active-lte-m-sessions	The total number of active LTE-M sessions per APN with RAT type LTE-M.
initiated-lte-m-sessions	The total number of initiated LTE-M sessions.

P-GW Schema

The following LTE-M RAT type feature related bulk statistics available in the P-GW schema.

Bulk Statistics	Description
sesstat-pdn-rat-lte-m	The total number of active PDN Type Statistics – LTE-M.
sessstat-rat-init-lte-m	The total number of initiated LTE-M PDNs (with RAT Type LTE-M).

S-GW Schema

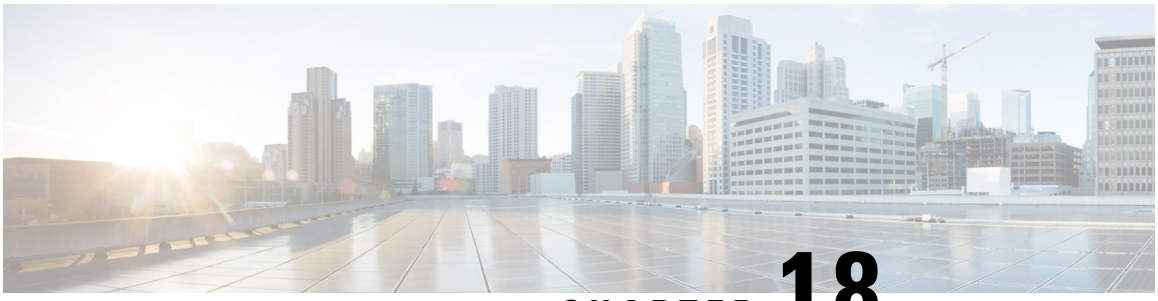
The following LTE-M RAT type feature related bulk statistics available in the S-GW schema.

Bulk Statistics	Description
sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sessstat-totcur-pdn-lte-m	The total number of active PDNs with LTE-M RAT type.

SAEGW Schema

The following LTE-M RAT type feature related bulk statistics available in the SAE-GW schema.

Bulk Statistics	Description
sgw-sessstat-totcur-ue-lte-m	The total number of active UEs with LTE-M RAT type.
sgw-sessstat-totcur-pdn-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sesstat-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.
pgw-sessstat-pdn-rat-init-lte-m	The total number of initiated LTE-M PDNs.
saegw-sgw-anchor-pdn-rat-lte-m	The total number of LTE-M PDNs (SGW anchored) with RAT Type LTE-M.
saegw-pgw-anchor-pdn-rat-lte-sm	The total number of LTE-M PDNs (PGW anchored) with RAT Type LTE-M.
saegw-collapsed-pdn-rat-lte-m	The total number of LTE-M PDNs (PGW anchored/Collapsed PDN) with RAT Type LTE-M.



CHAPTER 18

Maximum Receive Unit Configuration Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAE-GW • S-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

Prior to MRU Configuration support, the Maximum Receive Unit (MRU) setting was equal to the Maximum Transmission Unit (MTU).

When the MTU of eNB on the S1-U interface was increased to 2000 bytes but no changes were made on the MTU on S1-U interface on SAE-GW, packets were received at SAE-GW with size more than 1500 bytes. This resulted into those packets getting dropped at the S1-U interface on the SAE-GW with **Lport_MRU_exceeded** exception. This was affecting UEs that were trying to set up IKE Tunnels.

This Configure MRU feature allows you to configure MRU separately from MTU.

How It Works

To handle MRU independently of MTU, changes are made in Network Processing Unit (NPU), NPUSIM, NPUMGR, and CLI.

Configuring the MRU Feature

This section describes how to configure the MRU of the IP interface along with MTU using the **ip mtu** keyword under interface configuration.

Configuring MRU

To configure the MTU and MRU in the Ethernet Interface Configuration mode, use the following sample configuration.

```
config
  context context_name
    interface interface_name broadcast
    ip mtu mtu_size [ mru mru_size ]
    end
```

NOTES:

- **ip mtu** *mtu_size*: Specify the MTU size. *mtu_size* must be an integer in the range of 5762048 bytes.
- **mru** *mru_size*: Specify the MRU size. *mru_size* must be an integer in the range of 5762048 bytes.
- Use the **no ip mtu** command to disable the MTU configuration.
- The maximum configurable value for MTU is 2048 bytes.. If MTU is not configured, the default value is 1500 bytes.
- MRU attribute is optional and when it is not configured, MRU is set to the same value as MTU.
- MRU optional attribute is not applicable to VPC-DI and VPC-SI platforms. This attribute is only visible on ASR 5500.
- On CUPS or ICUPS, the following error is displayed you when you try to configure MRU on an interface.

```
Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
enabled!
```

- Although the product allows configuring asymmetric MTU and MRU values on the same interface is not advised as it may result into undesirable behavior on the network.

Configuring the MRU Feature when no MTU is specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     bfd interval 300 min_rx 300 multiplier 3
     #exit
#exit
```

Configuring the MTU Feature when no MRU is specified

MRU = Configured MTU for backward compatibility. MRU = MTU = 1970 bytes.

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1970
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Configuring the MTU Feature when both MTU and MRU are specified

MTU = default MTU, MRU = default MTU

For example:

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1600 mru 1700
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

Verifying the Configured MRU

The output of the is enhanced to display the configured MRU value.

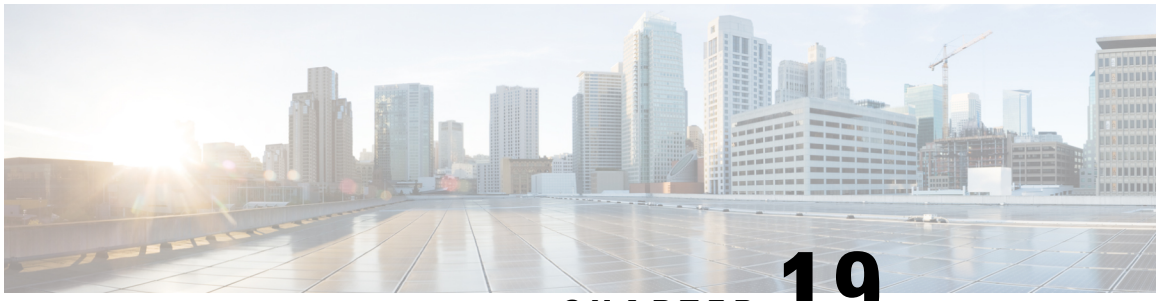
For example:

```
[EPC2]26kl-chassis# config
[EPC2]26kl-chassis(config)# context EPC2
[EPC2]26kl-chassis(config-ctx)# interface TO-EPC2-SGW-INGRESS
[EPC2]26kl-chassis(config-if-eth)# ip mtu 1500 mru 1970
```

```
[EPC2]26kl-chassis(config-if-eth)# end
[EPC2]26kl-chassis# show ipv6 interface
Intf Name: TO-EPC1-SGW-INGRESS
Intf Type: Broadcast
Description:
VRF: None
IP State: UP (Bound to 5/20 vlan id 190, 802.1P prior 0, ifIndex 85196802)
Router Advertisement: disabled MTU: 1500 MRU: 1970
IPv6 Link-Local Address: fe80::d272:dcff:fea3:8543/64
IPv6 Global Unicast Address: 2001::1:21/64
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 5
IPv6 Address: 2001::1:31/64
IPv6 Address: 2001::1:205/64
IP Address: 10.10.10.21 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.31 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.200 Subnet Mask: 255.255.255.0
```

NOTES:

- Use the **show ipv6 interface** command to verify if the Configurable MTU configuration is enabled or disabled.
- **no ip mtu**: Disables the Configurable MTU configuration.



CHAPTER 19

Multiple IP Versions Support

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC - DI • VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before release 21.2 and N5.1.

Revision Details	Release
This feature enables P-GW, S-GW, and SAEGW nodes to support the control messages received on all the transport addresses exchanged during the session setup.	21.8
First introduced.	Pre 21.2

Feature Description

This feature enables P-GW, S-GW, and SAEGW nodes to support the control messages received on all the transport addresses exchanged during the session setup.

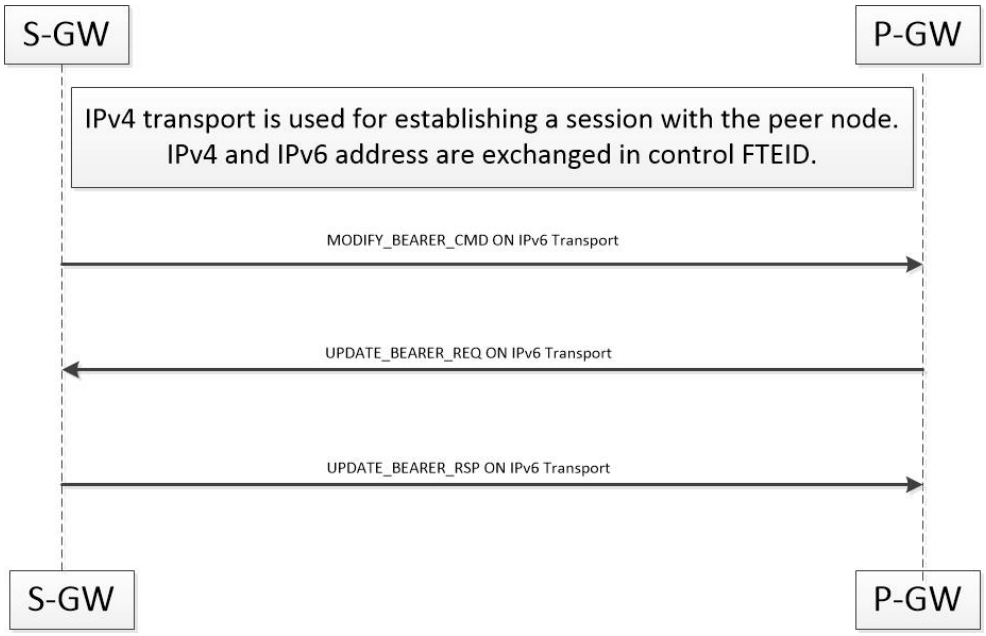
A new CLI command has been introduced at the egtp-service level to control the behavior of the BRCmd, MBCmd, and DBCmd messages.

How it Works

This section describes the working of this feature. Following is the sample call flow for MBCmd.

The following figure illustrates call flow when the feature is disabled:

The following figure illustrates the call flow when feature is enabled:



When a session is being established, P-GW, S-GW, and SAEGW node uses the IPv6 address as transport. This transport is used for establishing tunnel with peer node. If IPv4 and IPv6 addresses are exchanged in control FTEID then the node should handle MBCmd, BRCmd, and DBCmd messages on IPv4 transport by the nodes.

When a session is being established, if IPv4 address is used as a transport and is being used for establishing tunnel with peer node, and if IPv4 and IPv6 addresses are exchanged in control FTEID, then the MBCmd, BRCmd, and DBCmd messages are also handled on the IPv6 transport by the nodes.

When a session is being established, if IPv4 and IPv6 addresses are exchanged in data F-TEID by both peers, then the GTP-U data packets get handled on both IPv6 and IPv4 transport.

When a session is being established, if IPv4 address is used as a transport, however, C-TEID does not contain IPv4 address, then that message is rejected by the node. The nodes exhibit similar behavior for IPv6 addresses.

When a session is being established, if IPv4 and IPv6 addresses are exchanged in data F-TEID by both peers, then GTP-U data packets get handled on IPv6 and IPV4 transport both.

The following table displays the message handling behavior in different session establishment scenarios:

Table 27: Message Handling Behavior in Different Session Establishment Scenarios

Messages	Transport Used for Session Establishment	C-FTEID Sent During Session Establishment	Message Sent on Transport
MBR/DSR	IPv6	IPv4/IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv4/IPv6	IPv4
Change Notification	IPv6	IPv4/IPv6	IPv4
Suspend/Resume	IPv6	IPv4/IPv6	IPv4
MBR/DSR	IPv4	IPv4/IPv6	IPv6
MBC/DBC/BRC	IPv4	IPv4/IPv6	IPv6
Change Notification	IPv4	IPv4/IPv6	IPv6
Suspend/Resume	IPv4	IPv4/IPv6	IPv6
MBR/DSR	IPv6	IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv6	IPv4
Change Notification	IPv6	IPv6	IPv4
Suspend/Resume	IPv6	IPv6	IPv4
MBR/DSR	IPv4	IPv4	IPv6
MBC/DBC/BRC	IPv4	IPv4	IPv6
Change Notification	IPv4	IPv4	IPv6
Suspend/Resume	IPv4	IPv4	IPv6

Configuring Multiple IP Version Support

This section provides information on CLI commands available in support of this feature.

By default, this feature is enabled.

```
configure
  context context_name
    egtp-service service_name
      [no] gtpc command-messages dual-ip-stack-support
      end
```

NOTES:

- **no**: Disables the feature.
- **command-messages**: Configures MBC or DBC or BRC messages on S-GW and P-GW.
- **dual-ip-stack-support**: Enables P-GW, S-GW, SAEGW nodes to handle command messages on both IPv4/IPv6 transport, if supported.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot the Override Control Enhancement feature.

Show Commands and Outputs

This section provides information on show commands and their corresponding outputs for the Override Control Enhancement feature.

show configuration

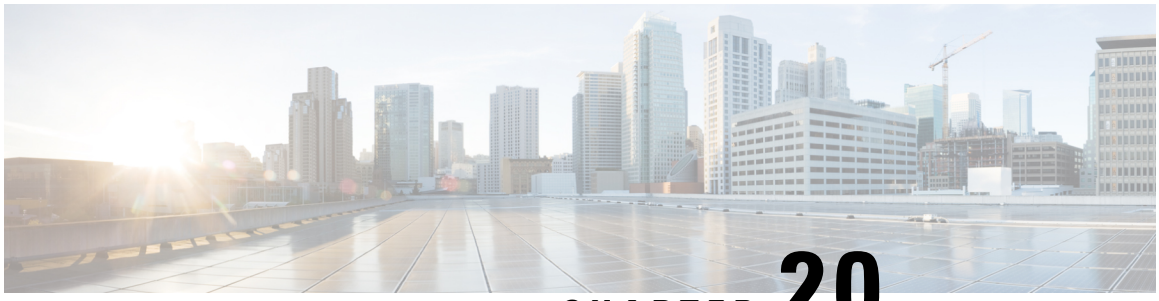
The following new fields are added to the output of this command:

- gtpc command-messages dual-ip-stack-support - Specifies the command messages on both IPv4/IPv6 transport if supported.

show egtp-service all

The following new fields are added to the output of this command:

- GTPC Command Messages Dual IP Support - Specifies the command messages on both IPv4/IPv6 transport if supported.



CHAPTER 20

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 5500. 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

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

A Look at Operator Policy on an SGSN

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

- APN information included in call activation messages are sometimes damaged, misspelled, missing. In such cases, the calls are rejected. The operator can ensure calls aren't rejected and configure a range of methods for handling APNs, including converting incoming APNs to preferred APNs and this control can be used in a focused fashion or defined to cover ranges of subscribers.
- In another example, it is not unusual for a blanket configuration to be implemented for all subscriber profiles stored in the HLR. This results in a waste of resources, such as the allocation of the default highest QoS setting for all subscribers. An operator policy provides the opportunity to address such issues by allowing fine-tuning of certain aspects of profiles fetched from HLRs and, if desired, overwrite QoS settings received from HLR.

A Look at Operator Policy on an S-GW

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

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

The Operator Policy Feature in Detail

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

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

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

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

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

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

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

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

Call Control Profile

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

- setting access restriction cause codes for rejection messages
- enabling/disabling authentication for various functions such as attach and service requests

- enabling/disabling ciphering, encryption, and/or integrity algorithms
- enabling/disabling of packet temporary mobile subscriber identity (P-TMSI) signature allocation (SGSN only)
- enabling/disabling of zone code checking
- allocation/retention priority override behavior (SGSN only)
- enabling/disabling inter-RAT, 3G location area, and 4G tracking area handover restriction lists (MME and S-GW only)
- setting maximum bearers and PDNs per subscriber (MME and S-GW only)

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

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

- 1 (only one) - call control profile can be associated with an operator policy
- 1000 - maximum number of call control profiles per system (e.g., an SGSN).
- 15 - maximum number of equivalent PLMNs for 2G and 3G per call control profile
  - 15 - maximum number of equivalent PLMNs for 2G per 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. In 21.4 and later releases, the configuration to enable default APN on failure of DNS query is enhanced to support S4-SGSN. When wildcard APN is

received in subscription, the DNS request is tried with the MS requested APN and on failure of DNS, it is retried with the APN value configured in the APN remap table.

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 can be converted to enable them to work with an SGSN. 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.

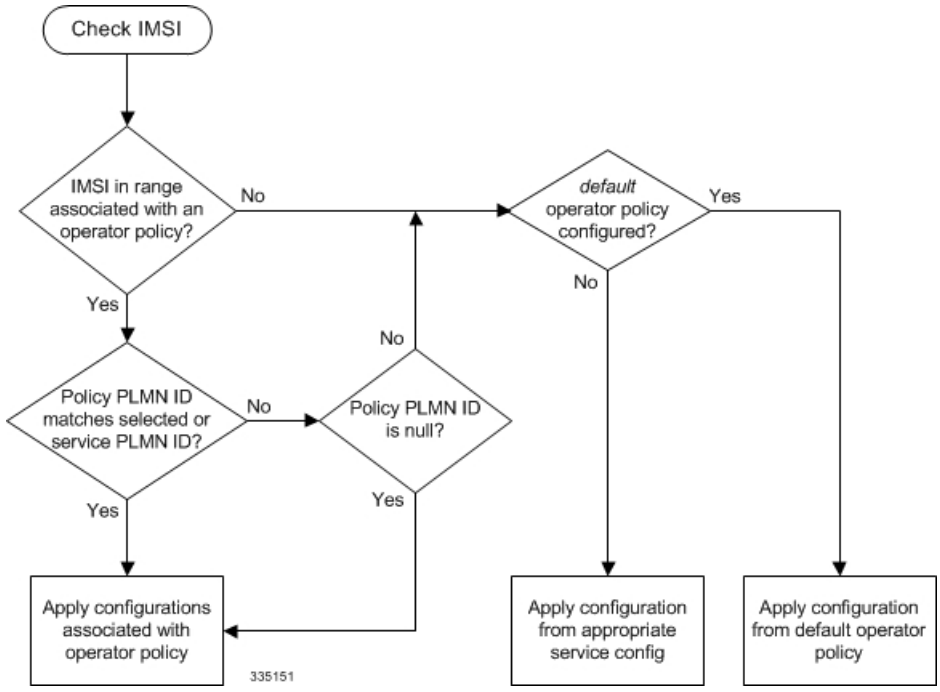
IMSI ranges are defined differently for each product supporting the operator policy feature.

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 47: 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.

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

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

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

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

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

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

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* .

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

Call Control Profile Configuration

This section provides the configuration example to create a call control profile and enter the configuration mode.

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

Configuring the Call Control Profile for an SGSN

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

```
configure
  call-control-profile profile_name>
    attach allow access-type umts location-area-list instance list_id
    authenticate attach
    location-area-list instance instance area-code area_code
    sgsn-number E164_number
    end
```

Notes:

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

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

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

```
configure
   call-control-profile profile_name
    associate hss-peer-service service_name  s6a-interface
    attach imei-query-type imei verify-equipment-identity
    authenticate attach
    dns-pgw context mme_context_name
    dns-sgw context mme_context_name
    end
```

Notes:

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

APN Profile Configuration

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

Use the **apn-profile** commands to define how calls are to be handled when the requests include an APN. More than one APN profile can be associated with an operator policy.

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

```
configure
  apn-profile profile_name
    gateway-address 209.165.200.227 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
    end
```

Notes:

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

APN Remap Table Configuration

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

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

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

```
configure
  apn-remap-table table_name
    apn-selection-default first-in-subscription
    wildcard-apn pdp-type ipv4 network-identifier apn_net_id
    blank-apn network-identifier apn_net_id (SGSN only)
    end
```

Notes:

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

- Some of the commands represented in the example above are common and some are product-specific. Refer to the *APN-Remap-Table Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Operator Policy Configuration

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

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

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

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

Notes:

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

IMSI Range Configuration

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

Configuring IMSI Ranges on the MME or S-GW

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

```
configure
  subscriber-map name
    lte-policy
      precedence number match-criteria imsi mcc mcc_number mnc mnc_number msin
 first start_range last end_range operator-policy-name policy_name
      end
```

Notes:

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

Configuring IMSI Ranges on the SGSN

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

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

Notes:

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

Associating Operator Policy Components on the MME

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

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

Use the following example to configure operator policy component associations:

```
configure
  operator-policy name
    associate apn-remap-table table_name
    associate call-control-profile profile_name
    exit
  lte-policy
    subscriber-map name
      precedence match-criteria all operator-policy-name policy_name
      exit
    exit
  context mme_context_name
    mme-service mme_svc_name
      associate subscriber-map name
      end
```

Notes:

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

Configuring Accounting Mode for S-GW

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

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

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

Notes:

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

Verifying the Feature Configuration

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

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

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

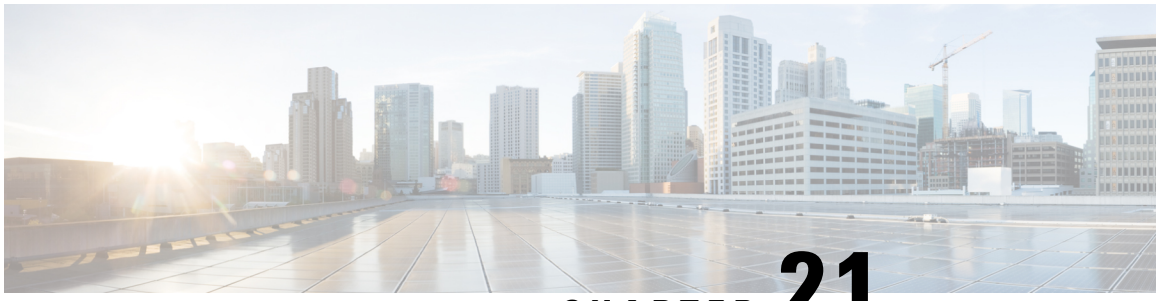
show operator-policy full name *oppolicy1*

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

```
show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name                    : ccprofile1
   Validity                                  : Valid
APN Remap Table Name                         : remap1
   Validity                                  : Valid
IMEI Range 711919739      to       711919777
   IMEI Profile Name                         : imeiprof1
      Include/Exclude                        : Include
        Validity                             : Valid
APN NI homers1
   APN Profile Name                          : apn-profile1
      Validity                               : Valid
```

Notes:

- If the profile name is shown as "Valid", the profile has actually been created and associated with the policy. If the Profile name is shown as "Invalid", the profile has not been created/configured.
- If there is a valid call control profile, a valid APN profile and/or valid IMEI profile, and a valid APN remap table, the operator policy is valid and complete if the IMSI range has been defined and associated.



CHAPTER 21

Overcharging Protection Support

This chapter describes the Overcharging Protection Support feature and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in the *P-GW Administration Guide*, the *S-GW Administration Guide*, or the *SAEGW Administration Guide* before using the procedures in this chapter.

This chapter includes the following sections:

Overcharging Protection Feature Overview

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

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

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

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

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

Once the criterion to signal "stop charging" is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. The MBReq will have an indication IE and/or a new private extension IE to send "stop charging" and "start charging" indication to P-GW. For Pause/Start Charging procedure (S-GW sends MBReq), MBRes from P-GW will have indication and/or private extension IE with Overcharging Protection information.

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

P-GW will resume charging downlink packets when either of these conditions is met:

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

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

Important When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.

License

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

Important Contact your Cisco account representative for information on how to obtain a license.

Configuring Overcharging Protection Feature

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

Configuring Overcharging Support on the P-GW

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

Important This configuration sequence is valid for the P-GW only.

```
configure
   apn-profile apn_profile_name
```

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

Notes:

- **remove:**

  Removes the specified configuration.

- **abnormal-s1-release:**

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

- **ddn-failure:**

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

- **drop-limit *drop_limit_value* { packets | bytes } }**

  Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.

  drop_limit_value is an integer from 1 through 99999.

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

Configuring Overcharging Support on the S-GW

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

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

Notes:

- Enabling this command indicates that the S-GW has to interact with a release 15 P-GW for the overcharging protection feature which does not support 3GPP TS 29.274 Release 12 – *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3*.
- When the **gtpc private-extension overcharge-protection** command is configured, the S-GW includes a Private Extension in the Create Session Request (CSReq) and Modify Bearer Request (MBReq) messages.
- Whenever a P-GW receives a CSReq with an Indication IE with the PDN Pause Support Indication flag set to 1, it responds only with an Indication IE.
- When a CSReq does not have an Indication IE with the PDN Pause Support Indication flag set to 1, but the P-GW supports Overcharging Protection, then it responds with both an Indication and Private Extension IE.

Monitoring and Troubleshooting

P-GW Schema

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

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

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

show apn statistics all

The following counters display overcharging protection stats for this APN:

- UL Ovrchrg Prtctn byte drop
- UL Ovrchrg Prtctn pkt drop
- DL Ovrchrg Prtctn byte drop
- DL Ovrchrg Prtctn pkt drop

show pgw-service all

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

- EGTP Overcharge Protection

show pgw-service statistics all

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

- Drops Due To Overcharge Protection
  - Packets
  - Bytes

show sgw-service statistics name <sgw_service_name>

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

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

show subscribers full

The following counters display Overcharging Protection for all subscribers:

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

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

show subscribers pgw-only full all

The following field and counters display Overcharging Protection:

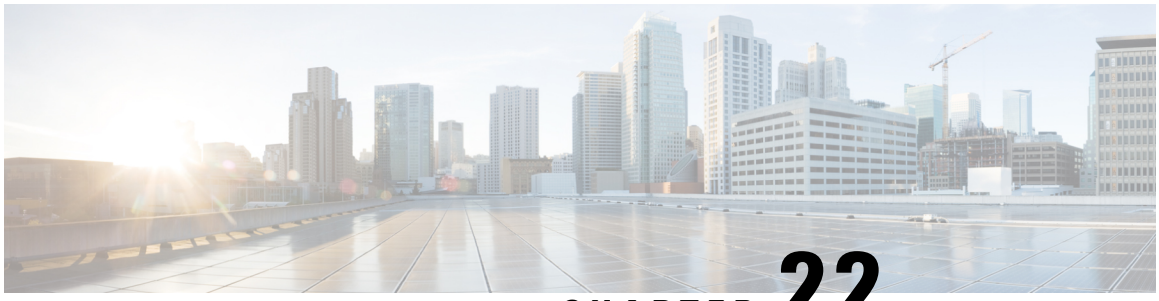
- Bearer State
  - in packet dropped overcharge protection
  - in bytes dropped overcharge protection
  - out packet dropped overcharge protection
  - out bytes dropped overcharge protection

show subscribers summary

The following counters display overcharging protection for all subscribers:

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

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



CHAPTER 22

Paging Policy Differentiation

This chapter describes the Paging Policy Differentiation feature and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in the *P-GW Administration Guide*, the *S-GW Administration Guide*, or the *SAEGW Administration Guide* before using the procedures in this chapter.

This chapter includes the following sections:

Feature Description

S-GW/P-GW provide configuration control to change the DSCP value of the user-datagram packet and outer IP packet (GTP-U tunnel IP header). DSCP marking is done at various levels depending on the configuration. When the Paging Policy Differentiation (PPD) feature is enabled, however, the user-datagram packet DSCP (tunneled IP packet) marking does not change.

Currently, standards specify QCI to DSCP marking of outer GTP-U header only. All configurations present at ECS, P-GW, and S-GW to change the user-datagram packet DSCP value are non-standard. The standards-based PPD feature dictates that P-CSCF or similar Gi entity marks the DSCP of user-datagram packet. This user-datagram packet DSCP value is sent in DDN message by S-GW to MME/S4-SGSN. MME/S4-SGSN uses this DSCP value to give paging priority.

Important P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Relationships

Since P-GW/S-GW support non-standard based DSCP marking, there is a conflict when both standard based PPD feature and non-standard based user-datagram packet DSCP configuration is enabled. To avoid this conflict:

- APN and service level configuration is ignored if PPD feature is enabled.
- S-GW/P-GW can alter the outer GTP-U header DSCP value, even if PPD feature is enabled.
- User-datagram packet DSCP value is unaltered by ECS, P-GW, and S-GW if PPD feature is enabled.
- At P-GW, APN-level configuration is added to enable/disable the PPD feature.
- At S-GW, service-level configuration is added to enable/disable the PPD feature. This is to send DSCP in Paging and Service Information IE of all the DDN messages triggered by either IMS-PDN or Internet-PDN, etc.

Important It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.

- Separate Paging feature and PPD feature co-exist in system. That means, if both features are enabled, both Paging and Service Information IE and Separate-paging IE are sent in DDN.
- Currently on P-GW, the DSCP configuration is getting applied at sub-session level during call setup time. So, when the PPD CLI is enabled for P-GW, it is applicable for new calls.
- Currently on S-GW, the DSCP configuration is getting applied at S-GW service level. So, when PPD CLI is enabled in S-GW service, it is applicable for both new and existing calls.
- Once the PPD CLI is enabled, it exists even after Session Recovery and ICSR switch over.
- The Paging and Service Information IE is used to carry per bearer paging and service information.

License

PPD is a license enabled feature. S-GW Paging Profile license key is required to enable PPD functionality for P-GW, S-GW, and SAEGW.

Important Contact your Cisco account representative for information on how to obtain a license.

How It Works

Architecture

S-GW

When S-GW supports the PPD feature, it shall include new Paging and Service Information IE in the Downlink Data Notification message triggered by the arrival of downlink data packets at the S-GW. The Paging Policy Indication value within this IE will contain the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the P-GW.

At S-GW, service-level configuration enables/disables the PPD feature. Once the PPD is configured, the feature is enabled and applicable for both existing and new calls.

P-GW

User-datagram packet DSCP value is unaltered by P-GW for downlink data. The PPD feature is supported only for S5/S8 interface. For all Handoff scenarios from other interface to S5/S8 interface, the PPD feature will get enabled if APN had it during its call setup time at that interface.

At P-GW, APN-level configuration enables/disables the PPD feature. If PPD feature is enabled for the call and handoff happens from S5/S8 interface to any other interface, PPD feature should get disabled. Now, if handoff happens and this call will come back to S5/S8 interface, PPD feature should become enabled.

SAEGW

To support PPD feature in SAEGW, both S-GW and P-GW configuration is required.

Relationships to Other Features

- The PPD feature is license controlled under the license for S-GW Paging Profile. Once the license is enabled, both features co-exist together and work independently. That means, DDN message might carry both DSCP marking specified by PPD feature and Priority DDN value specified by S-GW Paging Profile feature.
- At S-GW, the user-datagram packet DSCP value is used to send in DDN. S-GW can't change the DSCP, as per the local configuration (APN profile or service level). At eNodeB, the scheduling of the packet is based on the QCI instead of DSCP, however, any EPC node should not change/modify the inner DSCP value.
- If the PPD feature is enabled, none of the EPS nodes should change the user-datagram packet DSCP value. Therefore, ECS should avoid overwriting DSCP value of user-datagram packet when PPD is enabled.

Standards Compliance

The PPD functionality complies with the following standards:

- 29.274, CR-1565, "Paging Policy Indication in Downlink Data Notification Message"
- 23.401, CR-2731 "Paging policy differentiation for IMS voice"

Configuring Paging Policy Differentiation Feature

For the PPD feature to work, it must be enabled for P-GW and S-GW.

Both P-GW and S-GW services apply PPD configuration independently. Therefore, for any downlink data packet from an APN, there could be a case where P-GW does not have PPD configuration but S-GW has PPD configuration. To avoid such a conflict, you must configure the PPD functionality on both P-GW (APN level granularity) and S-GW (service level granularity).

Configuration

The following CLI commands are used to manage the functionality for the PPD feature.

Enabling on P-GW

The following command enables the PPD feature on P-GW at APN level.

```
configure
     context context_name
        apn apn_name
               paging-policy-differentiation
               end
```

Enabling on S-GW

The following command enables the PPD feature on S-GW at service level.

```
configure
     context context_name
        sgw-service service_name
               paging-policy-differentiation
               end
```

Notes:

- This is to send DSCP in Paging and Service Information IE of all the DDN messages triggered by either IMS-PDN or Internet-PDN, etc.
- It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.
- If PPD feature is enabled at S-GW service, it is applicable for all calls irrespective of the APN profiles.

Disabling on P-GW

The following command disables the PPD feature on P-GW at APN level.

```
configure
     context context_name
        apn apn_name
               no paging-policy-differentiation
               end
```

Disabling on S-GW

The following command disables the PPD feature on S-GW at service level.

```
configure
     context context_name
        sgw-service service_name
               no paging-policy-differentiation
               end
```

Monitoring and Troubleshooting Paging Policy Differentiation

This section includes show commands in support of the PPD feature.

P-GW Show Commands

This section provides information regarding P-GW show commands and/or their outputs in support of the PPD feature.

show apn name <apn_name>

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

show subscribers pgw-only full all

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

SAEGW Show Commands

This section provides information regarding SAEGW show commands and/or their outputs in support of the PPD feature.

show subscribers saegw-only full all

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

S-GW Show Commands

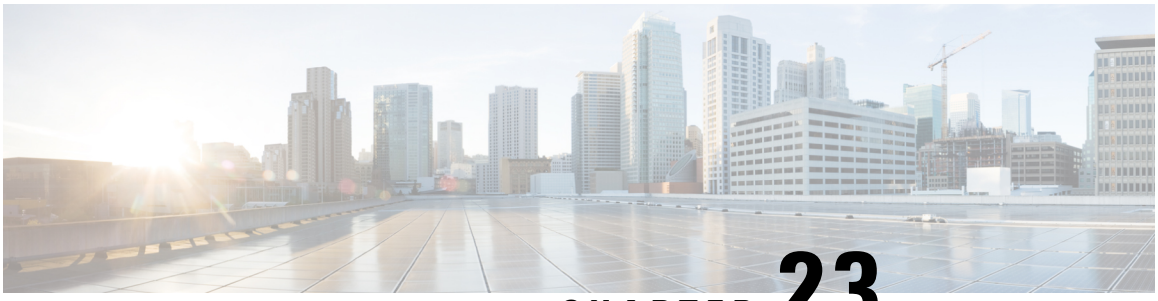
This section provides information regarding S-GW show commands and/or their outputs in support of the PPD feature.

show sgw-service name <service_name>

The following counter has been added to display PPD functionality.

```
Paging Policy Differentiation : Enabled
```

show sgw-service name <service_name>



CHAPTER 23

Presence Reporting Area

This chapter describes the following topics:

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW • S-GW
Applicable Platform(s)	ASR 5500
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.4

Feature Description

This feature adds support for the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards.

The Presence Reporting Area is an area defined within the 3GPP packet domain for reporting of UE presence within that area. This is required for policy control and in charging scenarios. In E-UTRAN, the PRA may consist in a set of neighbor or non-neighbor Tracking Areas, or eNBs or cells. There are two types of Presence Reporting Areas: "UE-dedicated Presence Reporting Areas" and "Core Network pre-configured Presence Reporting Areas" that apply to an MME pool.

This feature has the following highlights:

- This feature is supported for LTE/S4-SGSN related RAT-type. For any other RAT type, P-GW ignores PRA information received from the PCRF.
- Currently single PRA-ID is supported per session as specification compliance.
- Currently, in P-GW, core network pre-configured presence reporting area is supported.
- For ICSR to N-1 release, PRA feature is not supported.
- PRA-ID is not supported on CDR interface, that is, Gz, Gy and Rf.

How It Works

During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA are required for an IP-CAN session. This determination is made based on the subscriber's profile configuration and the supported AVP features. The parameter CNO-ULI is set for the same. If the reporting is required for the IP-CAN session, the PCRF provides Presence-Reporting-Area-Information AVP, which contains the PRA identifier within the Presence-Reporting-Area-Identifier AVP to the PCEF. For a UE-dedicated PRA, PCRF provides the list of elements consisting of the PRA within the Presence-Reporting-Area-Elements-List AVP to the PCEF. The PCRF might activate the reporting changes of the UE presence in the PRA by subscribing to the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event trigger at the PCEF at any time during the entire IP-CAN session.

When the UE enters or leaves the PRA, PCEF reports the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event. Also, the PCEF also reports the PRA status within the Presence-Reporting-Area-Status AVP and PRA identifier within Presence-Reporting-Area-Identifier AVP included in Presence-Area-Information AVP.

Following table describes the scenario and its associated behavior:

Scenario	Behavior
When PCRF sends a new PRA ID different than the initial call setup.	• P-GW receives the new PRA ID during the initial call setup and stores the PRA ID information. • In RAR, the PRA_EVENT_TRIGGER is registered. • P-GW send PRA_ACTION PRA ID="A", ACTION=start. • In CCA-U, a new PRA ID is received. • P-GW stores new PRA ID information • P-GW sends PRA_ACTION PRA ID = "B", Action=start but does not send Action=stop for the earlier PRA. **Important** Ideally, in above condition, PCRF disables the event triggers first and sends a new PRA-ID=B and enables the event trigger in subsequent message.
When PCRF sends a new PRA ID which is same as the initial call setup.	PRA ID does not send any PRA Action toward S-GW and P-GW ignores this.
PRA ID Decode Behavior	If PRA ID received is "core network pre-configured presence reporting area", then, P-GW ignores the "Element List" coming from PCRF. Otherwise, if PRA ID is "UE-dedicated Presence Reporting Area", then, P-GW parses the "Element List" and forwards it toward the access side.
If PRA ID values from PCRF are 1 octet, 2 octets, and 3 octets.	MSB of the value received from the PCRF is evaluated to find the PRA type. While encoding, GTPC side zeros are prepended to make it 3 octets. For example, if PRA ID = FC (1111 1100) is received from PCRF it is considered as UE-dedicated PRA and while decoding it is decoded as 00 00 FC. P-GW forwards PRA information toward the roaming subscriber if it is received from the PCRF or from UE. **Important** Change of UE presence in the Presence Reporting Area reporting does not apply to the roaming scenario.
Roaming Scenario	Change of UE presence in the Presence Reporting Area reporting does not apply to the roaming scenario. When the serving EPC node (MME, S4-SGSN) is changed, the Presence Reporting Area identifier is transferred for all PDN connections as part of the MM Context information to the target serving node during the mobility procedure. The list of Presence Reporting Area elements are also transferred if they are provided by the P-GW.

Scenario	Behavior
Handover Behavior: How the PRA identifier is communicated from source MME/S4-SGSN to target MME/S4-SGSN.	MME/S4-SGSN gets the PRA Identifier from source MME/S4-SGSN as part of MM Context information. When the serving EPC node (MME, S4-SGSN) is changed, the Presence Reporting Area identifier is transferred for all PDN connections as part of the MM Context information to the target serving node during the mobility procedure. The list of Presence Reporting Area elements are also transferred if they are provided by the P-GW.
Handoff Behavior: How PRA is disabled when the new access type is not supported PRA.	Depending on the access type and internal configuration PCRF deactivates the PRA, if the new access PRA is not supported. During an IP-CAN session, P-GW notifies the PCRF that the UE is located in an access type, where local PCRF configuration is such that the reporting changes of the UE presence in the PRA are not supported. The PCRF unsubscribes to the change of UE presence in the PRA, if previously activated.
Behavior if for E-UTRAN some nodes do not support PRA.	If PRA is enabled from PCRF, then EPC nodes supports it. If all nodes are not supported, then PRA PCRF activates the Location Change Reporting. **Important** For E-UTRAN access, homogeneous support of reporting changes of UE presence in a Presence Reporting Area in a network is assumed. When the PCRF configuration indicates that reporting changes of the UE presence in a PRA is supported for E-UTRAN, this means all P-GWs, all MME, and all S-GW support it, including the MME and S-GW working in the network sharing mode. If the change of UE presence in the PRA reporting is not supported, the PCRF may instead activate the location change reporting at the cell or serving area level.
When access side procedure failure or collision occurs (Create or Update Bearer procedure)	In Update or Create bearer procedure failure where the PRA action was sent in the request message and if PRA information was not received in response message, P-GW attempts to send the PRA action in next control procedure toward the remote peer. In Update or Create bearer procedure failure where PRA action was sent in the request message and if PRA information was not received in the response message, P-GW assumes it as PRA action was successfully communicated toward the remote peer. In the Update or Create bearer collision scenario where PRA action was sent in the request message and Update or Create procedure got aborted, P-GW attempts to send the PRA action in next control procedure toward the remote peer.

Multiple Presence Reporting Area

Important This feature is introduced in release 21.9.1.

P-GW supports negotiation of Multiple-Presence Reporting Area feature in Feature-List-ID 2 over Gx interface with PCRF. The CNO-ULI feature will be used only when the P-GW and/or the PCRF does not support Multiple-PRA and both P-GW and PCRF support CNO-ULI.

When the Multiple-PRA feature is supported during the lifetime of the IP-CAN session P-GW handles the change of UE Presence in Reporting Area(s) request from PCRF in PRA-Install AVP including the Presence-Reporting-Area-Information AVP(s) which each contains the Presence Reporting Area Identifier within the Presence-Reporting-Area-Identifier AVP.

P-GW Handling the Event Trigger

CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT from PCRF for the activation of the reporting changes of UE presence in Presence Reporting Area(s).

P-GW handles the PRA Identifier(s) modify request from PCRF with the new PRA within the PRA-Install AVP as described above and/or by removing the existing PRA(s) within the PRA-Remove AVP. In this case, the Presence-Reporting-Area-Identifier AVP of the removed PRA must be included within the Presence-Reporting-Area-Information AVP(s).

P-GW supports PRA-Install and PRA-Remove AVPs from PCRF in the following messages:

- CC-Answer (CCA) Command
- Re-Auth-Request (RAR) Command

The P-GW handles the request from PCRF to unsubscribe to the change of UE presence in Presence Reporting Area wherein PCRF provides the Event-Trigger AVP with the value CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) removed, if previously activated.

P-GW supports the maximum of 4 PRA(s) for a IP-CAN session at any given point of time. The maximum number of PRAs is configurable in PCRF and must be capped to 4. P-GW will ignore the Presence Reporting Area Identifiers entries beyond 4.

When the P-GW receives the presence reporting area information from the serving node over S5/S8 interface indicating that the UE is inside or outside of one or more presence reporting areas or any of the presence reporting areas is set to inactive, the P-GW will check if the reported presence reported area identifier corresponds to a presence reporting area that is relevant for the PCRF. In that case, the P-GW reports the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT event in the Event-Trigger AVP additionally, the P-GW also reports the presence reporting area status within the Presence-Reporting-Area-Status AVP and presence reporting area identifier within Presence-Reporting-Area-Identifier AVP included in Presence-Reporting-Area-Information AVP(s) for each of the presence reporting areas reported by the serving node.

The P-GW de-activates the relevant IP-CAN specific procedure for reporting change of UE presence in Presence Reporting Area, when the PCRF and OCS unsubscribe to change of UE presence in Presence Reporting Area.

PRA-Install AVP (3GPP-EPS access type) Definition

The PRA-Install AVP (AVP code 2845) is of type Grouped, and it is used to provision a list of new or updated Presence Reporting Area(s) for an IP-CAN session.

AVP Format:

```
PRA-Install ::= < AVP Header: 2845 >
 *[ Presence-Reporting-Area-Information ]
 *[ AVP ]
```

PRA-Remove AVP (3GPP-EPS access type) Definition

The PRA-Remove AVP (AVP code 2846) is of type Grouped, and it is used to stop the reporting of a list of Presence Reporting Area(s) for an IP-CAN session.

AVP Format:

```
PRA-Remove ::= < AVP Header: 2846 >
 *[ Presence-Reporting-Area-Identifier ]
 *[ AVP ]
```

Configuring Presence Reporting Area

Configuring PRA

Use the following configuration to enable the PRA:

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features cno-uli
            { default | no } diameter encode-supported-features
            end
```

NOTES:

- **diameter encode-supported-features**: Enables or disables encoding and sending of Supported-Features AVP.
- **cno-uli**: Enables Presence Reporting Area Information Reporting feature.
- **no**: Removes the previously configured supported features.
- **default**: Applies the default setting for this command.

Configuring Multiple-PRA

Use the following configuration to enable Multiple Presence Reporting Area (Multiple-PRA) Feature.

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features multiple-pra
```

```
{ default | no } diameter encode-supported-features
end
```

NOTES:

- **ims-auth-service** *service_name*: Creates an IMS authentication service. *service_name* must be an alphanumeric string of 1 through 63 characters.
- **policy-control**: Configures Diameter authorization and policy control parameter for IMS authorization.
- **diameter encode-supported-features**: Enables encoding and sending of Supported-Features AVP.
- **multiple-pra**: Enables the Multiple Presence Reporting Area Information Reporting feature.
- **no**: Removes the previously configured supported features.
- **default**: Applies the default setting for this command.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of this feature.

show ims-authorization service name *<service-name>*

The output of the above command is modified to display the negotiated conditional policy features related information. The modified output is as follows:

```
Context: ha
  IMS Authorization Service name: imsa-Gx
                  ……
  Diameter Policy Control:
    Endpoint: gx.st16.starentnetworks.com
    Origin-Realm: starentnetworks.com
    Dictionary: r8-gx-standard
    Supported Features:
      mission-critical-qcis
      conditional-policy-info-default-qos
cno-uli
    Request Timeout:
        Initial Request   : 100 deciseconds
        Update Request    : 100 deciseconds
        Terminate Request : 100 deciseconds
    Endpoint Peer Select: Not Enabled
    Reauth Trigger: All
    Custom Reauth Trigger:
      QoS-Change
```

show ims-authorization sessions full all

The output of this command includes the following fields:

```
CallId: 00004e26            Service Name: imsa-Gx
  IMSI:  123456789012349
  Session ID: gx.st16.starentnetworks.com;20006;2305;598ab8cf-102
  Bearer Type: GTP
  SGSN IP-Addr: 192.168.23.4
  APN: starent.com
  Bearer Control Mode: UE/NW
  State: Connected
  Negotiated Supported Features:
    3gpp-r8
    conditional-policy-info-default-qos
    cno-uli
  Auth Decision:
    Event Triggers:
      QoS-Change
      RAT-Change
      Change-Of-UE-Presence-In-PRA
      Usage-Report
      Resource-Modification-Request
    multiple-pra
```

show ims-authorization service statistics

The output of the above command is modified to display the PRA feature statistics. The modified output is as follows:

```
IMS Auth Service Statistics Summary:
Total Services:      2
Auth Session:
  Current Active:               1
  Current Fallback Session:     0             Current PCRF Session:          1
  Total Attempted:              1             Total Setup:                   1
  Total Failed:                 0             Total Released:                0
  Total Fallback:               0
Re-Authorization Triggers:
  SGSN Change:                  0             PLMN Change:                   0
  RAT Change:                   0             TFT Change:                    0
  Bearer Recovery:              0             Bearer Loss:                   0
  QoS Change:                   0             Policy Failure:                0
  IP-CAN Change:                0             Resources Limitation:          0
  Max Num of Bearers Rchd:      0             QoS Chng Exceeding Auth:       0
  RAI Change:                   0             User Location Change:          0
  TAI Change:                   0             ECGI Change:                   0
  PCRF Triggered ReAuth:        0             Preservation Changed:          0
  Reactivation Changed:         0             Revalidation Timeout:          0
  AN GW Changed:                0             Out Of Credit Reauth:          0
  Reallocation Of Credit:       0             Def EPS Bearer QoS Chng:       0
  Successful Resource Alloc:    0             Usage Report:                  0
  Service Flow Detection:       0             UE Timezone Change:            0
UE IP Address Allocate:         0             UE IP Address Release:         0
  Resource Modification Req:    0             APN AMBR Mod Failure:          0
  Def Bearer QOS Mod Failure:   0             Tethering Flow Detected:       0
  Chrg Correlation Exchange:    0             Subnet Change:                 0
  Session Recovery:             0             Session Sync:                  0
  Access Nw Info Report:        0             DCCA Failure Report:           0
  Application Start:            0             Application Stop:              0
  Change Of UE Presence In PRA: 1
Local Fallback:
CCRU sent:                      0
```

show subscribers pgw-only full all

The output of this command includes the following fields:

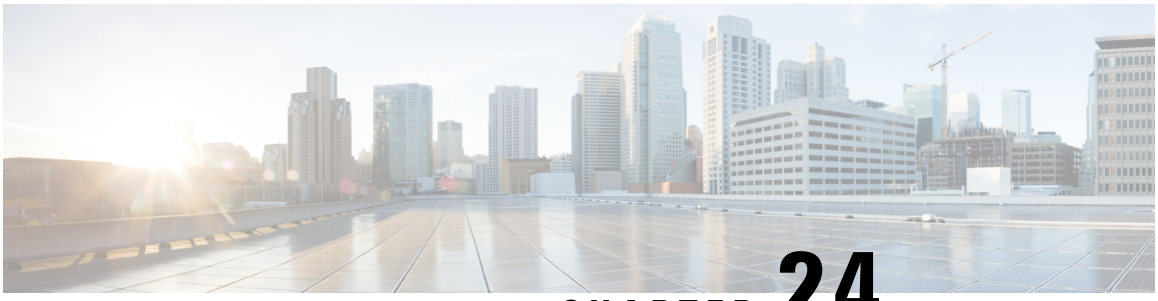
```
Username        : xyz
Subscriber Type : Visitor
Status          : Online/Active
State           : Connected
Connect Time    : Mon Aug 28 07:32:13 2017
Auto Delete     : No
Idle time       : 00h00m06s
MS TimeZone     : n/a                  Daylight Saving Time: n/a
Access Type: gtp-pdn-type-ipv4         Network Type: IP
Access Tech: eUTRAN                    pgw-service-name: pgw1
Callid: 00004e23                       IMSI: 123456789012349
MSISDN: 9326737733
Interface Type: S5S8GTP                Low Access Priority: N/A
TWAN Mode: N/A
eMPS Bearer: No
Emergency Bearer Type: N/A
IMS-media Bearer: No
S6b Auth Status: Enabled
Access Peer Profile: default
Acct-session-id (C1): C0A8170100000003
ThreeGPP2-correlation-id (C2): 00500660 / 002shwI-
Card/Cpu: 2/0                          Sessmgr Instance: 1
ULI:
 TAI-ID:
  MCC: 214  MNC: 365
  TAC: 0x6789
 ECGI-ID:
  MCC: 214 MNC: 365
  ECI: 0x1234567
PRA Information:
 PRA-ID: 0x801204      Action: Start           Status: In
PRA Information:
 PRA-ID: 0xA11202      Action: Start           Status: N/A
```

show subs saegw-only full all

The output of the above command is modified to include the PRA Information such as PRA-ID, PRA Status, and PRA Action. The modified output is as follows:

```
Username          : xyz
SAEGW Call mode   : Co-located
Subscriber Type   : Visitor
Status            : Online/Active
State             : Connected
Bearer State      : Active
Connect Time      : Mon Aug 28 08:21:45 2017

SAEGW UID         : 10001
Idle time         : 00h00m19s
Auto Delete       : No
Callid            : 4e25                        IMSI                : 241460144418770
Card/Cpu          : 2/0                         Sessmgr Instance    : 1
Source context    : ingress                     Destination context : egress
Bearer Type       : Default                     Bearer-Id           : 5
Access Type       : gtp-pdn-type-ipv4           Network Type        : IP
Access Tech       : eUTRAN                      saegw-service-name  : saegw
MSISDN            : 9326737733
```

```
TWAN Mode          : N/A
eMPS Bearer        : No
IPv6 alloc type    : n/a
ECS Rulebase       : prepaid
Chrg Char Sel Mod : Peer Supplied
Restoration priority level : n/a
HLCOM Session      : No
IP Address         : 10.0.0.5
Bearer capable for restoration: No
UE P-CSCF Restoration Support : No

Peer Profile       :
  PGW Access       : default
  SGW Access       : default
  SGW Network      : default

ULI                : TAI-ID
  MCC              : 214                          MNC              : 365
  LAC              : n/a                          TAC              : 0x6789
  SAC              : n/a                          RAC              : n/a
  CI               : n/a                          ECI              : 0x1234567

PRA Information    :
  PRA-ID: 0xFC0104     Action: Start           Status: In

Bearer QoS         :
 QCI               : 5
 ARP               : 0x08
 PCI               : 0 (Enabled)
 PL                : 2
 PVI               : 0 (Enabled)
 MBR Uplink(bps)   : 0                          MBR Downlink(bps)    : 0
 GBR Uplink(bps)   : 0                          GBR Downlink(bps)    : 0
```



CHAPTER 24

Revised Marking for Subscriber Traffic

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	• Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. This feature is fully qualified in this release.	21.20.2

Revision Details	Release
In this release P-GW supports configuration of 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. **Important** This feature is not fully qualified in this release, and is available only for testing purposes. For more information, contact your Cisco Account Representative.	21.20

Feature Description

802.1p/MPLS EXP marking helps in providing QoS treatment by prioritizing traffic at L2 level.

Currently, data traffic for different access types, such as GGSN, eHRPD, P-GW, and S-GW, refer to the QCI-QoS table and configure the appropriate 802.1p or MPLS-EXP (L2 QoS) markings based on the internal-qos value associated with particular row. However, the usage of internal-qos from the QCI-QoS table is not configurable and uses the default values. In addition, L2 QoS (802.1p/MPLS EXP) marking is not supported in GGSN, SAEGW, and GTPv1/eHRPD calls on P-GW.

With this feature, you can:

- Configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls.
- Mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. A new CLI command has been introduced to support service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Limitations

- This feature does not control the behavior of the control packets. The control packets (GTP-C) continue to get L2 marked based on DSCP derived L2 marking.
- This feature is not supported on standalone GGSN. It is supported on GnGp-GGSN node.

How It Works

You can configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. You can also mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Behavior Changes for Different Services

This section describes behavior of this feature for different services. Please see the *Command Changes* section for more information on the CLI command options and its behavior:

GGSN/P-GW GTPv1 Calls:

Previous Behavior: Earlier, the traffic was not marked for data path. This was default behavior for GGSN.

New Behavior: A new CLI command has been introduced to mark the traffic based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked. When the feature is not enabled, traffic is not marked.

P-GW GTPv2, S-GW, SAEGW Calls:

Previous Behavior: The QCI-QoS mapping feature used internal-QoS for L2 marking, which in turn uses QCI-Derived marking for data traffic. This was the default behavior for P-GW, S-GW, and SAEGW calls.

New Behavior: With this feature, the traffic is marked based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked and the default behavior is executed. When the feature is not enabled, traffic is not marked.

Configuring Revised Marking for Subscriber Traffic

By default, the traffic data path is supported with GGSN.. The internal priority can be configured in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. Subscriber traffic can also be marked with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Configuring Internal Priority

To configure internal priority in the QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls, use the following service specific configuration. This command in the GGSN service configuration overrides the behavior of QCI-QOS-mapping for data packets only.

```
configure
     context context_name
        ggsn-service service_name
           internal-qos data { dscp-derived | none | qci-derived }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           end
```

Notes:

- **no:** Disables the specified functionality.
- **default:** Disables the functionality.

- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.
- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show** *service-type* **{ all | name** *service_name* **}**

Please see the *Monitoring and Troubleshooting Revised Marking for Subscriber Traffic* section for the command output.

Configuring 802.1p and MPLS EXP Marking for User Data Traffic

This section describes how to configure the 802.1p and MPLS Experimental (EXP) bits marking for user data traffic. Configuring the feature consists of the following tasks:

1. Configure ip-dscp-iphb-mapping.
2. Configure L2-mapping
3. Configure qci-qos-mapping.
4. Associate the l2-mapping in Egress context.
5. Associate the l2-mapping in Igress context.
6. Associate internal-qos data in P-GW and S-GW service

Configure ip-dscp-iphb-mapping

Use the following example to access *QOS Profile Configuration Mode* and configure ip-dscp-iphb-mapping.

```
configure
  qos ip-dscp-iphb-mapping dscp Value  internal-priority cos  value
  end
```

Notes:

- *qos ip-dscp-iphb-mapping dscp* : Creates a QOS profile.
- **dscp** : Specify dscp mapping with Hexadecimal value between 0x0 and 0x3F.
- **internal-priority cos** : Define the Class of Service (cos) value between 0x0 and 0x7.

Configure L2-mapping

Use the following example to access *QOS L2 Mapping Configuration Mode* and configure L2 mapping.

```
configure
  qos l2-mapping-table name  { name map_table_name | system-default }
    internal-priority cos class_of_service_value color color_value [ 802.1p-value
 802.1p_value ] [ mpls-tc mpls_tc_value ]
      end
```

Notes:

- **qos l2-mapping-table name** : Maps qos from internal qos to l2 values.
- **internal-priority cos** : Maps internal QoS priority with Class of Service (COS) values.
  - *class_of_service_value*: Specify a Hexadecimal number between 0x0 and 0x7.
  - **802.1p-value** : Maps to a 802.1p value and *.802.1p_value* must be a Hexadecimal number between 0x0 and 0xF.
  - **mpls-tc** *mpls_tc_value*: Maps to an MPLS traffic class. *mpls_tc_value* must be a Hexadecimal number between 0x0 and 0x7.

Configure qci-qos

Use the following commands to configure qci-qos mapping.

```
Configure
  qci-qos-mapping  name
    qci  num [ arp-priority-level arp_value ] [ downlink [ encaps-header
 { copy-inner | dscp-marking  dscp-marking-value } ] [ internal-qos
priority  priority ] [ user-datagram dscp-marking  dscp-marking-value  ]
 ]  [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking
dscp-marking-value } ] [ internal-qos priority  priority ]  [ user-datagram
 dscp-marking  dscp-marking-value  ] ]
     end
```

Notes:

- **qci-qos-mapping** : Maps internal QoS priority with Class of Service (CoS) value.
- **quci num**: Specifies the non-standard, operator-defined QCI value to be enabled.
- **arp-priority-level** : Specifies the address retention priority (ARP) priority level.
- **downlink**: Configures parameters for downlink traffic.
- **encaps-header { copy-inner | dscp-marking** *dscp-marking-value}*: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.
  - **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
  - **dscp-marking** *dscp-marking-value*: Specifies that the DSCP marking is to be defined by this keyword.

dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

- **uplink**: Configures parameters for uplink traffic.
- **internal-qos priority** *priority* : Sets the internal QoS. These get resolved in L2 values.
- **user-datagram dscp-marking** *dscp-marking-value*: Specifies that the IP DSCP marking is to be defined by this keyword.*dscp-marking-value* is expressed as a hexadecimal number from 0x00 through 0x3F.

Associate L2-mapping table

Use the following commands to associate L2 mapping table in egress context and ingress context.

```
configure
   context egress context_name | ingress context_name
   associate l2-mapping-table { name table_name
   exit
   context ingress context_name
   associate l2-mapping-table { name table_name
   end
```

- **associate l2-mapping-table**: Maps qos from internal qos to l2 values.
- **{ name** *table_name* : Specifies the name of table to map qos from internal qos to l2 values. *table_name* must be a alphanumeric string of size 1 to 80.

Associate internal-qos-data in a P-GW and S-GW Service

Use the following commands to associate internal-qos-data in a P-GW and S-GW service.

```
configure
     context context_name
        pgw-service service_name
           internal-qos data { qci-derived | dscp-derived | none }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           exit
        sgw-service service_name
           internal-qos data { qci-derived | dscp-derived | none }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           end
```

Notes:

- **no:** : Disables the specified functionality.
- **default** : Disables the functionality.
- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.

- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Monitoring and Troubleshooting Revised Marking for Subscriber Traffic

The following section describes commands available to monitor Revised Marking for Subscriber Traffic.

Internal Priority Show Commands

The following section describes commands available to monitor Internal Priority.

show configuration

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
internal-qos data none
```

- When **internal-qos data** is configured as **qci-derived**:

```
internal-qos data qci-derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
internal-qos data dscp-ds-derived
```

- When **internal-qos data** is **not configured**:

```
no internal-qos data
```

show *service-type* { all | name *service_name* }

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:         None
```

- When **internal-qos data** is configured as **qci-derived**:

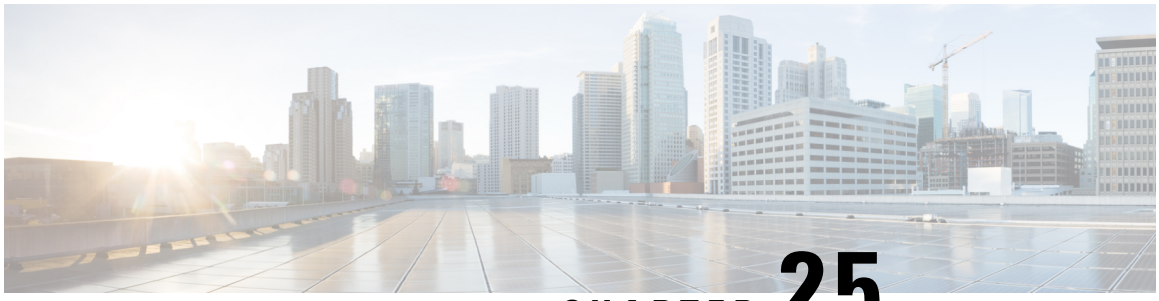
```
Internal QOS Application:   Enabled
Internal QOS Policy:        QCI Derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
 Internal QOS Application:    Enabled
 Internal QOS Policy:         DSCP Derived
```

- When **internal-qos data** is **not configured**:

```
        Internal QOS Application:     Backward-compatible
```



CHAPTER 25

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 for the following products:

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

Important The Rf interface is not supported on the S-GW.

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

This chapter includes the following topics:

Introduction

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

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

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

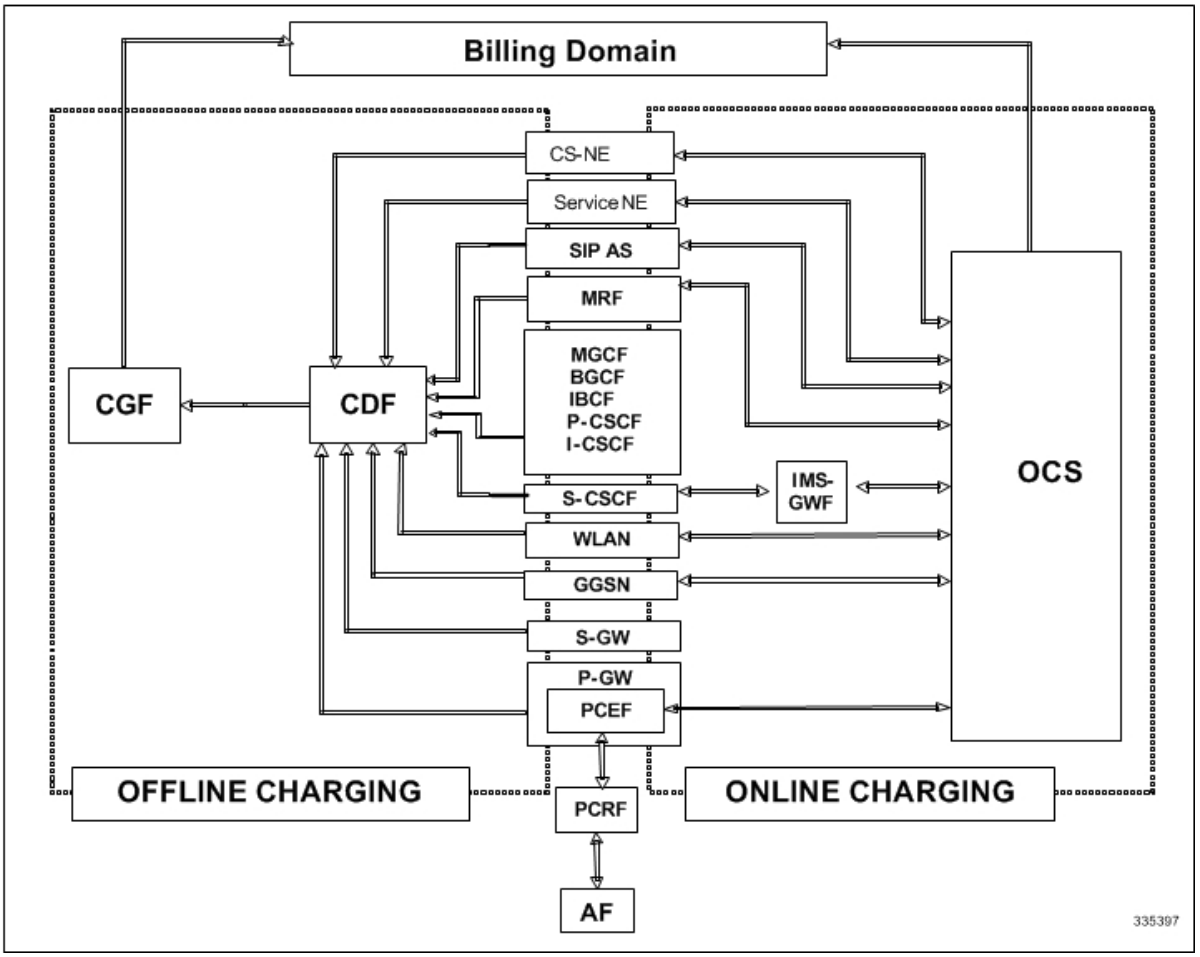
In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

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

Offline Charging Architecture

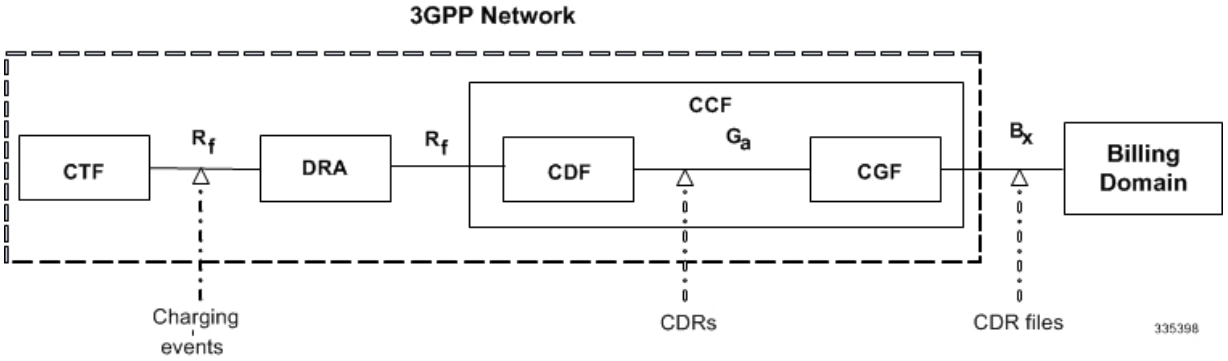
The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).

Figure 48: Charging Architecture



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

Figure 49: Logical Offline Charging Architecture



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

Charging Collection Function

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

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

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

Charging Trigger Function

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

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

Dynamic Routing Agent

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

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one

Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

License Requirements

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

Supported Standards

Rf interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release9)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• 5G Non Standalone Solution Guide • AAA Interface Administration and Reference • Command Line Interface Reference • MME Administration Guide • Statistics and Counters Reference

Revision History

Revision Details	Release
The StarOS 21.22 is enhanced, where an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW.	21.22

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 28: Rf ACR Event Types

Request	Description
START	Starts an accounting session
INTERIM	Updates an accounting session
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event

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 29: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE
	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 30: Diameter Rf Messages

Command Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

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.

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.

The 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.

Once a CCR-U was sent out over Gy interface, 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*.

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

The P-GW is not generating Rf records when the UE was identified to be in IDLE state and not sending any data. 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*.

QoS Change Scenarios

QOS_CHANGE Trigger in Rf Records During eHRPD-LTE Handoff

The SDC in the generated Rf record does not include QOS_CHANGE trigger during handoff from eHRPD to LTE.

QoS Change for Default Bearer

For a change in the QoS of default bearer, NR SDV containers will not be seen unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e. the default bearer.

Diameter Rf Duplicate Record Generation

This section describes the overview and implementation of Rf Duplicate Record Generation feature.

This section discusses the following topics for this feature:

- Feature Description, on page 342
- Configuring Rf Duplicate Record Generation, on page 344
- Monitoring and Troubleshooting the Rf Duplicate Record Generation, on page 346

Feature Description

This feature is introduced to support creation and communication of duplicate Rf records to secondary AAA group servers configured for the Rf interface.

To achieve this functionality, the following configurations must be enabled –

- **aaa group** CLI command under APN to configure a maximum of 2 AAA groups - primary and secondary AAA groups, or two different endpoints for Rf Diameter accounting servers
- **diameter accounting duplicate-record** under AAA group to allow Rf duplicate record creation

The **diameter accounting duplicate-record** is a new CLI command introduced in this release for duplicating the Rf START, INTERIM and STOP accounting records.

Important This is a license-controlled CLI command. For more information, contact your Cisco account representative.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.

Important The failed duplicate records will neither be written to HDD nor added to the archival list.

There is no change in the current behavior with the primary AAA group messages. The primary AAA group is independent of the secondary AAA group, and it has multiple Rf servers configured. When the Rf servers do not respond even after multiple retries as per the applicable configuration, the Rf records are archived and stored in HDD. This behavior continues as is irrespective of the configuration of secondary aaa-group.

Secondary aaa group has a very similar configuration as the primary aaa group except that the new CLI command **diameter accounting duplicate-record** is additionally included to configure the secondary aaa-group. It is also important to note that different Diameter endpoints and a separate set of Rf servers should be provisioned for both primary and secondary AAA groups.

If all the configured servers are down, the request message will be discarded without writing it in HDD or archiving at aaamgr.

The original and duplicate Rf messages use two different aaa-groups and two different Diameter endpoints. Hence, the values for Session-ID AVP will be different. Based on the configuration of primary and secondary endpoints the values for Origin-Host, Origin-Realm, Destination-Realm, and Destination-Host AVPs may be different. Also based on the configuration under policy accounting for inclusion of virtual/gn apn name for secondary group Called-Station-ID AVP might change. All other AVPs will have the same values as with the primary aaa group Rf message.

Also, note that the values such as Acct-Interim-Interval (AII) interval received in ACA from secondary group of AAA servers will be ignored.

Relationships to Other Features

This feature can be used in conjunction with Virtual APN Truncation feature to achieve the desired results.

The Virtual APN Truncation feature is new in release 21. For more information on this feature, see the administration guide for the product you are deploying.

Limitations

The following are the limitations of this feature:

- Only one secondary AAA group can be configured per APN.
- If all the Rf peers under secondary aaa group are down and duplicate Start Record is not sent, then the duplicate Interim and Stop records will also not be sent to any of the secondary aaa group servers even though they arrived later. However if the servers are up and duplicate Start record was sent but the server

did not respond, duplicate Start will be dropped after all the retries. In this case, the duplicate Interim and Stop records may be sent out to the server.

- In cases when duplicate Start record was sent, but during duplicate Interim/Stop record generation peers were not responding/down, after all retries duplicate Interim and Stop records will be dropped and will not be written to HDD.
- Minimal impact to memory and CPU is expected due to the duplicate record generation for every primary Rf record.

Configuring Rf Duplicate Record Generation

The following section provides the configuration commands to enable the Rf duplicate record generation.

Configuring Secondary AAA Group

Use the following configuration commands to configure the secondary AAA group for receiving the duplicate Rf records.

```
configure
   context context_name
      apn apn_name
         aaa group group_name
         aaa secondary-group group_name
         exit
```

Notes:

- **aaa group** *group_name*: Specifies the AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.
- **secondary group** *group_name*: Specifies the secondary AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

Configuring Duplication of Rf Records

Use the following configuration commands to configure the system to create a secondary feed of Rf records and send them to the secondary AAA group.

```
configure
   context context_name
      aaa group group_name
         diameter accounting duplicate-record
         exit
```

Notes:

- **duplicate-record**: Sends duplicate Rf records to configured secondary AAA group. This keyword is license dependent. For more information, contact your Cisco account representative.
- The default configuration is **no diameter accounting duplicate-record**. By default, this feature is disabled.
- The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

Verifying the Rf Duplicate Record Generation Configuration

Use the following commands to verify the configuration status of this feature.

show configuration

show aaa group all

- or -

show aaa group *group_name*

group_name must be the name of the AAA group specified during the configuration.

This command displays all the configurations that are enabled within the specified AAA group.

The following is a sample configuration of this feature.

```
configure
   context source
      apn domainname.com
         associate accounting-policy policy_accounting_name
         aaa group group1
         aaa secondary-group group2
         exit
      aaa group group1
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint1
         diameter accounting server rf_server1 priority 1
         diameter accounting server rf_server2 priority 2
         exit
      aaa group group2
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint2
         diameter accounting duplicate-record
         diameter accounting server rf_server3 priority 3
         diameter accounting server rf_server4 priority 4
         exit
      diameter endpoint rf-endpoint1
         use-proxy
         origin host rf-endpoint1.carrier.com address 192.50.50.3
         no watchdog-timeout
         response-timeout 20
         connection retry-timeout 5
         peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
         peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
         exit
      diameter endpoint rf-endpoint2
         use-proxy
         origin host rf-endpoint2.carrier.com address 192.50.50.2
         no watchdog-timeout
         response-timeout 20
         connection retry-timeout 5
         peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
         peer rf_server4 realm domainname.com address 192.50.50.5 port 4893
end
```

Notes:

- The **diameter accounting duplicate-record** CLI is license specific. So, the corresponding license must be enabled for the CLI command to be configured.
- Both primary and secondary aaa groups are preferred to have different accounting endpoint names.

Monitoring and Troubleshooting the Rf Duplicate Record Generation

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration** or **show aaa group all** CLI command. If not enabled, configure the diameter accounting duplicate-record CLI command and check if it works.
- Collect the output of **show diameter aaa statistics** command and analyze the debug statistics. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.

show diameter aaa-statistics

The following statistics are added to the output of this show command for duplicate Rf records which were dropped because of the failure in sending the Accounting records instead of adding them to HDD or archival list.

- Duplicate Accounting Records Stats
  - ACR-Start Dropped
  - ACR-Interim Dropped
  - ACR-Stop Dropped

These statistics are maintained per aaamgr instance level. For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

These statistics can also be collected per group basis/server basis for duplicate records i.e. through **show diameter aaa-statistics group** <*group_name*> and **show diameter aaa-statistics server** <*server_name*> CLI commands.

Truncation of Virtual APN for Rf Records

This feature enables the truncation of Virtual APN (VAPN) returned by S6b server to be sent to Gx, Gy and Rf interfaces.

Feature Description

Currently there is no way to quickly turn on the Rf accounting to the Data Streaming Service (DSS) server per Virtual APN (S6b-VAPN) without reaching all nodes in the network and provision the Virtual APN on each of them. This feature is implemented to truncate the virtual APN name returned by S6b server with the configured standard delimiters. In this way a single configuration per node can be utilized for all enterprises based on a virtual APN. This approach will significantly reduce the size and time to provision new enterprises with the requested feature.

To achieve this functionality, a configuration is added per APN to enable truncation of S6b-VAPN and also to configure the delimiter(s) where the APN name is to be truncated. Standard delimiters like (.) and (-) are used since APN name supports only these two characters apart from the alphanumeric ones.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

AAA manager performs the truncation of the Virtual APN name based on the APN configuration and provides the correct APN profile for the truncated APN name. If the truncation is successful, the full virtual APN name will be sent to Gx, Gy and Rf interfaces.

Accounting records are required to support real-time usage notification and device management functionality. So, the **apn-name-to-be-included** CLI command is extended to enable actual APN (Gn-APN) or virtual APN (S6b returned virtual APN) name to be included in Called-Station-ID AVP in the secondary Rf accounting records (secondary server group) under policy accounting configuration. Currently, policy accounting configuration supports sending the Gn-APN/S6b-VAPN in Called-Station-ID for primary Rf server. With this CLI command, this functionality is extended for the secondary Rf server.

A new AAA attribute “Secondary-Called-Station-ID” is added to support sending Gn/Virtual APN name in the Called-Station-ID AVP for duplicate Rf records sent to secondary group Rf server.

Configuring Virtual APN Truncation for Rf Records

The following section provides the configuration commands to enable the Virtual APN Truncation feature for Rf records.

Configuring Gn-APN/VAPN for Rf Accounting

Use the following configuration commands to configure the actual APN or Virtual APN (VAPN) for Rf accounting.

```
configure
  context context_name
    policy accounting policy_name
      apn-name-to-be-included { gn | virtual } [ secondary-group { gn |
 virtual } ]
      end
```

Notes:

- **apn-name-to-be-included**: Configures the APN name to be included in the Rf messages for primary server group.
- **secondary-group { gn | virtual }**: Configures the APN name to be included in the Rf messages for secondary server group.
- **gn**: Configures the Gn APN name to be included in the Rf messages.
- **virtual**: Configures the virtual APN name to be included in the Rf messages.
- By default, the apn name to be included in Called-Station-ID AVP is Gn-APN for both primary and secondary Rf server groups.
- If the secondary group configuration is not available, the default behavior is to have Gn APN for secondary Rf group duplicate records.

Configuring Truncation of Virtual APN

Use the following configuration commands to configure the gateway to truncate the APN name returned from S6b interface.

```
configure
   context context_name
      apn apn_name
        virtual-apn { gcdr apn-name-to-be-included { gn | virtual } |
truncate-s6b-vapn delimiter { dot [ hyphen ] | hyphen [ dot ] } }
        end
```

Notes:

- For information on the existing keywords, see the *Command Line Interface Reference* guide.
- **truncate-s6b-vapn**: Allows truncation of virtual APN received from S6b at the configured delimiter character.
- **delimiter { dot [hyphen] | hyphen [dot] }**: Configures the delimiter for truncation of virtual APN received from S6b. If the CLI command is configured, the S6b returned virtual APN will be truncated at the configured delimiter.
  - **dot**: Configures the delimiter to dot (.) for truncation of S6b-VAPN
  - **hyphen**: Configures the delimiter to hyphen (-) for truncation of S6b-VAPN
- Both dot and hyphen delimiters can be configured in the same line or a new line.
- **no virtual-apn truncate-s6b-vapn**: Disables the truncation of virtual APN name. If both delimiters should be disabled at once, use the **no virtual-apn truncate-s6b-vapn** CLI command.

  If a particular delimiter needs to disabled, it should be done explicitly. For example, if the dot delimiter should be disabled, use the **no virtual-apn truncate-s6b-vapn delimiter dot** CLI command.
- By default this feature will be disabled and no delimiter will be configured.
- This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message.
- If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

Verifying the Virtual APN Truncation Configuration

Use the following command to verify the configuration status of this feature.

```
show configuration apn apn_name
```

apn_name must be the name of the APN specified during the feature configuration.

This command displays all the configurations that are enabled within the specified APN name. The following is a sample output of this show command.

```
[local]st40# show configuration apn intershat
configure
   context ingress
      apn intershat
         pdp-type ipv4 ipv6
         bearer-control-mode mixed
```

```
virtual-apn truncate-s6b-vapn delimiter hyphen
end
```

Monitoring and Troubleshooting the Virtual APN Truncation

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration apn** *apn_name* CLI command. If not enabled, configure the **virtual-apn truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] } }** CLI command and check if it works.
- Collect the output of **show apn statistics** CLI command and analyze the debug statistics. For further assistance, contact Cisco account representative.

Important For P-GW, GGSN and SAEGW services, if the truncation of S6b returned virtual APN name fails and the virtual APN name is not configured, the call will be rejected with ‘unknown-apn-name’ cause.

show apn statistics

This show command uses the existing APN statistics to populate the truncated virtual APN name, if this feature is enabled.

show subscribers ggsn-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers pgw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

show subscribers saegw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a’.

- S6b Returned Virtual APN

Accounting Record Stop Location Report

Previous Behavior: When P-GW or S-GW sends new User Location Information (ULI) message in an ACR stop message to Offline Charging System (OFCS) through the Rf interface, the reported location at the end of sessions was not aligning with the expected location reporting. The location used in the Accounting Stop Record (ACR Stop) was inconsistent and during location reporting it caused an `ACR stop` interim messages rather than the location before the ACR was sent

New Behavior: In the StarOS 21.22 and later releases, an existing User Location Information (ULI) is sent to the Accounting Record (ACR) Stop message on offline charging (RF) interface for GGSN, P-GW, and SAEGW when Delete Session Request is received with a New ULI.

How it Works

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

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

Figure 50: Rf Call Flow for Event Based Charging

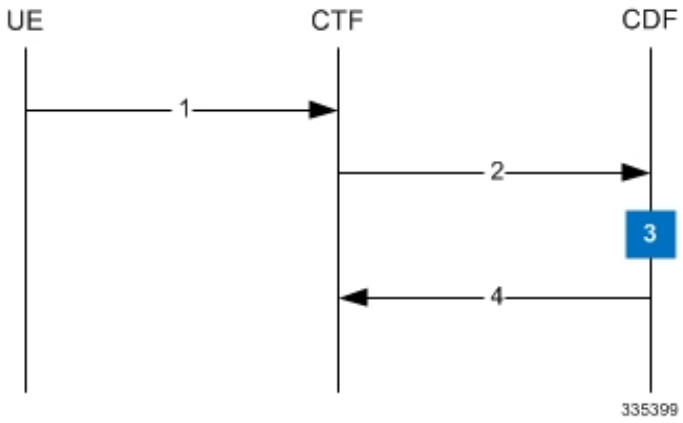


Table 31: Rf Call Flow Description for Event Based Charging

Step	Description
1	The network element (CTF) receives indication that service has been used/delivered.
2	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).
3	The CDF receives the relevant service charging parameters and processes accounting request.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.

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

Figure 51: Rf Call Flow for Session Based Charging

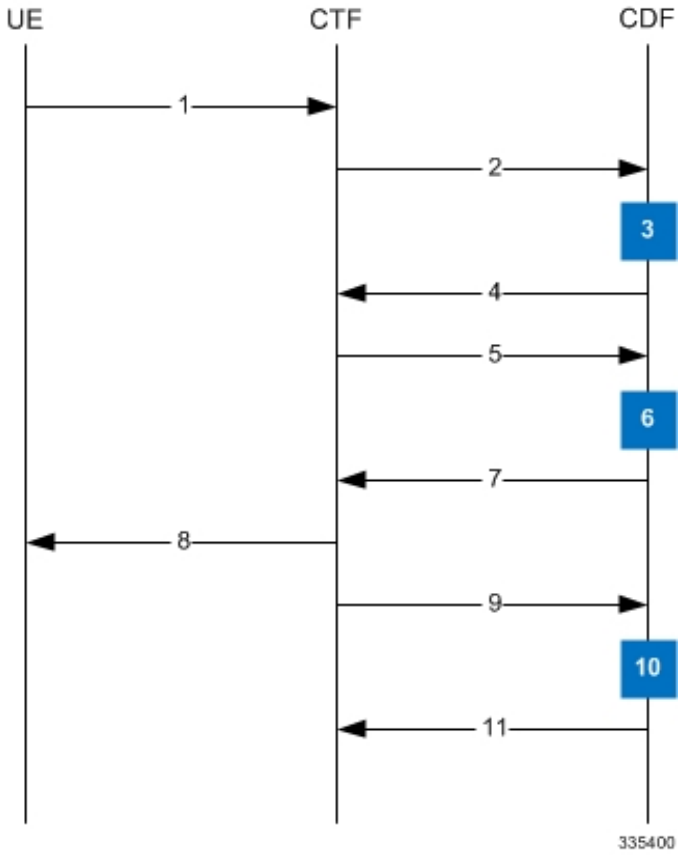


Table 32: Rf Call Flow Description for Session Based Charging

Step	Description
1	The CTF receives a service request. The service request may be initiated either by the user or the other network element.
2	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.
3	The session is initiated and the CDF opens a CDR for the current session.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.
5	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.
6	The CDF updates the CDR in question.
7	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.

Step	Description
8	The service is terminated.
9	The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.
10	The CDF updates the CDR accordingly and closes the CDR.
11	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.

Configuring Rf Interface Support

To configure Rf interface support:

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

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

3. Enable Rf accounting in ACS as described in Enabling Rf Interface in Active Charging Service, on page 353.
4. Configure Rf interface support as described in the relevant sections:
   - Configuring GGSN / P-GW Rf Interface Support, on page 353
   - Configuring P-CSCF/S-CSCF Rf Interface Support, on page 360

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

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

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

Enabling Rf Interface in Active Charging Service

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

```
configure
   active-charging service <service_name>
      rulebase <rulebase_name>
         billing-records rf
        active-charging rf { rating-group-override | service-id-override
 }
         end
```

Notes:

- Prior to creating the Active Charging Service (ACS), the **require active-charging** command should be configured to enable ACS functionality.
- The **billing-records rf** command configures Rf record type of billing to be performed for subscriber sessions. Rf accounting is applicable only for dynamic and predefined ACS rules.

  For more information on the rules and its configuration, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- The **active-charging rf** command is used to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

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

Configuring GGSN / P-GW Rf Interface Support

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

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

Notes:

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

  If the event trigger is one of the following, the containers will be released:
  - VOLUME_LIMIT
  - TIME_LIMIT
  - RAT_CHANGE
  - TIMEZONE_CHANGE
  - PLMN_CHANGE

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

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

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 33: P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/e-HRPD/GGSN

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Normal Release	YES	NO	YES	Normal Release	Normal Release	When PDN/IP session closed, C-C in both le will have Normal Release.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Normal Release	YES	NO	NO	N/A	Normal Release	Flow is closed, SD is populated and c container is added record. The contai this change condit will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
Stop	Abnormal Release	YES	NO	YES	Abnormal Release	Abnormal Release	When PDN/IP ses closed, C-C in bot will have Abnorm Release.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Abnormal Release	YES	NO	NO	N/A	Abnormal Release	Flow is closed, SD is populated and c container is added record. The contai this change condit will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	QoS-Change	YES	NO	NO	N/A	QoS-Change	The container for change condition cached by the P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Volume Limit	YES	YES	NO	Volume Limit	Volume Limit	For PDN/IP Session Volume Limit. The Volume Limit is configured as part of t Charging profile and t Charging-Characterist AVP will carry this charging profile that w passed on from the HSS/AAA to P-GW/GGSN through various interfaces. Th charging profile will b provisioned in the HS
Interim	Time Limit	YES	YES	NO	Time Limit	Time Limit	For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging-Characterist AVP will carry this charging profile that w passed on from the HSS/AAA to P-GW/GGSN through various interfaces. Th charging profile will b provisioned in the HS
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Serving Node Change	YES	NO	NO	N/A	Serving Node Change	The container for this change condition will cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.
Interim	Serving Node PLMN Change	YES	YES	NO	Serving Node PLMN Change	Serving Node PLMN Change	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	User Location Change	YES	NO	NO	N/A	User Location Change	This is BSID Char eHRPD. The conta for this change con will be cached by P-GW/GGSN and container will be i ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.
Interim	RAT Change	YES	YES	NO	RAT Change	RAT Change	
Interim	UE Timezone Change	YES	YES	NO	UE Timezone change	UE Timezone change	This is not applica eHRPD.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Tariff Time Change	YES	NO	NO	N/A	Tariff Time Change	Triggered when Ta Time changes. Tar Time Change requ online charging si change. The implementation of Change Condition dependent on implementation of Online Charging u
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Idled Out	YES	NO	NO	N/A	Service Idled Out	Flow Idled out. Th container for this c condition will be c by the P-GW/GGS the container will ACR Interim/Stop for partial record (Interim), final Re (Stop) or AII trigg (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Volume Limit	YES	NO	NO	N/A	Service Data Volume Limit	Volume Limit reached for a specific flow. Th container for this char condition will be cach by the P-GW/GGSN a the container will be i ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Time Limit	YES	NO	NO	N/A	Service Data Time Limit	Time Limit reached fo a specific flow. The container for this char condition will be cach by the P-GW/GGSN a the container will be i ACR Interim/Stop ser for partial record (Interim), final Recor (Stop) or AII trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Max Number of Changes in Charging Conditions	YES	YES	NO	YES	YES, Will include SDC that correponds 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 Volunme Limt, Service Data Time Limit)	This ACR[Interim triggered at the ins when the Max Nu of changes in char conditions takes p Max Change Cond is applicable for QoS-Change, Service-Idled Out change, Flow Nor Release, Flow Abr Release, Service D Volume Limit, Ser Data Time Limit, Timer ACR Interi Service Node Char only. The Max Nu of Changes in Cha Conditions is set a Example assuming flow in the PDN Se [1] Max Number o Changes in Charg Conditions set at P-GW/GGSN = 2. Change Condition takes place. No AC Interim is sent. P-GW/GGSN stor SDC. [3] Change Condition 2 takes An ACR Interim i Now Max Numbe Changes in Charg conditions is popu in the PS-Informa Service-Data-Con (1 for each change condition) are pop in the ACR Interi CCF creates the pa record.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Management Intervention	YES	NO	YES	YES	YES	Management intervent will close the PDN session from P-GW/GGSN.
Interim	-	YES	NO	NO	N/A	N/A	This is included here indicate that an ACR[Interim] due to timer will contain one more populated SDC/ for a/all flow/s, but Change-Condition AV will NOT be populate

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
         origin host <host_name> address <ip_address>
         peer <peer_name> address <ip_address>
         exit
      end
```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference*.

Gathering Statistics

This section explains how to gather Rf and related statistics and configuration information.

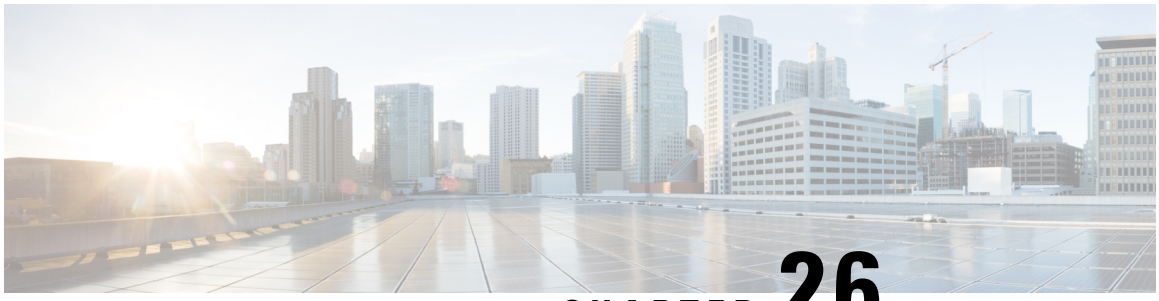
In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for Diameter Rf accounting sessions	**show diameter aaa-statistics**

The following is a sample output of the **show diameter aaa-statistics** command:

```
Authentication  Servers Summary
 ------------------------------
Message Stats :
  Total MA Requests:            0        Total MA Answers:             0
  MAR - Retries:                0        MAA Timeouts:                 0
  MAA - Dropped:                0
  Total SA Requests:            0        Total SA Answers:             0
  SAR - Retries:                0        SAA Timeouts:                 0
  SAA - Dropped:                0
  Total UA Requests:            0        Total UA Answers:             0
  UAR - Retries:                0        UAA Timeouts:                 0
  UAA - Dropped:                0
  Total LI Requests:            0        Total LI Answers:             0
  LIR - Retries:                0        LIA Timeouts:                 0
  LIA - Dropped:                0
  Total RT Requests:            0        Total RT Answers:             0
  RTR - Rejected:               0
  Total PP Requests:            0        Total PP Answers:             0
  PPR - Rejected:               0
  Total DE Requests:            0        Total DE Answers:             0
  DEA - Accept:                 0        DEA - Reject:                 0
  DER - Retries:                0        DEA Timeouts:                 0
  DEA - Dropped:                0
  Total AA Requests:            0        Total AA Answers:             0
  AAR - Retries:                0        AAA Timeouts:                 0
  AAA - Dropped:                0
  ASR:                          0        ASA:                          0
  RAR:                          0        RAA:                          0
  STR:                          0        STA:                          0
  STR - Retries:                0
Message Error Stats:
  Diameter Protocol Errs:       0        Bad Answers:                  0
  Unknown Session Reqs:         0        Bad Requests:                 0
  Request Timeouts:             0        Parse Errors:                 0
  Request Retries:              0
Session Stats:
  Total Sessions:               0        Freed Sessions:               0
  Session Timeouts:             0        Active Sessions:              0
STR Termination Cause Stats:
  Diameter Logout:              0        Service Not Provided:         0
  Bad Answer:                   0        Administrative:               0
  Link Broken:                  0        Auth Expired:                 0
  User Moved:                   0        Session Timeout:              0
  User Request:                 0        Lost Carrier                  0
  Lost Service:                 0        Idle Timeout                  0
  NAS Session Timeout:          0        Admin Reset                   0
  Admin Reboot:                 0        Port Error:                   0
  NAS Error:                    0        NAS Request:                  0
  NAS Reboot:                   0        Port Unneeded:                0
  Port Preempted:               0        Port Suspended:               0
  Service Unavailable:          0        Callback:                     0
  User Error:                   0        Host Request:                 0
 Accounting Servers Summary
 --------------------------
Message Stats :
  Total AC Requests:            0         Total AC Answers:            0
```

```
  ACR-Start:                    0       ACA-Start:                    0
  ACR-Start  Retries :          0       ACA-Start  Timeouts:          0
  ACR-Interim:                  0       ACA-Interim:                  0
  ACR-Interim  Retries :        0       ACA-Interim  Timeouts:        0
  ACR-Event:                    0       ACA-Event:                    0
  ACR-Stop :                    0       ACA-Stop:                     0
  ACR-Stop  Retries :           0       ACA-Stop  Timeouts:           0
  ACA-Dropped :                 0
AC Message Error Stats:
  Diameter Protocol Errs:       0       Bad Answers:                  0
  Unknown Session Reqs:         0       Bad Requests:                 0
  Request Timeouts:             0       Parse Errors:                 0
  Request Retries:              0
```



CHAPTER 26

S-GW Event Reporting

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

Note The S-GW Event Reporting feature is applicable to S-GW and SAEGW (Pure-S calls).

This chapter includes the following topics:

S-GW Event Reporting

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

Note The S-GW Event Reporting feature is applicable to S-GW and SAEGW (Pure-S calls).

This chapter includes the following topics:

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 34: S-GW Event Record Elements

Event Number	Description	Format	Size (bytes)	Applicable Event Numbers
1	Event identity (ID 1 – ID 6)	Integer [1-6]	1	All
2	Event Result (3GPP 29.274 Cause Code)	Integer [1-255]	3	All
3	IMSI	Integer (15 digits)	15	All
4	IMEISV	Integer (16 digits)	16	All
5	Callid	Integer (0-500000000000)	4	All
6	Start Time (GMT)	MM/DD/YYYY-HH:MM:SS:_MS (millisecond accuracy)	18	All
7	End Time (GMT)	MM/DD/YYYY-HH:MM:SS:_MS (millisecond accuracy)	18	2, 4
8	Protocol (GTPv2)	String	5	All
9	Disconnect code (ASR 5500)	Integer [1-999]	3	All
10	Trigger Event (3GPP 29.274 request cause code)	Integer [1-15]	3	All
11	Hostname	IPv4 or IPv6 address	255	All

Event Number	Description	Format	Size (bytes)	Applicable Event Numbers
12	Origination Node	String (CLLI)	10	All
13	Origination Node Type	String (SGW|HSGW|PGW|...)	3	All
14	EPS Bearer ID(Default)	Integer [0-15]	1 or 2	All
15	APN Name	String	34 to 255	All
16	PGW IP Address	IPv4 or IPv6 address	7 to 55	All
17	UE IPv4 Address	IPv4 address	7 to 15	All
18	UE IPv6 Address	IPv6 address	3 to 55	All
19	Uplink AMBR	Integer (0-4000000000)	1 to 10	All
20	Downlink AMBR	Integer (0-4000000000)	1 to 10	All
21	TAI - MCC/MNC/TAC	String (MCC;MNC;TAC)	14	All
22	Cell ID (ECI)	String (28 bits)	8	All
23	EPS Bearer ID (dedicated)	Integer (0-15)	1 or 2	21
24	Result Code (success/fail)	0=fail 1=success	1	All
25	QCI	Integer[1-255]	1 to 3	All
26	Uplink MBR (bps)	Integer (0-4000000000)	1 to 10	All
27	Downlink MBR (bps)	Integer (0-4000000000)	1 to 10	All
28	Uplink GBR (bps)	Integer (0-4000000000)	1 to 10	All
29	Downlink GBR (bps)	Integer (0-4000000000)	1 to 10	All
30	Downlink Packets Sent (interval)	Integer (0-4000000000)	1 to 10	2, 4, 5, 6
31	Downlink Bytes Sent (interval)	Integer (0-500000000000)	1 to 12	2, 4, 5, 6
32	Downlink Packets Dropped (interval)	Integer (0-500000000000)	1 to 12	2, 4, 5, 6
33	Uplink Packets Sent (interval)	Integer (0-500000000000)	1 to 12	2, 4, 5, 6
34	Uplink Bytes Sent (interval)	Integer (0-500000000000)	1 to 12	2, 4, 5, 6
35	Uplink Packets Dropped (interval)	Integer (0-4000000000)	1 to 10	2, 4, 5, 6
36	MME S11 IP Address	IPv4 or IPv6 address	7 to 55	All

Event Number	Description	Format	Size (bytes)	Applicable Event Numbers
37	S1u IP Address of eNodeB	IPv4 or IPv6 address	7 to 55	All

Active-to-Idle Transitions

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

Table 35: Subscriber-initiated Attach (initial) Call Flow Description

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

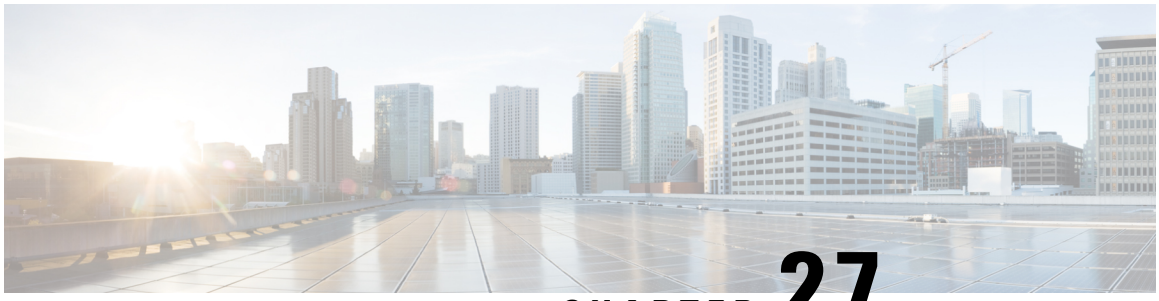
3GPP 29.274 Cause Codes

Table 36: 3GPP 29.274 Cause Codes

Cause Value	Meaning
Request	
2	Local Detach
3	Complete
4	RAT changed from 3GPP to Non-3GPP
5	ISR deactivation
6	Error Indication received from RNC/eNodeB
Accept	
16	Request accepted
17	Request accepted partially

Cause Value	Meaning
18	New PDN type due to network preference
19	New PDN type due to single address bearer only
Reject	
64	Context Not Found
65	Invalid Message Format
66	Version not supported by next peer
67	Invalid length
68	Service not supported
69	Mandatory IE incorrect
70	Mandatory IE missing
71	Reserved
72	System failure
73	No resources available
74	Semantic error in the TFT operation
75	Syntactic error in the TFT operation
76	Semantic errors in packet filter(s)
77	Syntactic errors in packet filter(s)
78	Missing or unknown APN
79	Unexpected repeated IE
80	GRE key not found
81	Relocation failure
82	Denied in RAT
83	Preferred PDN type not supported
84	All dynamic addresses are occupied
85	UE context without TFT already activated
86	Protocol type not supported
87	UE not responding
88	UE refuses

Cause Value	Meaning
89	Service denied
90	Unable to page UE
91	No memory available
92	User authentication failed
93	APN access denied - no subscription
94	Request rejected
95	P-TMSI Signature mismatch
96	IMSI not known
97	Semantic error in the TAD operation
98	Syntactic error in the TAD operation
99	Reserved Message Value Received
100	Remote peer not responding
101	Collision with network initiated request
102	Unable to page UE due to Suspension
103	Conditional IE missing
104	APN Restriction type Incompatible with currently active PDN connection
105	Invalid overall length of the triggered response message and a piggybacked initial message
106	Data forwarding not supported
107	Invalid reply from remote peer
116 to 239	Spare. This value range is reserved for Cause values in rejection response message.
Sub-Causes	
NO_INFORMATION	
ABORTED_BY_SESSION_DELETION	
NO_RESPONSE_FROM_MME	
INTERNALLY_TRIGGERED	
BEARERS_IN_MULTIPLE_PDN_CONNECTIONS	
EXPECTED_BEARERS_MISSING_IN_MESSAGE	
UNEXPECTED_BEARERS_PRESENT_IN_MESSAGE	



CHAPTER 27

S-GW Paging Enhancements

Feature Description

S-GW Paging includes the following scenarios:

Scenario 1: S-GW sends a DDN message to the MME/S4-SGSN nodes. MME/S4-SGSN responds to the S-GW with a DDN Ack message. While waiting for the DDN Ack message from the MME/S4-SGSN, if the S-GW receives a high priority downlink data, it does not resend a DDN to the MME/S4-SGSN.

Scenario 2: If a DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN, S-GW does not send DDN.

Scenario 3: DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received. DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.

To handle these scenarios, the following two enhancements have been added to the DDN functionality:

- High Priority DDN at S-GW
- MBR-DDN Collision Handling

These enhancements support the following:

- Higher priority DDN on S-GW and SAEGW, which helps MME/S4-SGSN to prioritize paging.
- Enhanced paging KPI and VoLTE services.
- DDN message and mobility procedure so that DDN is not lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A new CLI command **ddn temp-ho-rejection mbr-guard-timer** has been introduced to enable the guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.
- TAU/RAU with control node change triggered DDNs.

In addition to the above functionality, to be compliant with 3GPP standards, support has been enhanced for Downlink Data Notification message and Mobility procedures. As a result, DDN message and downlink data which triggers DDN is not lost. This helps improve paging KPI and VoLTE success rates in scenarios where DDN is initiated because of SIP invite data.

Licensing

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

How It Works

This section describes working of these features related to S-GW Paging.

High Priority DDN at S-GW

High Priority DDN at S-GW

1. S-GW sends a Downlink Data Notification message to the MME/S4-SGSN node for which it has control plane connectivity for the given UE.
2. The MME/S4-SGSN responds to the S-GW with a Downlink Data Notification Ack message.
3. The S-GW, while waiting for the user plane to be established, might send a second Download Data Notification based on the priority of received data. The following table lists the cases when it will happen.
4. The following table lists different scenarios with different DDN priorities and the action taken by the S-GW.

Table 37: DDN Priority Scenarios

Scenario	Action Taken by S-GW Action Taken by S-GW Prior This Feature	Action Taken by S-GW Action Taken by S-GW Post This Feature
ARP Priority of second bearer is higher than the first bearer on which first DDN was sent.	No DDN was sent.	Sends DDN message with higher priority to the MME/S4-SGSN.
ARP Priority of second bearer is higher than the first bearer on which first DDN was sent.	Buffers these downlink data packets and the does not send a new DDN. However, separate Paging DDN is always sent out and this restriction does not apply to it.	Buffers these downlink data packets and the does not send a new DDN. However, separate Paging DDN is always sent out and this restriction does not apply to it.
S-GW has sent the second DDN message indicating higher priority and receives extra downlink data packets for this UE.	Buffers these downlink data packets and the does not send a new DDN.	Buffers these downlink data packets and the does not send a new DDN.

Important Separate paging is always sent.

MBR-DDN Collision Handling

The following table lists different MBR-DDN collision scenarios and action taken by S-GW to handle these scenarios:

Table 38: MBR-DDN Collision Handling Scenarios

Scenario	Action Taken by S-GW Action Taken by S-GW Prior This Feature	Action Taken by S-GW Action Taken by S-GW Post This Feature
DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN without any data TEIDs.	No DDN was sent.	DDN is triggered to this new control node as part of mobility handover process.
DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received.	DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.	S-GW starts a guard timer and wait for TAU/RAU MBR from the new MME/S4-SGSN. The timer is stopped if any MBR or DDN failure indication is received. But, if none of them is received, and the timer expires all buffered downlink data packets are flushed. If this is followed by mobility handover without any data TEIDs, DDN is resent to this new control node as well.
MBR received with bearer context to be removed.	There is a possibility that DDN could be sent with EBIs corresponding to bearers marked for deletion.	Bearers marked for deletion are not included in any of the DDN messages.

Limitations

High Priority DDN at S-GW

This section lists the limitations for High Priority DDN at S-GW feature.

1. High Priority DDN is always enabled whenever the license is available.
2. High priority DDN is sent only once. Any further higher priority data does not trigger another DDN.
3. DDN delay timer and DDN throttling is not applicable to High Priority DDN.
4. Separate Paging DDN is always sent out and above restriction does not apply to it.
5. No-user-connect behavior restarts the moment high priority DDN is sent out.

MBR-DDN Collision Handling

This section lists the limitations for MBR-DDN Collision Handling feature.

1. EBI of a bearer marked for removal is not sent in any of the DDN messages.
2. TAU/RAU triggered DDN is sent only once and is never reattempted even if aborted due to the collision of MBR with DDN at the S-GW Ingress.
3. DDN delay and throttling are not applicable to the TAU/RAU triggered DDN.
4. No-user-connect behavior restarts the moment high priority DDN is sent out.
5. High Priority DDN is not sent if high priority downlink data is received:
   - After DDN Ack with Cause #110 is received
   - Before any MBR is received
6. Separate paging IE is not supported for TAU/RAU triggered DDN.
7. If DDN Ack with cause #110 is received and then later a downlink packet matches the configured 3-tuple of "Separate Paging", then also "Separate Paging DDN" is not sent as the UE is undergoing handoff.
8. The MBR guard timer is not restarted when the DDN Ack with cause #110 is received while the MBR guard timer is running.

Configuring High Priority DDN Interaction Feature

Operators can use this CLI command to enable guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.

Configuring mbr-guard-timer

This CLI sets the guard timer to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset.

If the guard timer is running and any MBR is received, the timer is stopped and no further action is taken.

If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken.

By default, this CLI command is always enabled.

```
configure
     context context_name
        sgw-service service_name
           ddn temp-ho-rejection mbr-guard-timer time_in_seconds
           { no | default } ddn temp-ho-rejection mbr-guard-timer
           end
```

Notes:

- **no:** Disables the guard timer.
- **default:** Enables the guard timer and sets it to the default value, 60 seconds.

- **temp-ho-rejection:** Action to be taken when peer node indicates temporary rejection of paging due to handover-in-progress.
- **mbr-guard-timer:** Sets the guard timer for a MBR when DDN Ack with Cause #110 (temp-ho-rejection) is received. When the timer expires, S-GW flushes all the buffered downlink data packets. The range of this timer is from 60 seconds to 300 seconds. Default timer value is 60 seconds.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show sgw-service statistics all**
- **show sgw-service [name <service-name> | all]**
- **show saegw-service statistics all function sgw**

See the section Monitoring and Troubleshooting High Priority DDN Interaction Feature, on page 373 for the command output.

Monitoring and Troubleshooting High Priority DDN Interaction Feature

The following section describes commands available to monitor and troubleshoot "High Priority DDN" & "DDN-MBR Collision Handling" Features .

Show Commands for High Priority DDN Interaction Feature

show sgw-service [name <service-name> | all]

This CLI is enhanced to show the MBR-guard-timer configuration which can be a value between "60-300 Seconds" when enabled OR "Disabled". The MBR-guard-timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received.

Important If the MBR-guard-timer is disabled, DDN Ack with Temporary-HO-Rejection is treated as DDN Failure Indication.

This command displays the following output:

```
show sgw-service name sgw-srv
Service name                    : sgw-srv
  Service-Id                    : 18
  Context                       : ingress
  Accounting context            : ingress
  Accounting gtpp group         : default
  Accounting mode               : Gtpp
  Accounting stop-trigger       : Default
  Status                        : STARTED
  Egress protocol               : gtp-pmip
```

```
Ingress EGTP service          : egtp-sgw-ingress
Egress context                : ingress
Egress EGTP service           : egtp-sgw-egress
Egress MAG service            : n/a
IMS auth. service             : n/a
Peer Map                      : n/a
Access Peer Map               : n/a
Accounting policy             : n/a
Newcall policy                : n/a
Internal QOS Application      : Backward-compatible
QCI-QOS mapping table         : n/a
Event Reporting               : Disabled
DDN Throttling                : Disabled
Page UE for PGW initiated proc: Disabled
Temp-Failure Handling for DBR proc: Disabled
PGW Ctrl FTEID in Relocation Create Session Response: Enabled
...
....
ddn success-action no-user-connect ddn-retry-timer: 60
ddn failure-action pkt-drop-time: 300
ddn isr-sequential-paging delay-time: 10
MBR Guard Timer for DDN Ack with Temporary-HO-Rejection: 60-300 seconds/Disabled

Idle timeout                  : n/a
PLMN ID List                  : Not defined
Subscriber Map Name: smap
SAEGW service                 : saegw
EGTP NTSR: Disabled
 Session Hold Timer: n/a
   Timeout: n/a

GTP-C Load Control Profile        : Not Defined
GTP-C Overload Control Profile    : Not Defined
```

show sgw-service statistics all

This CLI command has been enhanced to show the following:

- Number of times 'High Priority Paging' is triggered and number of times it could not be triggered as it was already sent. This shows data corresponding to only S-GW service(s) which is part of SAEGW service(s).
- Number of times DDN Ack with a cause #110 is received and number of times TAU/RAU MBR with control node change triggers a DDN automatically.
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received.
- This CLI shows data only corresponding to standalone sgw-service(s).

This command displays the following output:

```
show sgw-service statistics all
…
…
Paging Statistics:
  Requests:                          3    Success :                          2
  Rejects:                           1    Failures:                          0
  UE State Transitions:
    Idle-to-Active:                  0    Active-to-Idle:                    1
```

```
Data Statistics Related To Paging:
  Packets Buffered:                  3    Bytes Buffered:                   15
  Packets Discarded:                 9    Bytes Discarded:                  45
  Idle Mode ACL Statistics:
    Packets Discarded:               0    Bytes Discarded:                   0

Data Discarded By Reason-Type:
  Shared Buffer Full:
    Packets Discarded:               0    Bytes Discarded:                   0
  Dedicated Buffer Full:
    Packets Discarded:               0    Bytes Discarded:                   0
  S1U State Inactive:
    Packets Discarded:               0    Bytes Discarded:                   0
  Paging Throttled:
    Packets Discarded:               0    Bytes Discarded:                   0
  Paging Failure:
    Packets Discarded:               9    Bytes Discarded:                  45
  No User Connect Data Flushed:
    Packets Discarded:               0    Bytes Discarded:                   0
  MBR Guard Timer Expiry Flushed Data:
    Packets Discarded:           0    Bytes Discarded:                  0
  Buffered Data Flushed:
    Packets Discarded:               0    Bytes Discarded:                   0

 High Priority Paging Statistics:
   Initiated:                    1    Suppressed:                       1

 Handover Paging Statistics:
   DDN Ack with Temporary-HO-Rejection (Cause #110):                    0
   TAU/RAU MBR Triggered DDN:                                           1
...
...
```

show saegw-service statistics all function sgw

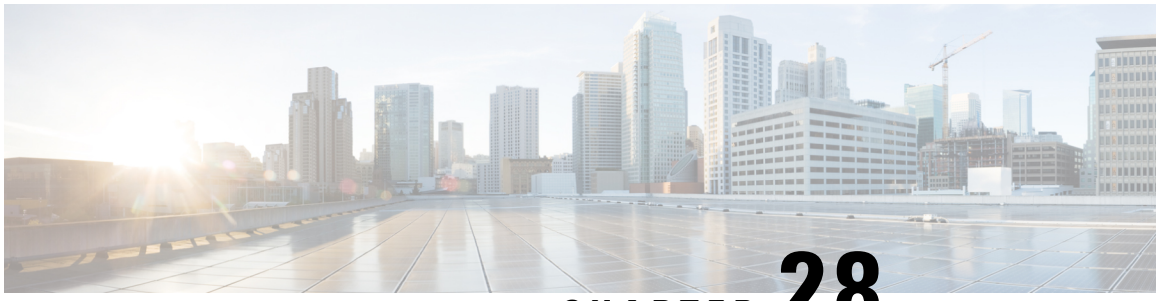
This CLI is enhanced to show the following:

- Number of times 'High Priority Paging' was triggered and number of times it could not be as it was already sent.
- Number of times DDN Ack with a cause #110 is received and number of times TAU/RAU MBR with control node change triggers a DDN automatically.
- Data only corresponding to the S-GW service(s) which is associated with a SAEGW service(s).
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received
- Packets/Bytes dropped due to MBR-guard-timer expiry are not shown for collapsed calls.

Important Paging packets dropped statistics are not incremented for collapsed calls and hence the newly added counter of "MBR Guard timer Expiry Flushed Data" is also not updated in that case.

This command displays the following output:

```
 show saegw-service statistics all function sgw
Paging Statistics:
  Requests:                          3    Success :                          2
  Rejects:                           1    Failures:                          0
  UE State Transitions:
    Idle-to-Active:                  0    Active-to-Idle:                    1

  Data Statistics Related To Paging:
    Packets Buffered:                3    Bytes Buffered:                   15
    Packets Discarded:               9    Bytes Discarded:                  45
    Idle Mode ACL Statistics:
      Packets Discarded:             0    Bytes Discarded:                   0

  Data Discarded By Reason-Type:
    Shared Buffer Full:
      Packets Discarded:             0    Bytes Discarded:                   0
    Dedicated Buffer Full:
      Packets Discarded:             0    Bytes Discarded:                   0
    S1U State Inactive:
      Packets Discarded:             0    Bytes Discarded:                   0
    Paging Throttled:
      Packets Discarded:             0    Bytes Discarded:                   0
    Paging Failure:
      Packets Discarded:             9    Bytes Discarded:                  45
    No User Connect Data Flushed:
      Packets Discarded:             0    Bytes Discarded:                   0
    MBR Guard Timer Expiry Flushed Data:
      Packets Discarded:             0    Bytes Discarded:                   0
    Buffered Data Flushed:
    Packets Discarded:             0    Bytes Discarded:                   0

    High Priority Paging Statistics:
      Initiated:                     1    Suppressed:                        1

    Handover Paging Statistics:
      DDN Ack with Temporary-HO-Rejection (Cause #110):                      0
      TAU/RAU MBR Triggered DDN:                                             1
```



CHAPTER 28

Support for One Million S1-U Peer-to-Peer Connections

This chapter describes StarOS support for the One Million S1-U Peer-to-Peer Connections feature.

Feature Description

Due to production forecasts, support has been added to the StarOS for one million S1-U connections on a single S-GW.

The S1-U interface is the user plane interface carrying user data between an eNodeB and an S-GW received from the terminal. The StarOS now has the capability to scale the number of S1-U peers to one million per VPN context.

A CLI command enables operators to set the number of S1-U peers for which statistics should be collected. The limit is restricted to less than one million peers (128k) due to StarOS memory limitations.

How it Works

The gtpumgr uses the following guidelines while allocating peers:

- When a session installation comes from the Session Manager, a peer is created. If statistics are maintained at the Session Manager, the gtpumgr also creates the peer record with the statistics.
- Peer records are maintained per service.
- The number of peers is maintained at the gtpumgr instance level. The limit is one million S1-U peers per gtpumgr instance.
- If the limit of one million peers is exceeded, then peer creation fails. It causes a call installation failure in the gtpumgr, which leads to an audit failure if an audit is triggered.

The feature changes impact all the interfaces/services using the gtpu-service including GGSN/S4-SGSN/S-GW/P-GW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW for:

- The Gn and Gp interfaces of the General Packet Radio Service (GPRS)
- The Iu, Gn, and Gp interfaces of the UMTS system
- The S1-U, S2a, S2b, S4, S5, S8, and S12 interfaces of the Evolved Packet System (EPS)

Recovery/ICSR Considerations

- After a session manager/gtpumgr recovery or after an ICSR switchover, the same set of peers configured for statistics collection is recovered.
  - Peers with 0 sessions and without statistics are not recovered.
  - Peers with 0 sessions and with statistics are recovered.
  - Peers with Extension Header Support disabled are recovered.
- While upgrading from a previous release, ensure the newer release chassis **gtpu peer statistics threshold** is equal to or greater than the previous release. This way the GTPU peer statistics are preserved during the upgrade. For example, if you are upgrading from StarOS release 19.0 to 20.2, and the StarOS 19.0 system has 17,000 GTPU sessions, then configure the threshold on the StarOS 20.2 system to 17,000 as well.

Configuration and Restrictions

- Due to the large number of GTP-U entities connecting to the StarOS, Cisco recommends disabling the GTP-U Path Management feature.
- The configured threshold is not the hard upper limit for statistics allocation because of the distributed nature of system. It is possible that total GTP-U peers with statistics exceeds the configured threshold value to some extent.
- It is assumed that all 1 million peers are not connected to the node in a point-to-point manner. They are connected through routers.
- There will not be any ARP table size change for the StarOS to support this feature.

Configuring the Feature

This section describes how to configure support for the One Million S1-U Peer Connections feature.

gtpu peer statistics threshold

This new command has been added to *Context Configuration Mode* to specify the number of S1-U peers for which the StarOS will maintain statistics.

Use the following example to configure the feature:

```
configure
  context context_name
    gtpu peer statistics threshold value
    end
```

Notes :

- *value* represents the number of S1-U peers for which statistics will be maintained. Valid entries are from 16000 to 128000. The default setting is 16000.
- The threshold cannot be configured to a lower value than the current value.

Show Command Output

This section describes the show command output changes made to support the One Million S1-U Peers feature.

clear gtpu statistics peer-address

The **all** keyword has been added to this command to enable operators to clear statistics for all S1-U peers for which statistics are being maintained.

```
clear gtpu statistics peer-address all
```

show gtpu statistics

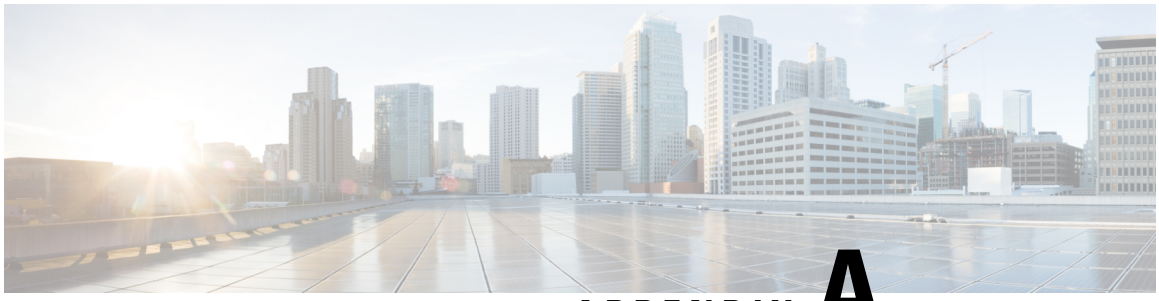
The output of this command has been enhanced to show the total number of GTPU peers, and the total number of GTPU peers configured for statistics collection.

- Total GTPU Peers:
- Total GTPU Peers with stats:

show session subsystem facility sessmgr

The output of this command has been enhanced to provide the total number of S1-U (GTP-U) peers that are configured for statistics collection.

- Total Gtpu Peers with stats



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 5500 for your network deployment. General and network-specific rules are located in the appendix of the *System Administration Guide* for the specific network type.

The following rules are covered:

Interface and Port Rules

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-U/S11 interface is created once the IP address of a logical interface is bound to an S-GW service. The S-GW supports a maximum of one million S1-U peers.
- 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 to understand outputs of **show** commands.

S-GW Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- A maximum of 2,048 local subscribers can be configured per context.
- Default subscriber templates may be configured on a per S-GW or MAG service.