ETSI TS 132 295 V14.0.0 (2017-04)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Telecommunication management;
Charging management;
Charging Data Record (CDR) transfer
(3GPP TS 32.295 version 14.0.0 Release 14)

Reference
RTS/TSGS-0532295ve00

Keywords
GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document is part of a series of Technical Specifications (TSs) that specify charging functionality and charging management in 3GPP networks (GSM/UMTS/EPS). The 3GPP core network charging architecture and principles are specified in TS 32.240 [1], which provides an umbrella for other charging management TSs that specify:

- the content of the CDRs per domain / subsystem / service (offline charging);
- the content of real-time charging messages per domain / subsystem / service (online charging);
- the functionality of online and offline charging for those domains / subsystems / services;
- the interfaces that are used in the charging framework to transfer the charging information (i.e. CDRs or charging events)

The complete document structure for these TSs is defined in TS 32.240 [1].

The present document specifies the transaction based mechanism for the near real time transfer of CDRs within the network.

The present document is related to other 3GPP charging TSs as follows:

- The common 3GPP charging architecture is specified in TS 32.240 [1];
- The parameters, abstract syntax and encoding rules for the CDRs are specified in TS 32.298 [51];
- The file based mechanism used to transfer the CDRs from the network to the operator's Billing Domain (e.g. the post-processing system or a mediation device) is specified in TS 32.297 [52];

The 3GPP Diameter application that is used for offline and online charging is specified in TS 32.299 [50].

All terms, definitions and abbreviations used in the present document, that are common across 3GPP TSs, are defined in the 3GPP Vocabulary, TR 21.905 [100]. Those that are common across charging management in 3GPP domains services, or subsystems are provided in the umbrella document TS 32.240 [1] and are copied into clause 3 of the present document for ease of reading. Finally, those items that are specific to the present document are defined exclusively in the present document.

Furthermore, requirements that govern the charging work are specified in TS 22.115 [101].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[2] - [9] Void.

[10] 3GPP TS 32.250: "Telecommunication management; Charging management; Circuit Switched (CS) domain charging".

[11] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[12] - [29] Void.

[30] 3GPP TS 32.270: "Telecommunication management; Charging management; Multimedia Messaging Service (MMS) charging".

[31] - [49] Void.

[50] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging application".

[51] 3GPP TS 32.298: "Telecommunication management; Charging management; Charging Data Record (CDR) parameter description".

[52] 3GPP TS 32.297: "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer".

[53] - [99] Void.

[100] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[101] 3GPP TS 22.115: "Service aspects; Charging and billing".

[102] - [199] Void.

[200] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[201] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[202] - [299] Void.

[300] - [399] Void.

[400] - [403] Void.

[404] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[405] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[406] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[407] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in TR 21.905 [50], TS 32.240 [1], and the following apply:

2G- / 3G-: prefixes 2G- and 3G- refers to functionality that supports only GSM or UMTS, respectively, e.g. 2G-CDF refers only to the GSM functionality of an CDF.

accounting: process of apportioning charges between the Home Environment, Serving Network and User.

billing: function whereby CDRs generated by the charging function are transformed into bills requiring payment.

Billing Domain: Part of the operator network, which is outside the core network, that receives and processes CDR files from the core network charging functions. It includes functions that can provide billing mediation and billing other (e.g. statistical) end applications. It is only applicable to offline charging (see "Online Charging System" for equivalent functionality in online charging).

chargeable event: activity utilizing telecommunications network infrastructure and related services for:

- user to user communication (e.g. a single call, a data communication session or a short message); or
- user to network communication (e.g. service profile administration); or
- inter-network communication (e.g. transferring calls, signalling, or short messages); or
- mobility (e.g. roaming or inter-system handover); and
- that the network operator wants to charge for.

charged party: user involved in a chargeable event who has to pay parts or the whole charges of the chargeable event, or a third party paying the charges caused by one or all users involved in the chargeable event, or a network operator.

charging: function whereby information related to a chargeable event is formatted and transferred in order to make it possible to determine usage for which the charged party may be billed.

Charging Data Record (CDR): A formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the call, amount of data transferred, etc) for use in billing and accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR shall be generated, i.e. more than one CDR may be generated for a single chargeable event, e.g. because of its long duration, or because more than one charged party is to be charged.

charging function: entity inside the core network domain, subsystem or service that is involved in charging for that domain, subsystem or service.

circuit switched domain: domain within GSM / UMTS in which information is transferred in circuit mode.

domain: part of a communication network that provides services using a certain technology.

GPRS: Packet Services for GSM and UMTS systems.

GTP': GPRS protocol, used for CDR transport. It is derived from GTP with enhancements to improve transport reliability necessary for CDRs. NOTE:This protocol is not used for tunnelling.

GSM only: qualifier indicating that this clause or paragraph applies only to a GSM system. For multi-system cases this is determined by the current serving radio access network.

inter-system change: change of radio access between different radio access technologies such as GSM and UMTS.

in GSM,...: qualifier indicating that this paragraph applies only to GSM System.

in UMTS,...: qualifier indicating that this paragraph applies only to UMTS System.

middle tier TS: used for the 3GPP charging TSs that specify the domain / subsystem / service specific, online and offline, charging functionality. These are all the TSs in the numbering range from TS 32.250 [10] to TS 32.27x [3x], e.g. TS 32.250 [10] for the CS domain, or TS 32.270 [30] for the MMS service. Currently, there is only one "tier 1" TS in 3GPP, which is the TS 32.240 [1] that specifies the charging architecture and principles. Finally, there are a number of top tier TSs in the 32.29x numbering range ([50] ff) that specify common charging aspects such as parameter definitions, encoding rules, the common BD interface or common charging applications.

near real time: near real time charging and billing information is to be generated, processed, and transported to a desired conclusion in less than one (1) minute.

observed IMEI ticket: record used to describe an EIR relevant event e.g. a blacklisted IMEI.

offline charging: charging mechanism where charging information **does not** affect, in real-time, the service rendered.

online charging: charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with session/service control is required.

Online Charging System: the entity that performs real-time credit control. Its functionality includes transaction handling, rating, online correlation and management of subscriber accounts/balances.

packet switched domain: domain in which data is transferred between core network elements.

Real-time: real time charging and billing information is to be generated, processed, and transported to a desired conclusion in less than 1 second.

subscriber: A subscriber is an entity (associated with one or more users) that is engaged in a Subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorized to enjoy these services, and also to set the limits relative to the use that associated users make of these services.

UMTS only: qualifier indicating that this clause or paragraph applies only to a UMTS system. For multi-system cases this is determined by the current serving radio access network.

user: An entity, not part of the 3GPP System, that uses network resources by means of a subscription. The user may or may not be identical to the subscriber holding that subscription.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Bx	The reference point between any (generic) 3G domain, subsystem or service CGF and the BD.
Ga	Reference point between a CDF and the CGF for CDR transfer.
Rf	Reference Point between the CTF within a 3G network element and the CDF for offline charging.

3.3 Abbreviations

For the purposes of the present document, the abbreviations defined in TR 21.905 [50] and the following abbreviations apply:

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AS	Application Server
ASN.1	Abstract Syntax Notation One
BD	Billing Domain
CDF	Charging Data Function
CDR	Charging Data Record
CG	Charging Gateway
CGF	Charging Gateway Function
CS	Circuit Switched
DRP	Data Record Packet
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
GTPv2-C	GTP version 2 – Control Plane
GTP'	GPRS protocol, used for CDR transport
IE	Information Element
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NE	Network Element
OAM&P	Operation, Administration, Maintenance and Provisioning
OCS	Online Charging System
PDN	Packet Data Network
PS	Packet-Switched
PT	Protocol Type (Field in GTP' header)
S-SMO-CDR	SGSN Short Message Mobile Originated - CDR
TAP	Transferred Account Procedure
TLV	Type, Length, Value (GTP header format)
TV	Type, Value

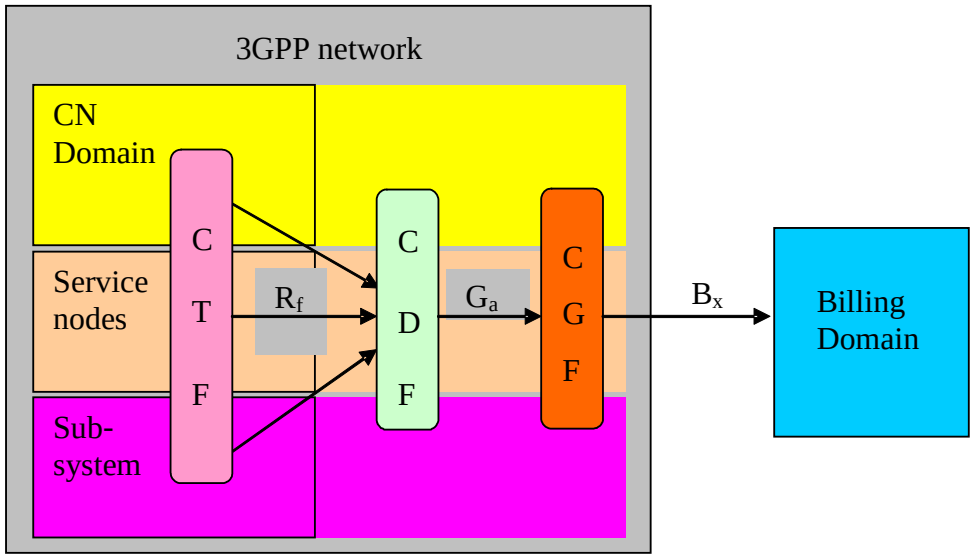
4 Architecture considerations

4.1 High level architecture

The Ga is the reference point from the Charging Data Function (CDF) to the Charging Gateway Function (CGF), which is intended for the transport of Charging Data Records (CDRs).

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

Figure 4.1.1 depicts the position of the Ga reference point within the overall 3GPP offline charging architecture.



CTF: **C**harging **T**rigger **F**unction
CDF: **C**harging **D**ata **F**unction
CGF: **C**harging **G**ateway **F**unction
BD: **B**illing **D**omain. This may also be a billing mediation device / post-processing system.

Figure 4.1.1: Logical ubiquitous offline charging architecture

As illustrated in figure 4.1.1, 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. Further details of the configuration refer to TS 32.240 [1]. Details of the implementation options per domain / subsystem / service (usually a subset of the overall possible variants described above) are specified in the respective middle tier TS, e.g. for EPC Charging in TS 32.251 [11].

The transport protocol associated to the Ga reference point, providing functions for transfer of CDRs from CDF to CGF, is GTP' (because of its derivation from the GTP protocol as specified in TS 29.060 [200]).

5 Transfer principles and scenarios

5.1 Transfer principles

5.1.0 General

The GTP' protocol is optional, and is used for CDR transport between the CDFs and the CGF.

5.1.1 Charging related transfer requirements

Each CDF has an OAM&P configurable address list of CGFs (Charging Gateways) to which it can send its CDRs. The list is organized in CGF address priority order. If the primary CGF is not available (e.g. out of service), then the CDF shall send the CDRs to the secondary CGF and so on.

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

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

5.1.2 CDR transport by GTP'

GTP' has been designed to deliver the CDR(s) from the CDF, which generates CDRs to the CGF(s). This protocol is required if the CGF resides outside the CDFs. It utilizes some aspects of GTP (defined in TS 29.060 [200]), which is used for packet data tunnelling in the backbone network.

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

GTP' performs the following functions:

- CDR transfer between the CDF and the CGF.
- Redirection of CDRs to another CGF.
- Detect communication failures between the communicating peers, using echo messaging.
- Advertise to peers about its CDR transfer capability (e.g., 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 GTP' messaging).

5.1.2.1 CDF - CGF communication

As illustrated in figure 5.1.2.1.1, the CDF - CGF communications are carried out using GTP' over UDP/TCP and IP.

Figure 5.1.2.1.1: Protocol layers e CDF and tl

5.1.2.2 CGF - CGF communication

If necessary, CGF to CGF communications are carried out usi er UDP/TCP an
This is illustrated in figure 5.1.2.2.1.

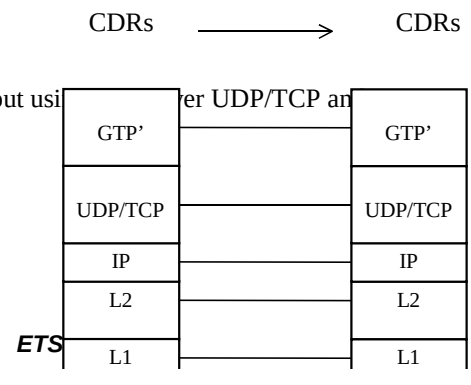
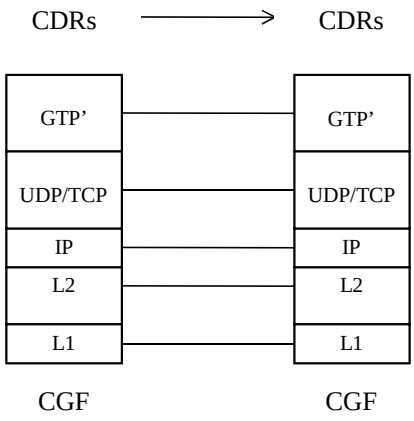


Figure 5.1.2.2.1: Protoc ween CGF



5.1.3 Port usage

Transporting the CDRs from the CDFs to the CGF over the Ga reference point may facilitate charging.
The Path Protocol may be UDP (compliant with STD 0006 [404]) or TCP (compliant with STD 0007 [405]) over IP.

- UDP as the Path Protocol

  Ports for signalling the request messages:

  - The UDP Destination Port may be the server port number 3386 which has been reserved for GTP'. Alternatively another port can be used, which has been configured by OAM&P, except Port Number 2123 which is used by GTPv2-C.
  - The UDP Source Port is a locally allocated port number at the sending network element.

  NOTE: UDP Source Port number should be different than UDP Source Port number allocated to GTPv2 (see TS 29.274 [201]).

  Ports for signalling the response messages:

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

- TCP as 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 OAM&P. Extra implementation-specific destination ports are possible but all CGFs shall support the server port number.

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

- Network layer and lower layers

  Beneath the Path Protocol there is the network IP layer, which shall be the Internet Protocol (IP) compliant with STD 0005 (see [406] and [407]). Beneath the network IP layer are the L2 and L1 layers, which are not specified, in the present document.

5.2 GTP' transfer scenarios

5.2.1 Basic principles

Each function (i.e. CDF and CGF) that supports the GTP' shall be capable of handling or responding with a "*Service/Version not supported*" message if that function is configured to be addressed by another peer function.

5.2.2 GTP' messaging cases

5.2.2.0 General

The following example cases represent the three different key "*Data Record Transfer Request/Response"* messaging related CDR handling schemes. Cases (2) and (3) represent situations involving the redundancy mechanism.

(1) The normal CDR packet transfer:

The CDF sends successfully a CDR packet to the CGF, and since the CDF gets a response (Request Accepted) for the Data Record Transfer Request, there is no need to use the CGF redundancy mechanism and redirect the CDR packet traffic flow to another CGF.

(2) The CDF-CGF connection breaks before a successful CDR reception:

In this case the CDR packet sent by the CDF is lost before it is received by the CGF. (The loss might be caused by a link failure or e.g. a major CGF failure.)

(3) The CDF-CGF connection breaks after a successful CDR reception:

In this case the CDR sent by the CDF is received correctly by the CGF and moved to its non-volatile memory (or even to the next NE in the communication chain). Anyhow, the CDF-CGF communication stops working, in this example case, before the CDF gets the positive response (Data Record Transfer Response: Request Accepted) which would acknowledge that the CDR packet was successfully received by CGF.

(4) CGF redundancy mechanism

An overview on the mechanism, involved in cases (2) and (3), preventing duplicated CDR packets to enter a BD.

The next four clauses describe in more detail each of these key "*Data Record Transfer Request / Response*" messaging schemes.

5.2.2.1 The normal CDR packet transfer

Figure 5.2.2.1.1 shows the default mode of CDR transfer from the CDR generating functions (CDFs) to the CDR collecting functions (CGFs).

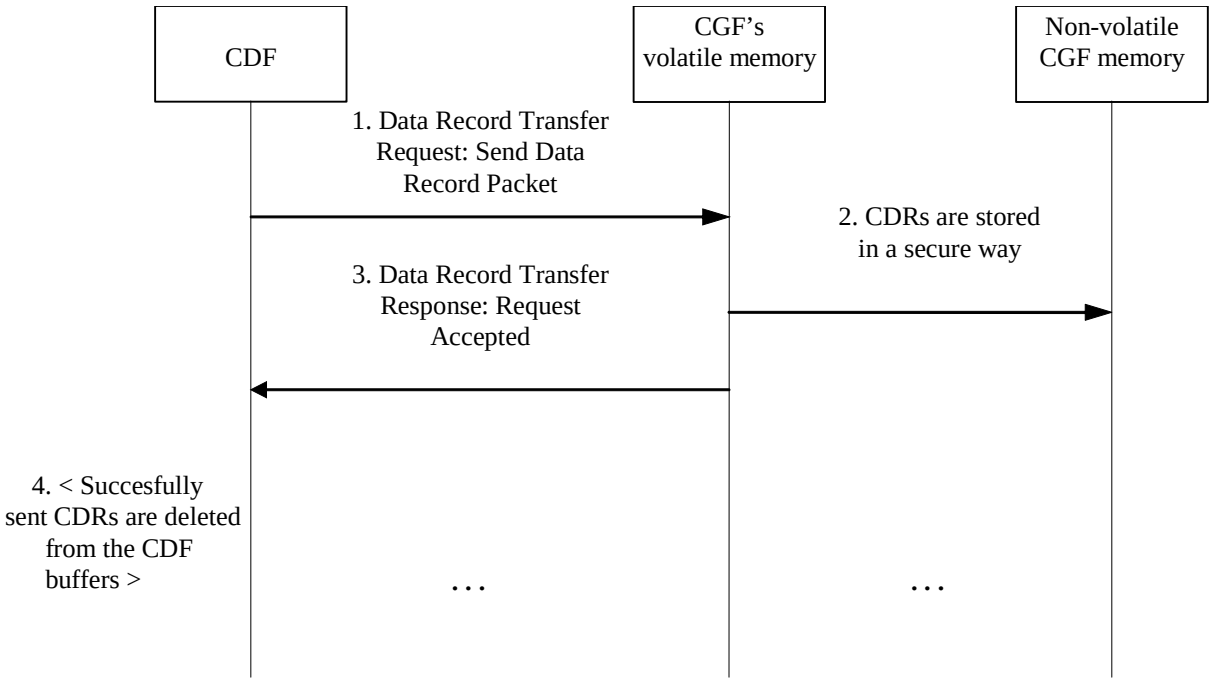


Figure 5.2.2.1.1: Normal CDR transfer process between a CDF and CGF

1) The CDR generating entity sends CDR(s) in a packet to CGF (that is the current primary Charging Gateway Functionality for the specific CDF, "CGF1"). The sending is performed by using the Data Record Transfer Request message, with the *Packet Transfer Command* IE having the value "Send Data Record Packet".

2) The CGF opens the received message and stores the packet contents in a safe way (to e.g. a redundant RAM memory unit or a mirrored non-volatile memory or even to another node).

3) The CDR receiving entity (CGF) sends confirmation of the successful packet reception to the CDF. The confirmation is performed by using the *Data Record Transfer Response* message, with the **Cause** value being "Request Accepted".

4) After the positive response "Request Accepted" is received by the CDF, it may delete the successfully sent CDRs from its send buffer.

The general principle of GTP' to retransmit the request if the response has not been received within a configurable time-out limit, is also followed here in point 1). The maximum amount of retries is a configurable value.

5.2.2.2 The CDF-CGF connection breaks before a successful CDR reception

Figure 5.2.2.2.1 shows the exceptional case when the CDR transfer from a CDR generating entity (CDF) to the primary CDR packet collecting entity (CGF1) fails in a way that the CGF1 is not able to store the CDR packet sent by the CDF. (The reason for the failure in packet transfer may be e.g. a link failure between the CDF and CGF1, or a capacity exhausting error in the storage device of CGF1, or a general CGF1 system failure or CGF1 maintenance break.)

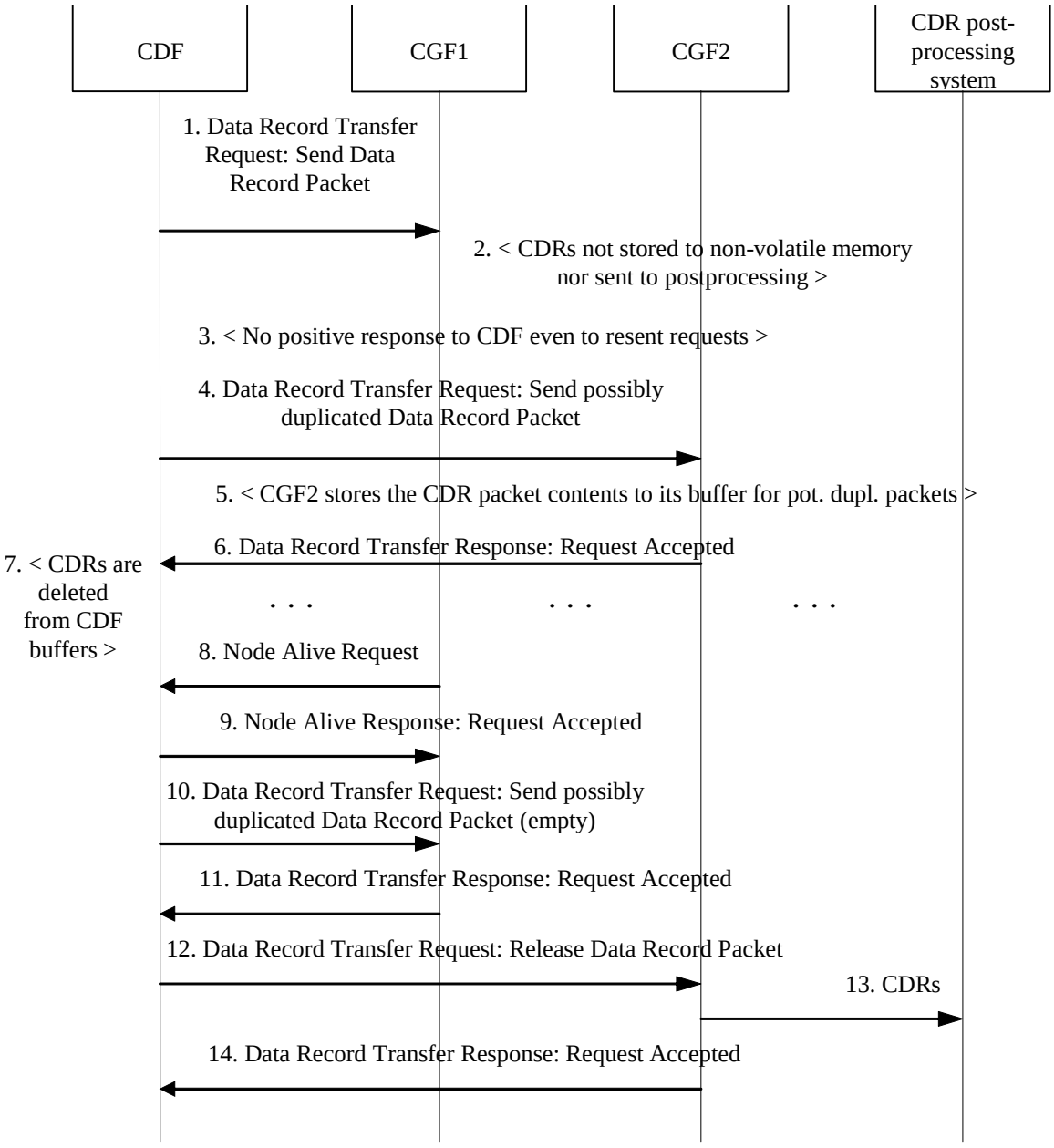


Figure 5.2.2.2.1: Duplicate prevention case: CDR sending via CGF1 had not succeeded

1) The CDR generating entity (CDF) sends CDR(s) in a packet to CGF (that is, the current primary CGF for the specific CDF, "CGF1"). The sending is performed by using the *Data Record Transfer Request* message, with the *Packet Transfer Command* IE having the value "Send Data Record Packet".

2) Due to a failure in the CDF-CGF1 communication link of CGF1, the CGF1 is not able to store the packet sent by the CDF in a safe way (to e.g. a redundant RAM memory unit or a mirrored non-volatile memory or to another node).

3) Therefore the CDF is not able to get a response (or it could alternatively get a negative response like "No resources available" as the **Cause** value in the *Data Record Transfer Response* message).

4) The CDF may now first test the CDF-CGF2 link by an Echo Request message that the CGF2 would respond by the Echo Response.) Then, the CDF sends the same CDR packet that could not be sent to CGF1 to the next CGF in its CGF preference list (here CGF2) using the *Data Record Transfer Request* message, with the *Packet Transfer Command* IE having the value "Send possible duplicated Data Record Packet".

5) As the connection to the CGF2 is working, the CGF2 is able to process the CDR packet. Since the packet was marked by the sending CDF to be potentially duplicated, it is stored into the CGF2, but not yet sent forward towards the BD.

6) The CGF2 sends confirmation of the successful packet reception to the CDF. The confirmation is performed by using the *Data Record Transfer Response* message, with the **Cause** value being "Request Accepted"

7) The CDF can now delete the now successfully sent (potentially duplicated) CDRs from its CDR buffer (but it keeps the sequence number(s) of the sent potentially duplicated packet(s) in a buffer dedicated for that.

8) When CGF1 is recovering after a system reboot, it sends a *Node Alive Request* message to the configured peer CDF(s), and so the CDF notices that it can again successfully communicate with the CGF1. (The CDF may also detect this by using the *Echo Request* messages, which would be answered by CGF1 by the *Echo Response* message.)

9) CDF acknowledges the CGF1 by *Node Alive Response* message.

10) For the earlier unacknowledged *Data Record Transfer Request* message(s), the CDF sends CGF1 empty test packet(s) (with no CDR payload in the Data Record Packet IE but just the other parts of the message frame).

11) CGF1 responds with *Data Record Transfer Response* message, with the **Cause** value being "Request Accepted", because in this example case CGF1 had lost the communication capability towards CDF before storing the previously received (and by CGF1 unacknowledged) CDR packet.

12) Now CDF knows that the CGF1 had not originally been able to process and forward the original version of the CDR packet from the CDF, and it indicates CGF2 that CGF2 can send the CDR packet(s) related to the previously unacknowledged GTP' *Sequence Number*(s) to post-processing. Those packets' *Sequence Numbers* are indicated in the *Sequence Numbers of the Released Packets* IE.

13) CGF2 shall now be able to send the released records towards the post-processing system.

14) CGF2 responds with *Data Record Transfer Response* message, with the **Cause** value being 'Request Accepted'.

After all the potentially duplicated packets are cleared from CGF(s), the CDF can continue in normal way the transfer of CDRs.

5.2.2.3 The CDF-CGF connection breaks after a successful CDR reception

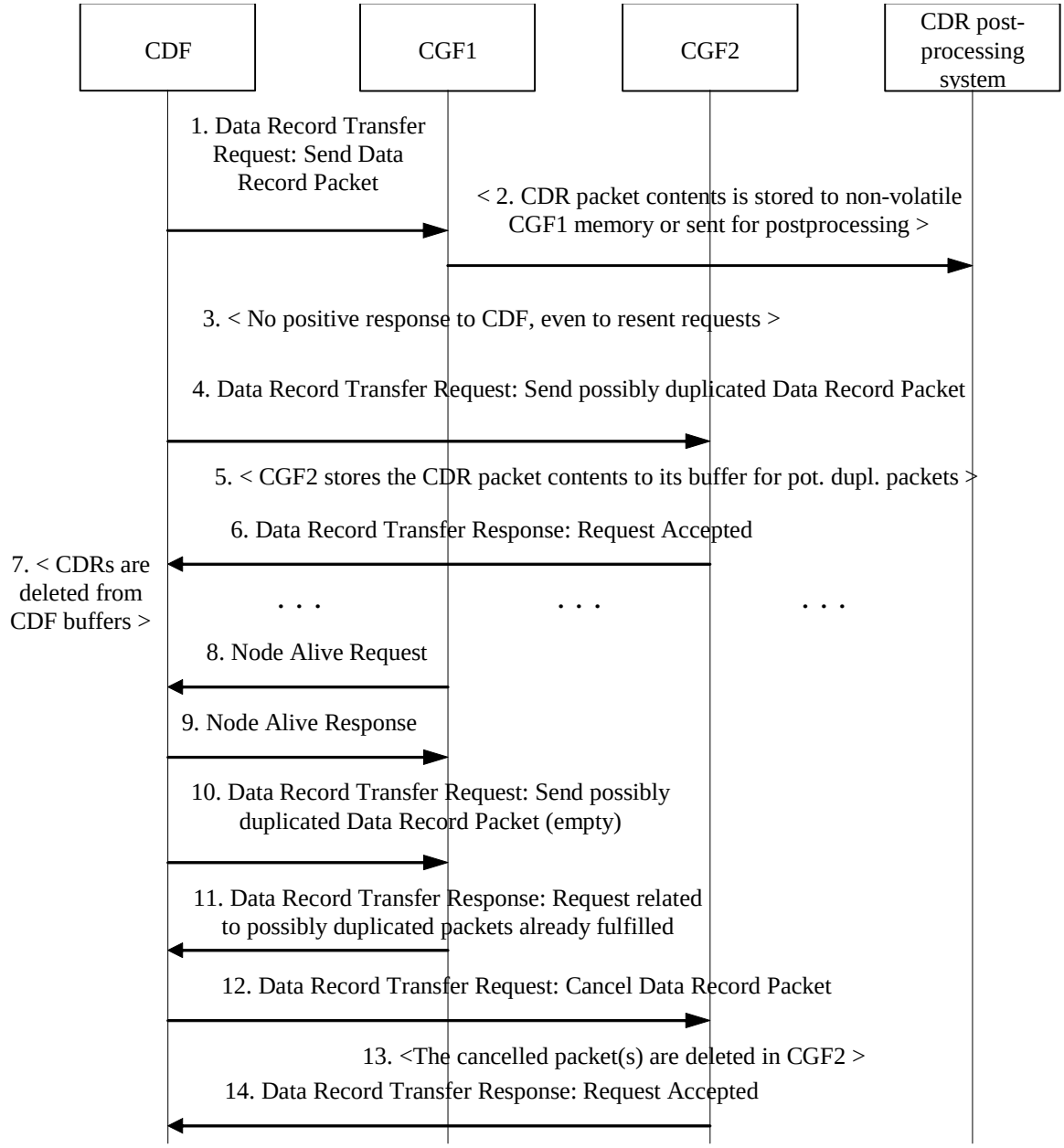


Figure 5.2.2.3.1: Duplicate prevention case: CDR sending via CGF1 had succeeded

1) The CDR generating entity (CDF) sends CDR(s) in a packet to CGF (that is the current primary Charging Gateway Functionality for the specific CDF, "CGF1"). The sending is performed by using the *Data Record Transfer Request* message, with the *Packet Transfer Command* IE having the value "Send Data Record Packet".

2) The CGF1 is able to store the packet sent by the CDF in a safe way (to e.g. a redundant RAM memory unit or a mirrored non-volatile memory or to another network element, e.g. post-processing system).

3) Since the CDF-CGF1 communication connection is now broken, the CDF is not able to get the response "Request Accepted" as the **Cause** value in the *Data Record Transfer Response* message.

4) Then the CDF sends the same CDR packet that could not be sent to CGF1 to the next CGF in its CGF preference list (here CGF2) a *Data Record Transfer Request* message, with the *Packet Transfer Command* IE having the

value "Send possible duplicated Data Record Packet". (That sending may be preceded by the testing of the CDF-CGF2 link by an *Echo Request* message; that the CGF2 would respond by the *Echo Response*.)

5) As the connection to CGF2 is working, CGF2 is able to process the CDR packet. Since the packet was marked by the sending CDF to be potentially duplicated, it is stored in CGF2, but not yet sent forward towards the post processing or BD.

6) The CGF2 sends confirmation of the successful packet reception to the CDF. The confirmation is performed by using the *Data Record Transfer Response* message, with the **Cause** value being "Request Accepted".

7) The CDF can now delete the now successfully sent (potentially duplicated) CDRs from its CDR buffer (but it keeps the sequence number(s) of the sent potentially duplicated packet(s) in a buffer dedicated for that.

8) When CGF1 is recovering after a system reboot, it sends a *Node Alive Request* message to the configured peer CDF(s), and so the CDF notices that it can again successfully communicate with the CGF1. (The CDF may also detect this by using the *Echo Request* messages, which would be answered by CGF1 by the *Echo Response* message.)

9) CDF acknowledges the CGF1 by *Node Alive Response* message.

10) For the earlier unacknowledged *Data Record Transfer Request* message(s), the CDF sends CGF1 empty test packet(s) (with no CDR payload in the *Data Record Packet* IE but just the other parts of the message frame).

11) CGF1 responds with *Data Record Transfer Response* message, with the **Cause** value being "Request related to possibly duplicated packets already fulfilled", because in this example case CGF1 had lost the communication capability towards CDF after storing the previously received (and by CGF1 unacknowledged) CDR packet.

12) Now CDF knows that the CGF1 had originally been able to process and forward the original version of the CDR packet from the CDF, and it indicates CGF2 that CGF2 can cancel the CDR packet(s) related to the previously unacknowledged GTP' CDF-CGF1 Sequence Number(s). Those packets' *Sequence Numbers* are indicated in the *Sequence Numbers of the Cancelled Packets* IE.

13) CGF2 shall now delete the cancelled packet(s) from its buffer for potentially duplicated packets.

14) CGF2 responds with *Data Record Transfer Response* message, with the **Cause** value being "Request Accepted".

After all the potentially duplicated packets are cleared form CGF(s), the CDF can continue in normal way the transfer of CDRs.

5.2.2.4 CGF redundancy mechanism

A summary of the CGF redundancy mechanism, which prevents duplicated CDR packets to enter the BS, is described below.
This, or other mechanisms, are deployed to enhance the reliability of CDR transport.

The general logic of the duplicate CDR packet prevention in CGF redundancy cases is shown in figure 5.2.2.4.1, where the messages are numbered sequentially, alternative messages are indicated by an index character ("a" or "b") that follows the arrow sequence number. The main mechanism of the messaging in CGF redundancy cases (when a CDF-CGF link is down or a CGF is not working) is based on CDF (1) first trying to send a CDR packet to CGF1.
In case no acknowledgement or a successful response is received (2) from CGF1 due to any reason, e.g. such as the request not reaching CGF1 despite repeated attempts (or the responses from CGF1 to the CDF are lost after the CGF1 has either stored it securely, or, forwarded it towards post-processing (2b)), the unacknowledged CDR packets are redirected to CGF2. The invocation for a re-transmission may be triggered by a time-out mechanism.

The CDF may first test the CDF-CGF2 link by sending an 'Echo Request' message to CGF2, in response to which CGF2 would respond with the 'Echo Response' message. The CDR packets not successfully received by the primary CGF (=CGF1) are sent to CGF2 (3), and are marked as potential duplicates, and CGF2 responds to the request(s) (4). Such CDRs, i.e. CDRs that are marked as potential duplicates would wait there for further commands from CDF.

When the CDF detects (5) and (6) that the primary CGF, in this case CGF1 is again able to communicate with it on receiving *Node Alive Request* (or getting a *Echo Response* from CGF2 to a *Echo Request* sent by the CDF) it answers by *Node Alive Response*. Then the CDF tests CGF1 with an empty packet (7), retrying continuously if no response is received, using e.g. increasing timeouts (using the old unacknowledged packet's Sequence Number, if the CGF1 would consider the packet to be a new one (8a) or an already received one (8b)). According to the response received from CGF1, the CDF gives the CGF2 a command to either release (9a) or cancel (9b) the corresponding CDR packet from CGF2. CGF2 then confirms the decision (10), and is able to send the CDRs towards the BS (11a).

Error handling: By default, retransmissions after configurable timeouts are used. If after the CGF1 communication failure, the CDR packet sending from CDF to CGF2 does not succeed, the CDF tries to use CGF3 as the intermediate CDR packet storage entity, etc. If no acknowledgement (10) is received by the CDF for its message(s) (9a) or (9b), the CDF retransmits the message (9a) or (9b) continuously and persistently, using e.g. increasing time intervals. An alarm should be sent to the OAM&P system if a communication link goes down. It shall be possible to release/cancel CDR packets from CGFs and unacknowledged sequence numbers from CDFs by OAM&P operations if permanent CDF-CGF link failures would occur. The buffers containing the Sequence Numbers of potentially duplicated packets, and the buffers containing the numbers of unacknowledged CDR packets shall be kept up to date (with CDR packet transfers) using transaction mechanisms. In the case of the CDF-CGF1 communication link being down, any new CDRs generated by the CDF are sent to a properly working CGF2, instead of the CGF1.

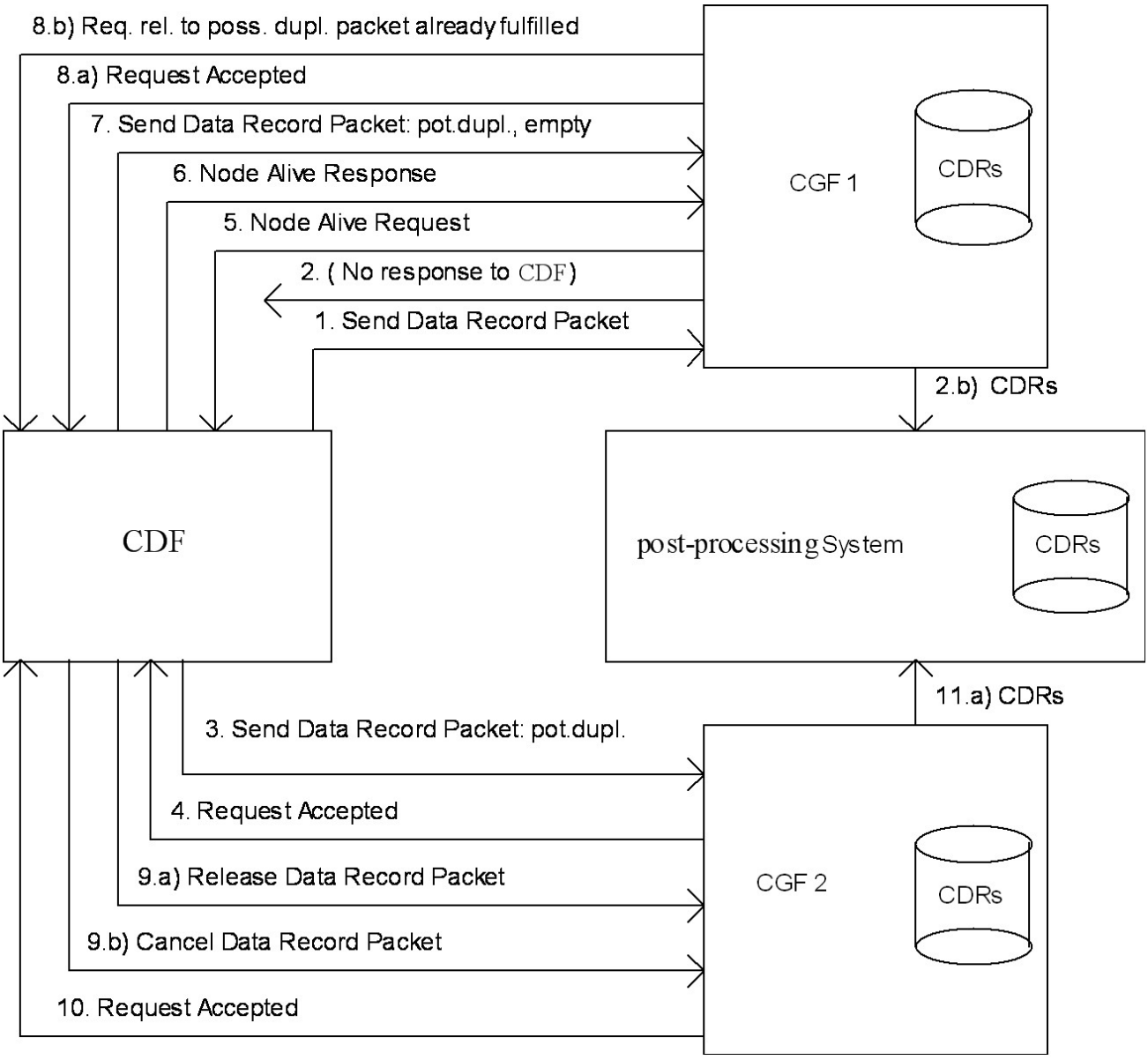


Figure 5.2.2.4.1: General CGF redundancy messaging scheme

A more detailed description of the CGF redundancy mechanism:

Due to a network failure/ congestion or a temporary node failure, a CGF might not be able to send a response within the configured timeout period to a request it got from a CDF. As a first attempt, retries of requests are to be used as defined in TS 29.060 [200], if the response is not received in the configured time.

If a CDF loses its connection to the CGF unexpectedly, it may send the CDRs to the next CGF in the priority list. If the CGF changes, the CDF can continue sending CDRs to different CGF nodes, depending on which CGF has been configured as the receiver of CDRs for a particular service.

Sequence number buffers: The CDF might lose its connection to its primary CGF due to a link failure or CGF going down. In this kind of redundancy condition the CDF attempts to redirect the CDR traffic to a secondary CGF (after possible retries have failed). The CDF maintains an internal buffer for Sequence Numbers of requests not yet successfully responded to by the primary CGF, for the case that it may become capable of communicating to the primary CGF at a later date. The CDF sends the not responded Data Record Packets (DRPs) to the secondary CGF, and the CDF maintains also a buffer for the Sequence Numbers related to those DRPs that have been temporarily stored to this secondary CGF. (If the communication towards the secondary CGF would not work, the transfer of possibly duplicated DRPs and Sequence Number bookkeeping would be done for a tertiary CGF etc.) Also the CGFs maintain Sequence Number buffers for each of their CDF links. The Sequence Numbers may in future be needed in relation to the possibly duplicated CDRs that the CGFs have got from the CDF(s). The Sequence Numbers are stored to wait for a final decision to release them towards the BS (if the primary CGF had not received successfully the packets originally

sent by a CDF) or to cancel them (if the primary CGF had received and processed successfully the originally by CDF sent packets).

The CDF is able to instruct CGF2 to cancel (or instruct CGF2 to transfer towards the BS), the CDR packets sent to a secondary CGF if the primary CGF becomes available for service. To make the right decision the CDF first sends an empty test packet with the 'Send possibly duplicated Data Record Packet' Packet Transfer Command to the primary CGF, using a previously not responded Sequence Number.

In case that the empty test packet to the primary CGF (which was temporarily down (or to which the link was down)) is responded with the **Cause** value "Request Accepted", the CDF releases the corresponding CDRs waiting for final decision in the secondary CGF, towards the BD with the Packet Transfer Command "Release Data Record Packet".

If the primary CGF responses this test message with the **Cause** value "Request related to possibly duplicated packets already fulfilled", the CDF cancels the corresponding CDRs waiting for final decision in the secondary CGF, using the Packet Transfer Command "Cancel Data Record Packet".

To enable that a CDF failure (destroying its Sequence Number buffers per each CGF link for non-responded requests or possibly duplicated packets) would not cause CDR packets to stay forever in the temporary decision waiting buffers of CGFs, there should also be OAM&P means of emptying those CGF buffers.

There shall also be a configurable parameter in the CGF for making the final decision, as to whether or not it is able to send the CDRs to the BS for the case where the backup buffering mechanism in the CDF could not be used until the end of the messaging sequence related to a certain CDR packet has been completed. This way the operator can:

A) Select that the CDFs and CGFs take care of duplicate prevention and the BS is not required to do duplicate checking due to possible duplicates caused by Network Element or CGF redundancy mechanisms.

B) Select that the BS performs the duplicate prevention. To do this in the most effective way, the CGF may include an additional flag linked to possibly duplicated CDRs sent to the BS, indicating that they have not been released by a CDF for BS use (or use special kind of file name if a file protocol is used between CGF and BS). This means that the BS has somewhat more processing work to do, but the BS would anyway get a duplicate free end result. CGF is in this case always authorized to forward CDRs towards the BS, also when they contain possibly duplicated data. For this case the CGFs may also have a configurable flag that *Data Record Packet Cancel/Release* operations are not needed.

6 Data description for the transfer

6.1 The GTP' charging protocol

6.1.0 General

This clause describes the features of GTP'. The message types described in clause 6.2.2 ("Reused GTP message types") are also described in the related clauses of TS 29.060 [200].

6.1.1 Usage of GTP header in charging

In GTP' messaging only the signalling plane of GTP is partly reused. The GTP' header is shown in figure 6.1.1.1.

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

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

Bit 1 of octet 1 is not used in GTP' (except in v0), and it is marked '0' in the GTP' header. It is in use in GTP' v0 and distinguishes the used header-length. In the case of GTP' 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 GTP', 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 GTP' header). The *Sequence Number* of the packet is part of the GTP' header.

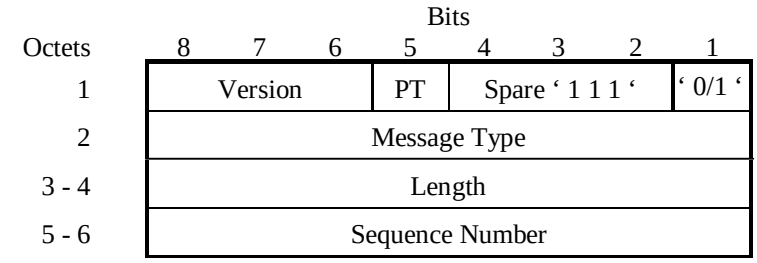


Figure 6.1.1.1: GTP' header

6.1.2 Information Elements (IEs)

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

Within the *Type* field the most significant bit is set to 0 when the TV format is used and set to 1 when the TLV format is used. This is illustrated in figures 6.1.2.1 and (b), respectively.

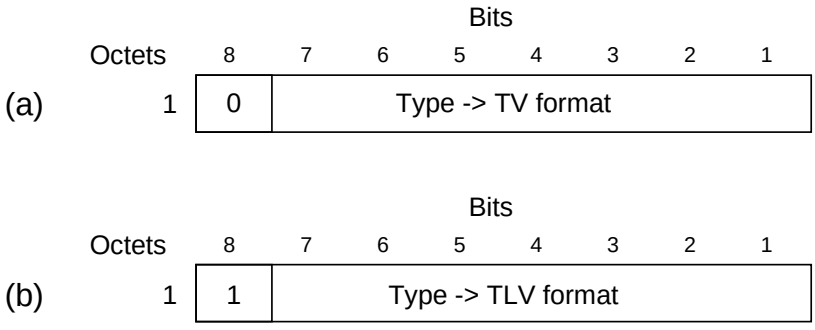


Figure 6.1.2.1: Type field for (a) TV and (b) TLV format

6.2 GTP' message types

6.2.1 List of all GTP' message types

GTP' defines a set of messages between two associated nodes. The GTP' messages defined are shown in table 6.2.1.1. The messages introduced by GTP' are in **boldface** letters**.** The other messages are inherited from the GTP protocol.

The GTP' introduced signalling message types
- Node Alive Request,
- Node Alive Response,
- Redirection Request and
- Redirection Response

belong to the "Path Management messages", while
- *Data Record Transfer Request* and
- *Data Record Transfer Response*

are from the message type group "Record Transmission messages".

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

GTP' reuses the GTP **Cause** values. The message type numbers required for the newly introduced GTP' messages have been derived from the unallocated message type number space specified in the GTP message table defined in TS 29.060 [200].

The number ranges allocated for GTP' are as follows:

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

TLV Information Element types introduced in the present document:
- 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 Cancelled Packets*
- 249 *Sequence Numbers of Released Packets*

TV Information Element types introduced in the present document:
- 127 *Charging ID*
- 126 *Packet Transfer Command*

For **Cause** Codes: **Cause** values used in requests: 49 to 63, **Cause** values used in responses indicating acceptance: 177 to 191, **Cause** values used in responses indicating rejection: 241 to 255.

Charging related **Cause** values introduced for the present document:

In requests:
- 63 *This node is about to go down*
- 62 *Another node is about to go down*
- 61 *The receive buffers are becoming full*
- 60 *The transmit buffers are becoming full*
- 59 *System failure*

In responses indicating acceptance:
- 177 *CDR decoding error*

In responses indicating rejection:
- 255 *Request not fulfilled*
- 254 *Sequence numbers of released/cancelled packets IE incorrect*
- 253 *Request already fulfilled*
- 252 *Request related to possibly duplicated packets already fulfilled*

The charging related message types are listed in table 6.2.1.1. Brief descriptions of the GTP messages reused in GTP' are provided in clause 6.2.2 ("Reused GTP message types") below. Further details are provided in TS 29.060 [200], the GTP specification.

Table 6.2.1.1: GTP' messages

Message Type value (Decimal)	GTP' 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

6.2.2 Reused GTP message types

The existing *Echo Request* and *Echo Response* messages defined in TS 29.060 [200] are also used in PS domain charging. They may be used by the CDF or by the CGF for checking if another CDF or CGF is alive. If the present document and TS 29.060 [200] differ in their description, then the TS 29.060 [200] is to be taken as the latest specification status of the related Information Elements. If the path protocol is TCP, *Echo Request* and *Echo Response* messages are not required.

The *Version Not Supported* message in the GTP' is similar to the corresponding GTP message. It indicates the latest GTP' version that the GTP' entity can support. If a receiving node receives a GTP' message of an unsupported version, then this node shall return a GTP' *Version Not Supported* message, indicating in the Version field of the GTP' header the latest GTP' version, this node supports. The received payload data of the GTP' packet shall then be discarded.

The *Version* bits in the GTP' header have currently the following possible values:

- GTP' version 0 (binary '000') identifies the following message type values:

  3 = Version Not Supported,
  4 = Node Alive Request,
  5 = Node Alive Response,
  6 = Redirection Request,
  7 = Redirection Response.

In clause 7.3.4.6 the Requests Responded information element has Length field in place of the Number of Requests Responded field, to make that TLV IE to be handled like normal TLV IEs.

If GTP' v0 is used in parallel with GTP' v2 or a later version, then, a 6-octet header length (with no trailing dummy octets) is used also with v0 (like in GTP' v2).

The mark of the usage of GTP' v0 with 6 octet header (instead of the original 20 octet long header) is then the version bits being 0 and the bit 1 of octet 1 being '1' (instead of '0').

- GTP' version 1 (binary '001') is the same as version 0 but has, in addendum, the duplicate CDR prevention mechanism, introduced in GSM 12.15 version 7.2.1 (1999-07) of the GPRS charging specification.

- GTP' version 2 (binary '010') is the same as version 1, but the header is just 6 octets long (no unused trailing octets). IPv6 address type is also supported (for Address of Recommended Node information element of the Redirection Request).

6.2.3 GTP message type modifications, implied by GTP'

The general principle is that the CDRs are always sent to a CGF residing in the same network as the CDF. In the case of roaming it is conceivable that some CDRs relating to the same service (e.g. in PS domain for the same IP-CAN bearer) are sent to different networks' CGFs. The cost balancing of the roaming traffic is to be agreed between operators.

6.2.4 GTP' message types

6.2.4.0 General

This clause describes the information elements used in the GTP' messages and the category in the tables are used according to the charging data configuration defined in clause 5.4 of TS 32.240 [1].

6.2.4.1 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. This message type is optional if the Path Protocol is TCP.

The *Node Alive Request* message allows a quicker reconnect capability than the *Echo Request* message based polling can provide, and its usage has a reduced load effect on the network, particularly when the number of network nodes using GTP' 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*.
The IEs in a Node Alive Request message are shown in table 6.2.4.1.1.

Table 6.2.4.1.1: IEs in a Node Alive Request

Information Element	Category
Node Address	M
Alternative Node Address	O
Private Extension	O

The Node Address format is the same as for the Charging Gateway Address format described in TS 29.060 [200]).

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 GTP' 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 Private Extension IE contains vendor- or operator-specific information.

6.2.4.2 Node Alive Response

The *Node Alive Response* message, shown in table 6.2.4.2.1, shall be sent as a response to a received *Node Alive Request*.

Table 6.2.4.2.1: IEs in a Node Alive Response

Information Element	Category
Private Extension	O

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

6.2.4.3 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 IEs in a *Redirection Request* Message are listed in table 6.2.4.3.1.
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* shall only describe an intra-PLMN node containing a CGF, and not a node in any other PLMN.

Table 6.2.4.3.1: IEs in a Redirection Request

Information Element	Category
Cause	M
Address of Recommended Node	O
Alternative Address of Recommended Node	O
Private Extension	O

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* information element, shown in figure 6.2.4.3.2, defines the IPv4 or IPv6 format address that the node is identified by in the 3GPP network.

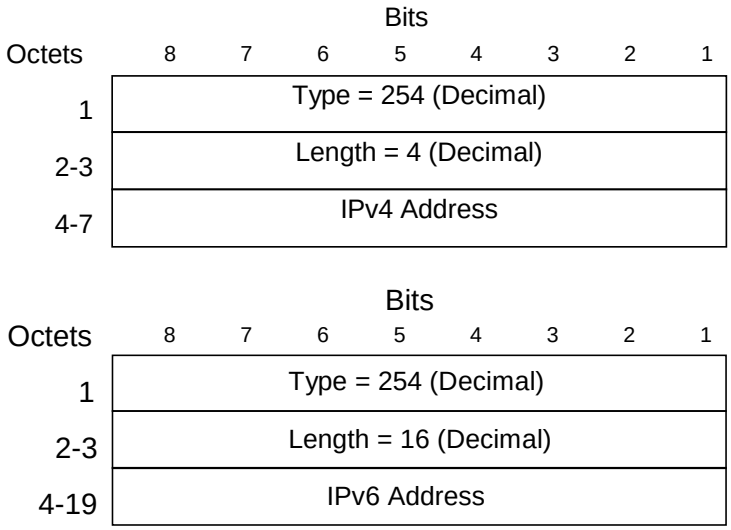


Figure 6.2.4.3.2: Address of Recommended Node information elements

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 GTP' 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 Private Extension contains vendor- or operator- specific information.

6.2.4.4 Redirection Response

A *Redirection Response* message shall be sent as a response of a received *Redirection Request*.
The IEs of this message are listed in table 6.2.4.4.1.

Table 6.2.4.4.1: IEs in a Redirection Response

Information Element	Category
Cause	M
Private Extension	O

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 Private Extension contains vendor- or operator-specific information.

6.2.4.5 Data Record Transfer Request

6.2.4.5.0 Introduction

This message is used to transmit the CDR(s) to the CGF. The CDRs are placed in the *Data Record Packet* IE.

6.2.4.5.1 Information Elements in Data Record Transfer Request

The Information Elements in *Data Record Transfer Request* message is specified in table 6.2.4.5.1.1.

Table 6.2.4.5.1.1: IEs in a Data Record Transfer Request

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

6.2.4.5.2 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.

1) **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. It is shown in figure 6.2.4.5.2.1. The other three commands are being used only in error recovery cases. Out of the three conditional IEs shown in table 6.2.4.5.1.1, only the "Data Record Packet" is present in this message.

2) **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.

3) **Cancel Data Record Packet**. Of the conditional IEs, the "Sequence Numbers of Cancelled Packets" is present in the message.

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

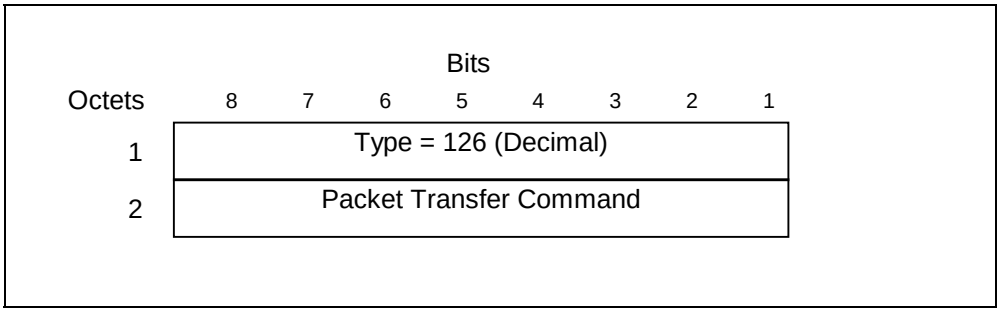


Figure 6.2.4.5.2.1: Packet Transfer Command IE

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.

6.2.4.5.3 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. This IE is illustrated in figure 6.2.4.5.3.1. 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.

As shown in figure 6.2.4.5.3.1, 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.
The formats of these two fields are described in detail in clauses 6.3 and 6.4.

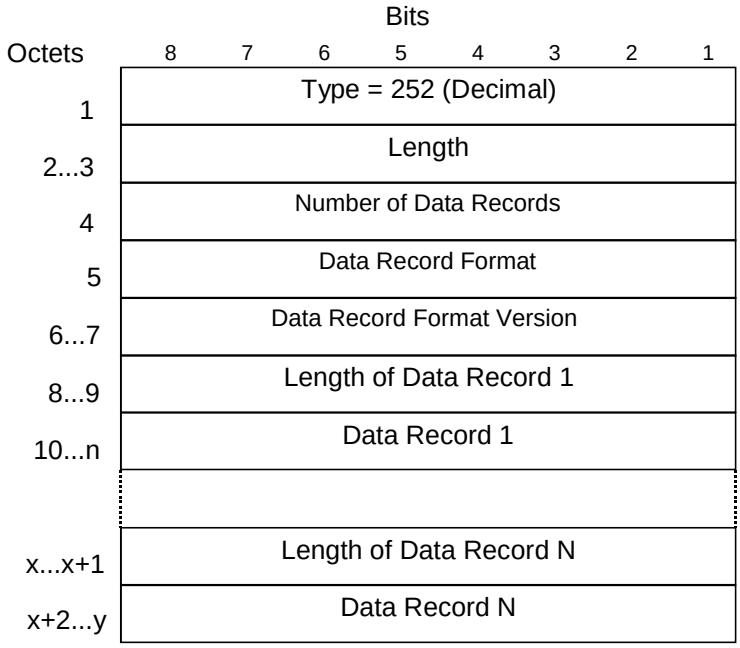


Figure 6.2.4.5.3.1: Data Record Packet IE

6.2.4.5.4 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 figure 6.2.4.5.4.1:

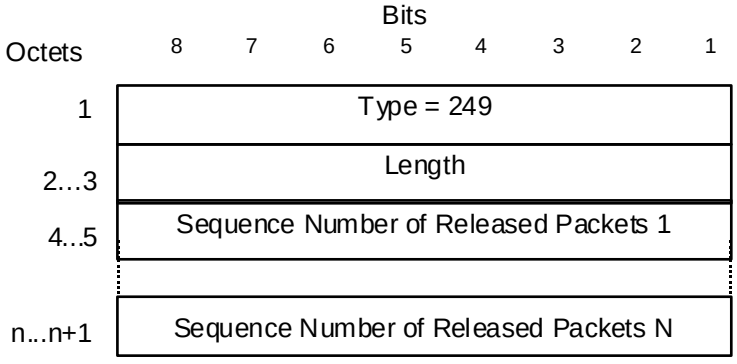


Figure 6.2.4.5.4.1: Sequence Numbers of Released Packets IE

6.2.4.5.5 Sequence Numbers of Cancelled Packets IE

The *Sequence Numbers of Cancelled Packets* information element is shown in figure 6.2.4.5.5.1 and contains the IE *Type*, *Length* and the *Sequence Number*(s) (each 2 octets) of the cancelled *Data Record Transfer Request*(s).
It is present if the *Packet Transfer Command* is "Cancel Data Record Packet".

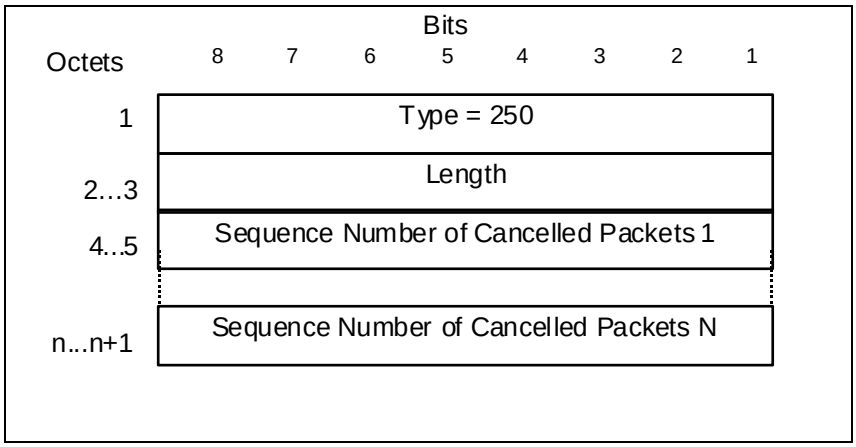


Figure 6.2.4.5.5.1: Sequence Numbers of Cancelled Packets IE

6.2.4.5.6 Private Extension IE

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

6.2.4.6 Data Record Transfer Response

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

Table 6.2.4.6.1: IEs in a Data Record Transfer Response

Information Element	Category
Cause	M
Requests Responded	M
Private Extension	O

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/cancelled 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 could alert the operator of a remote generating node of incompatible CDR encoding. It is optional and no action or response is required.

The **Requests Responded** information element contains the IE *Type*, *Length* and the *Sequence Numbers* (each 2 octets) of the *Data Record Transfer Requests*. It is shown in figure 6.2.4.6.2.

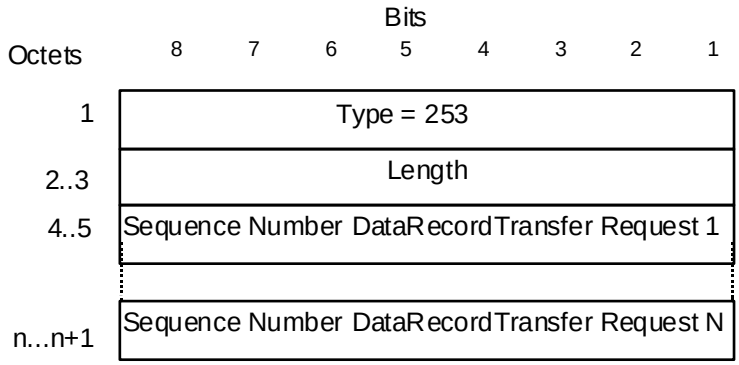


Figure 6.2.4.6.2: Requests Responded IE

The *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.

6.3 Data Record Format in GTP'

6.3.0 Introduction

The format of the PS domain CDRs, sent from CDF to CGF, is defined by the *Data Record Format*, which is the 5th octet of *Data Record Packet* IE, shown in figure 6.2.4.5.3.1.

The following rules govern the *Data Record Format*:
- This field consists of one octet (#5).
- The value range is 1-255 in decimal. The value '0' should not be used.
- Only the values 1-10 and 51-255 can be used for standards purposes.
- Values in the range of 11-50 are to be configured only by operators, and are not subject to standardization.
- The value '1' identifies ASN.1 Basic Encoding Rules (BER) encoding,
  which shall be supported in PS domain charging.
  Other values for optional encodings are specified in clause 6.3.1.

6.3.1 Standard Data Record Format

For the PS domain CDR transfer, defined by the present document, only an ASN.1 BER encoding is mandatory.
For this encoding, the *Data Record Format* value is '1'.
Other ASN.1 encodings may be supported optionally, with *Data Record Format* values as indicated below:

- "1" signifies the use of Basic Encoding Rules (BER)
- "2" signifies the use of unaligned basic Packed Encoding Rules (PER)
- "3" signifies the use of aligned basic Packed Encoding Rules (PER)

6.3.2 Private Data Record Formats

The *Data Record Format* values 11...50 (decimal) are reserved for private (implementation specific) format use.

6.4 Data Record Format Version for CDRs

The CDR release and versions numbers are defined by the '*Data Record Format Version*', in octet 6 and 7 of the *Data Record Packet* IE, shown in figure 6.2.4.5.3.1. The format of this field is depicted in figure 6.4.1.

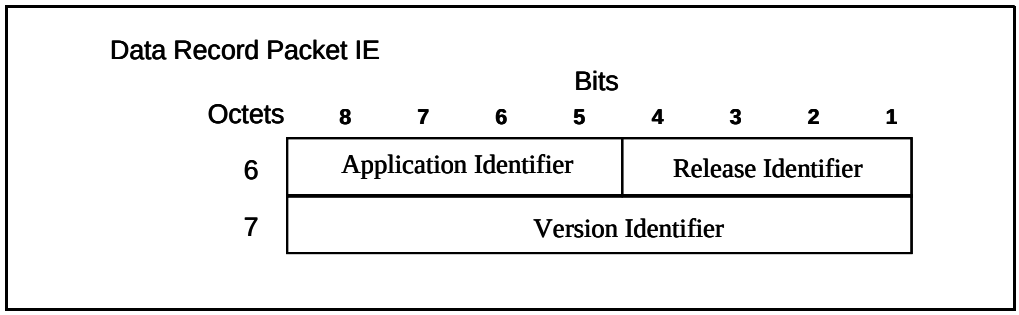
The first octet (#6 in *Data Record Packet* IE) is divided into two fields each with 4 bits:

The first field (bits 8-5 of octet 6, see figure 6.4.1) identifies the application. For charging purposes, the ***Application Identifier*** has a value of '1' (decimal).
Other possible applications of GTP' may use different numbers.

The second field (bits 4-1 of octet 6, see figure 6.4.1) identifies the release.
The ***Release Identifier*** indicates the TS release, used to encode the CDR, i.e. its value corresponds to the first digit of the version number of TS 32.298 [51], as shown on the cover sheet.

The second octet (#7 in *Data Record Packet* IE) identifies the version of the TS used to encode the CDR, i.e. its value corresponds to the second digit of the version number of TS 32.298 [51] (as shown on the cover sheet), plus '1'.
E.g. for version 3.4.0, the ***Version Identifier*** would be "5".
In circumstances where the second digit is an alphabetical character, (e.g. 3.b.0), the corresponding ASCII value shall be taken, e.g. the ***Version Identifier*** would be "66" (ASCII(b)).

Figure 6.4.1: The format of the *Data Record Format Version* field



Annex A (informative): Bibliography

This Annex is a placeholder for documents which are not explicitly cited in this specification.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Sep 2004	SA_25	SP-040553	--	--	Submitted to TSG SA#25 for Approval	1.0.0	6.0.0
Jun 2005	SA_28	SP-050275	0001	--	Correction to scope	6.0.0	6.1.0
Jun 2005	SA_28	SP-050275	0002	--	Correction to references	6.0.0	6.1.0
Jun 2005	SA_28	SP-050275	0003	--	Correction on the use of 'reference point' and 'interface' – Align with TR 21.905	6.0.0	6.1.0
Jun 2007	SA_36	--	--	--	Automatic upgrade to Rel-7 (no CR) at freeze of Rel-7.	6.1.0	7.0.0
Jun 2008	SA_40	SP-080274	0004	--	Implication on CDR transfer for EPC Charging	7.0.0	8.0.0
Sep 2009	SA_45	SP-090536	0005	--	UDP Port number differentiation between GTP'v2 and GTPv2	8.0.0	8.1.0
Dec 2009	-	-	-	-	Update to Rel-9 version (MCC)	8.1.0	9.0.0
Mar 2011	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	11.0.0
2013-09	SA_61	SP-130435	0007	1	Justification on usage of Sequence numbers	11.0.0	12.0.0
2014-07					Rapporteur/MCC: General editorial changes and clean-up.	12.0.0	12.0.1
2014-09	SA_65	SP-140564	008	1	Corrections for alignment between charging specifications	12.0.1	12.1.0
2014-12	SA_66	SP-140805	009	-	Additional corrections for removal of I-WLAN solution	12.1.0	12.2.0
			010	-	Corrections on definition for parameter category		
2016-01					Update to Rel-13 (MCC)	12.2.0	13.0.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	SA#75	SP-170138	0012	1	D	Remove reference to RFC 3588	14.0.0

History

Document history		
V14.0.0	April 2017	Publication