ERICSSON

CDR-Based Charging Interface Description

DESCRIPTION

2/1551-AXB 250 10/4-V3 Uen BF

Contents

1 Introduction

This document describes the Ga and Bp interfaces on the EPG for GSM, WCDMA, LTE, trusted non-3GPP, and untrusted non-3GPP networks. Ga and Bp run as interface applications through the Gom network.

1.1 Supported Nodes

This document describes functionality supported by the following logical nodes:

— GGSN

— PGW

— SGW

If any functionality described in this document is not applicable for all logical nodes, it is explicitly stated.

1.2 Scope

This document gives a description of the Ga and Bp interfaces for offline charging in the EPG and an overview of the two methods for transferring Charging Data Records (CDRs).

1.3 Target Groups

This document is intended for personnel performing configuration of the EPG. It assumes a basic knowledge of data communication and telecommunication.

2 Overview

The Ga and Bp charging interfaces enable a CGF or a BS to receive CDRs from the EPG.

Note: In this document the term CDR is used for common information. When information is only applicable for a specific CDR type it is explicitly stated or noted. For information on the different CDR types, see Offline Charging.

Figure 1 and Figure 2 displays the EPG interfaces for CDR transfer to a BS or CGF:

Bp Secure FTP (SFTP)-pull over TCP/IP

Ga GPRS Tunneling Protocol (GTP) Prime over User Datagram Protocol/Internet Protocol (UDP/IP)

Note: Near real-time CDR transfer over the Ga interface is not supported by the SGW.

Note: In SoC with 3GPP TS 23.125, Gz is specified as the interface reference point for offline flow-based bearer charging. From a charging architecture perspective, Gz is not a logical interface and related functions are equivalent to Ga.

If SFTP-pull is used as the CDR transfer protocol, the external node pulls CDRs from the GGSN, PGW, and SGW at regular time intervals. If GTP Prime is used to transfer CDRs, the GGSN and PGW push CDRs to the external node as soon as they are closed.

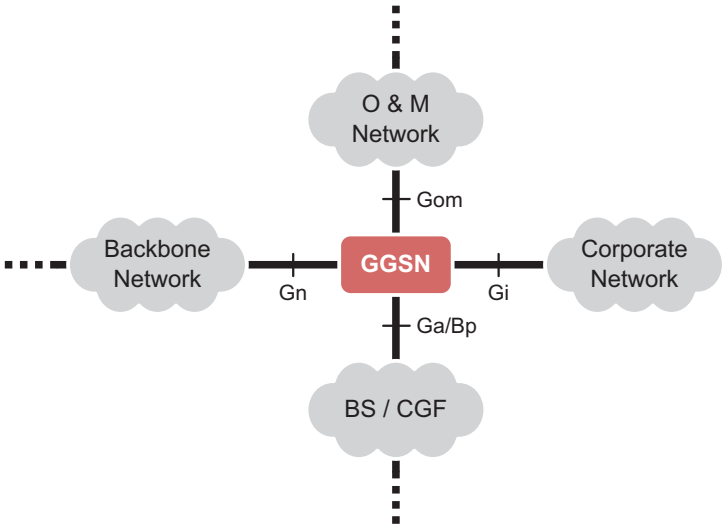

Figure 1 Charging Interfaces in the GPRS Network

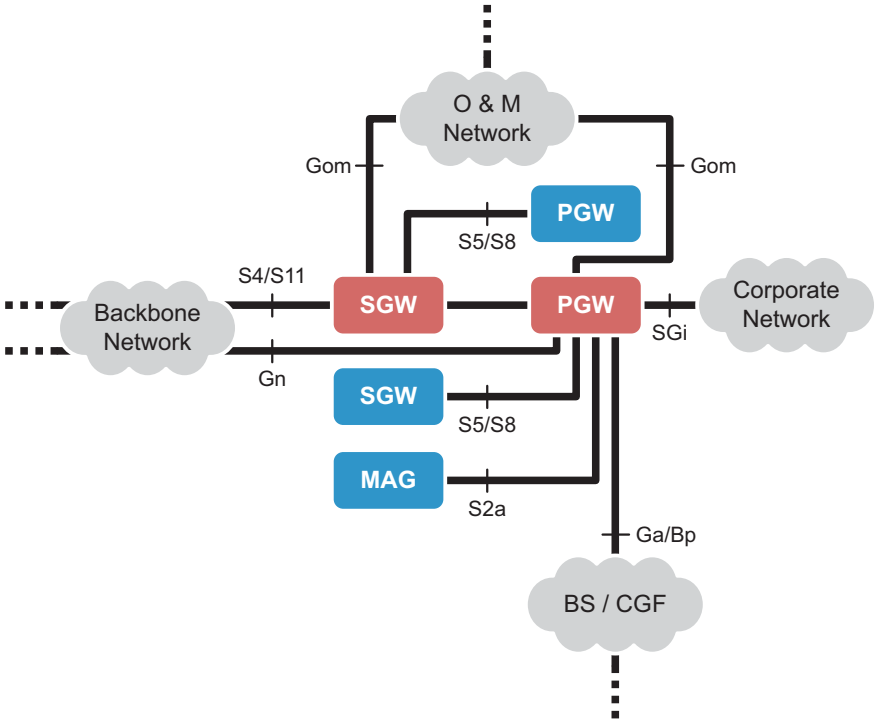

Figure 2 Charging Interfaces in the EPS Network

3 Protocols

The EPG supports two protocols for delivery of generated CDRs to a CGF or BS: SFTP and GTP Prime. The charging profile configuration determines whether one or both protocols are active. For more information, see Offline Charging. The corresponding protocol layers are shown in Figure 3.

Both the Bp and Ga interfaces belong to the generic Gom interface. The Bp interface for the SGW and PGW is supported by the Node Management Board (NMB) at the EPG node level whereas the Ga interface for the PGW is supported by the PGW CPBs. For more information, see Routing.

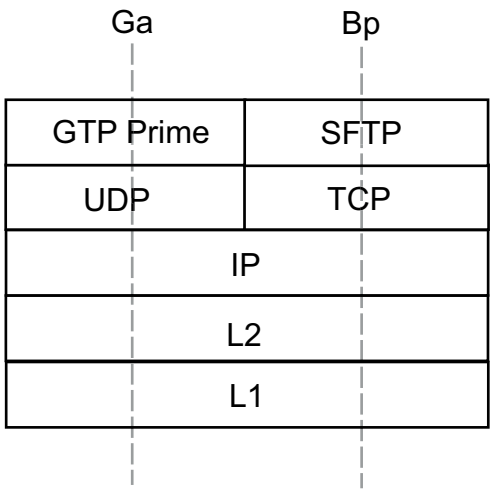

Figure 3 Interface Layers

3.1 SFTP

The EPG supports SFTP over the Bp interface (see Figure 3), to a CGF or BS, for retrieval of partial CDRs stored in the EPG charging data files. For compliance information, refer to SoC with 3GPP TS 32.297 (GGSN and PGW) and SoC with 3GPP TS 32.297 (SGW).

The following SFTP operations are supported by the EPG:

Operation	Definition
get remote-path [**local-path**]	Retrieve the remote file from **remote-path**.
ls [path]	Display the remote directory listing
pwd	Display the remote working directory
rm path	Delete the remote file
mkdir path	Create up to 10 subdirectories within a charging service[1]. The subdirectory name can be any valid Linux file system name with a maximum length of 256 characters. For example, `mkdir cdr/save`. • The subdirectory name must not conflict with an existing subdirectory name or an existing CDR file name.[2] • Only one level of subdirectory is allowed; a subdirectory cannot contain another subdirectory. For example, `mkdir cdr/save/test` is not allowed.

Operation	Definition
rmdir path	Remove an existing subdirectory as long as that subdirectory does not contain any CDR files. For example, `rmdir cdr/save`. • The command cannot be used to remove a CDR file, but only a subdirectory. • The top level charging service(1) cannot be removed. For example, `rmdir cdr` is not allowed.
rename old-path new-path	The **rename** command allows the following operations: • Renaming a CDR file in the same directory. To rename a CDR file in the same directory, use the lock extension. For example: **rename cdr/cdr_0000000001 cdr/cdr_0000000001 .lock** • Moving a CDR file from a subdirectory. For example: **rename cdr/cdr_0000000001 cdr/backup/cdr_000 0000001** The following restrictions apply to the **rename** command: • The top level charging service(1) cannot be renamed. For example, `rename cdr CDR` is not allowed. • The CDR file cannot be moved between charging services(1). For example, `rename cdr/cdr_0000000001 rfcdr/cdr_0000000001` is not allowed.

(1) Charging service here means the offline charging file directories predefined for EPG applications, such as `/var/opt/services/epg/cdr` or `/var/opt/services/epg/rfcdr`.
(2) If a subdirectory is created first and a CDR file of the same name is generated afterwards, that CDR file is allowed to be generated. When listing the file information using `ls`, the same name for both the subdirectory and the CDR file is displayed twice. To recover from this, simply use `rename` to rename the subdirectory to a different name.

3.2 GTP Prime

The GGSN and PGW support the GTP Prime charging protocol over the Ga interface (see Figure 3), to a CGF (CGF is used below when referring to the external GTP Prime node). GTP Prime version 0 (binary '000') is supported by the GGSN and PGW. Support for GTP Prime version 2 can be enabled. For instruction regarding the configuration of GTP Prime version support, see Offline Charging Configuration.

For compliance information, see SoC with 3GPP TS 32.295.

3.2.1 UDP/IP Port Usage

The ports for signalling request messages over the path protocol UDP/IP are as follows:

— The UDP Destination Port is the server port number 3386 which has been reserved for GTP Prime.

— The UDP Source Port is a locally allocated port number in the sending GGSN or PGW.

Note: Due to the EPG multi-core architecture, the EPG uses multiple UDP ports per PSC. Therefore, the CGF or BS must be prepared to accept and track data from several dynamic source ports for each GGSN and PGW IP address.

3.2.2 Message Format

In GTP Prime messaging, the signalling plane of GTP is partly reused. A GTP Prime message is sent within a GTP Prime Protocol Data Unit (PDU) which consists of a header and a payload part. The GTP Prime header is shown in Table 1.

Bit 5 of octet 1 of the GTP Prime header is the Protocol Type flag and is set to 0 if the protocol is GTP Prime.

The Version bits indicate the GTP Prime protocol version. The GGSN and PGW support GTP Prime version 0 (with both 6-byte and 20-byte headers) and version 2.

The Length indicates the length of payload (number of octets following the GTP Prime header).

The Sequence Number of the packet is part of the GTP Prime header.

Table 1 Six-Byte GTP Prime header

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Version			PT	Spare '111'			'0'
2	Message Type							
3-4	Length							
5-6	Sequence Number							

3.2.3 Message Types

GTP Prime defines a set of messages between two associated nodes. The GTP Prime messages defined are shown in Table 2 and Table 3.

Of signalling message types introduced by GTP Prime, `Node Alive Request`, `Node Alive Response`, `Redirection Request`, and `Redirection Response` belong to the Path Management messages, while the `Data Record Transfer Request` and `Data Record Transfer Response` belong to the Record Transmission messages.

Filled with 1s, the reserved fields in the signalling messages are intended for future use.

GTP Prime reuses the GTP Cause values. The GTP Prime messages inherited from the GTP protocol are shown in Table 2. The new messages introduced by GTP Prime are shown in Table 3.

The GGSN and PGW support all message types listed in Table 2 and Table 3.

Table 2 Message Types Inherited from the GTP Protocol

Message Type (Decimal)	GTP Prime message
1	Echo Request
2	Echo Response
3	Version not supported

Table 3 Message Types Introduced by GTP Prime

Message Type (Decimal)	GTP Prime message
4	Node Alive Request
5	Node Alive Response
6	Redirection Request
7	Redirection Response
240	Data Record Transfer Request
241	Data Record Transfer Response

The following sections describe the messages sent over the Ga interface, including the supported IEs and presence requirement in the EPG implementation.

3.2.3.1 Echo Request/Echo Response

The GTP Prime protocol implements path management similar to the GTP protocol. The format of the GTP Prime Echo Request and Echo Response messages are equal to the GTP Echo Request and Echo Response messages.

The Echo Request message element is defined in Table 4.

Table 4 Echo Request Message Element

Information Element	Presence Requirement
Private Extension	Not used, and is silently discarded if received

The Echo Response message element is defined in Table 5.

Table 5 Echo Response Message Element

Information Element	Presence Requirement
Recovery	Mandatory
Private Extension	Not used, and is silently discarded if received

On reception of an Echo Request message, the GGSN or PGW responds with an Echo Response message. The Recovery IE is always set to zero.

If GTP Prime path management is activated in the GGSN or PGW, Echo Request messages are periodically sent to currently available CGF nodes. If a CGF does not respond to Echo Request messages or any other messages sent by the GGSN or PGW, the GGSN or PGW declares the CGF unavailable. The GGSN or PGW considers such a CGF unavailable until it receives an Echo Response or Node Alive Request message from the CGF.

If a checkalive timer is configured, the GGSN or PGW periodically sends Echo Request messages to unavailable CGF nodes. By default, no Echo Requests are sent to an unavailable CGF. If no Echo Requests are sent, the GGSN or PGW cannot detect by itself when a failed communication path to a CGF has recovered. The CGF must, once it has recovered, send a Node Alive Request to the GGSN or PGW.

If the Ericsson Multi Mediation is used and a Ga link has been restored, the collector process of the affected Network Element (NE) can be stopped, drained, and started again to resume CDR transfer over GTP Prime.

3.2.3.2 Version Not Supported

Whenever the GGSN or PGW receives a Request message with a version that is not supported, the GGSN or PGW responds with a Version Not Supported message. This message contains only the GTP header and indicates the latest GTP version that the GGSN or PGW can support.

3.2.3.3 Node Alive Request

The Node Alive Request message is used to inform that a node in the network has started its service (for example after a service break due to software or hardware

maintenance or data service interruption after an error condition). A node may include a different IP address than its own in the Node Address IE, for example 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.

On reception of a Node Alive Request message from a CGF, the GGSN or PGW declares the CGF as available. If the newly available CGF is configured with a higher priority than the CGF currently receiving CDRs, future CDRs are redirected towards this CGF.

Whenever the GGSN or PGW receives a Node Alive Request message, it responds with a Node Alive Response message.

Upon start or restart of the EPG or a CPB running the PSC, a Node Alive Request message is sent to the preferred CGF. If the GGSN or PGW fails to receive a Node Alive Response, the CGF is declared unavailable and an alternative CGF is selected from the predefined list of CGFs to which the GGSN or PGW sends a Node Alive Request message.

The Node Alive Request message element is defined in Table 6.

Table 6 Node Alive Request

Information Element	Presence requirement
Node Address	Mandatory
Private Extension	Not used, and is silently discarded if received

3.2.3.4 Node Alive Response

The Node Alive Response message is sent by the GGSN, the PGW, and the CGFs as a response to a received Node Alive Request message. The Node Alive Response message element is defined in Table 7.

Table 7 Node Alive Response

Information Element	Presence requirement
Private Extension	Not used, and is silently discarded if received

3.2.3.5 Redirection Request

There are two kinds of usage for the Redirection Request message. One is to advise that CDR transfers are to be redirected to an alternative CGF due to that the CGF node is about to stop service (for example due maintenance or an error condition). The second purpose is to inform a CDR generating node (for example GGSN) that is currently transferring CDRs to this CGF, that the next node in the chain (for example a mediator device or Billing Computer) has lost connection to this node.

The Information Elements in a Redirection Request message includes a Cause element indicating the cause for the Redirection Request and an optional Address of Recommended Node element that provides an alternative CGF to be used.

On reception of a Redirection Request message, the GGSN or PGW redirects transfers of CDRs to the alternative CGF indicated in the Redirection Request message provided that an alternative CGF is included in the message and that any such alternative CGF is defined as valid CGF node in the GGSN or PGW. If no alternative CGF node is provided, or if the provided alternative CGF node is not defined as a valid CGF node in the GGSN or PGW, an alternative CGF node is selected from the predefined list of valid alternative CGF nodes.

On reception of a Redirection Request message, the GGSN or PGW declares the CGF node that sent the message unavailable until a Node Alive Request message is received, indicating that this node is once again operational. When the GGSN or PGW has declared a CGF node unavailable, redirection of CDR transfers towards such CGF does not occur.

Whenever the GGSN or PGW receives a Redirection Request message, it responds with a Redirection Response message.

The Redirection Request message element is defined in Table 8.

Table 8 Redirection Request

Information Element	**Presence requirement**
Cause	Mandatory
Address of Recommended Node	Optional
Private Extension	Not used, and is silently discarded if received

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

Note: The GGSN or PGW does not pay attention to the Cause value.

The Address of Recommended Node information element, shown in Table 9, defines the IPv4 format address that the CGF node is identified by in the GPRS/WCDMA network.

Table 9 Address of Recommended Node

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = 254 (Decimal)							
2-3	Length = 4 (Decimal)							
4-7	IPv4 Address							

3.2.3.6 Redirection Response

A Redirection Response message is sent by the GGSN and PGW as a response to a received Redirection Request message.

The Redirection Response message element is defined in Table 10.

Table 10 Redirection Response

Information Element	Presence requirement
Cause	Mandatory
Private Extension	Not used, and is silently discarded if received

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

3.2.3.7 Data Record Transfer Request

This message is used by the GGSN and PGW to transmit the CDR information to a CGF. The CDR information is placed in the Data Record Packet Information Element (IE).

The IEs in Data Record Transfer Request message are specified in Table 11.

Table 11 Data Record Transfer Request

Information Element	Presence requirement
Packet Transfer Command	Mandatory
Data Record Packet	Conditional
Private Extension	Not used, and is silently discarded if received

Packet Transfer Command IE

The value of the Packet Transfer Command, see Table 12, in its IE tells the nature of the message. The GGSN and PGW support the following command:

— Send Data Record Packet

Table 12 Packet Transfer Command

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = 126 (Decimal)							
2	Packet Transfer Command							

Data Record Packet IE

The Data Record Packet element may contain one or more CDRs (data records). This is illustrated in Table 13. 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.

Table 13 Data Record Packet

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = 252 (Decimal)							
2...3	Length							
4	Number of Data Records							
5	Data Record Format							
6...7	Data Record Format Version							
8...9	Length of Data Record 1							

10...n	Data Record 1
x...x+1	Length of Data Record N
x+2...y	Data Record N

The Data Record Format is ASN.1 (value 1).

The Data Record Format Version depends on the configured charging format:

— For version 97, 98, and 99, octets 6 and 7 are set to H'00 and H'01, respectively.

— For version 4, 5, 6, 7, 8, and 13, octets 6 and 7 indicate GTP Prime application, TS release and TS version as follows:

- Octet 6 is divided into two fields each with 4 bits. Bits 8-5 identify the GTP Prime application: charging (value 1). Bits 4-1 identify the release of the TS used to encode the CDR. Its value corresponds to the first digit of the TS version number. For example the value for version 4.1.0 would be 4.
- Octet 7 identifies the version of the TS used to encode the CDR. Its value corresponds to the second digit of the TS version number plus 1. For example the value for version 4.1.0 would be 2. In circumstances where the second digit is an alphabetical character, the corresponding ASCII value is taken, for example the value for version 4.b.0 would be 66 (ASCII(b)).

3.2.3.8 Data Record Transfer Response

A Data Record Transfer Response message is sent by the CGF as a response to one or more received Data Record Transfer Request messages. The information elements of this message are shown in Table 14.

Table 14 Data Record Transfer Response

Information Element	Presence Requirement
Cause	Mandatory
Request Responded	Mandatory
Private Extension	Not used, and is silently discarded if received

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/cancelled packets IE incorrect

The Requests Responded information element contains the IE Type, Length and the Sequence Numbers (each 2 octets) of the Data Record Transfer Requests, see Table 15.

Table 15 Request Responded Information Element

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = 253 (Decimal)							
2...3	Length							
4...5	Sequence Number 1							
n...n+1	Sequence Number 2							

The GGSN or PGW considers the Data Record Transfer Requests as successfully received by the CGF only if the cause is set to `Request Accepted` in the response.

4 File-Based CDR Transfer

This section describes file-based CDR transfer using the SFTP protocol over the Bp interface.

4.1 Standard CDR File Transfer using SFTP

Collection of CDRs from the CPB hard disks and transfer of CDRs to the BS is handled by SFTP over IP version 4 (IPv4). Only pull mode is available. It is recommended to delete the transferred files on the EPG after completion of the SFTP transfer.

Since the CDR files are in binary format, the SFTP transfer mode must be set to binary to avoid any potential damage to the CDR data.

A normal case is when the `SFTP-get` command is sent from the BS to the GGSN/PGW or SGW. The command contains a request for a specific CDR file. The GGSN/PGW or SGW then replies with the requested file, see Figure 4.

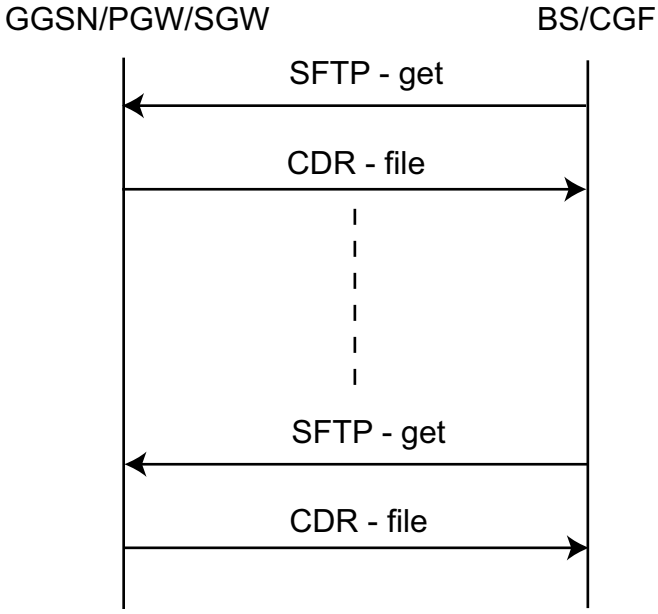

Figure 4 Standard CDR Transfer using SFTP

Charging data files are not automatically removed or overwritten; thus, the CGF or BS, having retrieved the files, is recommended to delete them from the GGSN/PGW or SGW.

4.2 CDR File Handling

Partial CDRs are first stored in a temporary file, which is closed and moved to a Control Processing Board (CPB) hard disk when either a maximum file size or file age is reached. However, if a configuration change affecting the GGSN/PGW or SGW has been committed, the temporary file might be closed and moved before the maximum file size or file age is reached. The charging data files are in binary format and contain the encoded CDRs with no delimiter in between.

Each charging data file is replicated to the hard disk of another CPB to ensure file redundancy in case of a CPB failure. Due to the distributed storage of CDR files, a central function in the node assigns unique and consecutive local record sequence numbers to each generated CDR. It also assigns unique sequence numbers, which, together with the configured GGSN/PGW or SGW node ID and the timestamp defining when the file is closed, are used to form the CDR file names.

Each CPB handles the charging data files independently. The sequence in which charging files are available on the disk does not necessarily follow the sequence number. For example, if a file with sequence number `100` includes many CDRs and another file with sequence number `101` includes few CDRs, the latter one requires less time to fill in the local record sequence numbers for the CDRs in the file and close it. This means that there is a temporary gap in the file sequence numbering on the disk.

All charging data files are linked to a virtual tree on the Node Management Board (NMB) that makes charging data files visible to operators that are allowed to access them. The charging data files can be removed from the EPG by an operator-command after retrieval. Both copies existing in the EPG are then removed. All charging data files are automatically compressed when stored on the CPB hard disk. If compression is not configured, the files are decompressed on the fly when they are retrieved.

Note: To decompress the files on the BS or CGF, it is recommended to use Unix native decompression method, since other tools may cause file corruption.

The path for the target directory on the NMB is `/var/opt/services/epg/cdr`.

The charging data file directories are restricted to users with the correct service roles assigned to their user account. For information on configuration of service roles and user accounts, see Security Management.

The following naming convention is used for the charging data files:

<nodeid>_<yyymmddhhmmss>_<sequence>

Where:

— **<nodeid>** is the configurable node identifier (for example `RM01GGSN`).

— **<yyyymmddhhmmss>** represents date and time of the file closing.

— **<sequence>** A progressive integer generated by a central function in the node (range [1–65535]). This sequence number wraps around when 65535 has been reached. The sequence number integrity is assured across system restarts, such as reload, NMB switchover, graceful restart, or a local board restart, but may be broken following a software upgrade or if the system fails.

An alarm is issued when the hard disk usage exceeds 80%. It is then recommended to start retrieving charging data files from the node. A PSC or SSC refuses to open a new charging data file if there is not enough free space on the charging partition of the CPB hard disk. When there is no temporary file available to write to, CDRs pend in output queues. It is then recommended to retrieve as many files as possible from the node. When hard disk usage is below 70%, the alarm is cleared. Whether there is enough space to open a file depends on the configuration of the charging data file parameter `maximumSize`. For more information, see Offline Charging Configuration.

If the hard disks are full or if the charging partition on the file system on a CPB is filled or unavailable, the PSC or SSC is able to temporarily store CDRs in output queues. If an output queue utilization reaches 75%, the PSC or SSC does not accept any new bearers and raises an alarm indicating that the queue is almost full. If the output queue utilization reaches 100%, the PSC or SSC discards new CDRs and raises an alarm indicating that the queue is full. When the rejection of new bearers is detected, it is recommended to check the disk usage of the CPBs by issuing the **`show disk card all | grep /disk`** or **`show rfm disk-usage`** command.

The charging partitions on the CPB hard disks are not circular, meaning that the charging files cannot be overwritten.

5 Near Real-Time CDR Transfer for the GGSN/PGW

This section describes near real-time CDR transfer using the GTP Prime protocol over the Ga interface.

When using near real-time CDR transfer, CDRs are transferred from each PSC to the CGF over GTP Prime in near real-time after CDR closure. GTP Prime supports UDP-over-IPv4 transmission.

5.1 Signalling

When the GTP Prime option is used, CDRs are transferred from the GGSN and PGW to the CGF using the GTP Prime protocol. GTP Prime offers reliable transfer

of CDRs using sequence numbers, retransmission, node alive detection and mechanisms for redirection of a CDR transfer to standby redundant CGFs. This section describes the mechanisms of this protocol as implemented in the GGSN and PGW.

Collection, Storage, and Transfer of CDRs

The generated partial CDRs are stored in an open GTP Prime PDU at the GGSN or PGW. The PDU contains the encoded CDRs as payload. The PDU is closed and sent towards a CGF as part of the Data Record Transfer Request message when either a maximum size or maximum age is reached.

One or more CGFs may be defined for redundancy reasons. If the primary CGF is unavailable, the GGSN or PGW chooses another predefined CGF to which it redirects its CDRs. If all configured CGFs are unavailable and saving to file at failure is activated, the GGSN or PGW stores CDRs destined for GTP Prime in a GTP Prime charging data file. The GTP Prime charging data file must be fetched from the EPG using SFTP, as described in Section 4.1 on page 15.

The GTP Prime charging data file parameters are shared with the ordinary charging data file. The path for its target directory is `/var/opt/services/epg/gtppcdr`.

CDR Transfer - Normal Case

This section describes a normal transfer of CDRs from the GGSN or PGW to a CGF.

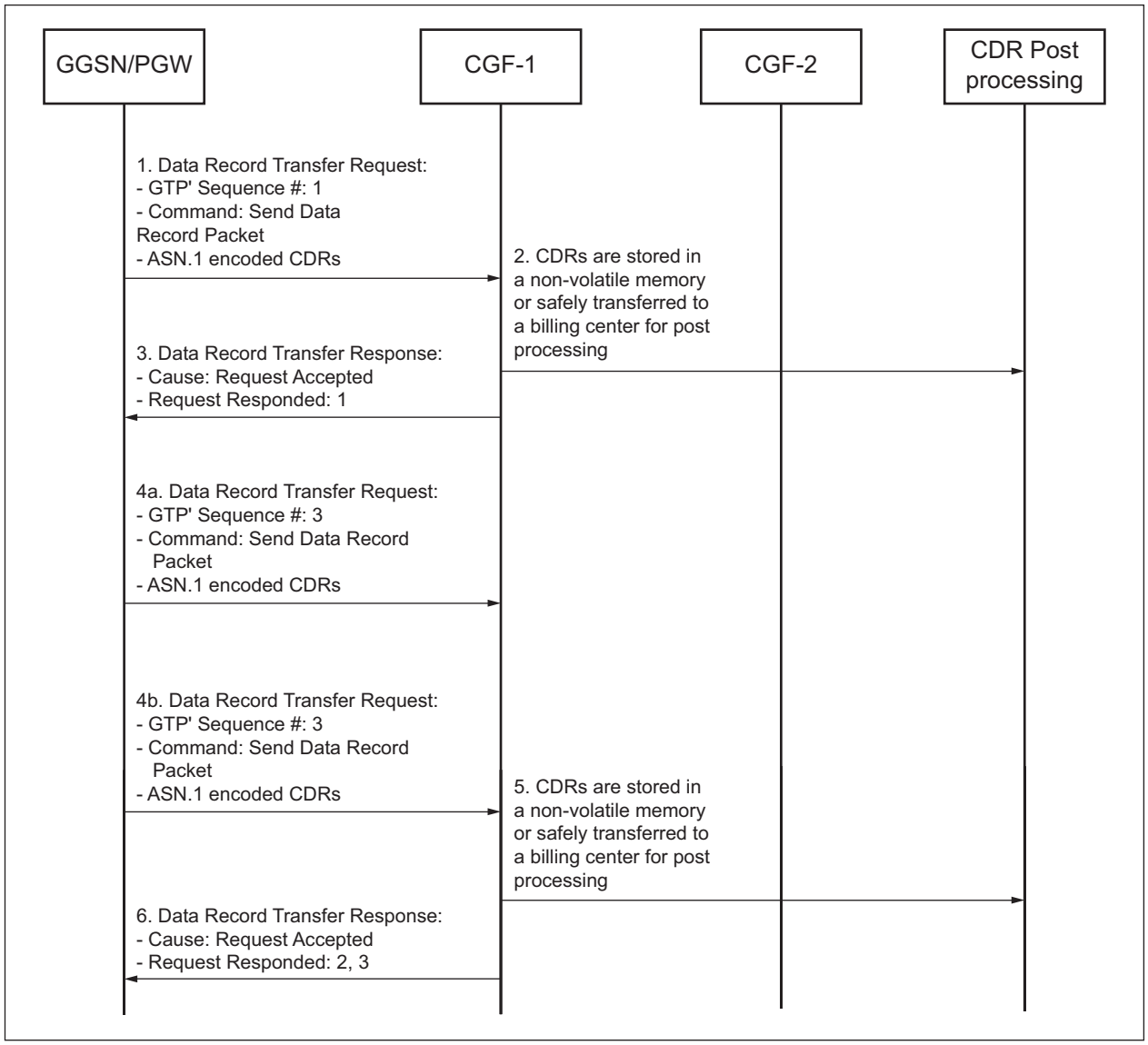

Figure 5 CDR Transfer — Normal case

1. The GGSN or PGW transfers the CDRs to the highest prioritized available CGF in the list of valid CGFs using GTP Prime, in this example CGF-1 is the preferred CGF. The message used is `Data Record Transfer Request` and the command is `Send Data Record Packet`. A sequence number for the message is provided in the GTP Prime header. The CDRs remain in the GGSN or PGW, and are not deleted until the successful reception of the CDRs has been acknowledged by the CGF.

2. The CGF stores the CDRs in a non volatile memory or safely sends them to a BS before acknowledging successful reception.

3. The CGF acknowledges the successful reception of the CDRs using the GTP Prime message `Data Record Transfer Response` with the cause code `Request Accepted` also providing the sequence number of the request for

which the acknowledgement refers to. After the GGSN or PGW has received a positive acknowledgement, the CDRs related to the acknowledgement are deleted automatically.

4. Several `Data Record Transfer Request` messages may be sent in sequence prior to acknowledgement.

5. The CGF stores the CDRs in a non-volatile memory or safely sends them to a BS before acknowledging successful reception.

6. The CGF acknowledges the successful reception of the CDRs received in multiple `Data Record Transfer Request` messages using the GTP Prime message `Data Record Transfer Response` with the cause code `Request Accepted` also providing all the sequence number of the requests for which the acknowledgement refers to. After the GGSN or PGW has received a positive acknowledgement, the CDRs related to the acknowledgement are deleted.

CDR Transfer - CGF failure

This section describes a CDR transfer session from a GGSN or PGW to a CGF in which the connection to the primary CGF is broken in the middle of the transfer and a backup CGF is used instead. CGF-1 is in this example the primary CGF and CGF-2 is the backup.

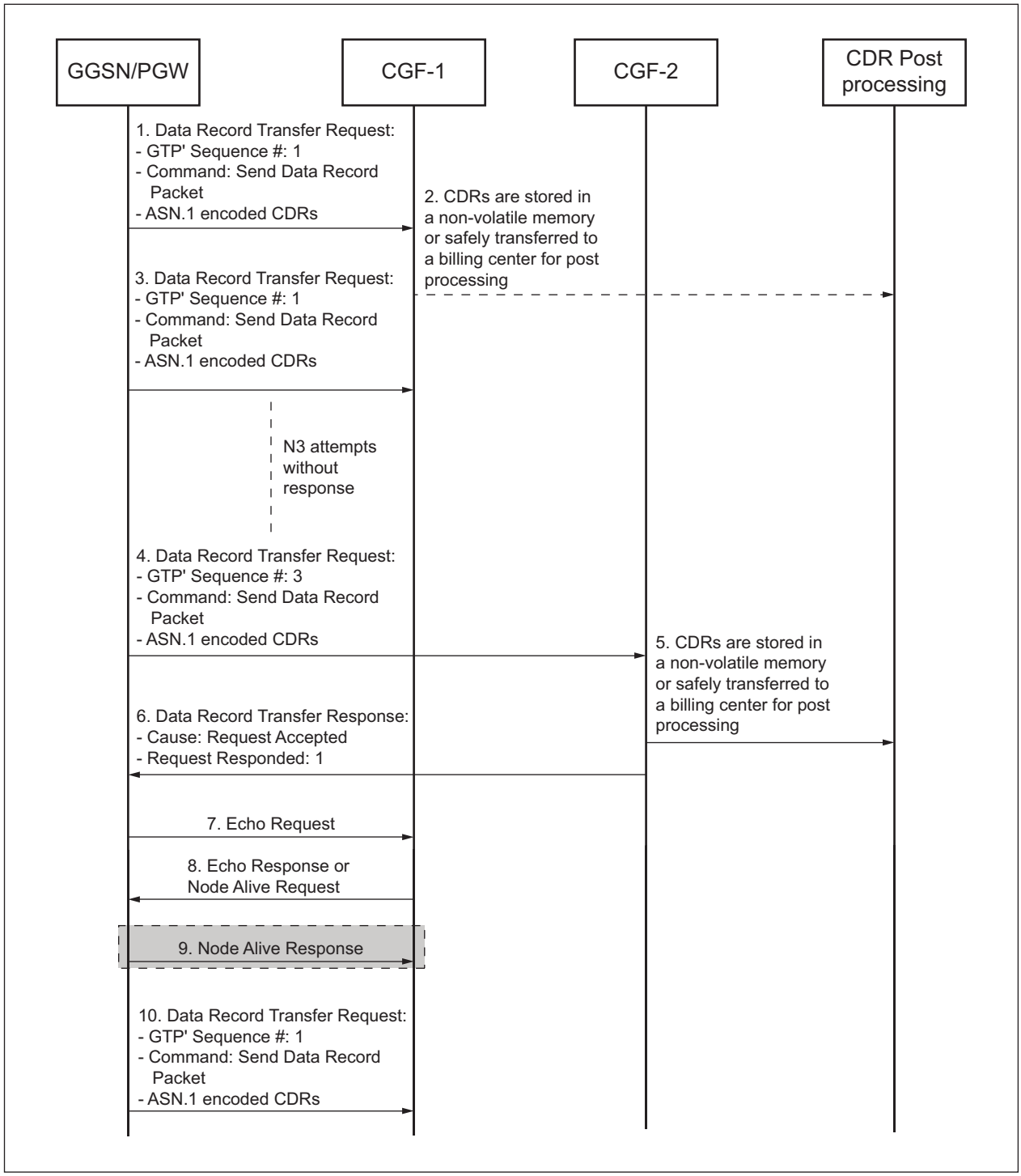

Figure 6 CDR Transfer — CGF failure

1. The GGSN or PGW transfers the CDRs to the highest prioritized operational CGF in the list of valid CGFs using GTP Prime. In this example CGF-1 is the preferred CGF. The message used is `Data Record Transfer Request` and the command is `Send Data Record Packet`. The sequence number for the

message is provided in the GTP Prime header. The CDRs remain in the GGSN or PGW and are not deleted until the successful reception of the CDRs is acknowledged by the CGF.

2. CGF-1 stores the CDRs in a non-volatile memory or sends them safely to a BS before acknowledging successful reception.

CGF-1 breaks or loses network connectivity.

3. After the T3 timer expires (default 20 seconds), the GGSN or PGW retries sending the `Data Record Transfer Request` message to CGF-1.

4. After having made n3 retries (default 5 attempts), CGF-1 is declared non-operational and a new CGF, namely, CGF-2, is picked from the list of CGFs. The GGSN or PGW transfers the CDRs to CGF-2. The CDRs remain in the GGSN or PGW, and are not deleted until the CGF acknowledges the successful reception of the CDRs.

5. CGF-2 stores the CDRs in a non-volatile memory or sends them safely to a BS before acknowledging successful reception.

   Note: This may potentially result in duplicate CDRs in the BS if CGF-1 sent the same CDRs to the BS before it broke. Therefore, post processing must be implemented in the BS to identify and resolve cases with duplicate CDRs.

6. CGF-2 acknowledges the successful reception of the CDRs using the GTP Prime message `Data Record Transfer Response` with the cause code `Request Accepted`, also providing the sequence number of the request to which the acknowledgement refers to. After the GGSN or PGW receives a positive acknowledgement, the CDRs related to the acknowledgement are deleted.

7. If GTP Prime path management is activated and a checkalive timer is configured, the GGSN or PGW periodically sends `Echo Request` messages to CGF-1.

CGF-1 regains operation.

8. CGF-1 responds with an `Echo Response` message or sends a `Node Alive Request` message to the GGSN or PGW.

9. The GGSN or PGW declares CGF-1 available and stops periodically sending `Echo Request` messages to CGF-1, and responds with a `Node Alive Response` message if it received a `Node Alive Request` message.

10. Further CDR transfers are now directed to CGF-1.

The following events cause the GGSN and PGW to consider a CGF unavailable:

— If GTP Prime path management is activated, and the CGF fails to respond to an `Echo Request` message.

— If the CGF fails to respond to a `Node Alive Request` message.

— If the CGF sends a `Redirection Request` message.

— If the CGF fails to respond to a `Data Record Transfer Request` message.

The GGSN and PGW consider a currently unavailable CGF as available for the following reasons:

— If the CGF responds to a `Node Alive Request` message.

— If the CGF sends a `Node Alive Request` message.

— If the CGF responds to an `Echo Request` message.