GTPP Accounting Overview

This chapter provides an overview of GPRS Tunneling Protocol Prime (GTPP) protocol accounting, and the following Charging Data Records (CDRs) in the Cisco ASR 5500 Multimedia Core Platform:

- Evolved Packet Data Gateway CDRs (ePDG-CDRs)
- Gateway GPRS Support Node (GGSN) CDRs (G-CDRs), Enhanced GGSN CDRs (eG-CDRs)
- Packet Data Network Gateway (P-GW) CDRs (PGW-CDRs)
- Serving Gateway (S-GW) CDRs (SGW-CDRs)
- Serving GPRS Support Node (SGSN) CDRs (S-CDRs, SM-MO-CDRs, SM-MT-CDRs), Mobility CDRs (M-CDRs)
- Wireless Local Area Network CDRs (WLAN-CDRs)

GTPP Interface Overview

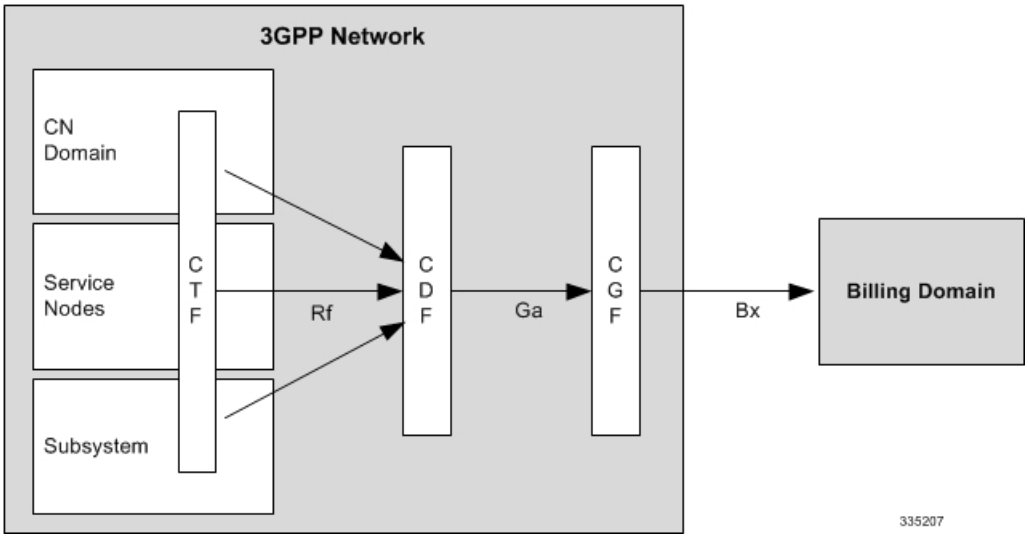
This section provides information on GTPP interface between Charging Gateway Function (CGF) and Cisco Systems' licensed products running on the ASR 5500 core platforms, including the GGSN, P-GW, S-GW, and SGSN in General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) data networks, 3GPP2 evolved High Rate Packet Data (eHRPD) and Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks.

The Ga is the reference point from Charging Data Function (CDF) to the CGF, which is intended for the transport of CDRs. The CDF could either be GGSN, P-GW, S-GW, or any other similar products.

By definition, dealing with CDRs only implies that Ga is solely related to offline charging.

The following figure depicts the position of the Ga reference point within the overall 3GPP offline charging architecture.

Figure 1: 3GPP Offline Charging Architecture



As illustrated in the above figure, the CDF in each network domain, service or subsystem is relevant for the network side of the Ga reference point. Different mappings of the ubiquitous offline charging functions, CDF and CGF, onto physical implementations are possible.

The transport protocol associated to the Ga reference point, providing functions for transfer of CDRs from CDF to CGF, is GTPP.

Each CDF will have an O&M; configurable address list of CGFs (Charging Gateways) to which it can send its CDRs. The list will be organized in CGF address priority order. If the primary CGF is not available (for example, out of service), then the CDF will send the CDRs to the secondary CGF and so on.

Each CDR generating function will only send the records to the CGF(s) of the same PLMN, not to CGF(s) located in other PLMNs.

Each CGF in the PLMN will know the other CGFs' network addresses (for example, for redundancy reasons, to be able to recommend another CGF address). This is achieved by O&M; configuration facilities that will enable each CGF to have a configurable list of peer CGF addresses.

The GTPP charging support is currently available for the following core multimedia gateway products:

- Evolved Packet Data Gateway (ePDG)
- Gateway GPRS Support Node (GGSN)
- IP Services Gateway (IPSG)
- Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG)
- Packet Data Network (PDN) Gateway (P-GW)
- Serving Gateway (S-GW)
- Serving GPRS Support Node (SGSN)
- S2a Mobility Over GTP (SaMOG) Gateway

CDR Transport by GTPP

GTPP has been designed to deliver the CDR(s) from the CDF to the CGF(s). This protocol is required if the CGF resides outside the CDFs. It utilizes some aspects of GTPP, which is used for packet data tunneling in the backbone network.

GTPP operates on the Ga interface and does not imply the use of any specific backbone network.

GTPP performs the following functions:

- CDR transfer between the CDF and the CGF
- Redirection of CDRs to another CGF
- Advertise to peers about its CDR transfer capability (for example, after a period of service downtime)
- Prevents duplicate CDRs that might arise during redundancy operations. If so configured, the CDR duplication prevention function may also be carried out by marking potentially duplicated CDR packets, and, delegating the final duplicate deletion task to a CGF or the Billing Domain (instead of handling the possible duplicates solely by GTPP messaging).

Path Protocol

GTPP uses path protocol to transport CDRs from CDF to CGF over the Ga interface so as to facilitate charging.

The following path protocols are supported for GTPP:

- UDP as the Path Protocol

  Ports for signaling the request messages:

  - The UDP Destination Port may be the server port number 3386 which has been reserved for GTPP. Alternatively, another port can be used as configured by O&M.;
  - The UDP Source Port is a locally allocated port number at the sending network element.

  Ports for signaling the response messages:

  - The UDP Destination Port can be the value of the Source Port of the corresponding request message.
  - The UDP Source Port can be the value from the Destination Port of the corresponding request message.

- TCP as the Path Protocol

  The TCP Destination Port may be the server port number 3386, which has been reserved for G-PDUs. Alternatively, another port may be used as configured by O&M.; Extra implementation-specific destination ports are possible but all CGFs support the server port number.

  The TCP Source Port is a random port locally assigned at the sending network element.

Important ASR chassis supports IPV4 only as a transport layer IP.

GTPP Message Types

GTPP defines a set of messages between two associated nodes. The GTPP messages defined are shown in the following table. The messages introduced by GTPP are in boldface letters. The other messages are inherited from GTPP protocol.

Table 1: GTPP Messages

Message Type value (Decimal)	GTPP Message
1	Echo Request
2	Echo Response
3	Version Not Supported
4	**Node Alive Request**
5	**Node Alive Response**
6	**Redirection Request**
7	**Redirection Response**
240	**Data Record Transfer Request**
241	**Data Record Transfer Response**
Others	Reserved for future use

The GTPP introduced the following signaling message types as Path Management Messages:

- Node Alive Request
- Node Alive Response
- Redirection Request
- Redirection Response

Important Echo messages and node-alive messages are not supported if the transport layer protocol is TCP.

The following signaling messages are grouped under the category "Record Transmission Messages":

- Data Record Transfer Request
- Data Record Transfer Response

The reserved fields in the signaling messages can be filled with ones, and are intended for future use.

GTPP reuses the GTPP Cause values. The message type numbers required for the newly introduced GTPP messages have been derived from the unallocated message type number space specified in the GTPP message table defined in TS 29.060.

The number ranges allocated for GTPP are as follows:

For Information Elements: 117-127 (TV type fields) and 239-254 (for TLV type fields).

The following table provides the information on the TLV and TV Information Element types introduced in this document:

Table 2: TLV and TV Information Element Types

TLV Information Element Types	
254	Address of Recommended Node
253	Requests Responded
252	Data Record Packet
251	Charging Gateway Address (this IE is also used in TS 29.060 [200])
250	Sequence Numbers of Canceled Packets
249	Sequence Numbers of Released Packets
TV Information Element Types	
127	Charging ID
126	Packet Transfer Command

Usage of GTPP Header in Charging

In GTPP messaging only the signalling plane of GTPP is partly reused. The GTPP header is shown in the following figure.

Bit 5 of octet 1 of the GTPP header is the Protocol Type (PT) flag: it is '0' if the message is GTPP.

The Version bits indicate the GTPP protocol version when the Protocol Type flag is '0'.

Bit 1 of octet 1 is not used in GTPP (except in v0), and it is marked '0' in the GTPP header. It is in use in GTPP v0 and distinguishes the used header-length. In the case of GTPP v0, this bit being marked one (1) indicates the usage of the 6 octets header. If the bit is set to '0' (usually the case) the 20-octet header is used. For all other versions of GTPP, this bit is not used and is set to '0'. However, this does not suggest the use of the 20-octet header, rather a shorter 6-octet header.

The Length indicates the length of payload (number of octets after the GTPP header). The Sequence Number of the packet is part of the GTPP header.

Information Elements

The messages contain several Information Elements (IEs). The TLV (Type, Length, Value) or TV (Type, Value) encoding formats will be used for the GTPP IEs. The GTPP messages have the IEs sorted with the *Type* fields in ascending order. The *Length* field contains the IE length excluding the Type and Length fields.

Within the *Type* field the most significant bit will be set to 0 when the TV format is used and set to 1 when the TLV format is used.

GTPP Messages

This section provides the detailed information on the GTPP message types.

Node Alive Request

The Node Alive Request message may be used to inform that a node in the network has started its service (e.g. after a service break due to software or hardware maintenance or data service interruption after an error condition). A node may send a different Node Address than its own in the Information Element, e.g. informing the "next node in the chain" that the "previous node in the chain" (which is located on the other side of the sender of this message) is now ready for service.

The Node Alive Request message allows a quicker reconnect capability than the Echo Request message based polling can provide, and its usage will have a reduced load effect on the network, particularly when the number of network nodes using GTPP is high. It may also be used to inform when a new network node has become available for service. If the Echo Request message is also used, then the usage of the Node Alive Request message allows the interval of Echo Requests to be longer, thus reducing network load by reducing number of Echo Requests.

Important Node Alive request messages are not supported if the transport layer protocol is TCP.

The Information elements in a Node Alive Request message are shown in the following table:

Table 3: Node Alive Request Message

Information Element	Presence Requirement
Node Address	Mandatory
Alternative Node Address	Optional
Private Extension	Optional

The Node Address format is the same as for the Charging Gateway Address format described in TS 29.060.

The format definition for the Node Address information element is the same as the format of the source and destination address of the IP packet that transports the GTPP messages. The optional Alternative Node Address IE can be used in the Node Alive Request if the message sender wants to advertise an IP address that is different from the node address format. This way both the IPv4 and IPv6 node address formats can be supported simultaneously in the messaging, regardless of whether IPv4 or IPv6 is used in the underlying transport.

The optional Private Extension IE contains vendor- or operator-specific information.

Node Alive Response

The *Node Alive Response* message, shown in the following table, will be sent as a response to a received *Node Alive Request*.

Table 4: Node Alive Response Message

Information Element	Presence Requirement
Private Extension	Optional

The optional Private Extension IE contains vendor- or operator-specific information.

Redirection Request

There are two use cases for the Redirection Request message:

- One is to advise that received CDR traffic is to be redirected to another CGF due to the sending CGF node is about to stop service (due to an outage for maintenance or an error condition).
- The second purpose is to inform a CDF which is currently sending data to this node (e.g. CGF), that the next node in the chain (e.g. a mediator device or Billing Computer) has lost connection to this node (e.g. CGF).

The Information Elements in a Redirection Request Message are listed in the following table. An *Address of Recommended Node* may be given if, for example, a CGF maintenance outage is handled by first introducing another CGF ready to take incoming CDRs. This way, the network performance can be maintained. The *Address of Recommended Node* describes an intra-PLMN node containing a CGF, and not a node in any other PLMN.

Table 5: Redirection Request Message

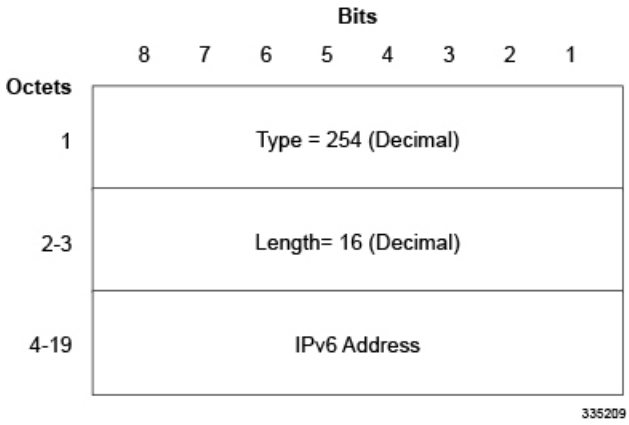
Information Element	Presence Requirement
Cause	Mandatory
Address of Recommended Node	Optional
Alternative Address of Recommended Node	Optional
Private Extension	Optional

Possible Cause values are:

- This node is about to go down
- Another node is about to go down
- System failure
- Receive buffers becoming full
- Send buffers becoming full

The Address of Recommended Node IE, shown in the following figure, defines the IPv4 or IPv6 format address that the node is identified by in the UMTS network.

Figure 2: Address of Recommended Node IE



The format definition for the Address of Recommended Node information element is the same as the format of the source and destination address of the IP packet that transports the GTPP messages. The optional Alternative Address of Recommended Node IE can be used in the Node Alive Request if the message sender wants to advertise an IP address that is different from the node address format. This way both the IPv4 and IPv6 node address formats can be supported simultaneously in the messaging, regardless of whether IPv4 or IPv6 is used in the underlying transport.

The optional Private Extension contains vendor- or operator- specific information.

Redirection Response

A Redirection Response message will be sent as a response of a received Redirection Request.

The information elements of this message are listed in the following table.

Table 6: Redirection Response Message

Information Element	Presence Requirement
Cause	Mandatory
Private Extension	Optional

Possible Cause values are:

- Request Accepted
- No resources available
- Service not supported
- System failure
- Mandatory IE incorrect
- Mandatory IE missing

- Optional IE incorrect
- Invalid message format
- Version not supported

The optional Private Extension contains vendor- or operator-specific information.

Data Record Transfer Request

This message is used to transmit the CDR(s) to the CGF.

The CDRs are placed in the Data Record Packet information element.

Information Elements in Data Record Transfer Request

The IEs in Data Record Transfer Request message are specified in the following table.

Table 7: Data Record Transfer Request Message

Information Element	Presence Requirement
Packet Transfer Command	Mandatory
Data Record Packet	Conditional
Sequence Numbers of Released Packets	Conditional
Sequence Numbers of Canceled Packets	Conditional
Private Extension	Optional

Packet Transfer Command IE

The value of the Packet Transfer Command in its Information Element tells the nature of the message:

- 1 = 'Send Data Record Packet'
- 2 = 'Send possibly duplicated Data Record Packet'
- 3 = 'Cancel Data Record Packet'
- 4 = 'Release Data Record Packet'

The following describes the usage of each Packet Transfer Command. The first command is for normal CDR transfer while the other values are only used as part of the redundancy mechanism.The following describes the usage of each Packet Transfer Command. The first command is for normal CDR transfer while the other values are only used as part of the redundancy mechanism.

Send Data Record Packet: This is the usual command used for sending CDRs under normal conditions when no error recovery is needed or the redirection mechanism is not involved. The other three commands are being used only in error recovery cases. Out of the three conditional IEs, only the "Data Record Packet" is present in this message.

Send possibly duplicated Data Record Packet: When the CDR packet is redirected to a secondary CGF (by a CDF) because the currently used CGF is not working or the CDR transfer is not working properly, or if

there is an error in the link between the CDF and the CGF, then this Packet Transfer Command is used instead of the normal 'Send Data Record Packet'. Of the conditional IEs, the "Data Record Packet" is present in the message, when sending the message to a CGF acting as temporary storage, when the original primary CGF could not be contacted. This Packet Transfer Command is used also when sending "empty" test packets with older (but not yet acknowledged) sequence numbers after a peer node or link recovery, to check if the CGF had received some Data Record Packets (whose acknowledgement did not come to the Data Record Packet sending node) before the link to the recipient node became inoperable.

Cancel Data Record Packet: Of the conditional IEs, the "Sequence Numbers of Canceled Packets" is present in the message.

Release Data Record Packet: Of the conditional IEs, the "Sequence Numbers of Released Packets" is present in the message.

After the CGF has received the Packet Transfer Command 'Release Data Record Packet' with the Sequence Number(s) for earlier sent 'Send possibly duplicated Data Record Packet' command(s), it can consider itself authorized to send the Data Record Packets previously marked as possibly duplicated towards the BD as normal (not duplicated) CDRs.

Data Record Packet IE

The Data Record Packet element, which is present conditionally if the Packet Transfer Command is 'Send Data Record Packet' or 'Send possibly duplicated Data Record Packet', may contain one or more CDRs. If an "empty packet" is to be sent, then the Data Record Packet IE contains only the Type (with value 252 in decimal) and the Length (with value 0) fields.

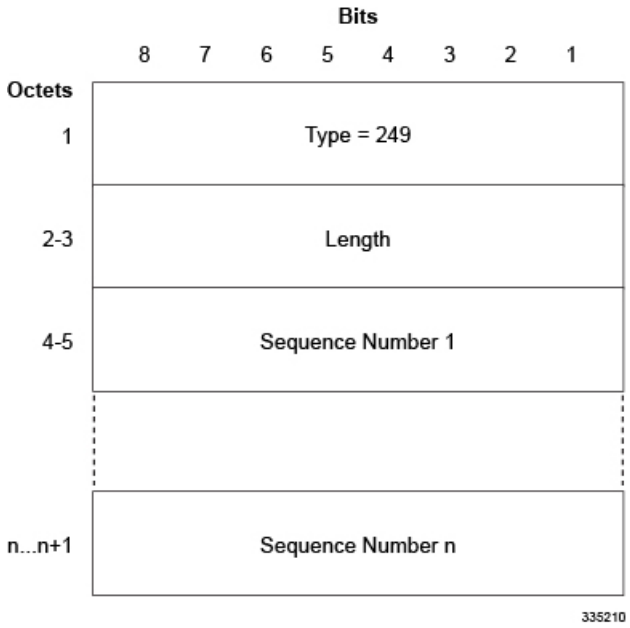
There are two fields identifying the CDR format: Data Record Format and Data Record Format Version.

The format of the CDRs is ASN.1 or some other format, as identified by the value of Data Record Format. The Data Record Format Version identifies the TS release and version numbers that were used for the CDR encoding.

Sequence Numbers of Released Packets IE

The Sequence Numbers of Released Packets is present if the Packet Transfer Command is 'Release Data Record Packet'. The format of the Information Element is described in the following figure:

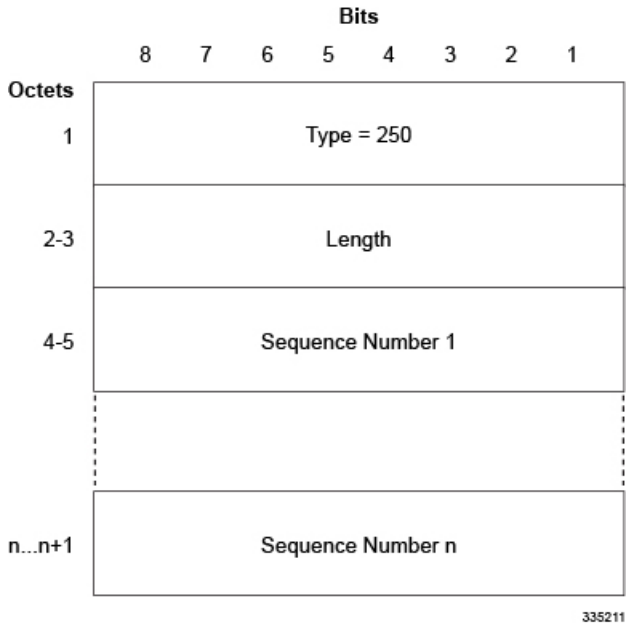
Figure 3: Sequence Numbers of Released Packets IE



Sequence Numbers of Canceled Packets IE

The following figure shows the sequence numbers of Canceled Packets IE that contains the IE Type, Length and the Sequence Number(s) (each 2 octets) of the canceled Data Record Transfer Request(s). It is present if the Packet Transfer Command is "Cancel Data Record Packet".

Figure 4: Sequence Numbers of Canceled Packets IE



Private Extension IE

The optional Private Extension contains vendor- or operator- specific information.

Data Record Transfer Response

The message will be sent as a response to a received Data Record Transfer Request. Also, several Data Record Transfer Requests can be responded by a single Data Record Transfer Response.

The Cause (whatever the value may be) applies for all those Data Record Transfer Requests, responded by that particular Data Record Transfer Response.

Possible Cause values are:

- Request Accepted
- No resources available
- Service not supported
- System failure
- Mandatory IE incorrect
- Mandatory IE missing
- Optional IE incorrect
- Invalid message format
- Version not supported
- Request not fulfilled
- CDR decoding error
- Request already fulfilled
- Request related to possibly duplicated packet already fulfilled
- Sequence numbers of released/canceled packets IE incorrect

The cause value "CDR decoding error" is optional, primarily intended to inform the CDF that the receiving node cannot decode the CDR. Thus, special features in the receiving node that are based on information within the CDR, would not be operable. This message alerts the operator of a remote generating node of incompatible CDR encoding. It is optional and no action or response is required.

The Requests Responded IE contains the IE Type, Length and the Sequence Numbers (each 2 octets) of the Data Record Transfer Requests.

The optional Private Extension contains vendor- or operator- specific information. Depending on the Cause value severity and general occurrence frequency, the node that sent the corresponding Data Record Transfer Request, may start to direct its CDRs to another CGF.

Handling Error Response Cause

By default, on getting an error response, the request is retried to the same CGF server until max-retries is reached. Then the server is marked as NOT ACTIVE and the request is retried to the secondary server. This behavior is seen for the below response causes.

- Mandatory IE incorrect
- Mandatory IE missing
- Optional IE incorrect
- Invalid message format

On getting the following error response causes, the request will NOT retried and the server will be marked as NOT ACTIVE immediately.

- No resources available
- Service not supported
- System failure

No special action is taken on getting "CDR Decoding error" response cause and the behavior is similar to getting a "Request Accepted" cause.

On getting "Version not supported" cause, the request is resent with the version supported by the CGF server (by default, GTPP v2 is supported).

Charging Characteristics

Whether or not the GGSN accepts charging characteristics from the SGSN, the accounting protocol can be configured on a per-APN basis based on whether the subscriber is visiting, roaming, or home.

By default, the GGSN always accepts the charging characteristics from the SGSN. They will be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary. The charging characteristics field is optional. If not provided by SGSN, the GGSN selects the locally configured values. Also, there is a provision to override the values from RADIUS as indicated in the following table.

Table 8: Charging Characteristics Selection Mechanism

CLI command configured on GGSN	Sent by SGSN	Sent by AAA	CC used	chargingCharSelMode
no cc-sgsn	**no cc**	**no cc**	Default	Home/Visiting/Roaming Default
		cc	Default	Home/Visiting/Roaming Default
	cc	**no cc**	SGSN	SGSN Supplied
		cc	SGSN	SGSN Supplied

CLI command configured on GGSN	Sent by SGSN	Sent by AAA	CC used	chargingCharSelMode
cc-sgsn use-ggsn	**no cc**	**no cc**	GGSN	GGSN Override
		cc	GGSN	GGSN Override
	cc	**no cc**	GGSN	GGSN Override
		cc	GGSN	GGSN Override
cc-sgsn radius-returned	**no cc**	**no cc**	Default	Home/Visiting/Roaming Default
		cc	AAA	AAA Supplied
	cc	**no cc**	SGSN	SGSN Supplied
		cc	AAA	AAA Supplied
cc-sgsn radius-returned use-ggsn	**no cc**	**no cc**	GGSN	GGSN Override
		cc	AAA	AAA Supplied
	cc	**no cc**	GGSN	GGSN Override
		cc	AAA	AAA Supplied

Please note that "Default" refers to the value set with the **cc-home**, **cc-roaming**, and **cc-visiting** commands. The "GGSN Override" and "AAA Override" are applicable ONLY for custom5 dictionary. Others will use Home/Visiting/Roaming Default based on the PLMN type.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level. The charging characteristics consists of a string of 16 bits designated as profile index and behavior settings. The GGSN supports up to 16 profile indexes numbered 0 through 15 whereas P-GW/S-GW supports up to a maximum of 256 charging profiles.

The profile indexes specify the criteria for closing accounting records based on specific criteria.

When a bearer is activated, an appropriate charging profile will be selected based on the following sources of input:

- Downloaded AAA attribute (ONLY in P-GW)
- MME/HSS via charging characteristics IE
- Local defaults

Following is the order of precedence when charging profile value is received from multiple sources.

- Profile index in the override rule on the APN
- Profile index in the override rule on the gateway
- Profile index from AAA in case of P-GW
- Profile index from non-override rule on the APN

- Profile index from non-override rule on the gateway

For more information on the commands that configure additional GTPP accounting properties, refer to the *Command Line Interface Reference*.

Charging Records

Charging records support details of the termination such as which end initiated the termination, termination type e.g. RST, FIN, etc. and in case of HTTP 1.1, whether or not the connection is still open. It is possible to pipeline up to 15 HTTP requests on the same TCP connection. The billing system, based on this information, decides upon the success or failure of the connection and charge or refund accordingly.

To cover the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the following types of usage records are provided:

- Standard G-CDRs
- eG-CDRs
- PGW-CDRs
- SGW-CDRs
- S-CDRs
- WLAN-CDRs

The Multimedia Core Platform supports multiple fields for use in these CDRs. The CDRs are encoded using the ASN.1 format and are sent to the CGF using the GTPP.

Important The behavior for several of the fields supported in CDRs can be modified. For more information, refer to the *Command Line Interface Reference*.

Important SGW-CDRs are suppressed and only PGW-CDRs are generated for a session hosted by the associated S-GW and P-GW service. SGW-CDRs are generated when the S-GW connects to an external P-GW.

In StarOS release 16.0, S2a Mobility Over GTP (SaMOG) Gateway supports generation of CDR files for offline charging. In Offline Charging, charging information is collected concurrently with resource usage. The charging information is then passed through a chain of logical charging functions, and the CDR files are generated by the network, which are then transferred to the network operator's Billing Domain.

As 3GPP specifications does not define a CDR format for SaMOG, the S-GW CDR and SGSN CDR record formats are used to define the CDR format for SaMOG 4G/3G subscribers. The record format can be selected using a CLI command under the GTPP Group Configuration Mode. By default, for an SaMOG license, the S-GW record type is used, and for an SaMOG 3G license, the SGSN record type is used.

File Format for CDRs

The file format determines the information organization and structure -- format -- of the generated data files. All file formats are different and are customizable.

The following file formats are supported for CDRs:

- **custom1 Format**: This file format encodes CDRs according to the following conventions:
  - **Header**: No header
  - **Contents**: *CDR1CDR2CDR3...CDRn*
  - **EoF marker**: \n
  - **File name format**:

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009+07_53_02_5_file1

- **custom2 Format**: This customer-specific file format encodes CDRs according to the following conventions:
  - **Header**: 24 byte header incorporating the following information:

Field	Description	Value
0x00 - 0x03	Offset	Offset from EoH to first Unread CDR (4 Bytes)
0x04 - 0x07	Encoding	Basic Encoding Rule (BER) i.e. 1 (4 Bytes)
0x08 - 0x0b	Number of CDRs	Total number of CDRs in the file (4 Bytes)
0x0c - 0x0f	Number of read CDRs	Total number of read CDRs in the file (4 Bytes)
0x10 - 0x13	File size	Size of CDR file in bytes (4 Bytes)
0x14 - 0x17	Abstract Syntax Notation One (ASN.1) format definition version	ASN.1 definition version information (4 Bytes)

  - **Contents**: *LEN1CDR1LEN2CDR2LEN3CDR3...LENnCDRn*
  - **EoF marker**: No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.

- **Example**:

  default3_07_15_2009_07_59_32_5_file2.u

Important With file format **custom2**, the files are generated with **.u** file extension indicating an unprocessed file by the billing system. Typically, the billing system would rename the file with **.p** extension after processing the files with CDR information.

Important Remember that the unprocessed CDR (*.u) files should never be deleted from HDD.

- **custom3 Format**: This customer-specific file format encodes CDRs according to the following conventions:
  - **Header**: No header
  - **Contents**: *CDR1CDR2CDR3...CDRn*
  - **EoF marker**: No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009_07_59_32_5_file2.u

- **custom4 Format**: This custom4 format was created to support writing CDRs in blocks. This file format is similar to custom3 file format except CDRs will be written in 2Kbyte blocks in a file.
  - **Header:** No Header
  - **Contents:** CDR1|CDR2FFFFFF|CDR3FFFFF..|..CDRnFFFF|

    where | represents the end of a 2K block
  - **EoF marker:** No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009_07_59_32_5_file2.u

- **custom5 Format**: This file format is similar to custom3 file format except that the sequence number for CDR file name is of six digits in length ranging from 000001 to 999999.

- **Header:** No Header
- **Contents**: *CDR1CDR2CDR3...CDRn*
- **EoF marker:** No EoF marker
- **File name format**:

  <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fixed-length-seqnum>.u
- **Example**:

  default3_07_15_2009_08_09_25_4_file000003.u

- **custom6 Format**: This file format is similar to custom4 file format except CDRs will be written in 8Kbyte blocks in a file.
  - **Header:** No Header
  - **Contents:** CDR1|CDR2FFFFFF|CDR3FFFFF..|..CDRnFFFF|

    where | represents the end of a 8K block
  - **EoF marker:** No EoF marker
  - **File name format:**

    <node-id-suffix+vpn-id>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u

    The *<fileseqnum>* denotes the file sequence number ranging from 1 through 4294967295.
  - **Example**:

    default3_07_15_2009_07_59_32_5_file2.u

Important These file formats are customer-specific. For more information on the file formats, contact your Cisco account representative.

Evolved Packet Data Gateway Call Detail Records (ePDG-CDRs)

ePDG-CDRs are generated according to 3GPP TS 32.298 V12.6.0.

ePDG-CDR Format

The ePDG-CDRs can be in ASN.1 format.

Standard G-CDRs

G-CDRs are generated according to 3GPP TS 32.251 V6.6.0. Currently ECS supports generation of CDRs using AAAMgrs only.

G-CDR Format

The G-CDRs can be in ASN.1 Format.

Enhanced G-CDRs

The ECS also supports enhanced G-CDRs, which is an enhanced format of standard G-CDRs to provide greater portability of charging information. eG-CDRs are compliant with 3GPP TS 32.298 v6.5.0 for Rel. 6 based dictionaries, and with 3GPP TS 32.298 v7.4.0 for Rel. 7 based dictionaries.

By default, the G-CDR does not support the traffic and vendor specific records. To support a traffic and vendor specific record, the ECS must be configured to generate eG-CDRs. eG-CDRs are useful to implement Time Based Charging (TBC) and Flow Based bearer Charging (FBC) to ECS.

eG-CDR supports customer specific formats configured in Ga context in a GGSN service with standard or custom specific GTPP dictionaries.

eG-CDR Format

The eG-CDRs can be in ASN.1 Format.

For more information on G-CDR and eG-CDR attributes and definitions, refer to the *G-CDR and Enhanced G-CDR Field Descriptions* chapter in this reference guide.

PDN Gateway Call Detail Records (PGW-CDRs)

PGW-CDRs are generated according to 3GPP TS 32.298 V8.5.0.

PGW-CDR Format

The PGW-CDRs can be in ASN.1 Format.

Serving Gateway Call Detail Records (SGW-CDRs)

SGW-CDRs are generated according to 3GPP TS 32.298 V8.7.0.

SGW-CDR Format

The SGW-CDRs can be in ASN.1 Format.

Standard SGSN CDRs

S-CDRs are generated according to 3GPP TS 32.215 V4.5.0 for Release 4 dictionaries, and 3GPP TS 32.298 V6.4.1 for Release 6 dictionaries.

S-CDR Format

The S-CDRs can be in ASN.1 Format.

Wireless LAN Call Detail Records (WLAN-CDRs)

WLAN-CDRs are generated according to 3GPP TS 32.298 V6.4.1.

WLAN-CDR Format

The WLAN-CDRs can be in ASN.1 Format.

Triggers for Generation of Charging Records

The following sections describe the triggers for the generation of partial and final CDRs.

ePDG-CDR Triggers

The ePDG will use the Charging Characteristics to determine whether to activate or deactivate CDR generation. The Charging Characteristics are also used to set the coherent chargeable event conditions (e.g. time/volume limits that trigger CDR generation or information addition). Multiple Charging Characteristics "profiles" are configured on the ePDG to allow different sets of trigger values.

ePDG-CDR Charging Information Addition

The "List of Traffic Data Volumes" attribute in the ePDG-CDR consists of a set of containers that are added when specific trigger conditions are met, and identify the volume count per QoS, separated for uplink and downlink traffic, on encountering that trigger condition.

The following table identifies the conditions that are supported to trigger ePDG-CDR charging information addition.

Table 9: Triggers for ePDG-CDR Charging Information Addition

Trigger Conditions	Description/Behavior
QoS Change	A change in the QoS will result that open "List of Traffic Data Volumes" containers being closed and added to the CDR and new bearer specific container is opened. This can happen when P-GW initiates UBRequest to modify the QoS for the session.
Tariff Time Change	On reaching the Tariff Time Change open "List of Traffic Data Volumes" containers will be closed and added to the CDR. Tariff-time change is for adding charging information to CDR during a particular tariff-time of day. For example, in a day CDR can be generated at 10 AM and 8:30 PM.
CDR Closure	Open "List of Traffic Data Volumes" containers will be closed and added to the ePDG-CDR.

Volume container identifies the uplink/downlink volume since the closure of the last container. When Charging Event is triggered by CDR Closure condition, this Change-Condition sub-field associated to the added volume

container will be omitted, except when CDR closure is due to "maximum number of charging condition changes", where it will be present with the original condition change.

Triggers for ePDG-CDR Closure

The ePDG-CDR will be closed on encountering some trigger conditions.

The following table identifies the conditions that are supported to permit closure of the ePDG-CDR.

Table 10: Triggers for ePDG-CDR Closure 3

Closure Conditions	Description/Behavior

End of bearer within the ePDG	Deactivation of the bearer (either default or dedicated) in the ePDG will result in the CDR being closed. The trigger condition covers:
	• termination of bearer;
	• any abnormal release (as listed below):
	  • GTP-C/GTP-U path failures in S2b interface
	  • Dead Peer Detection in SWu interface.
	  • IKESA/IPSESA rekey failure

Partial Record Reason	OAM&P; reasons permit the closure of the CDR for internal reasons. The trigger condition covers: • data volume limit; CDR generated based on every uplink/downlink/total volume limit. • time (duration) limit; CDR generated for every configured "x" seconds time • maximum number of charging condition changes (QoS/tariff time change); CDR generated when the max bucket limit is reached. By default its 4.Please check "cc profile <> buckets <>" CLI under accouting-policy configuration mode. • management intervention; (clear subscriber <>)

The Partial Record generation trigger thresholds are those associated with the Charging Characteristics. The Partial Record generation trigger thresholds are ePDG configuration parameters defined per Charging Characteristics profile by the operator through configuration options. In the event that the ePDG-CDR is closed and the bearer remains active, a further ePDG-CDR is opened with an incremented Sequence Number in the ePDG.

When Charging Event is triggered by the above listed conditions, the Change-Condition (at PS information level) associated to the CDR closure, indicating the appropriate condition will be present, and it will be omitted otherwise.

GGSN CDR Triggers

The following sections describe the triggers for the generation of partial and final G-CDRs and eG-CDRs.

G-CDR Triggers

G-CDRs are updated (not closed) for any of the following conditions:

- SGSN IP address change

  When the SGSN IP address changes, i.e. an Update PDP Context Request is received with a new SGSN IP address, the old address (if not already added) and the new address are added to the field "List of SGSN Addresses".

- QoS change

  When a QoS change is detected, i.e. an Update PDP Context Request is received with a new QoS value) and the maximum number of configured "buckets" has not been reached, then a traffic data volume container for the previous QoS and volume is added to the field "List of Traffic Data Volumes".

- Tariff Time Change

  When the tariff time changes and the maximum number of configured "buckets" has not been reached, then a traffic data volume container is added to the field "List of Traffic Data Volumes" for the volume before the tariff time.

The following events trigger closure and sending of a partial G-CDR:

- When the number of SGSN changes has reached the configured number of "sgsns". Before this, the new SGSN address is added to the list of SGSN IP addresses in the CDR. If "sgsns 4" is configured, this means that after 4 handovers the record is closed and the G-CDR will contain 5 SGSN IP addresses. The parameter can be set to 1 to 4 with a default of 4.
- When the number of QoS changes or tariff time changes, with up to 4 timestamps which can be configured using the tariff statement, has reached the configured number of "buckets" (1 to 4 with default of 4). Before this, another traffic data volume container is added to the CDR for every change.
- Every x seconds configured using "interval x"
- Every x octets configured using "volume x" (up/down/total)

A G-CDR is closed as the final record of a subscriber session for the following events:

- Delete PDP context received from SGSN
- Delete PDP context initiated by GGSN (e.g. expiry of idle or absolute timer)
- Abnormal Releases such as PDP context replacements

eG-CDR Triggers

eG-CDRs are updated (not closed) for any of the following conditions:

- PDP context modification

  When a change of PDP context conditions occurs (QoS change, SGSN change, PLMN Id change, RAT change) the List of Service Data (LOSDV) and the List of Traffic Volume (LOTV) containers are updated.

In case of SGSN change condition only LOSDV containers are updated and also the List of SGSN addresses is updated.

- Tariff time change

  When a change of tariff time occurs a set of LOSDV and LOTV containers, i.e. all active service data flow containers, will be added to eG-CDR.

- Failure handling procedure triggering

  When the failure handling mechanism is triggered and the failure action is set to "continue" a set of LOSDV and LOTV containers, i.e. all active service data flow containers, will be added to eG-CDR.

- Service data flow report

  When an expiry of time limit, volume limit or termination is detected for a service data flow a set of LOSDV container is added to eG-CDR.

- CDR closure

  When a CDR closure occurs all active LOSDV containers are added to eG-CDR.

- ULI change

  When the ULI changes, then a data volume container is added to the field "List of Service Data Volumes".

The eG-CDRs will be closed and sent as a partial record for any of the following triggers:

- Data volume limit
- Time duration limit
- Maximum number of charging condition changes (QoS/tariff time change)
- Maximum number of service data containers
- Management intervention
- MS/Subscriber time zone change
- Inter PLMN SGSN change
- Radio Access Technology (RAT) change

When an eG-CDR partial is written, all open LOSDVs will be closed as well with a matching change condition.

The eG-CDRs will be closed and sent as a final record upon the deactivation of the PDP context in the GGSN, both for normal termination and for any abnormal release.

All LOSDV which have been reported in previous partials but did not have a final change condition in the container are repeated in the final eG-CDR with a final change condition (e.g. pDPContextRelease). In case no volume has been transferred for this container since the last eG-CDR, then the timestamps for first and last usage will be set to the default value of "000101000000-0200".

The following table lists the values for the "CauseForRecordClosing" field based on trigger scenarios.

Table 11: Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	– Delete PDP from SGSN – Manual call clearing on GGSN – Radius disconnect – Idle and absolute timeout	Final	0	Yes
abnormalRelease	– Path failure – Context replacement	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
sGSNChange	– Configured limit of SGSN changes has been reached – inter-PLMN SGSN change	Partial	18	Yes
maxChangeCond	Configured limit of change conditions has been reached	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now**	Partial	20	Yes
rATChange	Radio access technology change	Partial	22	Yes
mSTimeZoneChange	MS changes time zone	Partial	23	Yes

PGW-CDR Triggers

The following events trigger closure and the sending of a partial PGW-CDR:

- When the number of QoS changes or tariff time changes has reached the configured maximum number of charging condition changes. Before this, service containers are added to the CDR for every change.
- Every x seconds configured using "interval x"

- Every x octets configured using "volume x" (up/down/total)
- Command **gtpp interim now active-charging egcdr**
- Transferring the context to a new SGW/SGSN (serving Node Change).
- Changing the access type within the same P-GW (RAT Change)

A PGW-CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from UE
- Delete bearer context request received from SGW.
- Manual subscriber clearing
- Abnormal Releases such as path failures

The following table lists the values for the "CauseForRecordClosing" field based on trigger scenarios.

Table 12: Cause for Record Closing

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	IP-CAN bearer release or detach	Final	0	Yes
abnormalRelease	Any other abnormal release	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
servingNodeChange	Serving node Address list overflow	Partial	18	Yes
maxChangeCondition	Maximum number of changes in charging conditions	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now active-charging egcdr**	Partial	20	Yes
RAT Change	Change of radio interface from (for example, EUTRAN to GSM to UMTS)	Partial	22	Yes
mSTimeZoneChange	MS changes time zone	Partial	23	Yes
PLMN Change	Change of PLMN-ID	Partial	24	Yes

PGW-CDR Charging Information Addition

The "List of Service Data" attribute in the PGW-CDR consists of a set of containers that are added when specific trigger conditions are met. Each container identifies the configured counts (volume separated for uplink and downlink, elapsed time, or number of events) per rating group or combination of the rating group and service id within the same IP-CAN bearer, on encountering that trigger condition.

Table 13: Triggers for PGW-CDR Charging Information Addition

Trigger Conditions	Description/Behavior
IP-CAN bearer modification	A change of IP-CAN bearer conditions (QoS change, SGSN/S-GW change, PLMN Id change, RAT change, user location change) results in a set of "List of Service Data" containers, such as all active service data flow containers, being added to the CDR.
Tariff Time Change	On reaching the Tariff Time Change, a set of "List of Service Data" containers, such as all active service data flow containers, is added to the CDR.
DCCA Failure-Handling procedure triggering	When the Diameter Credit-Control-Failure-Handling mechanism is triggered a "List of Service Data", such as all active service data flow containers, is added to the CDR. The causes are only relevant due to simultaneous usage of an active DCCA session.

Trigger Conditions	Description/Behavior
Service data flow report	For independent online and offline charging, a "List of Service Data" container for the service data flow is added at: • expiry of time limit • expiry of volume limit • expiry of unit limit • termination of service data flow For tight interworking of online and offline charging, a "List of Service Data" container for the service data flow is added when: • time threshold reached • volume threshold reached • unit threshold reached • time quota exhausted • volume quota exhausted • unit quota exhausted • expiry of quota validity timer • termination of service data flow – re-authorization request by OCS.

S-CDR Triggers

The SGSN will use the Charging Characteristics to determine whether to activate or deactivate CDR generation. The Charging Characteristics are also used to set the coherent chargeable event conditions (e.g. time/volume limits that trigger CDR generation or information addition). Multiple Charging Characteristics "profiles" may be configured on the SGSN to allow different sets of trigger values.

Triggers for S-CDR Closure

The following events trigger closure and sending of a partial S-CDR:

- The number of QoS changes or tariff time changes has reached the configured number of "buckets". Before this, another traffic data volume container is added to the CDR for every change.
- every x seconds configured using "interval x"
- every x octets configured using "volume x" (uplink/downlink/total)
- command "**gtpp interim now**"
- transferring the context to a new SGSN (Inter SGSN Routing Area Update)
- changing the access type within the same SGSN (Intra SGSN Inter System Change)

An S-CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from MS
- Delete PDP context request received from MS
- Delete PDP context request received from GGSN
- Cancel Location received from HLR
- Delete subscriber data received from HLR
- Inactivity timeout on the SGSN
- Manual subscriber clearing
- command "**clear subscribers all**"
- ISRAU scenario (PDP is released at the OLD SGSN)
- Abnormal Releases such as path failures

The following table lists the different values for the CauseForRecordClosing field depending on the different trigger scenarios.

Table 14: Cause for Record Closing 4

Cause For Record Closure				
Cause	**Scenarios**	**Partial/Final**	**Value**	**Configurable**
normalRelease	• delete PDP from MS • delete PDP from GGSN • PDP Release due to ISRAU scenario	Final	0	No
abnormalRelease	• Path failure • Attach on Attach	Final	4	No
SGSN Change	PDP Release in old SGSN due to ISRAU scenario.	Final	18	No
volumeLimit	configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	configured interval has been reached	Partial	17	Yes
maxChangeCondition	limit for the LOTV containers was exceeded	Partial	19	Yes

Cause For Record Closure				
Cause	**Scenarios**	**Partial/Final**	**Value**	**Configurable**
managementIntervention	e.g. using the command "**gtpp interim now**" and also "**clear subscribers all**"	Partial	20	No
managementIntervention	i.e. using the command "**clear subscribers all**"	Final	20	No
intraSGSNIntersystemChange	change of radio interface from GSM to UMTS or vice-versa	Partial	21	No

Triggers for S-CDR Charging Information Addition

The "List of Traffic Volumes" attribute of the S-CDR consists of a set of containers, which are added when specific trigger conditions are met, and identify the volume count per PDP context, separated for uplink and downlink traffic, on encountering that trigger condition.

Table 15: Triggers for S-CDR Charging Information Addition 5

Change Condition				
Cause	**Scenario**	**Partial/Final**	**Value**	**Configurable**
qoSChange	A change in the QoS will result in a "List of Traffic Data Volumes" container being added to the CDR.	Partial	0	Yes
tariffTime	On reaching the Tariff Time Change a "List of Traffic Data Volumes" container will be added to the CDR.	Partial	1	Yes

Change Condition				
Cause	**Scenario**	**Partial/Final**	**Value**	**Configurable**
Direct Tunnel establishment	When the SGSN establishes or removes a Direct Tunnel a "List of Traffic Data Volumes" container will be added to the CDR. When a direct tunnel is established, the SGSN will no longer be able to count data volumes associated with the IP-CAN bearer for which the direct tunnel is established.	Partial	8	Yes
Direct Tunnel Removal	When the SGSN establishes or removes a Direct Tunnel a "List of Traffic Data Volumes" container will be added to the CDR.	Partial	9	Yes
recordClosure	A list of "List of Traffic Data Volumes" container will be added to the S-CDR.	-	2	No

SGW-CDR Triggers

The following events trigger closure and sending of a partial SGW-CDR.

- When the number of QoS changes or tariff time changes or number of user location changes have reached the configured number of "buckets". Prior to this, another traffic data volume container is added to the CDR for every change.
- Every x seconds configured using "interval x"
- Every x octets configured using "volume x" (up/down/total)
- Command **gtpp interim now**
- Transferring the context to a new S-GW
- Changing the access type within the same S-GW (RAT Change)

An SGW-CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from UE
- Delete bearer context request received from MME

- Delete bearer context request received from P-GW
- Manual subscriber clearing
- Abnormal Releases such as path failures

The following table lists the different values for the "CauseForRecordClosing" field depending on the different trigger scenarios.

Table 16: Cause for Record Closing 6

Cause	Scenarios	Partial/Final	Value	Supported
normalRelease	IP-CAN bearer release or detach	Final	0	Yes
abnormalRelease	Any other abnormal release	Final	4	Yes
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
servingNodeChange	Serving node Address list overflow	Partial	18	Yes
maxChangeCondition	Limit for the LOTV containers was exceeded	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now**	Partial	20	Yes
RAT Change	Change of radio interface from (for example, EUTRAN to GSM to UMTS)	Partial	22	No
mSTimeZoneChange	MS changes time zone	Partial	23	Yes

Important The spec 3GPP TS 32.251 mentions that a CDR must be generated whenever the PLMN-ID of the serving node changes, but does not have a corresponding "cause for record closure" reason in 3GPP TS 32.298.

In the case when the MME changed during the call and the PLMN-ID has the same address, the MME is added to the "Serving Node Address" list. If a "Serving Node Address" list overflow occurs, a partial CDR will be generated with "cause for record closure" as "servingNodeChange".

Important The unsupported triggers mentioned above will be supported when the functionality is available.

SGW-CDR Charging Information Addition

The "List of Traffic Volumes" attribute of the SGW-CDR consists of a set of containers which are added when specific trigger conditions are met. They identify the volume count per QCI/ARP pair and are separated for uplink and downlink traffic after encountering that trigger condition.

The following table identifies which conditions are supported to trigger SGW-CDR charging information addition. Volume container identifies the uplink/downlink volume since the closure of the last container. The "Serving Node Address" attribute of the SGW-CDR consists of a list of serving node (for example, MME) addresses. A new serving node address is added to the list when MME changes.

Table 17: Triggers for SGW-CDR Charging Information Addition

Trigger Conditions	Description/Behavior
QoS Change	A change in the QoS will occur when the open "List of Traffic Data Volumes" containers are closed and added to the CDR, and a new IP-CAN bearer specific container is opened.
Tariff Time Change	After reaching the Tariff Time Change, open "List of Traffic Data Volumes" containers are closed and added to the CDR.
User Location Change	A change in the User Location Info (for example, ECGI, TAI, RAI, SAI or CGI) will close open "List of Traffic Data Volumes" containers. They are then added to the CDR if location reporting is required and a report of User Location Change is received.
ULI Change	When the ULI changes, then a data volume container is added to the field "List of Service Data Volumes".
Apn-Ambr Change	If APN AMBR changes container need to be added to a bearer based on the configuration of the trigger CLI command.
CDR Closure	Open "List of Traffic Data Volumes" containers are closed and added to the SGW-CDR.

WLAN-CDR Triggers

The following events trigger closure and sending of a partial WLAN-CDR:

- Time Trigger (every x seconds configured using "interval x")
- Volume Trigger (every x octets configured using "volume x" (up/down/total))
- On reaching maximum number of container limit
- command **gtpp interim now**

A WLAN-CDR is closed as the final record of a session for the following events:

- UE initiated call termination
- command **clear subscribers all**
- Abnormal Releases due to multiple software failures

The table below lists the different values for the "CauseForRecordClosing" field depending on the different trigger scenarios.

Table 18: Cause for Record Closing 7

Cause	Scenarios	Partial/Final	Value	Configurable
normalRelease	UE is terminating the call	Final	0	No
abnormalRelease	Failure within the chassis (due to multiple software failures)	Final	4	No
volumeLimit	Configured volume threshold has been exceeded	Partial	16	Yes
timeLimit	Configured interval has been reached	Partial	17	Yes
maxChangeCondition	Limit for the LOTV containers was exceeded	Partial	19	Yes
managementIntervention	For example, using the command **gtpp interim now**	Partial	20	No
managementIntervention	For example, using the command **clear subscribers all**	Final	20	No

WLAN-CDR Charging Information Addition

The "List of Traffic Volumes" attribute of the WLAN-CDR consists of a set of containers, which are added when specific trigger conditions are met, and identify the volume count per PDP context, separated for uplink and downlink traffic, on encountering that trigger condition.

The following table identifies which conditions are supported to trigger WLAN-CDR charging information addition. Volume container identifies the uplink/downlink volume since the closure of the last container. The "Serving Node Address" attribute of the SGW-CDR consists of a list of serving node (for example, MME) addresses. A new serving node address is added to the list when MME changes.

Table 19: Triggers for WLAN-CDR Charging Information Addition

Cause	Scenarios	Partial/Final	Value	Configurable
QoS Change	A change in the QoS will result that open "List of Traffic Data Volumes" containers being closed and added to the CDR and new bearer specific container is opened.	Partial	0	Yes
tariffTime	On reaching the Tariff Time Change a "List of Traffic Data Volumes" container will be added to the CDR.	Partial	1	Yes
recordClosure	A list of "List of Traffic Data Volumes" container will be added to the WLAN-CDR.	-	2	No

Supported Features

This section provides the list of features that are supported by GTPP interface.

CDR Push Functionality

This feature facilitates sending of local CDR (G-CDR, eGCDR, PGW/SGW CDR, or any other GTPP CDR) files to a remote host using the CLI command **gtpp storage-server local file push** in context configuration mode or GTPP group configuration mode.

When the push is enabled in a GTPP group then the AAA proxy registers with the HD controller for the push. If the registration is successful then the controller periodically (~1 min) checks to see if any of the registered clients have files, in the CDR_DIR (*/records/cdr/<gtpp-group>-<vpnid>/**), to be pushed to the configured remote host URLs. If yes, it will start the PUSH process for that particular client. After pushing all the files of this client, the requests for the next client will be serviced in sequence.

If the registration fails, the client will re-attempt to register indefinitely in intervals unless the configuration is removed. Upon each failure an error log will be printed.

Important The push framework does not support FTP or TFTP for pushing CDR files but it supports only SFTP.

Important After you configure the **gtpp storage-server local file push** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment.

For information on how to configure push functionality, refer to the *Configuring CDR Push* section in the *HDD Storage* chapter of this guide.

Zero Volume CDR Suppression

Important Use of the Zero Volume CDR Suppression feature requires that a valid ECS license key be installed. This feature is applicable to all types of CDRs – GGSN CDRs, PGW-CDRs, SGW-CDRs, and SGSN CDRs. Contact your Cisco account representative for information on how to obtain a license.

This feature is developed to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. The CDRs can be categorized as follows:

- Final-cdrs: These CDRs are generated at the end of a context.
- Internal-trigger-cdrs: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- External-trigger-cdrs: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

The customers can select the CDRs they want to suppress. A new CLI command **[default | no] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }** is introduced to enable this feature. This feature is disabled by default to ensure backward compatibility. For more information on this command, see *Cisco ASR 5500 Command Line Interface Reference*.

Automatic Transfer of Stranded CDRs on ICSR

During an ICSR switchover, the GTPP charging interface between the active chassis and CGF server goes down and all pending CDRs are written to internal hard disk. Once the chassis becomes standby, the CDRs will remain on HDD until the chassis becomes active.

This feature provides a way to move the stranded CDRs from the new standby chassis to the new active chassis and stream them to the OCG. The **gtpp push-to-active url** CLI command enables/disables the Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.

Releases prior to 16.0, CDRs from current standby chassis were manually transferred to current active chassis using the CLI command "**gtpp storage-server streaming start**". Once the transfer is complete, a CLI command in the Exec mode is configured to stream the CDRs to CGF.

In 16.0 and later releases, the stranded CDRs in the standby ICSR node (moved from active to standby) are automatically transferred to the newly active ICSR node. This automation process is achieved through the use of "**gtpp push-to-active url**" CLI command in the Global Configuration mode.

Limitations

This section provides the limitations with this feature.

- This feature could lead to duplicate CDRs. When streaming is in progress and ICSR switchover happens, the current file being streamed, will not complete the streaming as interface with CGF went down. This file will be transferred to new active chassis and streamed from beginning from new chassis.
- The accounting contexts should be in the same order in both the chassis. The directory names are created using vpn-id. If the accounting contexts are in different order, vpn-id will be different and the sub-directories in HDD will be different in both the chassis for same GTPP group.

How this Feature Works

This section describes the work flow for the stranded CDR automation process.

Step 1 Chassis-1 is Active and Chassis-2 in Standby State.

Step 2 SRP switchover is initiated from Chassis-1 to Chassis-2.

Step 3 Now, Chassis-1 becomes Standby and Chassis-2 becomes Active.

Step 4 Chassis-1 stores CDRs to HDD since the IP interface to CGF is down.

Step 5 After 12 min (time to write all CDRs to HDD), Chassis-1 initiates SFTP transfer of files to Chassis-2.

Step 6 Chassis-2 on getting the file transfer complete indication, reloads file list from HDD and streams transferred CDRs to CGF server.

Step 7 If ICSR switch-overs to Chassis-1 during the file transfer, file transfer stops and reverse transfer of files is initiated from Chassis 2 to Chassis 1.

Restructuring of CDR Module

Charging Data Records (CDRs) play very important role in billing of mobile subscribers and hence are of utmost importance for the mobile service providers. Though eGCDRs and PGW-CDRs comply to 32.298 3GPP standards, many customers have their own requirements (customizations) which may vary from the standards and hence there is a need to create and maintain a new "dictionary" which defines the fields and behavior of that customer's CDR.

GTPP dictionary will define all the attributes e.g. list of all the fields, encoding type (ASCII/ASN.1), release-compliance, supported product-type, etc.

The customizations include:

- Addition of new fields
- Encoding (ASN.1/ASCII)
- New cause codes
- New behavior e.g. suppress-zero-volume CDRs, bucket-updating based on certain dictionary.
- Management extensions
- 3GPP release compliance

There are various limitations/drawbacks with the current CDR dictionary implementation:

- High turnaround time – It takes approximately 2-3 weeks for doing any new minor customization.
- Error-prone implementation – The code changes are error-prone and likely to cause regressions.

- Outdated documentation – Either there is no documentation for various dictionaries or the document is out-of-sync with the actual implementation.

To nullify the above limitations, a new flexible and extensible framework has been implemented to generate eGCDR and PGW-CDR.

This new framework will be provided to define a dictionary in a structured format using a "Dictionary Definition Language (DDL)". Using this language customers can clearly define fields, encoding and behavior applicable for a particular GTPP dictionary. DDL file will be parsed at compilation time and metadata will be populated to generate eGCDR and PGW-CDR.

PGW-CDRs/eGCDRs have been moved onto flexible DDL based framework. The syntax of these dictionaries/field modified dictionaries can be validated using the *ddl_validate* binary provided.

In StarOS release 16.0, the CLI command "**gtpp egcdr new-path**" is used to activate new framework for customized/field defined CDR generations. In release 17.0, the CLI command "**gtpp egcdr dynamic-path**" should be used to to load the customized or dynamic DDL. This framework provides a mechanism to define and load a customized dictionary by providing the path to the appropriate DDL file through this CLI command.

Customers should explicitly configure the dictionary as there will be no default dictionary. If no dictionary is configured, then eGCDR/PGW-CDR will not be generated.

When customer wants to add/modify/remove a field, this information has to be updated in DDL. The DDL file is processed dynamically and the field reflects in CDR.

Important This framework works only for eGCDR and PGW-CDR.

It is not recommended to enable **gtpp egcdr dynamic-path** when there are active calls.

For more information on the command, refer to the *Command Line Interface Reference*.

GTPP Group Configuration with Same CGF Server IP and Different Ports

In a multi-product deployment environment where CDRs are received from different gateway services like ePDG, SaMOG and (pseudo) P-GW (in Local Breakout scenario), the mediation server finds it difficult to differentiate between the CDRs. Easy identification of CDRs is possible if CDRs corresponding to each gateway service are mapped to different ports of the same CGF server. To achieve this, CLI support is provided to configure multiple GTPP groups with the same CGF server IP address and different port numbers. This configuration provides the flexibility to send the ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

For ePDG and SaMOG, different GTPP groups should be configured in the respective call-control profiles. For P-GW LBO, GTPP group is selected from APN configuration.

In releases prior to 20.0, configuration of CGF server with the same IP address but different ports was not allowed within and across GTPP groups. In release 20.1 and later, configuration of CGF server with the same IP address and different ports is allowed across the GTPP groups. With this change, whenever AAA proxy logs are displayed, it includes both CGF IP address and port.

The use of optional keyword **port** in the **gtpp test accounting**, **show gtpp counters**, **show gtpp statistics** and **clear gtpp statistics** CLI commands enables this functionality. When port is specified along with IP address in these CLI commands, then the CGF server with the specified IP address and port is only considered. If the port is not specified, then all GTPP servers with the specified IP address will be considered irrespective of the configured port.

For more information on these CLI commands, refer to the *Command Line Interface Reference* guide.

Limitations

The following are the known limitations with this feature:

- Configuration of same IP address and different port is not permitted within a GTPP group. That is, it is not allowed to configure primary and secondary servers in a GTPP group with the same IP and different port.