

ETSI TS 123 007 V14.3.0 (2017-07)



**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Restoration procedures
(3GPP TS 23.007 version 14.3.0 Release 14)**



Reference

RTS/TSGC-0423007ve30

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2017.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and LTE™ are trademarks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

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

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	9
1 Scope	10
1.1 References	10
1.2 Abbreviations	12
1.3 Definitions.....	12
2 Design objectives	12
3 Restoration indicators in location registers and in GPRS support nodes	13
3.1 Restoration Indicators in the VLR.....	13
3.2 Restoration Indicators in the HLR.....	15
3.3 Restoration Indicators in the SGSN	15
3.4 Restoration Indicators in the MME	16
3.5 Restoration Indicator in the ProSe Function.....	17
3.6 Restoration Indicator in the V2X Control Function	18
4 Restoration of data in the VLR.....	18
4.0 VLR Failure with Restart	18
4.0a VLR Failure without Restart	18
4.1 Restart of the VLR	19
4.2 Restoration Procedures	19
4.2.0 General.....	19
4.2.1 Incoming Call	20
4.2.2 Mobile Terminated Short Message.....	21
4.2.3 Mobile Terminating Location Request (MT-LR)	22
4.2.4 Incoming LCS Information Request (GSM only).....	22
4.2.5 Outgoing MS request.....	23
4.2.6 Outgoing LMU Request (GSM only)	23
4.2.7 Location Updating or IMSI Attach	24
4.2.8 Use of TMSI	24
4.2.9 SGSN associations.....	25
4.2.10 MME associations	25
5 Restoration of data in the HLR/HSS	25
5.1 Restart of the HLR/HSS	25
5.2 Procedures During Restoration.....	26
5.2.1 Mobile terminated call.....	26
5.2.2 Mobile Originated Activity for CS	26
5.2.3 Mobile Originated Activity for ProSe.....	26
5.2.4 Procedures in the SGSN	26
5.2.5 Procedures in the MME	26
5.2.6 Mobile Originated Activity for V2X	27
6 Periodic location updating.....	27
7 Periodic routing area updating.....	27
8 Stand-alone operation of the VLR.....	27
9 Stand-alone operation of the SGSN	28
9A Stand-alone operation of the MME.....	28
10 Restoration of data in the GGSN.....	28
10.0 GGSN failure.....	28
10.1 Restart of the GGSN.....	28

10.2	Restoration Procedures	28
10.2.0	General	28
10.2.1	Mobile terminated transmission	29
10.2.2	Mobile originated transmission	29
11	Restoration of data in the SGSN	29
11.0	SGSN Failure	29
11.0.1	Gn/Gp SGSN failure	29
11.0.2	SGSN Failure using S4	30
11.1	Restart of the SGSN	30
11.2	Restoration Procedures	31
11.2.1	Mobile terminated user data transmission	31
11.2.2	Mobile terminated services requested by the MSC/VLR	31
11.2.3	Mobile terminated SMS over GPRS	31
11.2.4	Mobile originated Routeing Area Updating or Attach	31
11.2.5	Mobile originated LLC frame	32
11.2.6	Mobile originated Service Request	32
11.3	Use of TLLI	32
11.4	VLR associations	33
11.5	Restart of a peer node	33
11.5.1	SGW failure	33
11.5.2	MBMS-GW failure	33
12	Restoration of Data in an SMLC (GSM only)	33
12.1	Restart of an SMLC	33
12.2	Data Restoration for a Specific LMU	33
13	Restoration of Data in an LMU (GSM only)	34
14	Restoration of data in the MME	34
14.1	Restart of the MME	34
14.1.1	Restoration Procedures	34
14.1.2	Mobile originated Tracking Area Updating or E-UTRAN Attach	35
14.1.3	Mobile terminated services requested by the MSC/VLR	35
14.1.4	Mobile terminated user data transmission	36
14.1.5	Mobile originated Service Request	36
14.1.6	Mobile Terminated NIDD procedure	36
14.1A	Restart of a peer node	36
14.1A.1	SGW Failure	36
14.1A.2	MBMS GW failure	36
14.2	VLR associations	37
14.3	Partial Failure Handling at MME	37
14.3.1	General	37
14.3.2	Procedures during PDN Connection Establishment	37
14.3.3	Procedures during MME Partial Failure	37
14.3.4	Procedures during a Peer's Partial Failure	37
14.3.5	Procedures during PDN Connection Removal or Modification	38
15	Restoration of data in GERAN/UTRAN	38
15.1	BSS Failure (A/Gb mode)	38
15.2	RNC/BSC Failure (Iu mode)	38
15.3	RNC/BSC Failure (Iu mode) using S4	39
15.4	Other RNC functionality for MBMS restoration	39
15.5	Iu path failure using S4	40
15A	Restoration of data in E-UTRAN	40
15A.1	eNodeB Failure	40
15A.1.1	General	40
15A.1.2	PWS restoration	41
15A.2	S1-AP path failure	41
15A.3	MCE Failure	42
15A.4	M3AP path failure	42
15A.5	Other MCE functionality for MBMS restoration	43
15A.6	Other MME related functionality for MBMS restoration	44

16	Restoration of data in the SGW	44
16.1	Restart of the SGW	44
16.1.0	SGW Failure	44
16.1.1	Restoration Procedures	44
16.1a	Restart of the SGW-C	44
16.1a.1	SGW-C failure	44
16.1a.2	Restoration procedure	44
16.1b	Restart of the SGW-U	45
16.1b.1	SGW-U failure	45
16.1b.2	Restoration procedure	45
16.1A	Restart of a peer node	45
16.1A.1	MME/S4-SGSN Failure	45
16.1A.1.1	General	45
16.1A.2	PGW Failure	45
16.1A.3	SGW-C Failure	46
16.1A.4	SGW-U Failure	47
16.2	Partial Failure Handling at SGW	47
16.2.1	General	47
16.2.2	Procedures during PDN Connection Establishment	48
16.2.3	Procedures during SGW Partial Failure	48
16.2.4	Procedures during a Peer's Partial Failure	48
16.2.5	Procedures during PDN Connection Removal or Modification	49
17	Restoration of data in the PGW	50
17.1	Restart of the PGW	50
17.1.0	PGW Failure	50
17.1.1	Restoration Procedures	51
17.1a	Restart of the PGW-C	51
17.1a.1	PGW-C failure	51
17.1a.2	Restoration Procedures	51
17.1b	Restart of the PGW-U	51
17.1b.1	PGW-U failure	51
17.1b.2	Restoration Procedures	51
17.1A	Restart of a peer node	52
17.1A.1	SGW/ePDG/TWAN Failure	52
17.1A.2	PCRF Failure	52
17.1A.3	PGW-C Failure	52
17.1A.4	PGW-U Failure	53
17.2	Partial Failure Handling at PGW	53
17.2.1	General	53
17.2.2	Procedures during PDN Connection Establishment	53
17.2.3	Procedures during PGW Partial Failure	53
17.2.4	Procedures during a Peer's Partial Failure	54
17.2.5	Procedures during PDN Connection Removal or Modification	54
17A	Restoration of data in the MBMS GW	54
17A.1	Restart of the MBMS GW	54
17A.2	Restart of a peer node	55
17A.2.1	MME failure	55
17A.2.2	SGSN failure	55
17A.2.3	BM-SC failure	56
17B	Restoration of data in the ePDG	56
17B.1	Restart of the ePDG	56
17B.1.1	ePDG Failure	56
17B.1.2	Restoration Procedures	56
17B.1A	Restart of a peer node	56
17B.1A.1	PGW Failure	56
17B.2	Partial Failure Handling at ePDG	57
17B.2.1	General	57
17B.2.2	Procedures during PDN Connection Establishment	57
17B.2.3	Procedures during ePDG Partial Failure	57
17B.2.4	Procedures during PGW Partial Failure	57

17B.2.5	Procedures during PDN Connection Removal or Modification.....	58
17C	Restoration of data in the TWAN.....	58
17C.1	Restart of the TWAN	58
17C.1.1	TWAN Failure	58
17C.1.2	Restoration Procedures	58
17C.1A	Restart of a peer node.....	58
17C.1A.1	PGW Failure	58
17C.2	Partial Failure Handling at TWAN.....	58
17C.2.1	General.....	58
17C.2.2	Procedures during PDN Connection Establishment	59
17C.2.3	Procedures during TWAN Partial Failure.....	59
17C.2.4	Procedures during PGW Partial Failure.....	59
17C.2.5	Procedures during PDN Connection Removal or Modification.....	59
17D	Restoration of data in the BM-SC	60
17D.1	Restart of the BM-SC	60
17D.2	Restart of the GCS AS.....	60
17E	Restoration of data in the GCS AS.....	60
17E.1	Restart of the GCS-AS	60
17E.2	Restart of the BM-SC	60
18	GTP-C based restart procedures.....	61
19	PMIPv6 based restart procedures	62
19A	PFCP based restart procedures	62
20	Path management procedures.....	63
20.1	General	63
20.2	Signalling path failure detection and handling	63
20.2.1	General.....	63
20.2.2	SGW functionality	64
20.2.2.1	S11/S4 path failure.....	64
20.2.2.2	S5 path failure	64
20.2.3	MBMS GW functionality	64
20.2.3.1	Sm path failure	64
20.2.3.2	Sn path failure	66
20.2.3.3	SGmb path failure	66
20.2.4	MME functionality	67
20.2.4.1	Sm path failure	67
20.2.4.2	S5 path failure	68
20.2.5	SGSN functionality.....	68
20.2.5.1	Sn path failure	68
20.2.5.2	S5 path failure	69
20.2.6	BM-SC functionality.....	69
20.2.6.1	SGmb path failure	69
20.2.6.2	MB2-C path failure	71
20.2.7	PGW functionality	71
20.2.7.1	S5 path failure	71
20.2.8	GCS AS functionality	72
20.2.8.1	MB2-C path failure	72
20.2.9	Sx interface functionality.....	72
20.2.9.1	Sxa path failure	72
20.2.9.2	Sxb path failure	72
20.3	User plane path failure detection and handling	72
20.3.1	General.....	72
20.3.2	MBMS GW functionality	73
20.3.2.1	SGi-mb path failure.....	73
20.3.3	BM-SC functionality.....	73
20.3.3.1	SGi-mb path failure.....	73
20.3.4	With Control and User plane Separation of SGW or PGW nodes.....	73
21	Error Indication handling	74

21.1	General	74
21.2	GGSN	74
21.3	Gn/Gp SGSN	74
21.4	S4 SGSN	75
21.5	RNC or NodeB	75
21.6	eNodeB	75
21.7	SGW	76
21.8	PGW	77
21.9	MBMS GW	77
21.10	ePDG	77
21.11	TWAN	77
21.12	MME	78
22	Downlink Data Notification Handling at MME/S4 SGSN	78
23	General partial failure handling procedures	79
24	Restoration of data in the PCRF	84
24.1	Restart of the PCRF	84
24.1.0	PCRF Restart	84
25	Network triggered service restoration procedure	84
25.1	General	84
25.2	Network triggered service restoration procedure without ISR	84
25.2.1	General	84
25.2.2	SGW procedure	85
25.2.3	MME/SGSN procedure	86
25.3	Network triggered service restoration procedure with ISR	86
25.3.1	General	86
25.3.2	SGW procedure	87
25.3.3	MME/S4-SGSN procedure	88
26	Mobile terminated CS service delivery via an alternative MME in MME pool	88
27	Restoration of PDN connections after an SGW failure	90
27.1	General	90
27.2	Restoration of PDN connections after an SGW failure for UEs without ISR	90
27.2.1	General	90
27.2.2	MME/S4-SGSN triggered SGW restoration	90
27.2.2.1	General	90
27.2.2.2	MME/S4-SGSN procedure	91
27.2.2.3	PGW procedure	93
27.2.2.4	PCRF procedure	93
27.2.2.5	SGW procedure	93
27.2.3	PGW triggered SGW restoration	94
27.2.3.1	General	94
27.2.3.2	MME/S4-SGSN procedure	94
27.2.3.3	SGW procedure	95
27.2.3.4	PGW procedure	95
27.3	Restoration of PDN connections after an SGW failure for UEs with ISR	96
27.3.1	MME/S4-SGSN triggered SGW restoration for UEs with ISR	96
27.3.1.1	General	96
27.3.1.2	MME/S4-SGSN procedure	96
27.3.2	PGW triggered SGW restoration for UEs with ISR	97
27.3.2.1	General	97
27.3.2.2	MME/S4-SGSN procedure	97
28	Restoration of data in the CSS	98
28.1	Restart of the CSS	98
29	MBMS Heartbeat procedure	98
30	Restoration of the SCEF	99
30.1	Restart of the SCEF	99
30.1.1	Mobile Originated NIDD procedure	99

Annex A (informative): **Change history**100
History107

Foreword

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

The present document defines the restoration procedures within the 3GPP system.

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 data stored in location registers are automatically updated in normal operation; the main information stored in a location register defines the location of each mobile station and the subscriber data required to handle traffic for each mobile subscriber. The loss or corruption of these data will seriously degrade the service offered to mobile subscribers; it is therefore necessary to define procedures to limit the effects of failure of a location register, and to restore the location register data automatically. The present document defines the necessary procedures.

The basic principle is that restoration should be based on radio contact to avoid faulty data being spread in the system.

Subscriber data for supplementary services must also be correctly restored, although the impact on service of corruption of supplementary service data is less severe.

Procedures for supporting these functions are defined in 3GPP TS 29.002 [6] and 3GPP TS 29.060 [8].

The MAP operation "IMSI Attach" is used only in MAP version 1; in MAP version 2 the same function is performed by the MAP operation "Update Location Area". References in this specification to IMSI attach apply only to MAP version 1 network entities.

If the restoration of subscriber data in the VLR is triggered by Location Updating or IMSI Attach, the VLR retrieves subscriber data from the HLR by sending an "Update Location" request, which triggers one or more "Insert Subscriber Data" operations from the HLR. The "Update Location" request may also be used to send the LMSI to the HLR.

If the restoration of subscriber data in the VLR is triggered by a "Provide Roaming Number" request, the behaviour of the VLR depends on whether it is implemented according to MAP version 1 or MAP version 2. For MAP version 2, the VLR retrieves subscriber data from the HLR by sending a "Restore Data" request, which triggers one or more "Insert Subscriber Data" operations from the HLR. The "Restore Data" request is also used to send the LMSI to the HLR. For MAP version 1, the VLR retrieves subscriber data from the HLR by sending a "Send Parameters" request with parameter type "Subscriber Data", which cannot be used to send the LMSI to the HLR.

The VLR number and MSC number in the subscriber data in the HLR are updated by the "Update Location" procedure.

The GGSN (Gateway GPRS Support Node) is the point of PDN interconnection with the GSM PLMN supporting GPRS. The GGSN contains routing information for GPRS users with a PDP context active. The necessary procedures needed to restore GGSN data information after a restart are described in this document.

The SGSN (Serving GPRS Support Node) is the node that is serving the MS. The SGSN stores information regarding e.g. mobility management, routing and security. The necessary procedures needed to restore this SGSN information after a restart are described in this document.

The MME (Mobility Management Entity) is the node that is serving the UE when attached to E-UTRAN. The MME stores information regarding e.g. mobility management, routing and security. The necessary procedures needed to restore this MME information after a restart are described in this document.

A Type A LMU (Location Measurement Unit) is a network node, accessed over the GSM air interface, that is functionally similar to an MS. All requirements associated with a non-GPRS MS in this specification apply also to a Type A LMU except where specified otherwise.

1.1 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 TR 21.905: "Vocabulary of 3GPP Specifications".

- [2] Void
- [3] Void
- [4] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".
- [5] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [6] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".
- [7] 3GPP TS 29.018: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification".
- [8] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp interface".
- [9] 3GPP TS 43.005: "Technical performance objectives".
- [10] 3GPP TS 23.071: " Location Services (LCS); Functional description; Stage 2".
- [11] Void
- [12] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".
- [13] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3".
- [14] 3GPP TS 29.118: "Mobility Management Entity (MME) – Visitor Location Register (VLR) SGs interface specification".
- [15] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [16] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols; Stage 3".
- [17] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)".
- [18] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [19] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [20] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".
- [21] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".
- [22] IETF RFC 5847: "Heartbeat Mechanism for Proxy Mobile IPv6".
- [23] 3GPP TS 23.018: "Basic call handling; Technical realization".
- [24] 3GPP TS 23.236: "Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes".
- [25] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".
- [26] IETF RFC 7077: "Update Notifications for Proxy Mobile IPv6".
- [27] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".
- [28] 3GPP TS 36.444: "EUTRAN M3 Application Protocol (M3AP)".
- [29] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

- [30] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".
- [31] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) ".
- [32] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".
- [33] 3GPP TS 23.303: "Proximity based Services; Stage 2".
- [34] 3GPP TS 29.344: "Proximity-services (ProSe) Function to Home Subscriber Server (HSS) aspects; Stage 3".
- [35] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".
- [36] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".
- [37] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".
- [38] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".
- [39] 3GPP TS 23.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 2".
- [40] 3GPP TS 23.285: "Architecture enhancements for V2X services; Stage 2".
- [41] 3GPP TS 29.388: "V2X Control Function to V2X Control Function to Home Subscriber Server (HSS) aspects (V4)".
- [42] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".
- [43] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane of EPC Nodes; stage 3".

1.2 Abbreviations

For the purposes of the present document, the abbreviations listed in 3GPP TR 21.905 [1] apply.

1.3 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

PDN Connection: "PDN Connection" in this specification only refers to the PDN connection through the SGW and PGW.

SCEF PDN Connection: The PDN connection to the SCEF. Unless otherwise indicated in a clause or sub-clause, "PDN Connections" do not refer to any SCEF PDN Connection.

2 Design objectives

To avoid loss of all the data stored in a location register when part of the equipment of the location register fails, a regime must be implemented to secure the data. This regime can include replication of volatile storage units and periodic back-up of data to non-volatile storage. If the data security regime ensures the integrity of the data in spite of failure of part of the location register equipment then there will be no impact on service. This Technical Specification describes the procedures to be used when the integrity of data in the location register cannot be ensured; that situation is referred to below as "failure".

The VLR and SGSN shall erase all IMSI records affected by the failure when it restarts after a failure. The GGSN shall erase all non-static PDP records affected by the failure and restore static PDP records when it restarts after a failure.

For the HLR/HSS or CSS, periodic back-up of data to non-volatile storage is mandatory.

The reliability objectives of location registration are listed in 3GPP TS 43.005 [9].

The MME, S-GW and P-GW must similarly have a regime to secure the PDN connection and bearer data at failures. When an MME, SGW or PGW has a full node restart or fails all PDN connections and bearer records associated with the failing node shall be erased and any internal resources released.

Clause 18 "GTP-C based restart procedures" specifies how a GTP-C entity restart is detected and handled by the peer.

3 Restoration indicators in location registers and in GPRS support nodes

3.1 Restoration Indicators in the VLR

Three restoration indicators are provided in the VLR for each IMSI record: "Confirmed by Radio Contact", "Subscriber Data Confirmed by HLR" and "Location Information Confirmed in HLR".

The indicator "Confirmed by Radio Contact" indicates whether the VLR's record of location area identity and MSC number for the mobile station is confirmed by radio contact.

The indicator "Confirmed by Radio Contact" in an IMSI record is set to the initial value "Not Confirmed" when the VLR receives a "Provide Roaming Number" request, an "Update Location Area" request or an "IMSI Attach" request for an MS for which the VLR does not have an IMSI record. The indicator "Confirmed by Radio Contact" in an IMSI record may also be set to the initial value "Not Confirmed" when the VLR receives a Reset indication message from the SGSN serving the MS if the MS is attached to both GPRS and non-GPRS services (see 3GPP TS 29.018 [7]), or a Reset indication message from the MME serving the UE if the UE is attached to both EPS and non-EPS services or for SMS only (see 3GPP TS 29.118 [14]).

The indicator "Confirmed by Radio Contact" is set to "Confirmed" when the radio contact that has been established with the MS is authenticated.

The indicator "Subscriber Data Confirmed by HLR" indicates whether the subscriber data set for the mobile station held by the VLR is consistent with that held by the HLR.

The indicator "Subscriber Data Confirmed by HLR" is set to the initial value "Not Confirmed" when the VLR receives a "Provide Roaming Number" request, an "Update Location Area" request or an "IMSI Attach" request for an MS for which the VLR does not have an IMSI record.

The indicator "Subscriber Data Confirmed by HLR" is set to "Confirmed" at either of the following events:

- The VLR successfully performs an "Update Location" to the HLR;
- The VLR successfully performs a "Restore Data" operation to the HLR.

The indicator "Location Information Confirmed in HLR" indicates whether the HLR's record of VLR number and MSC number for the mobile station is confirmed by radio contact.

The indicator "Location Information Confirmed in HLR" is set to "Not Confirmed" at any of the following events:

- The VLR receives an "Update Location Area" request or an "IMSI Attach" request for an MS for which the VLR has no IMSI record;
- A VLR which serves two or more MSCs receives a "Provide Roaming Number" request for an MS for which the VLR has no IMSI record;
- The VLR receives a "Reset" message from the HLR with which the MS is registered;
- The VLR in a Super-Charged network receives a Send Identification message from the serving VLR;

- The VLR in a Super-Charged network receives a Cancel Location message that indicates an "updateProcedure".

The indicator "Location Information Confirmed in HLR" is set to "Confirmed" at either of the following events:

- A VLR which serves only one MSC receives a "Provide Roaming Number" request for an MS for which the VLR has no IMSI record;
- Successful completion of the "Update Location" procedure triggered by authenticated radio contact.

The indicator "Location Information Confirmed in SMLC" indicates whether an SMLC's record of MSC number for a particular LMU is confirmed by radio contact.

The indicator "Location Information Confirmed in SMLC" is set to "Not Confirmed" at any of the following events:

- The VLR receives an "Update Location Area" request or an "IMSI Attach" request for an MS for which the VLR has no IMSI record. The indicator, in this case, becomes valid only if HLR subscriber data later indicates an LMU;
- The VLR receives an "LCS Reset" message from an SMLC where the message is targetted to either a specific LMU or all LMUs registered with the SMLC;
- The VLR receives an "IMSI Detach" from an LMU that is registered with an SMLC.

The indicator "Location Information Confirmed in SMLC" is set to "Confirmed" at the following event:

- Successful completion of the "LCS Registration" procedure triggered by a successful location update;
- Successful transfer of an LCS Information message from an SMLC to the LMU.

Also the following two restoration indicators may be provided in the VLR for each IMSI record: "Subscriber Data Confirmed by CSS" and "Location Information Confirmed by CSS".

The indicator "Subscriber Data Confirmed by CSS" indicates whether the CSG subscriber data set for the roaming mobile station held by the VLR is consistent with that held by the CSS.

The indicator "Subscriber Data Confirmed by CSS" is set to the initial value "Not Confirmed" at the following event:

- The VLR receives a "Provide Roaming Number" request, an "Update Location Area" request or an "IMSI Attach" request for a roaming MS for which the VLR does not have an IMSI record.
- The VLR receives a "Cancel VCSG Location Request" message from the CSS after the VLR restart if the roaming MS attached to the macro cell after the VLR restart. The indicator "Subscriber Data Confirmed by CSS" is set to "Confirmed" at the following event:
 - The VLR successfully performs an "Update VCSG Location" to the CSS.
 - The VLR receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the VLR restart if the roaming MS attached to the macro cell after the VLR restart.

The indicator "Location Information Confirmed by CSS" indicates whether the VLR number for the roaming mobile station registered is confirmed by the CSS.

The indicator "Location Information Confirmed by CSS" is set to "Not Confirmed" at any of the following events:

- The VLR receives an "Update Location Area" request or an "IMSI Attach" request for a roaming MS for which the VLR has no IMSI record;
- The VLR receives a "Reset" message from the CSS with which the roaming MS is registered.
- The VLR receives a "Cancel VCSG Location Request" message from the CSS after the VLR restart if the roaming MS attached to the macro cell after the VLR restart.

The indicator "Location Information Confirmed by CSS" is set to "Confirmed" at the following event:

- Successful completion of the "Update VCSG Location" procedure to the CSS.

- The VLR receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the VLR restart if the roaming MS attached to the macro cell after the VLR restart.

3.2 Restoration Indicators in the HLR

As an implementation option, one restoration indicator may be provided in the HLR for each IMSI record: "Check SS".

The "Check SS" indicator is set to "Check Required" when the HLR restarts after a failure.

The "Check SS" indicator is checked whenever the HLR receives an "Update Location" request from a VLR. If it is set to "Check Required", after successful completion of subscriber data retrieval that ran embedded in the "Update Location" procedure the HLR sends a "Forward Check SS Indication" request message to the VLR and sets the "Check SS" indicator to "Check Not Required".

3.3 Restoration Indicators in the SGSN

Two restoration indicators are provided in the SGSN for each IMSI record: "Subscriber Data Confirmed by HLR" and "Location Information Confirmed in HLR".

The indicator "Subscriber Data Confirmed by HLR" indicates whether the subscriber data set for the mobile station held by the SGSN is consistent with that held by the HLR.

The indicator "Subscriber Data Confirmed by HLR" is set to the initial value "Not Confirmed" when the SGSN receives a Routing Area Update request or an IMSI- and/or GPRS Attach request for an MS for which the SGSN does not have an IMSI record.

The indicator "Subscriber Data Confirmed by HLR" is set to "Confirmed" at the following event:

- The SGSN successfully performs an Update GPRS Location to the HLR;

The indicator "Location Information Confirmed in HLR" indicates whether the HLR's record of the SGSN address for the mobile station is confirmed by radio contact.

The indicator "Location Information Confirmed in HLR" is set to "Not Confirmed" at any of the following events:

- The SGSN receives a Routing Area Update request or an IMSI- and/or GPRS Attach request for an MS for which the SGSN has no IMSI record;
- The SGSN receives a "Reset" message from the HLR with which the MS is registered;
- The SGSN in a Super-Charged network receives a Send Identification message from the serving SGSN;
- The SGSN in a Super-Charged network receives a Cancel Location message that indicates an "updateProcedure".

The indicator "Location Information Confirmed in HLR" is set to "Confirmed" at the following event:

- Successful completion of the Update GPRS Location procedure to the HLR.

The indicator "VLR-Reliable" indicates whether the VLR serving the MS has performed a restart.

The indicator "VLR-Reliable" is set to the value "false" when the SGSN receives a Reset indication message from the VLR serving the MS if the MS is attached to both GPRS and non-GPRS services. The indicator "VLR-Reliable" is set to the value "true" when the SGSN receives a confirmation from a VLR that a location update procedure to the affected VLR has been successfully performed.

The indicator "SGSN-Reset" indicates whether the SGSN has recently experienced a restart.

The indicator "SGSN-Reset" is set to the value "true" when the SGSN suffers a restart. This indicator is unique per SGSN. The indicator "SGSN-Reset" is set to the value "false" after a certain time specified by the operator. The value of the timer controlling the reset of the "SGSN-Reset" indicator shall be longer than the periodic routing area update timer value used by the MSs.

Also the following two restoration indicators may be provided in the SGSN for each IMSI record: "Subscriber Data Confirmed by CSS" and "Location Information Confirmed by CSS".

The indicator "Subscriber Data Confirmed by CSS" indicates whether the CSG subscriber data set for the roaming mobile station held by the SGSN is consistent with that held by the CSS.

The indicator "Subscriber Data Confirmed by CSS" is set to the initial value "Not Confirmed" at any of the following events:

- The SGSN receives a Routing Area Update request or an IMSI- and/or GPRS Attach request for a roaming MS for which the SGSN does not have an IMSI record.
- The SGSN receives a "Cancel VCSG Location Request" message from the CSS after the SGSN restart if the roaming MS attached to the macro cell after the SGSN restart.

The indicator "Subscriber Data Confirmed by CSS" is set to "Confirmed" at the following event:

- The SGSN successfully performs an "Update VCSG Location" to the CSS.
- The SGSN receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the SGSN restart if the roaming MS attached to the macro cell after the SGSN restart.

The indicator "Location Information Confirmed by CSS" indicates whether the SGSN address for the roaming mobile station registered is confirmed by the CSS.

The indicator "Location Information Confirmed by CSS" is set to "Not Confirmed" at any of the following events:

- The SGSN receives a Routing Area Update request or an IMSI- and/or GPRS Attach request for a roaming MS for which the SGSN has no IMSI record;
- The SGSN receives a "Reset" message from the CSS with which the roaming MS is registered.
- The SGSN receives a "Cancel VCSG Location Request" message from the CSS after the SGSN restart if the roaming MS attached to the macro cell after the SGSN restart. The indicator "Location Information Confirmed by CSS" is set to "Confirmed" at the following event:

- Successful completion of the "Update VCSG Location" procedure to the CSS.
- The SGSN receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the SGSN restart if the roaming MS attached to the macro cell after the SGSN restart.

3.4 Restoration Indicators in the MME

Two restoration indicators are provided in the MME for each IMSI record: "Subscriber Data Confirmed by HSS" and "Location Information Confirmed in HSS".

The indicator "Subscriber Data Confirmed by HSS" indicates whether the subscriber data set for the mobile station held by the MME is consistent with that held by the HSS.

The indicator "Subscriber Data Confirmed by HSS" shall be set to the initial value "Not Confirmed" when the MME receives a Tracking Area Update request or an Attach request for an UE for which the MME does not have an IMSI record.

The indicator "Subscriber Data Confirmed by HSS" shall be set to "Confirmed" at the following event:

- The MME successfully performs an Update Location to the HSS;

The indicator "Location Information Confirmed in HSS" indicates whether the HSS's record of the MME address for the UE is confirmed by radio contact.

The indicator "Location Information Confirmed in HSS" shall be set to "Not Confirmed" at any of the following events:

- The MME receives a Tracking Area Update request or an Attach request for an UE for which the MME has no IMSI record;

- The MME receives a "Reset" message from the HSS with which the UE is registered;

The indicator "Location Information Confirmed in HSS" shall be set to "Confirmed" at the following event:

- Successful completion of the Update Location procedure to the HSS.

Also the following two restoration indicators may be provided in the MME for each IMSI record: "Subscriber Data Confirmed by CSS" and "Location Information Confirmed by CSS".

The indicator "Subscriber Data Confirmed by CSS" indicates whether the CSG subscriber data set for the roaming UE held by the MME is consistent with that held by the CSS.

The indicator "Subscriber Data Confirmed by CSS" is set to the initial value "Not Confirmed" at any of the following events:

- The MME receives a Tracking Area Update request or an Attach request for a roaming UE for which the MME has no IMSI record;
- The MME receives a "Cancel VCSG Location Request" message from the CSS after the MME restart if the roaming UE attached to the macro cell after the MME restart.

The indicator "Subscriber Data Confirmed by CSS" is set to "Confirmed" at the following event:

- The MME successfully performs an "Update VCSG Location" to the CSS.
- The MME receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the MME restart if the roaming UE attached to the macro cell after the MME restart.

The indicator "Location Information Confirmed by CSS" indicates whether the MME address for the roaming UE registered is confirmed by the CSS.

The indicator "Location Information Confirmed by CSS" is set to "Not Confirmed" at any of the following events:

- The MME receives a Tracking Area Update request or an Attach request for a roaming UE for which the MME has no IMSI record;
- The MME receives a "Reset" message from the CSS with which the roaming UE is registered.
- The MME receives a "Cancel VCSG Location Request" message from the CSS after the MME restart if the roaming UE attached to the macro cell after the MME restart.

The indicator "Location Information Confirmed by CSS" is set to "Confirmed" at the following event:

- Successful completion of the "Update VCSG Location" procedure to the CSS.
- The MME receives an "Insert/Delete VCSG Subscription Data Request" message from the CSS after the MME restart if the roaming UE attached to the macro cell after the MME restart.

3.5 Restoration Indicator in the ProSe Function

One restoration indicator is provided in the ProSe Function for each IMSI record: "Subscriber Data Confirmed by HSS".

The indicator "Subscriber Data Confirmed by HSS" indicates whether the subscriber data set for the user equipment held by the ProSe Function is consistent with that held by the HSS.

The indicator "Subscriber Data Confirmed by HSS" shall be set to "Confirmed" at the following event:

- Successful retrieval of ProSe subscriber information from the HSS.

The indicator "Subscriber Data Confirmed by HSS" shall be set to "Not Confirmed" at the following event:

- The ProSe Function receives a request for ProSe Service from an UE for which the ProSe Function does not have associated UE context;
- The ProSe Function receives a "Reset" message from the HSS with which the UE is registered.

3.6 Restoration Indicator in the V2X Control Function

One restoration indicator is provided in the V2X Control Function for each IMSI record: "Subscriber Data Confirmed by HSS".

The indicator "Subscriber Data Confirmed by HSS" indicates whether the subscriber data set for the user equipment held by the V2X Control Function is consistent with that held by the HSS.

The indicator "Subscriber Data Confirmed by HSS" shall be set to "Confirmed" at the following event:

- Successful retrieval of V2X subscriber information from the HSS.

The indicator "Subscriber Data Confirmed by HSS" shall be set to "Not Confirmed" at the following event:

- The V2X Control Function receives a request for V2X Service from an UE for which the V2X Control Function does not have associated UE context;
- The V2X Control Function receives a "Reset" message from the HSS with which the UE is registered.

4 Restoration of data in the VLR

The effect on service of failure of a VLR is different from the effect of failure of an HLR. The procedures for restoration of a VLR and an HLR are therefore different.

4.0 VLR Failure with Restart

When a VLR fails, all its associations with SGSNs affected by the failure become invalid and may be deleted. Based on configuration data, the MSC/VLR sends a BSSAP+ Reset message to each of its associated SGSNs. The SGSNs mark all associations containing the restarted VLR as invalid. For an MS that is both GPRS-attached and IMSI-attached, the SGSN may then:

- upon reception of a combined routing area update request, perform immediately the location update for non-GPRS services procedure towards the VLR; or
- upon reception of a periodic routing Area update request, dependent on network configuration and operator policy,
 - return a Detach Request (Detach Type) message with the Detach Type set to IMSI Detach immediately after the completion of the periodic routing area update procedure, in order to request the MS to perform a combined routing area update, , or
 - perform immediately the location update for non-GPRS services procedure towards the VLR.

When a VLR fails, all its associations with MMEs affected by the failure become invalid and may be deleted. The VLR and MME shall behave as per subclause 4.2.10. For a UE that is attached to both EPS and non-EPS services, the MME may then:

- upon reception of a combined tracking area update request, perform immediately the location update for non-EPS services procedure towards the VLR; or
- upon reception of a periodic tracking area update request, dependent on network configuration and operator policy,
 - request the UE to re-attach to non-EPS services immediately after the completion of the periodic tracking area update procedure; or
 - perform immediately the location update for non-EPS services procedure towards the VLR.

4.0a VLR Failure without Restart

If the VLR serving a MS that is attached for non-GPRS services is no longer in service, the SGSN may:

- upon reception of a combined routing area update request, perform immediately the location update for non-GPRS services procedure towards an alternative (available) VLR; or
- upon reception of a periodic routing area update request, dependent on network configuration and operator policy,
 - request the MS to re-attach to non-GPRS services immediately after the completion of the periodic routing area update procedure and then select an alternative (available) VLR to serve the UE for non-GPRS services during the subsequent combined routing area update procedure; or
 - perform immediately the location update for non-GPRS services procedure towards an alternative (available) VLR.

See 3GPP TS 29.018 [7].

If the VLR serving a UE that is attached for non-EPS services is no longer in service, the MME may :

- upon reception of a combined tracking area update request, perform immediately the location update for non-EPS services procedure towards an alternative (available) VLR; or
- upon reception of a periodic tracking area update request, dependent on network configuration and operator policy,
 - request the UE to re-attach to non-EPS services immediately after the completion of the periodic tracking area procedure and then select an alternative (available) VLR to serve the UE for non-EPS services during the subsequent combined tracking area update procedure; or
 - perform immediately the location update for non-EPS services procedure towards an alternative (available) VLR.

Upon reception of an Uplink NAS Transport message from a UE that is attached for non-EPS service, if the VLR serving the UE is no longer in service, the MME may request the UE to re-attach to non-EPS services and then select an alternative available VLR to serve the UE for MO SMS and other CS services during the subsequent combined TA / LA update procedure.

See 3GPP TS 29.118 [14].

NOTE: How an SGSN or MME detects that a VLR is no longer in service is implementation specific, e.g. if there are no more SCTP associations in service with that VLR for a given period.

4.1 Restart of the VLR

When a VLR restarts after a failure, all IMSI records affected by the failure are erased.

There will be no subscriber data or location information stored for an affected mobile station until after the VLR has received either a "Provide Roaming Number" request or an "Update location Area" request for that mobile station.

The VLR causes all affected TMSIs and all affected LMSIs to become invalid. "Invalid" in this context means that the TMSI and LMSI can no longer be regarded as accurate. The term is used to avoid unnecessary constraints on the implementation.

On receipt of either a "Provide Roaming Number" request or an "Update Location Area" request, restoration of subscriber data in the VLR is triggered individually for each IMSI record as described below.

4.2 Restoration Procedures

4.2.0 General

The objective of the restoration procedure is to handle all traffic for each mobile subscriber correctly. In order to meet this objective, the procedure must make the subscriber data in the VLR consistent with that in the HLR or in the CSS, and make the location information in the HLR and VLR or the location information in the CSS and VLR reflect accurately the current location of the MS.

4.2.1 Incoming Call

a) Send Routing Information (GMSC->HLR):

The HLR sends "Provide Roaming Number" to the VLR as for normal operation. The LMSI is updated by the VLR when the VLR requests the transfer of subscriber data from the HLR using the "Restore Data" operation.

b) Provide Roaming Number (HLR->VLR):

- Regardless of whether the VLR has an IMSI record corresponding to the IMSI in the "Provide Roaming Number", it returns an MSRN. If no IMSI record exists, the VLR creates a skeleton IMSI record, sets the indicators "Subscriber Data Confirmed by Radio Contact" and "Subscriber Data Confirmed by HLR" to "Not Confirmed" and (if IMSI Attach is used) marks the IMSI as attached. If the VLR serves two or more MSCs, the VLR sets the indicator "Location Information Confirmed in HLR" to "Not Confirmed". Otherwise, if the VLR serves only one MSC, the indicator "Location Information Confirmed in HLR" is set to the initial value "Confirmed". Also the VLR may set the indicators "Subscriber Data Confirmed by CSS" and "Location Information Confirmed by CSS" to "Not Confirmed".
- If the indicator "Subscriber Data Confirmed by HLR" is "Not Confirmed" the VLR requests authentication data, if required and still not available and subscriber data from the HLR. When the dialogue that covers the subscriber data retrieval procedure is completed successfully, the VLR sets the indicator "Subscriber Data Confirmed by HLR" to "Confirmed". The indicators "Confirmed by Radio Contact" and "Location Information Confirmed in HLR" remain unchanged.
- If the IMSI record for the MS is marked "Subscriber Data Confirmed by HLR" but "Not Confirmed by Radio Contact" the operator may choose an appropriate method to limit the number of "Search for MS" procedures for that MS.

c) Send Information for I/C Call Setup (MSC->VLR)

- If the VLR has no IMSI record, or if the record is marked "Subscriber Data Not Confirmed by HLR" the VLR returns a "System Failure" error.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Not Confirmed by Radio Contact", the VLR handles the request in the normal way, except that the "Search for MS" procedure is used instead of the "Page MS" procedure.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Confirmed by Radio Contact", the VLR handles the request in the normal way; for this MS, VLR restoration is complete.
- The state of the indicator "Location Information Confirmed in HLR" does not affect the "Send Information for I/C Call Setup" procedure.

d) Process Access Request in Response to Search (MSC->VLR):

- If the MS responds to paging, the MSC sends a positive response to the search request and a "Process Access Request" to the VLR. After successful authentication, if required, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed", sets the location area information for the MS, and handles the request in the normal way.
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".
- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" the VLR shall start an "Update VCSG Location" procedure to the CSS if the roaming MS is still in the CSG cell. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this MS, VLR restoration is complete.

4.2.2 Mobile Terminated Short Message

a) Send Routing Information for MT SMS (SMS-GMSC->HLR):

The HLR returns the MSC number as for normal operation.

b) Send Information for MT SMS (MSC->VLR) - MAP version 2:

- If the VLR has no IMSI record, or if the record is marked "Subscriber Data Not Confirmed by HLR", the VLR proceeds as follows:
 - the VLR returns an "Unidentified Subscriber" error. This causes the MSC to report a short message delivery failure, with cause "Unidentified Subscriber", to the SMS gateway MSC. The Gateway MSC sends a "Report SM Delivery Status" request, with a cause of "Absent Subscriber", to the HLR. This causes the HLR to set the "Mobile Station Not Reachable Flag" for the MS, as described in Technical Specifications 3GPP TS 23.040 [4] and 3GPP TS 29.002 [6]; or
 - the VLR performs the data restoration procedure as specified in subclause 4.2.1 for an incoming call and delay the mobile terminating SMS until the data restoration procedure is complete. During the data restoration procedure, the HLR shall send to the VLR the MME name or/and the SGSN Number if the subscriber is registered on this VLR and is registered to EPS or/and GPRS services respectively.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Not Confirmed by Radio Contact", the VLR handles the request in the normal way, except that the "Search for MS" procedure is used instead of the "Page MS" procedure.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Confirmed by Radio Contact", the VLR handles the request in the normal way; for this MS, VLR restoration is complete.
- The state of the indicator "Location Information Confirmed in HLR" does not affect the "Send Information for MT SMS" procedure.

c) Send Information for I/C Call Setup (MSC->VLR) - MAP version 1:

- If the VLR has no IMSI record, or if the record is marked "Subscriber Data Not Confirmed by HLR", the VLR proceeds as follows:
 - the VLR returns a "System Failure" error. This causes the MSC to report a short message delivery failure, with cause "System Failure", to the SMS gateway MSC; or
 - the VLR performs the data restoration procedure as specified in subclause 4.2.1 for an incoming call and delay the mobile terminating SMS until the data restoration procedure is complete. During the data restoration procedure, the HLR shall send to the VLR the MME name or/and the SGSN Number if the subscriber is registered on this VLR and is registered to EPS or/and GPRS services respectively.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Not Confirmed by Radio Contact", the VLR handles the request in the normal way, except that the "Search for MS" procedure is used instead of the "Page MS" procedure.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Confirmed by Radio Contact", the VLR handles the request in the normal way; for this MS, VLR restoration is complete.
- The state of the indicator "Location Information Confirmed in HLR" does not affect the "Send Information for MT SMS" procedure.

d) Process Access Request in Response to Search (MSC->VLR):

- If the MS responds to paging, the MSC sends a positive response to the search request and a "Process Access Request" to the VLR. After successful authentication, if required, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed", sets the location area information for the MS, and handles the request in the normal way.
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed, the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".

- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" the VLR shall start an "Update VCSG Location" procedure to the CSS if the roaming UE is still in the CSG cell. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this MS, VLR restoration is complete.

4.2.3 Mobile Terminating Location Request (MT-LR)

Receipt of an MT-LR for a target MS identified by its IMSI in a serving MSC during VLR restoration is supported by the procedures below.

a) Provide Subscriber Location (GMLC->MSC/VLR):

- If the VLR has no IMSI record, or if the record is marked "Subscriber Data Not Confirmed by HLR" the VLR returns an "Unidentified Subscriber" error. This causes the MSC to report a location failure, with cause "Unidentified Subscriber", to the GMLC.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Not Confirmed by Radio Contact", the VLR handles the request in the normal way, except that the "Search for MS" procedure is used instead of the "Page MS" procedure when paging for the MS.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Confirmed by Radio Contact", the VLR handles the request in the normal way; for this MS, VLR restoration is complete.
- The state of the indicator "Location Information Confirmed in HLR" does not affect the "Provide Subscriber Location" procedure.

b) Process Access Request in Response to Search (MSC->VLR):

- If the MS responds to paging, the MSC sends a positive response to the search request and a "Process Access Request" to the VLR. After successful authentication, if required, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed", sets the location area information for the MS, and handles the request in the normal way.
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed, the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".
- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" and the roaming MS is still in the CSG cell, the VLR shall start an "Update VCSG Location" procedure to the CSS. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this MS, VLR restoration is complete.

4.2.4 Incoming LCS Information Request (GSM only)

Receipt of an incoming BSSMAP-LE LMU Connection Request from an SMLC directed to a specific Type A LMU is supported by the procedures below.

a) Request associated with an LMU (SMLC->MSC/VLR):

- If the VLR has no IMSI record, or if the record is marked "Subscriber Data Not Confirmed by HLR", the VLR returns an "Unidentified Subscriber" error.

- If the VLR has an IMSI record for an LMU marked "Subscriber Data Confirmed by HLR" and "Not Confirmed by Radio Contact", the VLR handles the request in the normal way, except that the "Search for MS" procedure is used instead of the "Page MS" procedure when paging for the LMU.
- If the VLR has an IMSI record marked "Subscriber Data Confirmed by HLR" and "Confirmed by Radio Contact", the VLR handles the request in the normal way. For this LMU, data restoration is complete.
- The state of the indicator "Location Information Confirmed in HLR" does not affect the incoming LMU Connection Request.

b) Process Access Request in Response to Search (MSC->VLR):

- If the LMU responds to paging, the MSC sends a positive response to the search request and a "Process Access Request" to the VLR. After successful authentication, if required, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed", sets the location area information for the LMU, and handles the request in the normal way.
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed, the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".
- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" and the roaming MS is still in the CSG cell, the VLR shall start an "Update VCSG Location" procedure to the CSS. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this LMU, VLR restoration is complete.

4.2.5 Outgoing MS request

An outgoing request (MS originated call, mobile originated Short Message or call-independent supplementary service activity) from the MS causes the VLR to check its IMSI record for that MS.

- If the MS is unknown in this VLR (i.e. the VLR has no IMSI record for the MS) or there is an IMSI record marked "Subscriber Data Not Confirmed by HLR" the outgoing request is rejected with error cause "Unidentified Subscriber". This causes the MS to initiate the location registration procedure described below.
- If the VLR has an IMSI record for the MS marked "Subscriber Data Confirmed by HLR" the request is handled in the normal way, and after any necessary authentication and/or IMEI checking the record is marked "Confirmed by Radio Contact".
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".
- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" and the roaming MS is still in the CSG cell, the VLR shall start an "Update VCSG Location" procedure to the CSS. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this MS, VLR restoration is complete.

4.2.6 Outgoing LMU Request (GSM only)

An outgoing request (CM ServiceRequest) for LCS from a Type A LMU causes the VLR to check its IMSI record for that LMU.

- If the LMU is unknown in this VLR (i.e. the VLR has no IMSI record for the LMU) or there is an IMSI record marked "Subscriber Data Not Confirmed by HLR" the outgoing request is rejected with error cause "Unidentified Subscriber". This causes the LMU to initiate the location registration procedure described below.
- If the VLR has an IMSI record for the MS marked "Subscriber Data Confirmed by HLR", the request is handled in the normal way, and after any necessary authentication and/or IMEI checking the record is marked "Confirmed by Radio Contact".
- The VLR checks the indicator "Location Information Confirmed in HLR". If it indicates "Not Confirmed" the VLR starts an "Update Location" procedure to the HLR. When this procedure is successfully completed the VLR sets the indicator "Location Information Confirmed in HLR" to "Confirmed".
- If the MS is roaming, the VLR checks the indicators "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS". If either of them indicates "Not Confirmed" the VLR and the roaming MS is still in the CSG cell, may start an "Update VCSG Location" procedure to the CSS. When this procedure is successfully completed the VLR sets the indicator "Subscriber Data Confirmed by CSS" if the CSS has the corresponding valid CSG subscription data and "Location Information Confirmed by CSS" to "Confirmed".

For this LMU, VLR restoration is complete.

4.2.7 Location Updating or IMSI Attach

A location registration request (location updating or IMSI attach) from an MS causes the VLR to check its IMSI record for that MS.

- If the MS is unknown in this VLR (i.e. the VLR has no IMSI record for the MS) the VLR creates a skeleton IMSI record for the MS and sets the indicators "Confirmed by Radio Contact", "Location Information Confirmed in HLR", "Subscriber Data Confirmed by HLR", "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" to "Not Confirmed". If authentication is required, the VLR retrieves authentication data. When the radio contact with the Mobile Station is authenticated, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed". The VLR then performs an "Update Location" to the HLR. If this is successful, the VLR sets the indicators "Location Information Confirmed in HLR" and "Subscriber Data Confirmed by HLR" to "Confirmed". For this MS, VLR restoration is complete. If the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the VLR may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the VLR sets the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" to "Confirmed" if the CSS has the corresponding valid CSG subscription data.
- If the VLR has an IMSI record for the MS, after successful authentication, if required, the VLR sets the indicator "Confirmed by Radio Contact" to "Confirmed". If the record is marked "Location Information Not Confirmed in HLR" or "Subscriber Data Not Confirmed by HLR" the VLR performs an "Update Location" to the HLR. If this is successful, the VLR sets the indicators "Location Information Confirmed in HLR" and "Subscriber Data Confirmed by HLR" to "Confirmed". For this MS, VLR restoration is complete. If the record is marked "Location Information Not Confirmed by CSS" or "Subscriber Data Not Confirmed by CSS" if the CSS has the valid CSG subscription data, and the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the VLR may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the VLR sets the indicators "Location Information Confirmed by CSS" if the CSS has the valid CSG subscription data and "Subscriber Data Confirmed by CSS" to "Confirmed".

4.2.8 Use of TMSI

After the VLR has restarted but before the next authenticated radio contact the TMSI known by the MS is invalid, as it was allocated before the VLR restarted. The VLR therefore uses the IMSI to identify the MS on the first radio contact during restoration.

- A VLR which initiates a "Search for Subscriber" procedure uses the IMSI to identify the MS.
- If an MS identifies itself by a TMSI in a "Location Registration" request, the VLR proceeds as follows:
 - a) The VLR checks the location area identity (LAI) of the previous location area sent by the MS. If this LAI is in a VLR different from the current one, the request is handled in the normal way.

b) If the LAI is in the current VLR, the status of the TMSI is checked:

- If the TMSI was allocated after the VLR restarted, and corresponds to a valid IMSI record, the request is handled as described in subclause 4.2.7.
- If the TMSI was allocated before the VLR restarted, or does not correspond to a valid IMSI record, the VLR requests the IMSI from the MS. If the MS returns an IMSI the VLR proceeds as described in subclause 4.2.7. If the MS does not return an IMSI the network aborts the location registration procedure.
- If an MS identifies itself by a TMSI in an outgoing MS request, the VLR proceeds as follows:
- If the TMSI was allocated after the VLR restarted, and corresponds to a valid IMSI record, the request is handled as described in subclause 4.2.5.
- If the TMSI was allocated before the VLR restarted, or does not correspond to a valid IMSI record, the VLR requests the IMSI from the MS. If the MS returns an IMSI the VLR proceeds as described in subclause 4.2.5. If the MS does not return an IMSI the network aborts the outgoing request.

4.2.9 SGSN associations

Based on configuration data, "Reset" messages are sent on the Gs-interface to the SGSNs in the Location Areas served by the VLR as described in the 3GPP TS 29.018 [7]. The SGSNs mark all associations with the VLR as unreliable by setting the restoration indicator "VLR-Reliable" to "False" for the UEs served by that VLR. The associations will be re-initiated one by one by the SGSN at the next Routing Area update or combined RA/LA update from each UE.

4.2.10 MME associations

Based on configuration data, "Reset" messages are sent on the SGs-interface to the MMEs by the VLR as described in the 3GPP TS 29.118 [14]. The MMEs mark all associations with the VLR as unreliable by setting the restoration indicator "VLR-Reliable" to "False" for the UEs served by that VLR. The associations will be re-initiated one by one by the MME at the next Tracking Area update or combined TA/LA update from each UE.

5 Restoration of data in the HLR/HSS

The loss or corruption of subscriber data in the HLR/HSS has an impact not only in the HLR/HSS's own PLMN but also on the service for its mobiles in other PLMNs. Restoration of the data in the HLR/HSS requires co-operation from all the VLRs, SGSNs and MMEs at which its mobiles are registered.

5.1 Restart of the HLR/HSS

The periodic backup of HLR/HSS data to non-volatile storage is mandatory.

When an HLR/HSS restarts after failure it shall perform the following actions for the subscriber data records that have been affected by the HLR/HSS fault:

- reload all data from the non-volatile back-up;
- reset all "MS Purged" flags;
- mark each subscriber record "SS Check Required" by setting the "Check SS" indicator if the "Forward Check SS Indication" service is implemented;
- send a "Reset" message to each VLR where one or more of its MSs are registered. This causes each VLR concerned to mark each relevant subscriber record "Location Information Not Confirmed in HLR", and
- send a "Reset" message to each SGSN where one or more of its MSs are registered. This causes each SGSN to mark each relevant MM context "Location Information Not Confirmed in HLR".
- send a "Reset" message to each MME where one or more of its UEs are registered. This causes each MME to mark each relevant MM context "Location Information Not Confirmed in HSS".

- send a "Reset" message to each ProSe Function (see 3GPP TS 23.303 [33]), where one or more of its UEs are registered for ProSe Services. This causes each ProSe Function to mark each relevant UE context "Subscriber Data Not Confirmed by HSS".
- send a "Reset" message to each V2X Control Function (see 3GPP TS 23.285 [40]), where one or more of its UEs are registered for V2X Services. This causes each V2X Control Function to mark each relevant UE context "Subscriber Data Not Confirmed by HSS".

5.2 Procedures During Restoration

5.2.1 Mobile terminated call

If the VLR receives a "Process Access Request" request in response to a "Page" or "Search for MS" operation, after successful authentication, if required, it checks the indicator "Location Information Confirmed in HLR". If this indicates "Not Confirmed" the VLR triggers an "Update Location" to the HLR as described in subclause 4.2.1.d).

When the HLR receives the "Update Location" request it stores the VLR number, MSC number and LMSI in the subscriber record as for normal operation.

If the "Forward Check SS Indication" service is implemented, the HLR checks the indicator "Check SS". If this indicates "Check Required", after successful completion of the subscriber data retrieval procedure that ran embedded in the "Update Location" procedure the HLR sends a "Forward Check SS Indication" to the VLR and marks the subscriber record "Check Not Required". When the VLR receives the "Forward Check SS Indication" request it forwards an indication to the MS to alert the user that supplementary service parameters should be checked.

5.2.2 Mobile Originated Activity for CS

When the VLR receives a request from an MS (MS originated call, mobile originated Short Message, call-independent supplementary service activity or location registration request) whose IMSI record is marked "Location Information Not Confirmed in HLR", it will perform an "Update Location" to the HLR as described in subclauses 4.2.5 and 4.2.7 above.

When the HLR receives an "Update Location" request from the VLR, it proceeds as described in subclause 5.2.1.

5.2.3 Mobile Originated Activity for ProSe

When the ProSe Function receives a request for ProSe Service from a UE whose associated context is marked as "Subscriber Data Not Confirmed by HSS", it shall initiate a "ProSe Subscriber Information Retrieval" request to the HSS as described in the 3GPP TS 29.344 [34].

When the HSS receives a "ProSe Subscriber Information Retrieval" request from the ProSe Function, it shall proceed as described in the 3GPP TS 29.344 [34].

5.2.4 Procedures in the SGSN

Upon receipt of a HLR/HSS reset, the SGSN shall mark each relevant MM contexts as invalid and shall set the Non-GPRS Alert Flag (NGAF) if an SGSN - MSC/VLR association exists. After detection of any activity (either signalling or data) from a marked MS or any other implementation dependent trigger for a marked MS in PMM-CONNECTED state with Direct tunnel, the SGSN performs an update location to the HLR/HSS as in the attach or inter-SGSN RA update procedures and, if NGAF is set, the procedure of "Non-GPRS Alert" is followed (see subclause 7 in 3GPP TS 29.018 [7]).

The update location procedure and the procedure towards the VLR may be delayed by the SGSN for a maximum operator configuration-dependent time period to avoid high signalling load.

5.2.5 Procedures in the MME

Upon receipt of a HSS reset, the MME shall mark each relevant MM contexts as invalid and shall set Non-EPS Alert Flag (NEAF) if an MME - MSC/VLR association exists. After detection of any activity (either signalling or data) from a marked UE or any other implementation dependent trigger for a marked UE in ECM-CONNECTED state, the MME

performs an update location to the HSS as in the attach or inter-MME TA update procedures and, if NEAF is set, the procedure of "NON-EPS Alert" is followed (see subclause 5.3 in 3GPP TS 29.118 [14]).

The update location procedure and the procedure towards the VLR may be delayed by the MME for a maximum operator configuration-depending time period to avoid high signalling load.

5.2.6 Mobile Originated Activity for V2X

When the V2X Control Function receives a request for V2X Service from a UE whose associated context is marked as "Subscriber Data Not Confirmed by HSS", it shall initiate a "V2X Subscriber Information Retrieval" request to the HSS as described in the 3GPP TS 29.388 [41].

When the HSS receives a "V2X Subscriber Information Retrieval" request from the V2X Control Function, it shall proceed as described in the 3GPP TS 29.388 [41].

6 Periodic location updating

The time taken to confirm the location of an MS after location register failure is governed by the frequency with which the MS establishes radio contact with the network. The location information for an MS which remains silent for a long time will remain doubtful for a long time.

A method of reducing this time is to require the MS to establish radio contact with the network at intervals, purely to confirm its location, if the MS does not move to a new location area (which would lead to a normal location registration) or respond to paging for a mobile terminated call or request a mobile originated call or call-independent supplementary service activity.

The interval between successive periodic location updatings is controlled by a timer in the MS; this timer is reset to its initial value at the end of each successfully established radio contact between the MS and the network.

The use of the periodic location update timer is described in 3GPP TS 23.122 [27].

7 Periodic routeing area updating

All GPRS-attached MSs, except MSs in class-B mode of operation engaged in CS communication, shall perform periodic RA updates. For MSs that are both IMSI-attached and GPRS-attached, the periodic updates depend on whether the Gs interface is installed or not:

- If the Gs interface is installed, periodic RA updates shall be performed, and periodic LA updates shall not be performed. If the SGSN has the indicator "VLR-reliable" set to 'false' the SGSN shall perform a location area update procedure towards the VLR
- If the Gs interface is not installed, both periodic RA updates and periodic LA updates shall be performed independently. RA updates are performed via the Gb interface, and LA updates are performed via the A interface.

The periodic routeing area update is described in 3GPP TS 23.060 [5].

8 Stand-alone operation of the VLR

In a 2G authentication regime, triplets, regardless of its nature (generated in a 2G AuC or derived from quintuplets in a 3G VLR or a 3G HLR), may be reused when no unused authentication triplets are available in the VLR for an IMSI record. It is an operator option to define how many times an authentication triplet may be reused in the VLR.

In a 3G authentication regime, quintuplets, regardless of its nature (generated in a 3G AuC or derived from triplets in a 3G VLR), shall not be reused when no unused authentication quintuplets are available in the VLR for an IMSI record.

If the Update Location response contains an error different from "Unknown Subscriber" or "Roaming Not Allowed" or if there is a parameter problem (e.g. no HLR number included), no error shall be indicated to the MSC and the IMSI

record in the VLR shall not be affected, provided that the associated "Subscriber Data Confirmed by HLR" indicator is in the "Confirmed" status.

9 Stand-alone operation of the SGSN

In a 2G authentication regime, triplets, regardless of their nature (generated in a 2G AuC or derived from quintuplets in a 3G SGSN or a 3G HLR), may be reused when no unused authentication triplets are available in the SGSN for an IMSI record. It is an operator option to define how many times an authentication triplet may be reused in the SGSN.

In a 3G authentication regime, quintuplets, regardless of their nature (generated in a 3G AuC or derived from triplets in a 3G SGSN), shall not be reused when no unused authentication quintuplets are available in the SGSN for an IMSI record.

9A Stand-alone operation of the MME

In a E-UTRAN authentication regime, EPS authentication vectors shall not be reused when no unused EPS authentication vectors are available in the MME for an IMSI record.

10 Restoration of data in the GGSN

10.0 GGSN failure

When a GGSN fails, all its PDP contexts affected by the failure become invalid and may be deleted. GGSN storage of subscriber data is volatile.

When the GGSN receives a GTP-U PDU for which no PDP context exists, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (the SGSN or, if Direct Tunnel is established, the RNC).

The GGSN should ensure as far as possible that previously used TEID values are not immediately reused after a GGSN restart, in order to avoid inconsistent TEID allocation throughout the network.

10.1 Restart of the GGSN

After a GGSN restart, all the PDP contexts, the MBMS UE contexts, and the MBMS Bearer contexts stored in the GGSN and affected by the restart become invalid and may be deleted.

When the SGSN detects a restart in a GGSN (see clause 18 "GTP-C based restart procedures") with which it has one or more PDP contexts activated, it shall deactivate all these PDP contexts and request the MS to reactivate them. When the SGSN detects a restart in a GGSN with which it has MBMS Bearer context(s) and/or MBMS UE context(s), it shall delete all these MBMS Bearer context(s) and/or MBMS UE context(s).

10.2 Restoration Procedures

10.2.0 General

The GGSN will receive the SGSN restart counters in GTPv1 echo response from the SGSN. When a GGSN detects that a peer SGSN has restarted it shall delete all PDP context(s), MBMS UE context(s), MBMS Bearer context(s) associated with the peer node that failed as well as freeing any internal GGSN resources associated with those PDP context(s), MBMS UE context(s) and MBMS Bearer context(s). The GGSN may optionally perform other implementation specific actions such as messages to clear other external resources (e.g. PCC messages).

If the GGSN needs to send a request for IP-CAN Session Modification procedure towards a PCRF which is known to have restarted since the IP-CAN session establishment, the GGSN may discard the request and may tear down all the PDP context(s) associated with the PDP address of the IP-CAN session, based on operator policy, by initiating a PDP

Context Deactivation procedure towards the SGSN with the cause set to "Reactivation requested". This leads the UE to initiate PDP Context Activation procedure for the same APN. Emergency sessions should not be torn down.

NOTE: The procedure above just enables to clean up all the PDP Context(s) associated with the PDP address of the IP-CAN session, affected by the PCRF failure when a specific interaction with the PCRF is required. Prior to that interaction, PCC controlled services can not be provided to the UE.

10.2.1 Mobile terminated transmission

When the GGSN receives a mobile terminated PDU for which no valid PDP context exists the GGSN discards the received PDU and may also return an appropriate Error message depending on the protocol used. No further actions are performed by the GGSN. Alternatively, if the GGSN has static PDP information about the PDP address, the GGSN may try to deliver the PDU by initiating the Network-Requested PDP Context Activation procedure (see 3GPP TS 23.060 [5]).

10.2.2 Mobile originated transmission

When the GGSN receives a tunnel PDU for which no PDP context exists it discards the tunnel PDU and sends an Error indication message to the originating SGSN. The SGSN deactivates the PDP context and sends an Error indication to the MS. The MS may then re-activate the PDP context.

11 Restoration of data in the SGSN

11.0 SGSN Failure

11.0.1 Gn/Gp SGSN failure

When an SGSN fails, it deletes all MM and PDP contexts affected by the failure. SGSN storage of subscriber data is volatile. Based on configuration data, the SGSN may send a Reset message to each of its associated VLRs. If a Reset message is sent, the VLR may mark all associations containing the restarted SGSN as unreliable. See 3GPP TS 29.018 [7]. In the case of optional CAMEL interaction the failing SGSN shall invoke the CAMEL-GPRS-Exception procedure towards the GSM-SCFs.

If data or signalling, except GPRS attach and RA update, is received in an SGSN from an MS for which no MM context exists in the SGSN, the SGSN shall discard the data or signalling.

If an RA update request is received in an SGSN from an MS for which no MM context exists in the SGSN, or in the old SGSN for the inter-SGSN RA update case, the SGSN shall reject the RA update with an appropriate cause. In order to remain GPRS-attached, the MS shall then perform a new GPRS attach and should (re-)activate PDP contexts.

If a service request is received in a 3G-SGSN from an MS for which no MM context exists in the 3G-SGSN, the 3G-SGSN shall reject the service request with an appropriate cause. In order to remain GPRS-attached, the MS shall then perform a new GPRS attach and should (re-) activate PDP contexts.

NOTE: In some cases, user interaction may be required, and then the MS cannot (re-)activate the PDP contexts automatically.

When the SGSN receives a PDU Notification Request message for which no MM context exists, the SGSN returns a PDU Notification Response message to the GGSN with an appropriate cause (see clause "Unsuccessful Network-Requested PDP Context Activation Procedure" in 3GPP TS 23.060 [5]), and the SGSN may search the MS by paging with the IMSI in the SGSN area. An MS that is paged for PS services with IMSI as the identifier shall perform a new GPRS attach and should (re-)activate PDP contexts.

When the SGSN receives a GTP-U PDU from the GGSN for which no PDP context exists, it shall discard the GTP-U PDU and send a GTP error indication to the originating GGSN.

When the SGSN receives a GTP-U PDU from the RNC for which no PDP context exists, the SGSN shall discard the GTP-U PDU and send a GTP error indication to the originating RNC.

When the SGSN receives a mobile-terminated SM from the SMS-GMSC for an IMSI unknown in the SGSN, it rejects the request.

When the SGSN receives a paging request over the Gs interface for an IMSI unknown in the SGSN and the SGSN has not completed recovery, the SGSN may page the MS for packet services with IMSI as identifier in the area specified by the location information provided by the MSC/VLR. If no such location information is provided, the SGSN may page the MS in the routing areas corresponding to that MSC/VLR. After the MS performs a combined GPRS attach, the SGSN may continue serving the Gs interface paging request.

11.0.2 SGSN Failure using S4

When the SGSN receives a GTP-U PDU from the Serving GW for which no Bearer context exists, it shall discard the GTP-U PDU and send a GTP error indication to the originating Serving GW.

When the SGSN receives a GTP-U PDU from the MBMS GW for which no MBMS Point to Point Bearer context exists, it shall discard the GTP-U PDU and send a GTP Error Indication to the originating MBMS GW.

An S4-SGSN and an SGW supporting the optional network triggered service restoration procedure shall behave as specified in clause 25.

When the S4-SGSN which does not support the optional network triggered service restoration procedure as specified in clause 25 receives a Downlink Data Notification message for which no MM context exists, the S4-SGSN returns a Downlink Data Notification Acknowledge message to the Serving GW with an appropriate cause. The Serving GW shall delete the related Bearer context related to S4-SGSN; and if there is no ISR associated MME recorded on the related Bearer context the Serving GW shall also notify the PDN GW to delete the Bearer context.

11.1 Restart of the SGSN

After an SGSN restart, the SGSN deletes all MM, PDP, MBMS UE, and MBMS Bearer contexts affected by the restart.

When the GGSN detects a restart in an SGSN (see clause 18 "GTP-C based restart procedures") with which it has PDP context(s) activated and/or MBMS UE context(s), it shall delete all these PDP context(s) and/or MBMS UE context(s). When the GGSN detects a restart in an SGSN with which it has any MBMS Bearer context, it shall not delete the MBMS bearer context unless all SGSNs connected to the GGSN restart.

When the MBMS GW detects a restart in an SGSN (see clause 18 "GTP-C based restart procedures") with which it has at least one MBMS Bearer context, the MBMS GW should re-establish the active MBMS bearer services affected by the SGSN restart by initiating MBMS Session Start procedure(s) towards the restarted SGSN (or an alternative SGSN in the same SGSN pool). The MBMS GW shall encode the contents of the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or as per the last MBMS Session Update Request received from the BM-SC if the original parameters were updated) with the following exceptions:

- the MBMS GW shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- the MBMS GW may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in UTRAN;
- the MBMS GW should set the estimated session duration to a value corresponding to the remaining duration of the session.

NOTE: If the MBMS GW receives an MBMS Session Update Request from the BM-SC during the SGSN restart, the contents of the MBMS Session Start Request sent to the SGSN after the SGSN restart can also differ from the parameters sent to the SGSN before its restart for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer).

The MBMS GW shall not delete the MBMS Bearer context unless all SGSNs/MMEs serving the MBMS bearer service and connected to the MBMS GW have restarted and the MBMS-GW does not support re-establishing MBMS bearer services after an SGSN restart.

11.2 Restoration Procedures

11.2.1 Mobile terminated user data transmission

When a Gn-SGSN receives a tunnel PDU for which no PDP context or MBMS Bearer Context exists it discards the tunnel PDU and sends an Error indication message to the originating GGSN.

An S4-SGSN and an SGW supporting the optional network triggered service restoration procedure shall behave as specified in clause 25.

11.2.2 Mobile terminated services requested by the MSC/VLR

When the SGSN receives a request for CS paging from an MSC/VLR for an IMSI unknown by the SGSN, if the "SGSN-Reset" indicator is set to "true", the SGSN sends the paging request with the location information provided by the VLR. If no such location information is provided, the SGSN should page for the MS in all the routing areas corresponding to that SGSN.

If the "SGSN-Reset" indicator is set to "false" and the IMSI is unknown or the MS is marked as GPRS or non-GPRS detached by the SGSN, the paging request is rejected.

If the "SGSN-Reset" indicator is set to "false" and the IMSI is known and the MS is marked as GPRS and is non-GPRS attached by the SGSN, the paging request shall be sent to the MS.

11.2.3 Mobile terminated SMS over GPRS

- a) Send Routing Information for MT SMS (SMS-GMSC -> HLR):

The HLR returns the SGSN number as for normal operation.

- b) Send Information for MT SMS:

- When the SGSN receives a mobile terminated SMS for an unknown MM context for the MS, or if the SGSN indicator "Subscriber Data Confirmed by HLR" is marked "Not Confirmed" it rejects the SMS request and returns a failure report with cause value "Unidentified Subscriber" to the SMS gateway MSC indicating unsuccessful delivery of the SMS. The Gateway MSC sends a "Report SM Delivery Status" request, with a cause of "Absent Subscriber", to the HLR. This causes the HLR to set the "Mobile Station Not Reachable for GPRS Flag" for the MS, as described in the Technical Specifications 3GPP TS 23.040 [4] and 3GPP TS 29.002 [6].
- If the SGSN has the indicator "Subscriber Data Confirmed by HLR" set to "Confirmed", the SGSN handles the SMS request in the normal way.

The state of the indicator "Location Information Confirmed in HLR" does not affect the Mobile Terminated SMS procedure.

11.2.4 Mobile originated Routing Area Updating or Attach

For attach, where the MS is unknown in the SGSN (i.e. the SGSN has no MM context for the MS) the SGSN creates an MM context for the MS and sets the indicators "Location Information Confirmed in HLR", "Subscriber Data Confirmed by HLR", "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" to "Not Confirmed". If authentication is required, the SGSN retrieves authentication data. The SGSN then performs an "Update GPRS Location" to the HLR. If this is successful, the SGSN sets the indicators "Location Information Confirmed in HLR" and "Subscriber Data Confirmed by HLR" to "Confirmed". If the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the SGSN may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the SGSN sets the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

For routing area update, where the MS is unknown in the SGSN (i.e. the SGSN has no MM context for the MS) or for inter-SGSN routing area update, where the MS is unknown in the old SGSN, the SGSN shall reject the RA update with an appropriate cause. In order to remain GPRS-attached, the MS shall then perform a new GPRS attach and should (re-)activate its PDP contexts.

If the SGSN has an MM context for the MS, and the indicators "Location Information Confirmed in HLR" or "Subscriber Data Confirmed by HLR" is set to "Not Confirmed" the SGSN performs an "Update GPRS Location" to the HLR. If this is successful, the SGSN sets the indicators "Location Information Confirmed in HLR" and "Subscriber Data Confirmed by HLR" to "Confirmed". If the indicators "Location Information Confirmed by CSS" or "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data is set to "Not Confirmed", and the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the SGSN may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the SGSN sets the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

If the SGSN has an MM context for the MS with the indicator "Subscriber Data Confirmed by HLR" marked "Confirmed" the originated transmission is handled in the normal way.

The SGSN retrieves subscriber data from the HLR by sending an "Update GPRS Location" request, which triggers one or more "Insert Subscriber Data" operations from the HLR.

The SGSN retrieves CSG subscriber data from the CSS by sending an "Update VCSG Location" request, which triggers one or more "Insert Subscriber Data" operations from the CSS if the CSS has the valid CSG subscription data.

11.2.5 Mobile originated LLC frame

If an SGSN receives an LLC frame for which no MM context exists in the SGSN, and if the LLC frame does not contain an Attach Request or a Routing Area Update Request signalling message, then the LLC frame shall be discarded. The MS may determine that the network is not responding and attempt to re-attach or eventually a periodic Routing Area Update message is sent by the MS which initiates the attach procedures.

11.2.6 Mobile originated Service Request

For service request, where the MS is unknown in the SGSN (i.e. the SGSN has no MM context for the MS), the SGSN shall reject the service request with an appropriate cause. In order to remain GPRS-attached, the MS shall then perform a new GPRS attach and should (re-)activate its PDP contexts.

If the SGSN has an MM context for the MS, and the indicators "Location Information Confirmed by CSS" or "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data is set to "Not Confirmed", and the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the SGSN may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the SGSN sets the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

The SGSN retrieves CSG subscriber data from the CSS by sending an "Update VCSG Location" request, which triggers one or more "Insert Subscriber Data" operations from the CSS if the CSS has the valid CSG subscription data.

11.3 Use of TLLI

After the SGSN has restarted but before the next authenticated radio contact the P-TMSI and TLLI known by the MS are invalid, as the P-TMSI was allocated before the SGSN restarted. The SGSN may request the MS to identify itself with the IMSI in order to make a relationship between the IMSI and the received old TLLI. The SGSN shall allocate a new P-TMSI for that MS.

If an MS identifies itself by a TLLI in an MS originating transmission, the SGSN proceeds as follows:

- a) The SGSN checks the routing area identity (RAI) of the previous routing area sent by the MS. If this previous RAI belongs to a different SGSN, the request is handled in the normal way.
- b) If the previous RAI belongs to the current SGSN, the status of the TLLI is checked.
 - If the P-TMSI derived from the TLLI was allocated after the SGSN restarted, and corresponds to a valid IMSI record, then the request is handled in the normal way.

- If the P-TMSI derived from the TLLI was allocated before the SGSN restarted, or does not correspond to a valid IMSI record, then the SGSN requests the IMSI from the MS. If the MS returns an IMSI the SGSN proceeds in the normal way. If the MS does not return an IMSI the network aborts the originating transmission request or location registration procedure.

11.4 VLR associations

All associations with VLRs affected by the restart of an SGSN are marked as unreliable and may be deleted. Based on configuration data, Reset messages may be sent on the Gs-interface to the VLRs served by the SGSN. If Reset messages are sent, the VLRs may mark all associations with the SGSN as unreliable by setting the restoration indicator "Confirmed by radio contact" to "Not Confirmed" for the MSs served by that SGSN. See 3GPP TS 29.018 [7]. The associations will be re-initiated one by one by the SGSN at the next Routing Area update, or combined RA/LA update from each MS.

11.5 Restart of a peer node

11.5.1 SGW failure

When an SGSN detects that a peer SGW has failed with or without restart (relying on restart counter as specified in clause 18 "GTP-C based restart procedures" or implementation e.g. preconfigured path failure timer) it shall either:

- as a default delete all PDN connection table data/MM bearer contexts associated with the peer node that has failed as well as freeing any internal SGSN resources associated with those PDN connections. The SGSN may optionally perform other implementation specific actions such as to clear external resources (e.g. Iu messages to clear UTRAN resources) or more advanced forms of restoration;

or

- follow the procedures specified in clause 27 to restore the PDN connections affected by the SGW failure, if the SGSN and the PGW support these procedures.

NOTE: The SGSN will have the identity of the PGW and SGW currently in use for a PDN connection available in the SGSN's PDN connection table as part of existing EPC procedures as well as other peer state data.

11.5.2 MBMS-GW failure

The behaviour of an SGSN when it detects that a peer MBMS GW has restarted is described in subclause 17A.1.

12 Restoration of Data in an SMLC (GSM only)

12.1 Restart of an SMLC

When an SMLC restarts after a failure, it performs the following actions for those of its associated LMUs whose records have been affected by the fault:

- Reload all administered LMU data from non-volatile back-up;
- Reinitialize other temporary data for each LMU to indicate no ongoing measurement or diagnostic activities;
- Perform data restoration for each affected Type A and Type B LMU as described below.

12.2 Data Restoration for a Specific LMU

An SMLC may restore data for a specific LMU when the data in the SMLC or LMU is considered unreliable (e.g. if there is no communication between the SMLC and LMU for a long time or if messages received by the SMLC are inconsistent with the LMU state kept by the SMLC). To restore data for a specific LMU, the SMLC shall open a

signalling connection to the LMU if this is Type A, as described in 3GPP TS 23.071 [10]. For both a Type A LMU and a Type B LMU, the SMLC shall then send an LLP Reset message to the LMU. On receiving an LLP Reset, an LMU shall cancel any LCS measurement and O&M tasks previously ordered by the SMLC and shall return an LLP Reset acknowledgement to the SMLC.

13 Restoration of Data in an LMU (GSM only)

When an LMU restarts following a failure, it shall reinitialize all data concerning LCS measurement and O&M tasks to indicate that no tasks ordered by an SMLC are active. A Type A LMU shall then perform an "IMSI Attach". A Type A LMU shall then open a signaling connection to its controlling SMLC as described in 3GPP TS 23.071 [10]. Both a Type A LMU and a Type B LMU shall send an LLP Status Update message to their controlling SMLC containing an indication that the LMU has restarted following a failure. The SMLC shall update its data regarding the state of the LMU and shall return an LLP Update Status acknowledgment to the LMU.

14 Restoration of data in the MME

14.1 Restart of the MME

14.1.1 Restoration Procedures

After an MME restart, the MME shall delete all MM Bearer contexts affected by the restart that it may have stored.

When the MBMS GW detects a restart in an MME (see clause 18 "GTP-C based restart procedures") with which it has at least one MBMS Bearer context, the MBMS-GW should re-establish the active MBMS bearer services affected by the MME restart by initiating MBMS Session Start procedure(s) towards the restarted MME (or an alternative MME in the same MME pool). The MBMS GW shall encode the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or as per the last MBMS Session Update Request received from the BM-SC if the original parameters were updated) with the following exceptions:

- the MBMS GW shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- if no absolute start time ("MBMS data transfer start" parameter) has been received, the MBMS GW may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the MBMS GW should set the estimated session duration to a value corresponding to the remaining duration of the session.

The MCE shall be able to accept MBMS session requests with an absolute start time ("MBMS data transfer start" parameter) in the past.

NOTE: If the MBMS GW receives an MBMS Session Update Request from the BM-SC during the MME restart, the contents of the MBMS Session Start Request sent to the MME after the MME restart can also differ from the parameters sent to the MME before its restart for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

The MBMS GW shall not delete the MBMS Bearer context unless all SGSNs/MMEs serving the MBMS bearer service and connected to the MBMS GW have restarted and the MBMS-GW does not support re-establishing MBMS bearer services after an MME restart.

If the MCE receives an M3 Reset message from the MME (i.e. in case the restart event has resulted in loss of some or all M3 transactions reference information) with which it has at least one MBMS Bearer context, the MCE shall deactivate all the related MBMS Bearer contexts locally and towards E-UTRAN within which the MBMS bearer service is active, either immediately or after a pre-configured time period if the corresponding MBMS Bearer contexts are not re-established via any MME.

An MME and an SGW supporting the optional network triggered service restoration procedure shall behave as specified in clause 25.

When the MME which does not support the optional network triggered service restoration procedure as specified in clause 25 receives a Downlink Data Notification message for which no MM context exists, the MME returns a Downlink Data Notification Acknowledge message to the Serving GW with an appropriate cause. The Serving GW shall delete the related Bearer context related to MME; and if there is no ISR associated S4-SGSN recorded on the related Bearer context the Serving GW shall also notify the PDN GW to delete the Bearer context.

14.1.2 Mobile originated Tracking Area Updating or E-UTRAN Attach

For attach, where the UE is unknown in the MME (i.e. the MME has no MM context for the UE) the MME shall create an MM context for the UE and shall set the indicators "Location Information Confirmed in HSS", "Subscriber Data Confirmed by HSS", "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" to "Not Confirmed". If authentication is required, the MME shall retrieve the authentication data. The MME then performs an "Update Location" to the HSS. If this is successful, the MME shall set the indicators "Location Information Confirmed in HSS" and "Subscriber Data Confirmed by HSS" to "Confirmed". If the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the MME may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the MME shall set the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

For tracking area update, where the UE is unknown in the MME (i.e. the MME has no MM context for the UE) or for inter-MME tracking area update, where the UE is unknown in the old MME, the MME shall reject the TA update with an appropriate cause. In order to remain attached, the UE shall then perform a new attach and should (re-)activate its EPS Bearer contexts.

If the MME has an MM context for the UE, and the indicator "Location Information Confirmed in HSS" or "Subscriber Data Confirmed by HSS" is set to "Not Confirmed" the MME shall perform an "Update Location" to the HSS. If this is successful, the MME shall set the indicators "Location Information Confirmed in HSS" and "Subscriber Data Confirmed by HSS" to "Confirmed". If the indicators "Location Information Confirmed by CSS" or "Subscriber Data Confirmed by CSS" is set to "Not Confirmed", and the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the MME may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the MME shall set the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

If the MME has an MM context for the UE with the indicator "Subscriber Data Confirmed by HSS" marked "Confirmed" the originated transmission shall be handled in the normal way.

The MME retrieves subscriber data from the HSS by sending an "Update Location" request, which triggers an "Update Location" answer which contains the subscriber data.

The MME retrieves CSG subscriber data from the CSS by sending an "Update VCSG Location" request, which triggers an "Update VCSG Location" answer which may contain the valid CSG subscription data.

14.1.3 Mobile terminated services requested by the MSC/VLR

An MME and a VLR supporting mobile terminated CS service delivery via an alternative MME in MME pool shall behave as specified in clause 26.

When the MME receives a request for CS paging from an MSC/VLR for an IMSI unknown by the MME, if the "MME-Reset" indicator is set to "true", the MME sends the paging request with the location information provided by the VLR. If no such location information is provided, the MME should page for the UE in all the tracking areas corresponding to that MME. The MME may support and apply this procedure to a UE using extended idle mode DRX for MT-SMS service.

NOTE: How the restarted MME knows the UE's DRX parameter or the extended DRX parameters to page the UE is implementation dependent.

If the "MME-Reset" indicator is set to "false" and the IMSI is unknown or the UE is marked as EMM-DEREGISTERED by the MME, the paging request is rejected.

If the "MME-Reset" indicator is set to "false" and the IMSI is known and the UE is marked as EMM-REGISTERED by the MME, the paging request shall be sent to the UE.

14.1.4 Mobile terminated user data transmission

An MME and an SGW supporting the optional network triggered service restoration procedure shall behave as specified in clause 25.

14.1.5 Mobile originated Service Request

For service request, where the UE is unknown in the MME (i.e. the MME has no MM context for the UE), the MME shall reject the service request with an appropriate cause. In order to remain attached, the UE shall then perform a new attach and should (re-)activate its EPS Bearer contexts.

If the MME has an MM context for the UE, and the indicators "Location Information Confirmed by CSS" or "Subscriber Data Confirmed by CSS" is set to "Not Confirmed", and the VPLMN supports Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN, the MME may perform an "Update VCSG Location" to the CSS if the requested cell is a CSG/hybrid cell. If this is successful, the MME shall set the indicators "Location Information Confirmed by CSS" and "Subscriber Data Confirmed by CSS" if the CSS has the valid CSG subscription data to "Confirmed".

The MME retrieves CSG subscriber data from the CSS by sending an "Update VCSG Location" request, which triggers an "Update VCSG Location" answer which may contain the valid CSG subscription data.

14.1.6 Mobile Terminated NIDD procedure

During the Mobile Terminated NIDD procedure, if the SCEF receives a MT-Data-Answer from the MME/SGSN with a failure cause that UE cannot be found, the SCEF shall delete all the bearer contexts of this UE and may notify the Operation and Maintenance network element.

NOTE: After that, if the SCEF receives a following NIDD Submit request from the SCS/AS for the deleted bearer, the SCEF behaves as specified in subclause 5.13.3 of TS 23.682[38] step 2.

14.1A Restart of a peer node

14.1A.1 SGW Failure

When an MME detects that a peer SGW has failed with or without restart (relying on restart counter as specified in clause 18 "GTP-C based restart procedures" or implementation e.g. preconfigured path failure timer) it shall either:

- as a default delete all PDN connection table data/MM bearer contexts associated with the peer node that has failed as well as freeing any internal MME resources associated with those PDN connections. The MME may optionally perform other implementation specific actions such as to clear external resources (e.g. S1-MME messages to clear eNodeB resources) or more advanced forms of restoration;

or

- follow the procedures specified in clause 27 to restore the PDN connections affected by the SGW failure, if the MME and the PGW support these procedures.

NOTE: The MME will have the identity of the PGW and SGW currently in use for a PDN connection available in the MME's PDN connection table as part of existing EPC procedures as well as other peer state data.

14.1A.2 MBMS GW failure

The behaviour of an MME when it detects that a peer MBMS GW has restarted is described in subclause 17A.1.

14.1A.3 MCE Restart

When the MME detects a restart in an MCE (i.e. when the MME receives an M3 Reset or M3 Setup Request message from the MCE) with which it has at least one MBMS Bearer context, the MME shall behave as specified in clause 15A.3.

14.2 VLR associations

All associations with VLRs affected by the restart of an MME are marked as unreliable and may be deleted. Based on configuration data, Reset messages may be sent on the SGs interface to the VLRs served by the MME. If Reset messages are sent, the VLRs may mark all associations with the MME as unreliable by setting the restoration indicator "Confirmed by radio contact" to "Not Confirmed" for the UEs served by that MME. See 3GPP TS 29.118 [14]. The associations will be re-initiated one by one by the MME at the next Combined TA/LA update from each UE.

14.3 Partial Failure Handling at MME

14.3.1 General

See Section 23.

14.3.2 Procedures during PDN Connection Establishment

If the MME supports the feature, the following procedures apply.

During a PDN connection establishment, the MME shall provide one MME FQ-CSID containing exactly one CSID for that particular PDN connection to the SGW in the S11 Create Session Request. The MME shall store the Node-ID and CSID values from the FQ-CSID provided by the SGW and the PGW in the S11 Create Session Response in its PDN Connection table maintained as part of MME MM and EPS Bearer Contexts as specified in Table 5.6.2-15.7.2-1 in 3GPP TS 23.401 [15].

The MME should ensure as far as possible that previously used FQ-CSIDs are not immediately reused after a partial/full failure of an MME.

The MME determines that the SGW supports partial failure handling by the presence of the SGW FQ-CSID in the S11 Create Session Response.

14.3.3 Procedures during MME Partial Failure

If the MME supports the feature the following procedures apply.

When an MME detects that it has undergone a partial failure, it shall verify that one or more corresponding CSID(s) are present for the component(s) undergoing a partial fault. If there is no such CSID, then the following does not apply. When one or more CSIDs are currently assigned, the MME shall perform the following.

The MME may perform implementation-specific operations to clean up any residual state associated with the CSID(s).

The MME shall send a GTPv2 Delete PDN Connection Set Request containing all the MME CSID(s) of the component(s) failing in MME FQ-CSID(s) to the SGW peers that support the feature.

Upon receiving a GTPv2 Delete PDN Connection Set Response message with Cause value "Success", the MME shall conclude that the SGW peer has initiated the internal deletion of the PDN connections corresponding to the FQ-CSID(s) present in the GTPv2 Delete PDN Connection Set Request message.

Regardless of the "Cause" value in the response, the MME is not required to perform any further recovery actions towards SGW and PGW peers for PDN connections in the connection set identified by the MME FQ-CSID(s).

14.3.4 Procedures during a Peer's Partial Failure

If the MME supports the feature, the following procedures apply.

When an MME receives a GTPv2 Delete PDN Connection Set Request message from an SGW, the MME shall retrieve all the PDN connections corresponding to each of the FQ-CSID(s) present in the message. The MME shall delete all the retrieved PDN connections and the associated resources. Other implementation-specific actions may be performed.

As a response, the MME shall send a GTPv2 Delete PDN Connection Set Response message with appropriate Cause value immediately to the SGW.

14.3.5 Procedures during PDN Connection Removal or Modification

If an MME and an SGW support the feature, the following procedures apply.

During an S11 procedure, impacting an existing PDN connection removal or modification the following apply:

- 1) If the SGW is being relocated then the MME shall clear the currently stored SGW FQ-CSID .
- 2) If an MME relocation occurs (for example, TAU with MME change), or if an SGW relocation occurs, (for example, TAU with SGW change), the MME shall include its MME FQ-CSID in the S11 Create Session Request for SGW change and the S11 Modify Bearer Request for MME change without SGW change.
- 3) Additionally, if MME decides to change own FQ-CSID, the MME shall include MME FQ-CSID in other S11 messages.
- 4) If the MME receives a FQ-CSID value of an SGW over S11, the MME shall overwrite the current stored SGW FQ-CSID value with the received value.
- 5) If the MME receives a FQ-CSID value of a PGW over S11, the MME shall overwrite the current stored PGW FQ-CSID value with the received value.
- 6) During a S11 procedure removing an existing PDN connection the MME removes the PDN data as well as any stored FQ-CSID values(s) of the PGW FQ-CSID and SGW FQ-CSID. The same actions are done on the old MME if there is an MME relocation.

The MME determines that the SGW supports partial failure handling by the presence of the SGW FQ-CSID in the S11 Create Session Response with SGW change; and S11 Modify Bearer Response without SGW change.

15 Restoration of data in GERAN/UTRAN

15.1 BSS Failure (A/Gb mode)

When a BSS fails, all its BSS contexts affected by the failure become invalid and shall be deleted. BSS storage of data is volatile.

15.2 RNC/BSC Failure (Iu mode)

When an RNC/BSC fails, all its RNC/BSC contexts affected by the failure become invalid and shall be deleted. RNC/BSC storage of data is volatile. An SGSN that recognises unavailability of an RNC/BSC or receives a Reset from an RNC/BSC, shall locally release the RABs for all affected PDP contexts.

Any affected PDP contexts that use Direct Tunnel and have an invalid tunnel in GGSN will be recovered when the SGSN receives an Iu connection establishment request from the MS or when the GGSN informed the SGSN that the GGSN has received a GTP error indication from RNC.

When the RNC/BSC receives a GTP-U PDU for which no RAB context exists, the RNC/BSC shall discard the GTP-U PDU and return a GTP error indication to the originating node that may be SGSN or GGSN if Direct Tunnel is established.

The RNC should ensure as far as possible that previously used TEID values are not immediately reused after an RNC restart, in order to avoid inconsistent TEID allocation throughout the network.

15.3 RNC/BSC Failure (Iu mode) using S4

When an RNC/BSC fails, all its RNC/BSC contexts affected by the failure become invalid and shall be deleted. RNC/BSC storage of data is volatile. An SGSN that recognises unavailability of an RNC/BSC or receives a Reset from an RNC/BSC, shall locally release the RABs for all affected PDP contexts. If ISR is activated or direct tunnel is established, the S4-SGSN shall initiate release of the access bearer for all bearers towards the Serving GW as defined in Iu Release Procedure Using S4 in 3GPP TS 23.060 [5]. For the other cases, the S4-SGSN may send the Release Access Bearers Request message to the Serving GW to remove the downlink user plane address and TEID as specified in 3GPP TS 23.060 [5]. In addition, based on operator policy, the SGSN may initiate the Dedicated Bearer Deactivation procedure for bearers using streaming or conversational traffic class. Any affected EPS bearers contexts in Serving GW are recovered when the SGSN receives an Iu connection establishment request from the MS or when the Serving GW initiates the Network Triggered Service Request procedure as specified in 3GPP TS 23.060 [5].

When the RNC/BSC receives a GTP-U PDU for which no RAB Context exists, the RNC/BSC shall discard the GTP-U PDU and return a GTP Error Indication to the originating node that may be SGSN or Serving GW if Direct Tunnel is established.

An S4-SGSN that recognises unavailability of an RNC (e.g. no more SCTP association in service) or receives a Reset message from an RNC shall maintain the related MBMS bearer contexts but shall locally delete the RNC related information (i.e. Iu related resources) for all MBMS service association(s) or those indicated in the Reset message. See subclause 8.26 of 3GPP TS 25.413 [29].

Upon receipt of a Reset message from the RNC, the S4-SGSN should then subsequently re-establish the MBMS bearer services affected by the RNC failure by initiating MBMS Session Start procedure(s) towards the RNC. The S4-SGSN shall encode the contents of the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request received from the MBMS GW if the original parameters were updated) with the following exceptions:

- if the S4-SGSN has received recently an MBMS session re-establishment indication from the MBMS GW (i.e. within a past short period covering the time during which the same MBMS session may exist simultaneously in two S4-SGSNs of the S4-SGSN pool), the S4-SGSN shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session. Otherwise, the S4-SGSN shall not set "MBMS session re-establishment indication" flag;
- the S4-SGSN should set the estimated session duration to a value corresponding to the remaining duration of the session.

NOTE 1: During an Sn path failure when the MBMS GW moves the control of an MBMS session to an alternative S4-SGSN in the S4-SGSN pool (see subclause 20.2.3.2), the MBMS session can exist in the old and in the new S4-SGSN for a short period of time. This time period is not bigger than the value of the maximum Sm path failure timer configured at the S4-SGSN. If an RNC happens to restart during this time, both S4-SGSNs will try to re-establish the MBMS session. In this case, it needs to be ensured that the control of the MBMS session remains at the new S4-SGSN, whatever the order of the MBMS Session Start Request messages the RNC will receive from both S4-SGSNs. The setting of the "MBMS session re-establishment indication" flag by the new S4-SGSN as specified above ensures that the new S4-SGSN, which has acquired the control of the MBMS session in the recent past, will get the control of the MBMS session.

NOTE 2: If the S4-SGSN receives an MBMS Session Update Request from the MBMS GW during the RNC failure, the contents of the MBMS Session Start Request sent to the RNC after the RNC recovery can also differ from the parameters sent to the RNC before its failure for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer).

15.4 Other RNC functionality for MBMS restoration

The RNC should accept an MBMS Session Start Request received for an ongoing MBMS session (i.e. with the same TMGI)

- from the same or a different SGSN than the SGSN that currently controls the MBMS session, if the message contains the "MBMS session re-establishment indication" flag; or

- from the SGSN that currently controls the MBMS session, if the RNC supports the option to maintain MBMS bearer contexts during a pre-configured time period after an Iu path failure and the message is received during that period without the "MBMS session re-establishment indication" flag.

If it accepts the request from the SGSN, and if the message contains the "MBMS session re-establishment indication" flag, the RNC shall:

- replace the Iu related resources for this MBMS service associated to the previous SGSN by those assigned in the MBMS Session Request (if different) and consider that the MBMS session is now being controlled by the new SGSN (if different from the previous SGSN); for IP Unicast over Iu, the RNC receives the user plane data for this MBMS session via the new SGSN (if different from the previous SGSN);
- the RNC shall leave the former M1 transport network IP multicast address and join the new M1 transport network IP multicast address (including the IP address of the multicast source) if the MBMS Session Start Request contains a different transport network IP multicast distribution address and/or a different IP multicast source address; the RNC shall also use the C-TEID received in the MBMS Session Start Request

NOTE: This can also result in a change from IP Multicast to IP unicast or vice versa for the Iu userplane.

15.5 Iu path failure using S4

Upon detection of an Iu path failure (i.e. no more SCTP association in service),

- the RNC shall release all the MBMS services affected by the Iu path failure either immediately or after a pre-configured time period if the corresponding MBMS bearer contexts are not re-established via any S4-SGSN;
- the S4-SGSN shall maintain the related MBMS bearer contexts but shall locally delete the RNC related information (i.e. Iu related resources) for all MBMS service association(s).

Upon recovery of the Iu path, the RNC should initiate a Reset procedure towards the related S4-SGSN. Upon receipt of the Reset message from the RNC, the S4-SGSN should behave as specified for RNC failure in subclause 15.3.

15A Restoration of data in E-UTRAN

15A.1 eNodeB Failure

15A.1.1 General

An MME which does not support UE context retention at SCTP recovery and recognises unavailability of an eNodeB (e.g. no more SCTP association in service) or an MME which receives a Reset or a S1 Setup message with UE Retention Information not set to "ues-retained" from an eNodeB, shall locally delete the eNodeB related information ("eNodeB Address in Use for S1-MME" and "eNodeB UE S1AP ID"). In this case, the MME initiates release of all S1 bearers towards the Serving GW by sending a Release Access Bearer Request message as defined in the S1 Release procedure in 3GPP TS 23.401 [15]. The MME shall initiate the Dedicated Bearer Deactivation procedure to deactivate the GBR bearers in the packet core; as an option, the MME may defer the deactivation of the GBR bearers for a short period (e.g. in the order of seconds) so as to allow the re-establishment of the corresponding radio and S1 bearers and thus avoid the GBR bearers deactivation if the MME receives a NAS Service Request or a GTP-C Downlink Data Notification message as a result of the SGW having received an Error Indication message from the eNodeB (see clause 22).

If the Serving GW receives Release Access Bearers Request message, the Serving GW shall release all eNodeB related information (address and TEIDs) for the UE, but other elements of the UE's Serving GW context shall not be affected. Any Bearer contexts affected by eNodeB failure that have no valid S1-U tunnel in Serving GW are recovered during the UE Triggered Service Request or during the Network Triggered Service Request procedure as specified in 3GPP TS 23.401 [15].

An MME, which supports UE context retention at SCTP recovery and recognises unavailability of an eNodeB (e.g. no more SCTP association in service), shall keep the UEs in ECM-CONNECTED and suspended UE Context data for UEs in ECM-IDLE, which have used the S1 signalling connection before it was broken. Upon the subsequent S1 Setup

procedure, the MME and the eNB may agree that UE-related contexts and related signalling connection that have been existing before the S1 Setup shall not be affected as specified in the subclause 19.2.2.8 of 3GPP TS 36.300 [32].

The eNodeB should ensure as far as possible that previously used TEID values are not immediately reused after an eNodeB restart, in order to avoid inconsistent TEID allocation throughout the network.

15A.1.2 PWS restoration

After an (H)eNodeB has restarted, it shall delete all its warning message data. If the warning message service is operational in one or more cell(s) of the (H)eNodeB, the (H)eNodeB shall send a PWS Restart Indication message, which shall include the identity of the (H)eNodeB, the identity of the restarted cell(s), and the TAI(s) and EAI(s) with which the restarted cell(s) are configured, to the CBC to request the CBC to re-load its warning message data if applicable.

The (H)eNB should send the PWS Restart Indication message via two MMEs of the MME pool, if possible, to ensure that the CBC receives the message even if one MME can not propagate it to the CBC (e.g. due to an SBc path failure).

For HeNBs, the HeNB GW (respectively the MME) shall check the cell identity (respectively the HeNB identity) received in the PWS Restart Indication, as specified in subclause 4.6.2 of 3GPP TS 36.300 [32].

Upon receipt of a PWS Restart Indication message, the CBC shall consider that the warning message service is restarted in the reported cell(s), i.e. the service is operational and no warning messages are being broadcast in the cell(s). The CBC shall then re-send the warning message data (with the same message identifier and serial number) to the (H)eNodeB for these cells, if any. When doing so, the CBC:

- shall include the identity of the (H)eNodeB received in the PWS Restart Indication into the Write-Replace-Warning-Request message(s) to enable the MME to forward the message(s) only to the (H)eNodeB (or HeNB GW) involved in the restart;
- should set the warning area list to the identities of the cell(s) to be reloaded which are relevant to the warning message data being reloaded; and
- may update the number of broadcasts requested, if necessary.

NOTE 1: Setting the warning area list to the identities of the cell(s) to be reloaded enables, for example, the HeNB GW to forward the message only to the involved HeNB when the restarted HeNB is connected to a HeNB GW.

The CBC shall consider a PWS Restart Indication message received shortly after a preceding one for the same cell identity as a duplicate restart indication for that cell which it shall ignore.

NOTE 2: The broadcast of warning messages can be configured in the network per individual cell, TAI and/or EAI. The CBC can use the list of cell(s), the TAI(s) and EAI(s) received in the PWS Restart Indication to derive the list of warning messages to be broadcast in the respective cell(s), TAI(s) and EAI(s).

Likewise, in other scenarios where the (H)eNodeB may need to reload its warning message data (e.g. when an individual cell is restarted), the (H)eNodeB shall send a PWS Restart Indication message (including the identity of the (H)eNodeB, the identity of the restarted cell(s), and the TAI(s) and EAI(s) with which the restarted cell(s) are configured) to the CBC to request the CBC to re-load its warning message data if applicable. The (H)eNodeB, MME and CBC shall then proceed as specified above for an (H)eNodeB restart.

15A.2 S1-AP path failure

Upon detection of an S1-AP path failure (i.e. no more SCTP association in service),

- the eNodeB shall either release the RRC connection of the affected UEs, or if UE context retention at SCTP recovery is supported, the eNodeB shall keep those UEs in RRC_CONNECTED and suspended UE Context data for UEs in ECM-IDLE, which have used the S1 signalling connection before it was broken;
- the MME shall proceed as specified for the eNodeB failure in subclause 15A.1.

The eNodeB shall continue to broadcast warning messages, if any, during an S1AP path failure. Upon recovery of the S1AP path, the eNodeB shall proceed as if no S1AP path failure had occurred.

During an S1AP path failure, the warning message data stored in the eNodeB may become desynchronized with the CBC, e.g. if the CBC attempts to modify the warning message data during the S1AP path failure. The CBC and MME(s) should support the Write-Replace-Warning-Indication and Stop-Warning-Indication procedures (see 3GPP TS 23.041 [30]) to keep the warning message data synchronized in the eNodeB and the CBC.

15A.3 MCE Failure

When an MCE fails, the MCE shall release all the MBMS services affected by the failure locally and towards E-UTRAN within which the MBMS bearer services are active, either immediately or after a pre-configured time period if the corresponding MBMS bearer contexts are not re-established via any MME.

An MME that recognises unavailability of an MCE (e.g. no more SCTP association in service) or receives a Reset or a M3 Setup Request message from an MCE shall maintain the related MBMS bearer contexts but shall locally delete the MCE related information (i.e. M3 related resources) for all MBMS service association(s) or those indicated in the RESET message. See subclauses 8.5 and 8.7 of 3GPP TS 36.444 [28].

Upon receipt of a Reset or M3 Setup Request message from the MCE, the MME should then subsequently re-establish the MBMS bearer services affected by the MCE failure by initiating MBMS Session Start procedure(s) towards the MCE. The MME shall encode the contents of the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request received from the MBMS GW if the original parameters were updated) with the following exceptions:

- if the MME has received recently an MBMS session re-establishment indication from the MBMS GW (i.e. within a past short period covering the time during which the same MBMS session may exist simultaneously in two MMEs of the MME pool), the MME shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session. Otherwise, the MME shall not set "MBMS session re-establishment indication" flag;
- if no absolute start time ("MBMS data transfer start" parameter) has been received, the MME may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the MME should set the estimated session duration to a value corresponding to the remaining duration of the session.

The MCE shall be able to accept MBMS session requests with an absolute start time ("MBMS data transfer start" parameter) in the past.

NOTE 1: During an Sm path failure when the MBMS GW moves the control of an MBMS session to an alternative MME in the MME pool (see subclause 20.2.3.1), the MBMS session can exist in the old and in the new MME for a short period of time. This time period is not bigger than the value of the maximum Sm path failure timer configured at the MME. If an MCE happens to restart during this time, both MMEs will try to re-establish the MBMS session. In this case, it needs to be ensured that the control of the MBMS session remains at the new MME, whatever the order of the MBMS Session Start Request messages the MCE will receive from both MMEs. The setting of the "MBMS session re-establishment indication" flag by the new MME as specified above ensures that the new MME, which has acquired the control of the MBMS session in the recent past, will get the control of the MBMS session.

NOTE 2: If the MME receives an MBMS Session Update Request from the MBMS GW during the MCE failure, the contents of the MBMS Session Start Request sent to the MCE after the MCE recovery can also differ from the parameters sent to the MCE before its failure for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

15A.4 M3AP path failure

Upon detection of an M3AP path failure (i.e. no more SCTP association in service),

- the MCE shall release all the MBMS services affected by the M3AP path failure locally and towards E-UTRAN within which the MBMS bearer services are active, either immediately or after a pre-configured time period if the corresponding MBMS bearer contexts are not re-established via any MME;

- the MME shall maintain the related MBMS bearer contexts but shall locally delete the MCE related information (i.e. M3 related resources) for all MBMS service association(s).

Upon recovery of the M3AP path, the MCE should initiate a Reset or M3 Setup Request procedure towards the related MME. Upon receipt of the Reset or M3 Setup Request message from the MCE, the MME should then subsequently re-establish the MBMS bearer services affected by the M3AP path failure by initiating MBMS Session Start procedure(s) towards the MCE. The MME shall encode the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request received from the MBMS GW if the original parameters were updated) with the following exceptions:

- if the MME has received recently an MBMS session re-establishment indication from the MBMS GW (i.e. within a past short period covering the time during which the same MBMS session may exist simultaneously in two MMEs of the MME pool), the MME shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session. Otherwise, the MME shall not set "MBMS session re-establishment indication" flag;
- if no absolute start time ("MBMS data transfer start" parameter) has been received, the MME may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the MME should set the estimated session duration to a value corresponding to the remaining duration of the session.

The MCE shall be able to accept MBMS session requests with an absolute start time ("MBMS data transfer start" parameter) in the past.

NOTE 1: During an Sm path failure when the MBMS GW moves the control of an MBMS session to an alternative MME in the MME pool (see subclause 20.2.3.1), the MBMS session can exist in the old and in the new MME for a short period of time. This time period is not bigger than the value of the maximum Sm path failure timer configured at the MME. If an M3AP path failure and recovery happens during this time, both MMEs will try to re-establish the MBMS session. In this case, it needs to be ensured that the control of the MBMS session remains at the new MME, whatever the order of the MBMS Session Start Request messages the MCE will receive from both MMEs. The setting of the "MBMS session re-establishment indication" flag by the new MME as specified above ensures that the new MME, which has acquired the control of the MBMS session in the recent past, will get the control of the MBMS session.

NOTE 2: If the MME receives an MBMS Session Update Request from the MBMS GW during the M3AP path failure, the contents of the MBMS Session Start Request sent to the MCE after the M3AP path recovery can also differ from the parameters sent to the MCE before the M3AP path failure for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

15A.5 Other MCE functionality for MBMS restoration

The MCE should accept an MBMS Session Start Request received for an on-going MBMS session (i.e. with the same TMGI)

- from the same or a different MME than the MME that currently controls the MBMS session, if the message includes the "MBMS session re-establishment indication" flag; or
- from the MME that currently controls the MBMS session, if the MCE supports the option to maintain MBMS bearer contexts during a pre-configured time period after an M3AP path failure, MME restart or MCE failure, and the message is received during that period without the "MBMS session re-establishment indication" flag.

If the MCE accepts the request from the MME, and if the message contains the "MBMS session re-establishment indication" flag,

- the MCE shall replace the M3 related resources for this MBMS service associated to the previous MME by those assigned in the MBMS Session Start Request (if different) and consider that the MBMS session is now being controlled by the new MME (if different from the previous MME);
- the eNodeB(s) involved in the broadcast of the MBMS session shall leave the former M1 transport network IP multicast address and join the new M1 transport network IP multicast address (including the IP address of the multicast source) if the MBMS Session Start Request contains a different transport network IP multicast

distribution address and/or a different IP multicast source address; the eNodeB(s) shall also use the C-TEID received in the MBMS Session Start Request.

The MCE shall be able to accept MBMS session start/update/stop requests with an absolute start time ("MBMS data transfer start" or "MBMS data transfer stop" parameter) in the past.

15A.6 Other MME related functionality for MBMS restoration

When establishing MBMS bearer services in an MCE to ensure the distribution of content from ongoing MBMS sessions to an MCE which modifies the lists of the MBMS Service Areas it serves via the MCE Configuration Update procedure (see subclause 5.9.2 of 3GPP TS 23.246 [12]), the MME shall encode the MBMS Session Start Request as specified in subclause 15A.3 upon receipt of a Reset or M3 Setup Request message from the MCE.

16 Restoration of data in the SGW

16.1 Restart of the SGW

16.1.0 SGW Failure

When a SGW fails, all its Bearer contexts affected by the failure become invalid and may be deleted. SGW storage of subscriber data is volatile.

When the SGW receives a GTP-U PDU for which no Bearer context exists, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (the PGW, the eNodeB, the S4-SGSN, or if Direct Tunnel is established, the RNC) or follow the procedures specified in clause 27.2.2.5 if the restoration of PDN connections after an SGW failure is supported.

The SGW should ensure as far as possible that previously used TEID values are not immediately reused after a SGW restart, in order to avoid inconsistent TEID allocation throughout the network.

16.1.1 Restoration Procedures

After an SGW restart, the SGW shall delete all MM Bearer contexts affected by the restart that it may have stored.

During or immediately after an SGW Restart the SGW shall place local SGW restart counter value in all GTPv2 Echo requests/responses messages and PMIPv6 heartbeat responses the SGW sends.

16.1a Restart of the SGW-C

16.1a.1 SGW-C failure

When a SGW-C fails, all its Bearer and Session contexts, Sx Association(s) affected by the failure become invalid and may be deleted.

If F-TEID allocation is performed in the SGW-C, the SGW-C should ensure as far as possible that previously used F-TEID values are not immediately reused after a SGW-C restart, in order to avoid inconsistent TEID allocation throughout the network.

NOTE: This is to ensure that F-TEIDs are not reused until earlier PDN connections using them are released e.g. in eNB or PGW.

16.1a.2 Restoration procedure

During or immediately after an SGW-C Restart, the SGW-C shall place local SGW-C Recovery Time Stamp value in all Heartbeat Request/Response and Sx Association Setup Request/Response Messages.

16.1b Restart of the SGW-U

16.1b.1 SGW-U failure

When a SGW-U fails, all its Sx session contexts and Sx Association(s) affected by the failure become invalid and may be deleted.

If F-TEID allocation is performed in the SGW-U, the SGW-U shall ensure that previously used F-TEID values are not immediately reused after a SGW-U restart, in order to avoid inconsistent TEID allocation throughout the network and to enable the restoration of Sx sessions affected by the failure. How this is ensured is implementation specific. NOTE: As the user plane F-TEID pool is partitioned in the SGW-U across the multiple SGW-Cs controlling the SGW-U, the SGW-U does not need to wait for the re-establishment of all the Sx associations from all SGW-Cs to start assigning new F-TEID for new Sx sessions for a particular SGW-C.

16.1b.2 Restoration procedure

During or immediately after an SGW-U Restart, the SGW-U shall place local SGW-U Recovery Time Stamp value in all Heartbeat Request/Response and Sx Association Setup Request/Response Messages.

16.1A Restart of a peer node

16.1A.1 MME/S4-SGSN Failure

16.1A.1.1 General

The SGW will receive the MME/S4-SGSN restart counter in GTPv2 Echo requests and Echo response messages that the SGW receives from the MME/S4-SGSN.

When an SGW detects that a peer MME /S4-SGSN has restarted (see clause 18 "GTP-C based restart procedures") it shall either:

- delete all PDN connection table data/MM bearer contexts associated with the peer node that fails as well as freeing any internal SGW resources associated with those PDN connections. The SGW may optionally perform other implementation specific actions such as messages to clear other external resources (e.g. PCC messages to clear the resources in the PCRF or GTP/PMIP messages to release the corresponding PDN connection in the PGW);

or

- follow the network triggered service restoration procedure as specified in clause 25 if the MME, the S4-SGSN and the SGW support this procedure.

16.1A.2 PGW Failure

The SGW will receive the PGW restart counter in GTPv2 Echo requests/ responses and PMIPv6 heartbeat responses that the SGW receives from the PGW.

When an SGW detects that a peer PGW has restarted (see clause 18 "GTP-C based restart procedures") it shall delete all PDN connection table data/MM bearer contexts associated with the peer node that fails as well as freeing any internal SGW resources associated with those PDN connections. In addition, if the optional feature PGW Restart Notification is supported by the SGW and MME/S4-SGSN as specified in clause 8.83 in 3GPP TS 29.274[13], the SGW shall initiate the cleanup of the hanging PDN connections associated with the SGW and the restarted PGW at the corresponding MMEs/S4-SGSNs by sending GTPv2 message(s) PGW Restart Notification, with the control plane IP address of the restarted PGW and the control plane IP address of the SGW on the S11/S4 interface included. The SGW may optionally perform other implementation specific actions such as messages to clear other external resources (e.g. PCC messages).

If an SGW detects that a peer PGW has failed and not restarted, it may delete all PDN connection table data/MM bearer contexts associated with the peer node that fails as well as freeing any internal SGW resources associated with those

PDN connections. In addition, if the optional feature PGW Restart Notification is supported by the SGW and MME/S4-SGSN as specified in clause 8.83 in 3GPP TS 29.274[13], the SGW may also send a PGW Restart Notification message to the MME or S4-SGSN. The PGW Restart Notification message shall include the control plane IP address of the PGW, the control plane IP address of the SGW on the S11/S4 interface and the cause value "PGW not responding". It is an implementation matter how an SGW becomes aware that a PGW has failed and has not restarted, e.g. the SGW detects a signalling path failure with the PGW for a duration exceeding the maximum path failure duration timer (see clause 20.2.1).

When the MME/S4-SGSN receives this message, according to the control plane IP address of the restarted PGW and the control plane IP address of the SGW on the S11/S4 interface included in the message, the MME/S4-SGSN should delete all PDN connection table data/MM bearer contexts associated with the SGW and the restarted PGW as well as freeing any internal MME/S4-SGSN resources associated with those PDN connections. Additionally the MME/S4-SGSN may decide to restore certain PDN connections based on operator's policy e.g. based on the QCI and/or ARP and/or APN. If so,

- the S4-SGSN shall deactivate the corresponding PDN connections using the "reactivation requested" cause value as specified in clause 9.2.4.2 of 3GPP TS 23.060 [5];
- the MME shall deactivate the corresponding PDN connections using the "reactivation requested" cause value as specified in clause 5.10.3 of 3GPP TS 23.401 [15] if only a subset of the PDN connections of the UE need to be restored or if the UE has a SCEF PDN connection or if the UE supports Attach without PDN connectivity as specified in clause 5.3.8.3 of 3GPP TS 23.401 [15]; if all the PDN connections of the UE need to be restored and the UE does not have a SCEF PDN connection and the UE does not support Attach without PDN connectivity, the MME shall initiate the "explicit detach with reattach required" procedure as specified in clause 5.3.8.3 of 3GPP TS 23.401 [15].

The MME/S4-SGSN may prioritize the PDN connections to restore based on operator's policy e.g. based on the QCI and/or APN. Besides, the MME/S4-SGSN may use the subscribed Restoration Priority per APN, if received from the HSS, and if permitted by service level agreements for in-bound roamers, to determine the relative restoration priority among PDN connections to the same APN. The MME/S4-SGSN may use a locally configured value as default restoration priority if the restoration priority for a user's PDN connection is not received from the HSS or not permitted by service level agreement for in-bound roamers.

NOTE 1: The Restoration Priority can e.g. allow to restore with a higher priority users with an IMS voice subscription over IMS users without an IMS voice subscription.

The MME/S4-SGSN may optionally perform other implementation specific actions such as to clear external resources (e.g. S1-MME messages to clear eNodeB resources or Iu messages to clear RNC resources) or more advanced forms of restoration.

NOTE 2: The SGW will have the identity of the MME/S4-SGSN and PGW currently in use for a PDN connection available in the SGW's PDN connection table as part of existing EPC procedure.

If PMIPv6 based S5/S8 interface is used and if the SGW needs to send a request for Gateway Control and QoS Policy Rules Provision procedure towards a PCRF which is known to have restarted since the Gateway Control Session Establishment, the SGW may discard the request and may tear down the associated PDN connection, based on operator policy, by sending a Delete Bearer Request message for the default bearer towards the MME/S4-SGSN with the cause set to "Reactivation requested". Additionally, SGW initiates an SGW initiated PDN Disconnection procedure towards PGW. This leads the UE to initiate a UE requested PDN connectivity procedure for the same APN. Emergency and eMPS sessions should not be torn down.

NOTE 3: The procedure above just enables to clean up the PDN connection affected by the PCRF failure when a specific interaction with the PCRF is required. Prior to that interaction, PCC controlled services can not be provided to the UE.

For a split SGW, if the SGW-C detects a PGW failure, it shall initiate a Sx Session Deletion procedure towards the SGW-U.

16.1A.3 SGW-C Failure

The SGW-U will receive the SGW-C recovery time stamps in Sx association setup Request/Response and PFCP heartbeat requests/responses.

When an SGW-U detects that a peer SGW-C has restarted, the SGW-U shall delete all its Sx session contexts and the Sx Association affected by the SGW-C restart. When the SGW-U receives a GTP-U PDU not matching any PDRs, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (the PGW, the eNodeB, the S4-SGSN, or if Direct Tunnel is established, the RNC); as an exception, if the restoration of PDN connections after an SGW failure is supported, the SGW-U shall not send Error indication message for a configurable period after the SGW-C restart.

NOTE: The period needs to be longer than the time required for the peer node to detect the restart of the SGW-C, e.g. the interval between two echo request messages. This ensures that the MME/SGSN or PGW does not deactivate the bearers before it detects the SGW-C failure and triggers the restoration procedure.

16.1A.4 SGW-U Failure

The SGW-C will receive the SGW-U recovery time stamps in Sx association setup Request/Response and PFCP heartbeat requests/responses.

After and SGW-U restart, the Sx association between SGW-C(s) and the SGW-U has to be re-established.

Restoration of Sx sessions may start immediately after the Sx association setup procedure:

- if the restoration is supported in the SGW-C on a proactive basis, the SGW-C may start re-establishing Sx sessions matching any PDRs.
- if the restoration is supported in the SGW-C on a reactive basis:
 - the SGW-C shall establish an Sx session with a wildcarded PDR to instruct the UP function to forward G-PDU packets which are not matching any other PDRs to the CP function (to a F-TEID uniquely assigned in the CP function for this Sx-u tunnel);
 - upon receipt of G-PDUs from this Sx-u tunnel, the CP function shall then check if it has an active session for each received G-PDU packet:
 - if so, the CP function shall perform Sx Session establishment procedures to re-establish the corresponding Sx sessions in the SGW-U;
 - otherwise the CP function shall generate a GTP-U Error Indication with a destination address set to the source IP address of the received G-PDU, and send it to the UP function. The UP function shall forward this GTP-U Error Indication transparently. The CP function shall delete the G-PDU after the check for active sessions.

NOTE 1: The SGW-U can filter the G-PDU packets with same target F-TEID and send only one such G-PDU to the CP function.

NOTE 2: Such Sx-u tunnel to forward GTP-U Error Indication can be established per UP function and can also be used to send End Marker packets generated by the CP function. See subclause 5.3.2 of TS 29.244 [43]

The SGW-U shall not send Error indication message for a configurable period after an SGW-U restart when the SGW-U receives G-PDU not matching any PDRs.

NOTE 3: If restoration on a reactive basis is used, the period needs to be longer than the time required by the SGW-C to detect the SGW-U restart, establish the Sx association and provision the wildcarded PDR. Otherwise, the period needs to be longer than the time required by the SGW-C to restore all the Sx sessions on a proactive basis.

When the SGW-C detects the failure of an SGW-U without a restart, the SGW-C may select an alternative SGW-U which can take over the IP addresses of the failed one to restore the Sx sessions in the UP function. How this is performed is implementation specific.

16.2 Partial Failure Handling at SGW

16.2.1 General

See Section 23.

In addition, the following applies. If an SGW, which supports the feature receives Delete PDN Connection Set Request/Reply messages from MME or the PGW it shall forward the messages to the appropriate peer.

If the SGW does not support the feature then partial failure handling does not apply to that specific PDN connection.

16.2.2 Procedures during PDN Connection Establishment

If the SGW supports the feature, the following procedures apply.

During a PDN connection establishment, the SGW shall provide one SGW FQ-CSID for that particular PDN connection to the PGW. Similarly, the SGW shall provide one SGW FQ-CSID for that particular PDN connection to the MME if the MME supports partial failure handling. The SGW shall store the Node-ID and CSID from the FQ-CSID provided by the PGW and the MME respectively for that particular PDN connection in its PDN Connection table maintained as part of "EPS Bearer Contexts" table as specified in Table 5.7.3-1 in 3GPP TS 23.401 [15].

The SGW shall forward the MME FQ-CSID provided by the MME on S11 to the PGW in the S5/S8 Create Session Request (Proxy Binding Update for PMIPv6) for that PDN connection. Similarly, the SGW shall forward the PGW FQ-CSID provided by the PGW on S5/S8 to the MME in the S11 Create Session Response for that PDN connection if the MME supports partial failure handling.

The SGW determines that the MME supports partial failure handling by the presence of the MME FQ-CSID in the S11 Create Session Request.

The SGW determines that the PGW supports partial failure handling by the presence of the PGW FQ-CSID in the S5/S8 Create Session Response for GTPv2 based S5/S8 and the Proxy Binding Acknowledgement for PMIPv6 based S5/S8.

16.2.3 Procedures during SGW Partial Failure

If the SGW supports the feature, the following procedures apply.

When an SGW detects that it has undergone a partial failure, it shall verify that one or more corresponding CSID(s) are present for the component undergoing a partial fault. If there is no such CSID, then the following does not apply. When one or more CSIDs are currently assigned, the SGW shall perform the following.

The SGW may perform implementation-specific operations to clean up any residual state associated with the CSID(s).

The SGW shall send the GTPv2 Delete PDN Connection Set Request containing all the SGW CSIDs of the component(s) failing in SGW FQ-CSID to MME peers supporting the feature. The SGW shall send the GTPv2 Delete PDN Connection Set Request (or PMIPv6 Binding Revocation Indication with G bit set) message containing the equivalent SGW FQ-CSID(s) to PGW peers supporting the feature.

Upon receiving a GTPv2 Delete PDN Connection Set Response message with Cause value "Success", the SGW shall conclude that the PGW (for GTPv2 S5/S8) or the MME (for S11) has initiated the internal deletion of the PDN connections corresponding to the FQ-CSID(s) present in the GTPv2 Delete PDN Connection Set Request message. Similarly, upon receiving a successful PMIPv6 Binding Revocation Acknowledgment message with G bit set, the SGW shall conclude that the PGW has initiated the internal deletion of the PDN connections corresponding to the CSID(s) present in the PMIPv6 Binding Revocation Indication message.

The SGW is not required to perform any further recovery actions towards MME and PGW peers for PDN connections in the connection set identified by the SGW FQ-CSID(s).

16.2.4 Procedures during a Peer's Partial Failure

If the SGW supports the feature, the following procedures apply.

When an SGW receives a S11 GTPv2 Delete PDN Connection Set Request message from an MME, the SGW shall retrieve all the PDN connections corresponding to each of the FQ-CSID(s) present in the message. The SGW shall send a S5/S8 GTPv2 Delete PDN Connection Set Request (or PMIPv6 Binding Revocation Indication with G bit set) message containing the FQ-CSID(s) provided by the MME to PGW peers supporting the feature. The SGW shall delete all the retrieved PDN connections and the associated resources. Other implementation-specific actions may be performed.

As a response, the SGW shall send a S11 GTPv2 Delete PDN Connection Set Response message with an appropriate Cause value immediately to the MME.

When an SGW receives a S5/S8 GTPv2 Delete PDN Connection Set Request (or PMIP6 Binding Revocation Indication with G bit set) message from a PGW, the SGW shall retrieve all the PDN connections corresponding to each of the FQ-CSID(s) present in the message. The SGW shall send a S11 GTPv2 Delete PDN Connection Set Request message containing the FQ-CSID(s) provided by the PGW to MME peers supporting the feature. The SGW shall delete all the retrieved PDN connections and the associated resources. Other implementation-specific actions may be performed.

As a response, the SGW shall send a S5/S8 GTPv2 Delete PDN Connection Set Response message with an appropriate Cause value to the PGW. On PMIP6-based S5/S8 interface, the SGW shall send a PMIP6 Binding Revocation Acknowledgment message with G bit set.

If the SGW detects the full/complete failure of an MME or PGW, e.g., through the Echo Request/Echo Response procedure, it may send a Delete PDN Connection Set Request (or PMIP6 Binding Revocation Indication with G bit set) message, containing all of the FQ-CSIDs of the associated hanging PDN connections of the failed node, to the corresponding remote node (MME or PGW).

16.2.5 Procedures during PDN Connection Removal or Modification

Only if the SGW supports the feature, the following procedures apply.

During a S11 or an S5/S8 procedure, impacting an existing PDN connection removal or modification the following apply:

- 1) If the MME is being relocated then the SGW shall clear the currently stored MME FQ-CSID value (if any).
 - 2) For inter MME and intra SGW HO/TAU, and if the new MME supports the feature, then the SGW shall:
 - include SGW FQ-CSID in the S11 Modify Bearer Response. If PGW supports the feature, the SGW shall also include PGW FQ-CSID into the message.
 - inform the feature supporting PGW about the change of FQ-CSID values with the following messages:
 - Modify Bearer Request, when Modify Bearer Request message needs to be sent to the PGW as specified in the 3GPP TS 23.401 [15], e.g. if the sending of this message is triggered by user location reporting procedure. The message shall contain both SGW FQ-CSID and MME FQ-CSID.
 - Update PDN Connection Set Request message, only if Modify Bearer Request is not sent. The message shall contain both SGW FQ-CSID and MME FQ-CSID.
 - Proxy Binding Update (if PMIPv6 is used). The message shall contain both SGW FQ-CSID and MME FQ-CSID.
 - 3) For inter MME and intra SGW HO/TAU, and if the new MME does not support the feature, then the SGW shall:
 - not include any FQ-CSID in the S11 Modify Bearer Response.
 - inform the feature supporting PGW with the following messages:
 - Modify Bearer Request when Modify Bearer Request message needs to be sent to the PGW as specified in the 3GPP TS 23.401 [15], e.g. if the sending of this message is triggered by user location reporting procedure. The message shall contain only SGW FQ-CSID.
 - Update PDN Connection Set Request message, only if Modify Bearer Request is not sent. The message shall contain only SGW FQ-CSID.
 - Proxy Binding Update (if PMIPv6 is used). The message shall contain only the SGW FQ-CSID.
- NOTE: The partial failure handling is not supported by the S4-SGSN, therefore, during the RAU/HO to S4-SGSN procedure, the SGW can behave in the same way as the TAU/HO to a MME which does not support the feature.
- 4) For inter SGW HO/TAU, if the new MME supports the feature, then the new SGW shall:
 - include SGW FQ-CSID in the S11 Create Session Response. If PGW supports the feature, the SGW shall also include PGW FQ-CSID into the message.

- inform the feature supporting PGW about the change of FQ-CSID values with the following messages:
 - Modify Bearer Request. The message shall contain both SGW FQ-CSID and MME FQ-CSID.
 - Proxy Binding Update (if PMIPv6 is used). The message shall contain both SGW FQ-CSID and MME FQ-CSID.
- 5) For inter SGW HO/TAU, if the MME does not support the feature, then the SGW shall:
 - not include any FQ-CSID in the S11 Create Session Response.
 - inform the feature supporting PGW about the change of SGW FQ-CSID value with the following messages:
 - Modify Bearer Request. The message shall contain only SGW FQ-CSID
 - Proxy Binding Update (if PMIPv6 is used). The message shall contain only the SGW FQ-CSID.
- 6) If the SGW receives a FQ-CSID value of a PGW over S5/S8, or a FQ-CSID value of a MME over S11, the SGW shall overwrite the current stored FQ-CSID value with the received value.
- 7) During the PDN connection removing procedures, a PGW removes the PDN data as well as any stored FQ-CSID values(s) of the MME and SGW FQ-CSIDs.
- 8) For the following procedures, if the procedures as specified in 3GPP TS 23.401 [15] e.g. Location Change reporting is enabled, the SGW shall send its own FQ-CSID and the MME FQ-CSID in Modify Bearer Request and Proxy Binding Update across S5/S8 interface to the respective PGW even if the MME did not update its FQ-CSID, e.g.:
 - X2-based Handover without SGW relocation
 - TAU without MME and without SGW relocation
 - UE Triggered Service Request

During a S11 or S5/S8 procedure removing an existing PDN connection the SGW simply removes the PDN data as well as any stored FQ-CSID values(s) of the PGW FQ-CSID and MME FQ-CSID or pointers to such data. The same actions are done on the old SGW if there is an SGW relocation.

An SGW determines that the MME supports partial failure handling if MME FQ-CSID is present in the received S11 Modify Bearer Request or S11 Create Session Request (with both MME and SGW change) messages.

A new SGW determines that the PGW supports partial failure handling if PGW FQ-CSID is present in the S5/S8 Modify Bearer Response for GTPv2 based S5/S8 or in the Proxy Binding Acknowledgement for PMIPv6 based S5/S8.

17 Restoration of data in the PGW

17.1 Restart of the PGW

17.1.0 PGW Failure

When a PGW fails, all its Bearer contexts affected by the failure become invalid and may be deleted. PGW storage of subscriber data is volatile.

When the PGW receives a GTP-U PDU for which no Bearer context exists, it shall discard the GTP-U PDU and return a GTP error indication to the originating node i.e. the SGW/ePDG/TWAN.

The PGW should ensure as far as possible that previously used TEID values are not immediately reused after a PGW restart, in order to avoid inconsistent TEID allocation throughout the network.

17.1.1 Restoration Procedures

After a PGW restart, the PGW shall delete all MM Bearer contexts affected by the restart that it may have stored.

During or immediately after a PGW Restart, the PGW shall place this PGW restart counter value in all GTPv2 echo requests/responses and PMIPv6 heartbeat responses the PGW sends.

17.1a Restart of the PGW-C

17.1a.1 PGW-C failure

When a PGW-C fails, all its Bearer, session contexts and Sx associations affected by the failure become invalid and may be deleted.

If F-TEID allocation is performed in the PGW-C, the PGW-C should ensure as far as possible that previously used F-TEID values are not immediately reused after a PGW-C restart, in order to avoid inconsistent TEID allocation throughout the network.

NOTE: This is to ensure that F-TEIDs are not reused until earlier PDN connections using them are released.

17.1a.2 Restoration Procedures

After a PGW-C restart, the PGW-C shall delete all MM Bearer and session contexts, and Sx Associations affected by the restart that it may have stored.

During or immediately after a PGW-C Restart, the PGW-C shall place local PGW-C Recovery Time Stamp value in all Heartbeat Request/Response and Sx Association Setup Request/Response Messages.

17.1b Restart of the PGW-U

17.1b.1 PGW-U failure

When a PGW-U fails, all its Session contexts and Sx associations affected by the failure become invalid and may be deleted.

If F-TEID allocation is performed in the PGW-U, the PGW-U shall ensure that previously used F-TEID values are not immediately reused after a PGW-U restart, in order to avoid inconsistent TEID allocation throughout the network and to enable the restoration of Sx sessions affected by the failure. How this is ensured is implementation specific.

The PGW-U shall not send Error indication message for a configurable period after an PGW-U restart when the PGW-U receives G-PDU not matching any PDRs.

17.1b.2 Restoration Procedures

During or immediately after an PGW-U Restart, the PGW-U shall place local PGW-U Recovery Time Stamp value in all Heartbeat Request/Response and Sx Association Setup Request/Response Messages.

Immediately after the re-establishment of an Sx association between the PGW-C and the PGW-U, the PGW-C may start restoring Sx sessions in the PGW-U.

NOTE : Restoring Sx sessions in a PGW-U on a reactive basis (like defined for an SGW-U restart in subclause 16.1A.4) is not supported in this release. In some cases, a restarted PGW-U cannot determine from the UE IP address the CP function responsible for an incoming packet for which no session exists, e.g. when a UP function is controlled by multiple CP function for the same APN and when the UE IP address was assigned by the PDN.

17.1A Restart of a peer node

17.1A.1 SGW/ePDG/TWAN Failure

The PGW will receive the SGW/ePDG/TWAN restart counters in GTPv2 echo requests/responses and PMIPv6 heartbeat responses that the PGW receives from the SGW/ePDG/TWAN.

When a PGW detects that a peer ePDG/peer TWAN has restarted it shall delete all PDN connection table data/MM bearer contexts associated with the peer node that fails as well as freeing any internal PGW resources associated with those PDN connections. The PGW may optionally perform other implementation specific actions such as messages to clear other external resources (e.g. PCC messages).

When a PGW detects that a peer SGW has failed with or without restart it shall either:

- proceed as specified above when the PGW detects that a peer ePDG/TWAN fails; or
- follow the procedures specified in clause 27 to restore the PDN connections affected by the SGW failure, if the MME/S4-SGSN and the PGW support these procedures.

NOTE: The PGW will have the identity of SGW/ePDG/TWAN currently in use for a PDN connection available in the PGW's PDN connection table as part of existing EPC procedure.

For multi-access PDN connection in the Network-initiated NBIFOM mode, when the PGW detects ePDG/TWAN has failed, the PGW may:

- maintain the PDN connection on the 3GPP access and notify the PCRF the removal of Non-3GPP access. Then the PCRF can determine to move the affected traffic to the 3GPP access by updating the PCC rules as specified in the subclause 5.8 in the 3GPP TS 23.161 [39].

For multi-access PDN connection in the Network-initiated NBIFOM mode, when the PGW detects that the SGW has failed, the PGW may:

- maintain the PDN connection on the Non-3GPP access and notify the PCRF the removal of 3GPP access. Then the PCRF can determine to move the affected traffic to the 3GPP access by updating the PCC rules as specified in the subclause 5.8 in the 3GPP TS 23.161 [39], if the SGW restoration procedures as specified in clause 27 are not supported; or,
- follow the SGW restoration procedures specified in clause 27, e.g. maintain the PDN connection on both non-3GPP access and 3GPP access without notify the PCRF about SGW failure, if the SGW restoration procedures are supported.

17.1A.2 PCRF Failure

If the PGW needs to send a request for IP-CAN Session Modification procedure towards a PCRF which is known to have restarted since the IP-CAN session establishment, the PGW may discard the request and may tear down the associated PDN connection, based on operator policy, by initiating a PGW initiated bearer deactivation procedure for the default bearer towards the MME/S4-SGSN with the cause set to "Reactivation requested". This leads the UE to initiate a UE requested PDN connectivity procedure for the same APN. Emergency and eMPS sessions should not be torn down.

NOTE: The procedure above just enables to clean up the PDN connection affected by the PCRF failure when a specific interaction with the PCRF is required. Prior to that interaction, PCC controlled services can not be provided to the UE.

17.1A.3 PGW-C Failure

The PGW-U will receive the PGW-C recovery time stamps in Sx Association Setup Request/Response and PFCP heartbeat requests/responses.

When a PGW-U detects that a peer PGW-C has restarted, the PGW-U shall delete all session contexts and the Sx association contexts affected by the restart that it may have stored.

17.1A.4 PGW-U Failure

The PGW-C will receive the PGW-U recovery time stamps in Sx Association Setup Request/Response and PFCP heartbeat requests/responses.

Immediately after the re-establishment of an Sx association between the PGW-C and the PGW-U, the PGW-C may start restoring Sx sessions in the PGW-U.

17.2 Partial Failure Handling at PGW

17.2.1 General

See Section 23.

17.2.2 Procedures during PDN Connection Establishment

If the PGW supports the feature, the following procedures apply.

During a PDN connection establishment, the PGW shall provide one FQ-CSID containing exactly one CSID for that particular PDN connection to the SGW, the ePDG or the TWAN. The PGW shall store the FQ-CSID provided by the SGW and the MME in the PDN Connection table maintained as part of P-GW Context as specified in Table 5.7.3-1 in 3GPP TS 23.401 [15]. Similarly, the PGW shall store the FQ-CSID received from the ePDG or the TWAN.

The PGW should ensure as far as possible that previously used FQ-CSIDs are not immediately reused after a partial/full failure of a PGW.

PGW determines that the partial failure handling does not apply to this PDN connection if it does not receive an SGW FQ-CSID in the S5/S8 Create Session Request (for GTP based interface) or in Proxy Binding Update (for PMIPv6 based interface), or if it does not receive a TWAN FQ-CSID in the S2a Create Session Request (for GTP based S2a) or in Proxy Binding Update (for PMIPv6 based S2a), or if it does not receive an ePDG FQ-CSID in the S2b Create Session Request (for GTP based S2b) or in Proxy Binding Update (for PMIPv6 based S2b).

17.2.3 Procedures during PGW Partial Failure

If the PGW supports the feature, the following procedures apply.

When a PGW detects that it has undergone a partial failure, it shall verify that one or more corresponding CSID(s) are present for the component(s) undergoing a partial fault. If there is no such CSID, then the following does not apply. When one or more CSIDs are currently assigned, the PGW shall perform the following:

- The PGW may perform implementation-specific operations to clean up any residual state associated with the CSID(s).
- The PGW shall send the GTPv2 Delete PDN Connection Set Request (or PMIPv6 Binding Revocation Indication with G bit set) message containing all the PGW FQ-CSID(s) of the component(s) failing to the SGW, the TWAN or the ePDG that support the feature.

Upon receiving a GTPv2 Delete PDN Connection Set Response message with Cause value "Success", the PGW shall conclude that the SGW, the ePDG peer or the TWAN peer has initiated the internal deletion of the PDN connections corresponding to the FQ-CSID(s) present in the GTPv2 Delete PDN Connection Set Request message. Similarly, upon receiving a PMIPv6 Binding Revocation Acknowledgment message with G bit set, the PGW shall conclude that the SGW, the ePDG or the TWAN has initiated the internal deletion of the PDN connections corresponding to the CSID(s) present in the PMIPv6 Binding Revocation Indication message with G bit set.

The PGW is not required to perform any further recovery actions towards SGW, MME peers, an ePDG peer or a TWAN peer for PDN connections in the connection set identified by the PGW FQ-CSID regardless of the "Cause" value in the response.

17.2.4 Procedures during a Peer's Partial Failure

If the PGW supports the feature, the following procedures apply.

When a PGW receives a GTPv2 Delete PDN Connection Set Request (or PMIPv6 Binding Revocation Indication with G bit set) message from an SGW, an ePDG or a TWAN, the PGW shall retrieve all the PDN connections corresponding to each of the FQ-CSIDs present in the message. The PGW shall delete all the retrieved PDN connections and the associated resources. Other implementation-specific actions may be performed.

As a response, the PGW shall send a GTPv2 Delete PDN Connection Set Response message. On PMIPv6-based S5/S8 interface, the PGW shall send a PMIPv6 Binding Revocation Acknowledgment message with G bit set.

17.2.5 Procedures during PDN Connection Removal or Modification

If the PGW supports the feature, the following procedures apply.

During a S5/S8 procedure, impacting an existing PDN connection Removal or Modification the following apply:

- 1) If an SGW is being relocated then the PGW shall clear the currently stored MME and SGW FQ-CSID values.
- 2) If the SGW includes a SGW FQ-CSID in the S5/S8 Modify Bearer Request (Proxy Binding Update for PMIPv6), or Update PDN Connection Request message, then the PGW shall include PGW FQ-CSID in the S5/S8 Modify Bearer Response (Proxy Binding Acknowledgement for PMIPv6), or Update PDN Connection Response message.
- 3) If the new SGW does not include a SGW FQ-CSID in the S5/S8 Modify Bearer Request (Proxy Binding Update for PMIPv6), then the new SGW does not support the feature and the feature does not apply for this PDN connection. In such case, PGW shall not include PGW FQ-CSID in the S5/S8 Modify Bearer Response (Proxy Binding Acknowledgement for PMIPv6).
- 4) If the PGW receives an SGW FQ-CSID and/or an MME FQ-CSID value of a SGW over S5/S8 then the PGW shall overwrite the respective stored FQ-CSID value with the received value.
- 5) If the PGW receives an Update PDN Connection Request, a Modify Bearer Request or Proxy Binding Update with an SGW FQ-CSID but without an MME FQ-CSID then the PGW shall erase the MME FQ-CSID value (i.e. the current MME does not support the feature).
- 6) During a S5/S8 procedure removing an existing PDN connection the PGW simply removes the PDN data as well as any stored FQ-CSID values(s) of the MME and SGW or pointers to such data.

During an S2a/S2b procedure, impacting an existing PDN connection Removal or Modification the following apply:

- 1) If the PGW receives a TWAN or an ePDG FQ-CSID value then the PGW shall overwrite the respective stored FQ-CSID value with the received value;
- 2) During an S2a/S2b procedure removing an existing PDN connection, the PGW removes the corresponding PDN data as well as any stored FQ-CSID value of the TWAN or the ePDG FQ-CSID.

17A Restoration of data in the MBMS GW

17A.1 Restart of the MBMS GW

When a MBMS GW fails, all its MBMS Bearer contexts affected by the failure become invalid and will be deleted. MBMS GW storage of subscriber data is volatile.

After a MBMS GW restart, all the MBMS Bearer contexts stored in the MBMS GW and affected by the restart become invalid and will be deleted. All the SGmb Diameter sessions affected by the restart are also lost in the MBMS GW.

When the SGSN/MME detects a restart in a MBMS GW (see clause 18 "GTP-C based restart procedures") with which it has MBMS Bearer contexts activated, it shall deactivate all the related MBMS Bearer contexts locally and towards E-UTRAN/UTRAN in which the MBMS bearer service is active. The MME shall initiate a M3AP Reset procedure (see

subclause 8.5 of 3GPP TS 36.444 [28]), or an MBMS Session Stop procedure per affected MBMS service (see subclause 8.3 of 3GPP TS 36.444 [28]), towards the MCE(s) to deactivate the related MBMS services in E-UTRAN. The SGSN shall initiate an MBMS Session Stop procedure per affected MBMS service (see subclause 8.38 of 3GPP TS 25.413 [29]), towards the RNC(s) to deactivate the related MBMS services in UTRAN.

If the MBMS GW receives a non-initial message (i.e. MBMS session update or MBMS session stop request) from the BM-SC for which no SGmb Diameter session exists, the MBMW GW shall discard the message and return a Diameter error indication to the originating BM-SC.

In deployments without a Diameter Agent between the BM-SC and the MBMS GW, the BM-SC shall detect a restart in the MBMS GW using either:

- the Diameter Origin-State-Id AVP as specified in the Diameter Base Protocol. To enable fast detection of restart, the Diameter Origin-State-Id AVP shall be included (at least) in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands; or
- the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the MBMS GW, the BM-SC shall detect a restart in the MBMS GW using the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29).

NOTE 1: The intermediate Diameter Agent can remove or update the Diameter Origin-State-Id AVP, e.g. if it needs to modify the Origin-Host-ID. Thus the Diameter Origin-State-Id AVP, if received by the BM-SC or MBMS GW, does not reflect the state of the remote MBMS peer but the state of the Diameter Agent.

When the BM-SC detects a restart in a MBMS GW with which it has at least one MBMS Bearer context, the BM-SC shall maintain the related MBMS bearer context(s), assume that all related SGmb Diameter session(s) have been terminated and clean-up internal resources associated with these lost session(s). The BM-SC should then re-establish the active MBMS bearer services affected by the MBMS GW restart by initiating MBMS Session Start procedure(s) towards the restarted MBMS GW (or an alternative MBMS GW). The BM-SC shall encode the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request sent by the BM-SC if the original parameters were updated) with the following exceptions:

- the BM-SC shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- if no absolute start time ("MBMS data transfer start" parameter) has been sent, the BM-SC may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the BM-SC should set the estimated session duration to a value corresponding to the remaining duration of the session.

NOTE 2: If the BM-SC is instructed to modify an MBMS Session during the MBMS GW failure/restart, the contents of the MBMS Session Start Request sent to the MBMS GW after the MBMS GW restart can also differ from the parameters sent to the MBMS GW before its restart for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

17A.2 Restart of a peer node

17A.2.1 MME failure

The behaviour of an MBMS GW when it detects that a peer MME has restarted is described in subclause 14.1.1.

17A.2.2 SGSN failure

The behaviour of an MBMS GW when it detects that a peer SGSN has restarted is described in subclause 11.1.

17A.2.3 BM-SC failure

In deployments without a Diameter Agent between the BM-SC and the MBMS GW, the MBMS GW shall detect a restart in the BM-SC using either:

- the Diameter Origin-State-Id AVP as specified in the Diameter Base Protocol. To enable fast detection of restart, the Diameter Origin-State-Id AVP shall be included (at least) in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands; or
- the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the MBMS GW, the MBMS GW shall detect a restart in the BM-SC using the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29).

NOTE: The intermediate Diameter Agent can remove or update the Diameter Origin-State-Id AVP, e.g. if it needs to modify the Origin-Host-ID. Thus the Diameter Origin-State-Id AVP, if received by the BM-SC or MBMS GW, does not reflect the state of the remote MBMS peer but the state of the Diameter Agent.

When the MBMS GW detects a restart of the BM-SC with which it has at least one MBMS Bearer context, the MBMS GW shall assume that all related SGmb Diameter session(s) have been terminated and shall deactivate all the related MBMS Bearer contexts locally and towards E-UTRAN/UTRAN in which the MBMS bearer service is active by sending MBMS Session Stop messages to their controlling MME/SGSNs.

17B Restoration of data in the ePDG

17B.1 Restart of the ePDG

17B.1.1 ePDG Failure

When an ePDG fails, all its Bearer contexts/PDN connections affected by the failure become invalid and may be deleted. ePDG storage of subscriber data is volatile.

When the ePDG receives a GTP-U PDU over GTPv2 based S2b for which no Bearer context exists, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (i.e. the PGW).

The ePDG should ensure as far as possible that previously used TEID values are not immediately reused after an ePDG restart, in order to avoid inconsistent TEID allocation throughout the network.

When the ePDG receives a user packet with an unknown GRE Key over PMIPv6 based S2b, the ePDG shall discard the packet and optionally response back with an ICMP message, as specified in Sections 8.2 and 8.3 of IETF RFC2473 [31] for the node unreachable error case.

17B.1.2 Restoration Procedures

After an ePDG restart, the ePDG shall delete all MM Bearer contexts affected by the restart that it may have stored.

During or immediately after an ePDG Restart the ePDG shall place local ePDG restart counter value in all GTPv2 Echo requests/responses messages and PMIPv6 heartbeat responses the ePDG sends to the PGW.

17B.1A Restart of a peer node

17B.1A.1 PGW Failure

The ePDG will receive the PGW restart counter in GTPv2 Echo requests/ responses and PMIPv6 heartbeat responses that the ePDG receives from the PGW.

When an ePDG detects that a peer PGW has restarted (see clause 18 "GTP-C based restart procedures" and clause 19 "PMIPv6 based restart procedures") it shall delete all PDN connection table data/MM bearer contexts associated with the peer node that fails, free any internal ePDG resources associated with those PDN connections and initiate the release of the corresponding SWu instances (i.e. IKEv2 tunnels).

17B.2 Partial Failure Handling at ePDG

17B.2.1 General

See section 23.

The partial failure feature is optional for ePDG.

If the ePDG does not support the feature then partial failure handling does not apply to that specific PDN connection.

17B.2.2 Procedures during PDN Connection Establishment

If the ePDG supports the feature, the following procedures apply.

During a PDN connection establishment, the ePDG shall provide one ePDG FQ-CSID containing exactly one CSID for that particular PDN connection to the PGW. The ePDG shall store the Node-ID and CSID from the FQ-CSID provided by the PGW for that particular PDN connection in its PDN Connection table.

The ePDG determines that the PGW supports partial failure handling by the presence of the PGW FQ-CSID in the Create Session Response for GTPv2 based S2b and/or Proxy Binding Acknowledgement message for PMIPv6 based S2b.

17B.2.3 Procedures during ePDG Partial Failure

If the ePDG supports the feature, the following procedures apply.

When an ePDG detects that it has undergone a partial failure, it shall verify that one or more corresponding CSID(s) are present for the component undergoing a partial fault. If there is no such CSID, then the following does not apply. When one or more CSIDs are currently assigned, the ePDG shall perform the following.

The ePDG may perform implementation-specific operations to clean up any residual state associated with the CSID(s).

The ePDG shall send Delete PDN Connection Set Request containing all the ePDG CSIDs of the component(s) failing in ePDG FQ-CSID over the GTPv2 based S2b interface or PMIPv6 Binding Revocation Indication with G bit set message containing the equivalent ePDG FQ-CSID(s) over the PMIPv6 based S2b interface to PGW peers supporting the feature.

On the GTPv2 based S2b interface, upon receiving a GTPv2 Delete PDN Connection Set Response message with Cause value "Success", the ePDG shall conclude that the PGW has initiated the internal deletion of the PDN connections corresponding to the FQ-CSID(s) present in the GTPv2 Delete PDN Connection Set Request message. Similarly, on the PMIPv6 based S2b interface, upon receiving a successful PMIPv6 Binding Revocation Acknowledgment message with G bit set, the ePDG shall conclude that the PGW has initiated the internal deletion of the PDN connections corresponding to the CSID(s) present in the PMIPv6 Binding Revocation Indication message.

The ePDG is not required to perform any further recovery actions towards PGW peers for PDN connections in the connection set identified by the PGW FQ-CSID(s).

17B.2.4 Procedures during PGW Partial Failure

If the ePDG supports the feature, the following procedures apply.

When an ePDG receives a GTPv2 Delete PDN Connection Set Request or PMIPv6 Binding Revocation Indication with G bit set message from a PGW, the ePDG shall retrieve all the PDN connections corresponding to each of the FQ-CSID(s) present in the message. The ePDG shall delete all the retrieved PDN connections, free the associated internal resources and initiate the release of the corresponding SWu instances (i.e. IKEv2 tunnels). Other implementation-specific actions may be performed.

As a response, the ePDG shall send a GTPv2 Delete PDN Connection Set Response message with an appropriate Cause value or a PMIPv6 Binding Revocation Acknowledgment message with G bit set to the PGW.

17B.2.5 Procedures during PDN Connection Removal or Modification

For the modification of an existing PDN connection established over 2b, if the corresponding ePDG and PGW support the partial failure feature, when the ePDG receives an FQ-CSID value of a PGW over S2b, the ePDG shall overwrite the currently stored FQ CSID value with the received value.

For the removal of an existing PDN connection established over S2b, if the corresponding ePDG and PGW support the partial failure feature, an ePDG removes the corresponding PDN data as well as any relevant stored FQ-CSID value of the PGW FQ-CSID.

17C Restoration of data in the TWAN

17C.1 Restart of the TWAN

17C.1.1 TWAN Failure

When a TWAN fails, all its Bearer contexts/PDN connections affected by the failure become invalid and may be deleted. TWAN storage of subscriber data is volatile.

When the TWAN receives a GTP-U PDU over GTPv2 based S2a for which no Bearer context exists, it shall discard the GTP-U PDU and return a GTP error indication to the originating node (i.e. the PGW).

The TWAN should ensure as far as possible that previously used TEID values are not immediately reused after a TWAN restart, in order to avoid inconsistent TEID allocation throughout the network.

When the TWAN receives a user packet with an unknown GRE Key over PMIPv6 based S2a, the TWAN shall discard the packet and optionally respond back with an ICMP message, as specified in Sections 8.2 and 8.3 of IETF RFC2473 [31] for the node unreachable error case.

17C.1.2 Restoration Procedures

After a TWAN restart, the TWAN shall delete all Bearer contexts affected by the restart that it may have stored and place local TWAN restart counter value in all GTPv2 Echo requests/responses messages and PMIPv6 heartbeat responses the TWAN sends to the PGW.

17C.1A Restart of a peer node

17C.1A.1 PGW Failure

The TWAN will receive the PGW restart counter in GTPv2 Echo requests/ responses and PMIPv6 heartbeat responses that the TWAN receives from the PGW.

When a TWAN detects that a peer PGW has restarted (see clause 18 "GTP-C based restart procedures" and clause 19 "PMIPv6 based restart procedures") it shall delete all PDN connection table data/bearer contexts associated with the peer node that fails, and may free the associated internal TWAN resources.

17C.2 Partial Failure Handling at TWAN

17C.2.1 General

See section 23.

The partial failure feature is optional for TWAN.

If the TWAN does not support the feature then partial failure handling does not apply to that specific PDN connection.

17C.2.2 Procedures during PDN Connection Establishment

If the TWAN supports the feature, the following procedures apply.

During a PDN connection establishment, the TWAN shall provide one TWAN FQ-CSID containing exactly one CSID for that particular PDN connection to the PGW. The TWAN shall store the Node-ID and CSID from the FQ-CSID provided by the PGW for that particular PDN connection in its PDN Connection table.

The TWAN determines that the PGW supports partial failure handling by the presence of the PGW FQ-CSID in the Create Session Response for GTPv2 based S2a and/or Proxy Binding Acknowledgement message for PMIPv6 based S2a.

17C.2.3 Procedures during TWAN Partial Failure

If the TWAN supports the feature, the following procedures apply.

When a TWAN detects that it has undergone a partial failure, it shall verify that one or more corresponding CSID(s) are present for the component undergoing a partial fault. If there is no such CSID, then the following does not apply. When one or more CSIDs are currently assigned, the TWAN shall perform the following.

The TWAN may perform implementation-specific operations to clean up any residual state associated with the CSID(s).

The TWAN shall send Delete PDN Connection Set Request containing all the TWAN CSIDs of the component(s) failing in TWAN FQ-CSID over the GTPv2 based S2a interface or PMIPv6 Binding Revocation Indication with G bit set message containing the equivalent TWAN FQ-CSID(s) over the PMIPv6 based S2a interface to PGW peers supporting the feature.

On the GTPv2 based S2a interface, upon receiving a GTPv2 Delete PDN Connection Set Response message with Cause value "Success", the TWAN shall conclude that the PGW has initiated the internal deletion of the PDN connections corresponding to the FQ-CSID(s) present in the GTPv2 Delete PDN Connection Set Request message. Similarly, on the PMIPv6 based S2a interface, upon receiving a successful PMIPv6 Binding Revocation Acknowledgment message with G bit set, the TWAN shall conclude that the PGW has initiated the internal deletion of the PDN connections corresponding to the CSID(s) present in the PMIPv6 Binding Revocation Indication message.

The TWAN is not required to perform any further recovery actions towards PGW peers for PDN connections in the connection set identified by the PGW FQ-CSID(s).

17C.2.4 Procedures during PGW Partial Failure

If the TWAN supports the feature, the following procedures apply.

When an TWAN receives a GTPv2 Delete PDN Connection Set Request or PMIPv6 Binding Revocation Indication with G bit set message from a PGW, the TWAN shall retrieve all the PDN connections corresponding to each of the FQ-CSID(s) present in the message. The TWAN shall delete all the retrieved PDN connections, and may free the associated internal TWAN resources.

As a response, the TWAN shall send a GTPv2 Delete PDN Connection Set Response message with an appropriate Cause value or a PMIPv6 Binding Revocation Acknowledgment message with G bit set to the PGW.

17C.2.5 Procedures during PDN Connection Removal or Modification

For the modification of an existing PDN connection established over S2a, if the corresponding TWAN and PGW support the partial failure feature, when the TWAN receives an FQ-CSID value of a PGW over S2a, the TWAN shall overwrite the currently stored FQ CSID value with the received value.

For the removal of an existing PDN connection established over S2a, if the corresponding TWAN and PGW support the partial failure feature, a TWAN removes the corresponding PDN data as well as any relevant stored FQ-CSID value of the PGW FQ-CSID.

17D Restoration of data in the BM-SC

17D.1 Restart of the BM-SC

When a BM-SC fails, all its MBMS Bearer contexts affected by the failure become invalid and will be deleted.

After a BM-SC restart, all the MBMS Bearer contexts stored in the BM-SC and affected by the restart become invalid and will be deleted. All the SGmb Diameter sessions affected by the restart are also lost in the BM-SC. If Group Communication Service (GCS) is supported, the BM-SC also loses the knowledge of the TMGIs it had allocated to the Group Communication Service Application Server(s) (GCS AS) before restarting.

When the MBMS GW detects the restart of a BM-SC, it shall behave as described in subclause 17A.2.3.

When the GCS AS detects the restart of a BM-SC, it shall behave as described in subclause 17E.1. The restoration of MBMS services by content providers other than GCS AS after a BM-SC failure or restart is out of scope of 3GPP.

NOTE: The reference point from content providers other than GCS AS to the BM-SC is not standardised by 3GPP.

17D.2 Restart of the GCS AS

In deployments without a Diameter Agent between the GCS AS and the BM-SC, the BM-SC shall detect a restart in the GCS AS using either:

- the Diameter Origin-State-Id AVP as specified in the Diameter Base Protocol. To enable fast detection of restart, the Diameter Origin-State-Id AVP shall be included (at least) in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands; or
- the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the GCS AS and the BM-SC, the BM-SC shall detect a restart in the GCS AS using the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29).

NOTE: The intermediate Diameter Agent can remove or update the Diameter Origin-State-Id AVP, e.g. if it needs to modify the Origin-Host-ID. Thus the Diameter Origin-State-Id AVP, if received by the BM-SC or GCS AS, does not reflect the state of the remote MBMS peer but the state of the Diameter Agent.

When the BM-SC detects a restart of the GCS AS, the BM-SC shall deallocate (locally) all the TMGIs that had been assigned to the restarted GCS AS and the BM-SC shall stop all the related MBMS bearers to free the corresponding resources in E-UTRAN.

17E Restoration of data in the GCS AS

17E.1 Restart of the GCS-AS

After a GCS AS restart, the GCS AS loses its MBMS bearer contexts and the knowledge of the TMGIs it had been allocated by the BM-SC(s) before restarting.

When the BM-SC detects the restart of a GCS AS, it shall behave as described in subclause 17D.2.

17E.2 Restart of the BM-SC

In deployments without a Diameter Agent between the GCS AS and the BM-SC, the GCS AS shall detect a restart in the BM-SC using either:

- the Diameter Origin-State-Id AVP as specified in the Diameter Base Protocol. To enable fast detection of restart, the Diameter Origin-State-Id AVP shall be included (at least) in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands; or
- the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the GCS AS and the BM-SC, the GCS AS shall detect a restart in the BM-SC using the Diameter Restart-Counter AVP as specified in the MBMS Heartbeat procedure (see clause 29).

NOTE: The intermediate Diameter Agent can remove or update the Diameter Origin-State-Id AVP, e.g. if it needs to modify the Origin-Host-ID. Thus the Diameter Origin-State-Id AVP, if received by the BM-SC or GCS AS, does not reflect the state of the remote MBMS peer but the state of the Diameter Agent.

When the GCS AS detects a restart of the BM-SC, the GCS AS shall assume that all the TMGIs that had been assigned by the restarted BM-SC have been de-allocated and that all the related MBMS bearers have been deactivated.

The GCS AS may restore the MBMS delivery using the MB2-C procedures specified in 3GPP TS 29.468 [35].

18 GTP-C based restart procedures

Across GTP-C based interfaces an SGSN, GGSN, MME, SGW, PGW, TWAN, ePDG and HRPD Access Node utilize either GTPv1-C or GTPv2-C Echo Request and Echo Response messages or GTP-C messages containing the Recovery Information Element to detect and handle a restart.

A GTP-C entity shall maintain two Restart counters:

- in volatile memory a remote Restart counter of a peer with which the entity is in contact;
- in non-volatile memory own, or local Restart counter that was sent to a peer.

After a GTP-C entity has restarted, it shall immediately increment all local Restart counters and shall clear all remote Restart counters.

A GTP-C entity may have a common local Restart counter for all peers, or it may have a separate local Restart counter for each peer.

A GTP-C entity may probe the liveness of each peer with which it is in contact by sending an Echo Request message (see clause 20 "Path management procedures") . The presence of the Restart counter in Echo Request or in a GTP-C message depends on the GTP-C version and therefore is specified in 3GPP TS 29.060 [8] and 3GPP TS 29.274 [13], respectively. The restart counter signalled in the GTP-C message is associated with the GTP-C entity identified by the sender's F-TEID or SGSN/GGSN IP address for control plane if present in the message, otherwise (e.g. in echo request message) it is associated with the GTP-C entity identified by the source IP address of the message.

The GTP-C entity that receives a Recovery Information Element in an Echo Response or in another GTP-C message from a peer, shall compare the received remote Restart counter value with the previous Restart counter value stored for that peer entity.

- If no previous value was stored the Restart counter value received in the Echo Response or in the GTP-C message shall be stored for the peer.
- If the value of a Restart counter previously stored for a peer is smaller than the Restart counter value received in the Echo Response message or the GTP-C message, taking the integer roll-over into account, this indicates that the entity that sent the Echo Response or the GTP-C message has restarted. The received, new Restart counter value shall be stored by the receiving entity, replacing the value previously stored for the peer.
- If the value of a Restart counter previously stored for a peer is larger than the Restart counter value received in the Echo Response message or the GTP-C message, taking the integer roll-over into account, this indicates a possible race condition (newer message arriving before the older one). The received new Restart counter value shall be discarded and an error may be logged.

19 PMIPv6 based restart procedures

Across PMIPv6 based interfaces, SGW, PGW, TWAN and ePDG utilize PMIPv6 Heartbeat mechanism for node restart detection as specified in 3GPP TS 29.275 [16].

A PMIPv6 entity shall maintain two restart counters:

- in volatile memory a remote restart counter of a peer with which the entity is in contact;
- in non-volatile memory an own, or local restart counter that was sent to a peer.

After a PMIPv6 entity has restarted, it shall immediately increment all local restart counters and shall clear all remote restart counters.

A PMIPv6 entity may have a common local restart counter for all peers, or it may have a separate local restart counter for each peer.

19A PFCP based restart procedures

Across PFCP based interfaces, an SGW-C, SGW-U, PGW-C and PGW-U Node shall utilize PFCP Heartbeat Request and Heartbeat Response messages or PFCP messages containing the Recovery Time Stamp to detect and handle a peer PFCP failure or restart.

A PFCP entity shall maintain two Recovery Time Stamps:

- in volatile memory a remote Recovery Time Stamp of a peer with which the entity is in contact;
- in non-volatile memory own, or local Recovery Time Stamp that was sent to a peer.

After a PFCP entity has restarted, it shall immediately update all local Recovery Time Stamps and shall clear all remote Recovery Time Stamps.

A PFCP entity may have a common local Recovery Time Stamp for all peers, or it may have a separate local Recovery Time Stamp for each peer.

A PFCP entity may probe the liveness of each peer with which it is in contact by sending a Heartbeat Request message (see clause 20 "Path management procedures"). The Recovery Time Stamp signalled in the PFCP message is associated with the PFCP entity identified by the sender's F-SEID or IP address of CP or UP function if present in the message, otherwise (e.g. in Heartbeat request message) it is associated with the PFCP entity identified by the source IP address of the message.

The PFCP entity that receives a Recovery Time Stamp Information Element in a Heartbeat Response or in another PFCP message from a peer shall compare the received remote Recovery Time Stamp value with the previous Recovery Time Stamp value stored for that peer entity.

- If no previous value was stored, the Recovery Time Stamp value received in the Heartbeat Response or in the PFCP message shall be stored for the peer.
- If the value of a Recovery Time Stamp previously stored for a peer is smaller than the Recovery Time Stamp value received in the Heartbeat Response message or the PFCP message, this indicates that the entity that sent the Heartbeat Response or the PFCP message has restarted. The received, new Recovery Time Stamp value shall be stored by the receiving entity, replacing the value previously stored for the peer.
- If the value of a Recovery Time Stamp previously stored for a peer is larger than the Recovery Time Stamp value received in the Heartbeat Response message or the PFCP message, this indicates a possible race condition (newer message arriving before the older one). The received Sx node related message and the received new Recovery Time Stamp value shall be discarded and an error may be logged.

20 Path management procedures

20.1 General

This clause specifies path management procedures for GTP-C based, PMIP and PFCP based interfaces.

For GTP based interfaces, Echo Request / Response procedure is used. The usage depends on the GTP-C version in the following way:

- GTPv1-C entity may periodically send an Echo Request message as specified in 3GPP TS 29.060 [8].
- GTPv2 entity shall probe the liveness of each peer with which it is in contact by sending an Echo Request messages (see TS 29.274 [13]). When and how often a GTPv2 Echo Request message may be sent is implementation specific but an Echo Request shall not be sent more often than every 60 s on each path. This does not prevent resending an Echo Request with the same sequence number according to the T3-RESPONSE timer.

It is recommended that GTPv2 Echo Request should be sent only when a GTP-C entity has not received any GTP response message for a previously sent request message on the GTP-C path for, an implementation dependent period of time.

A GTP-C entity (both GTPv1-C and GTPv2) shall be prepared to receive an Echo Request message at any time and it shall reply with an Echo Response message.

For the PMIP based S5/S8 interface, the SGW and PGW shall detect respectively a peer PGW and SGW as currently unavailable by sending a series of PMIPv6 Heartbeat Request messages, and not receiving within a period of time respectively a PMIPv6 Heartbeat Response message (see 3GPP TS 29.275 [16]).

For PFCP based Sxa/Sxb/Sxc interfaces, the CP function shall detect a peer UP function (or vice versa) as currently unavailable by sending a series of PFCP heartbeat Request messages, and not receiving within a period of time respectively a PFCP Heartbeat Response message (see 3GPP TS 29.244 [43])

20.2 Signalling path failure detection and handling

20.2.1 General

GTP-C entities shall support detection of path failure by using Echo Request / Echo Response messages in the following way. A peer's IP address specific counter shall be reset each time an Echo Response message is received from that peer's IP address and incremented when the T3-RESPONSE timer expires for an Echo Request message sent to that peer's IP address. The path shall be considered to be down if the counter exceeds N3-REQUESTS.

PMIP entities shall support detection of path failure as specified for Failure Detection in IETF RFC 5847 [22].

Upon detecting a path failure, the network node should notify the failure via the Operation and Maintenance system and may either:

- delete the PDN connections (EPS bearer contexts) or PDP contexts associated with this peer's IP address; or
- maintain the PDN connections (EPS bearer contexts) or PDP contexts associated with the peer's IP address during an operator configurable maximum path failure duration. The network node shall delete the maintained resources if the path is still down when this duration expires. The network node may delete the maintained resources if control/user plane signalling is received across other interface(s) during the path failure and before the maximum path failure duration timer expires.

NOTE 1: During transient path failures (e.g. path failures not exceeding few minutes at most), maintaining the EPS bearer contexts or PDP contexts associated with the peer's IP address enables the delivery of end user services (when the path is reestablished again) and also avoids unnecessary signalling in the network for restoring those connections.

NOTE 2: It is not intended to maintain PDN connections during long path failures (e.g. exceeding few minutes at most) as this would imply undesirable effects like undue charging.

The following subclauses specify further specific network element requirements.

20.2.2 SGW functionality

20.2.2.1 S11/S4 path failure

It is optional for the SGW to maintain the S5/S8 bearer contexts when the SGW detects a path failure to the MME/S4-SGSN (see subclause 20.2.1). However upon detecting a path failure to the MME/S4-SGSN, an SGW that supports the network triggered service restoration procedure (see clause 25) should maintain the S5/S8 bearer contexts eligible for network initiated service restoration and proceed with the network triggered service restoration procedure with the following modification:

- if the path to the MME/S4-SGSN is down for a duration exceeding the maximum path failure duration and if there is no alternative reachable path, e.g. another MME/S4-SGSN in the same pool or another control plane IP address belonging to the same MME/S4-SGSN, the SGW should locally delete the maintained PDN connections associated with the failed path.

In addition, for UEs in connected state associated with the failed path, the SGW should continue sending downlink packets to the eNodeB/RNC as long as the impacted PDN connections are maintained, regardless of whether the SGW supports the network triggered service restoration procedure or not.

20.2.2.2 S5 path failure

The SGW may support the PGW triggered SGW restoration for an S5 path failure. If so, then the SGW should support the PGW Restart Notification procedure. After detecting a path failure to the PGW, the SGW may delete all the PDN connections affected by the path failure and should also send a PGW Restart Notification message to the MME or S4-SGSN if the PGW Restart Notification procedure is supported by the SGW and MME/S4-SGSN (see subclause 16.1A.2).

- NOTE: The PGW Restart Notification procedure can help the MME to restore the PDN connections earlier since the SGW will detect the S5 path failure and send PGW Restart Notification triggering a PDN connection restoration at the MME, before the PGW sends the PGW Downlink Triggering Notification.

The SGW should proceed with the PGW triggered SGW restoration procedure (see subclause 27.2.3.3) with the following modification:

- The SGW shall include the PGW F-TEID or PGW IP address and GRE key for control plane in the PGW Downlink Triggering Notification message that it sends to the MME/S4-SGSN, if this information is present in the PGW Downlink Triggering Notification/PMIP Update Notification message received from the PGW.

20.2.3 MBMS GW functionality

20.2.3.1 Sm path failure

The MBMS GW may be provisioned with the list (or a sublist) of the MMEs pertaining to the MME pool.

- NOTE 1: The MBMS GW expects only one MME of the MME pool in BM-SC requests received across the SGmb interface.

Upon detecting an Sm path failure, the MBMS GW should maintain the MBMS bearer contexts associated with the peer's MME IP address.

During a transient Sm path failure (e.g. before the maximum path failure duration timer expires), the MBMS GW may process MBMS requests from the BM-SC and intended for the MME for which the Sm path has failed as follows:

- for new MBMS Session Start Request, the MBMS GW may select an alternative MME in the same MME pool and send the MBMS Session Start Request to this alternative MME;
- for MBMS Session Update Request or MBMS Session Stop Request, the MBMS GW may select an alternative MME in the same MME pool, send a MBMS Session Start Request message to this alternative MME and, if successful, send subsequently the MBMS Session Update Request or MBMS Session Stop Request to this alternative MME.

After having selected an alternative MME, the MBMS GW shall consider the MME answering to the MBMS Start Request as the controlling MME for the MBMS session and send any subsequent MBMS Session Update or MBMS Session Stop for this MBMS Session to this MME.

NOTE 2: Each MME of the MME pool provisioned in the MBMS GW supports an M3 interface with the MCE(s).

When detecting a non-transient Sm path failure at the MBMS GW (e.g. the maximum path failure duration timer of the MBMS GW expires), the MBMS GW may move the control of all the affected active MBMS sessions to another MME in the same MME pool (if any other MME is reachable by the MBMS GW) by initiating new MBMS Session Start Request(s) to alternative MME(s).

NOTE 3: This allows to re-establish the MBMS sessions when a MME fails without restart.

The maximum path failure duration timer of the MBMS GW should be configured with a shorter value than the maximum path failure duration timer of the MME to avoid interrupting active MBMS sessions upon a non-transient Sm path failure. The MBMS GW timer should be shorter than the MME timer by at least the period between two Echo Request messages sent by the MME, to avoid that the MME timer expires before the MBMS GW timer if the MME starts its timer before the MBMS GW.

NOTE 4: This enables the MCE to receive a MBMS Session Start request from the new MME controlling the MBMS session before the MCE receives a request to stop the MBMS service from the previous controlling MME.

When sending an MBMS Session Start Request sent to an alternative MME, the MBMS GW shall encode the contents of the request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request sent by the MBMS GW if the original parameters were updated) with the following exceptions:

- the MBMS GW shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- if no absolute start time ("MBMS data transfer start" parameter) has been received, the MBMS GW may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the MBMS GW should set the estimated session duration to a value corresponding to the remaining duration of the session.

NOTE 5: Per the requirements above, if the MBMS GW had started an MBMS session within an MME with the MBMS Service Area (1, 2, 3) and receives during an Sm path failure (towards this MME) an MBMS Session Update from the BM-SC modifying the MBMS Service Area to (3, 4, 5), the MBMS GW will encode the original MBMS Service Area (1, 2, 3) in the MBMS Session Start Request sent to the alternative MME and subsequently send an MBMS Session Update Request with the MBMS Service Area (3,4,5) to the new MME controlling the MBMS session.

NOTE 6: If the previous MME received an MBMS Session Update Request from the MBMS GW but could not propagate it to the MCE due to a M3AP path failure, the contents of the MBMS Session Start Request sent to the MCE via the new MME can also differ from the parameters sent to the MCE via the previous MME for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

After detecting an Sm path failure, the MBMS GW shall determine whether the failure is transient or non transient from the perspective of the MME (e.g. the MBMS GW is provisioned with the maximum path failure timer of the MME). The MBMS GW shall assume that the failure is non transient from the perspective of the MME if the Sm path recovers after a period longer than the maximum path failure timer of the MME plus the period between two Echo Request messages sent by the MME, to ensure that the MME also determines this is a non transient path failure if the MBMS GW starts its timer before the MME. The MBMS GW shall consider that the MBMS session has been released by the MME if the Sm path failure is non transient for the MME. If the Sm path failure remains transient for the MME, the MBMS GW shall behave as follows upon detecting the Sm path recovery:

- if the MBMS GW has already moved the control of the MBMS session to an alternative MME(s), the MBMS GW shall send an MBMS Session Stop Request message to the MME previously controlling the MBMS session with a "Local MBMS bearer context release" indication to instruct that MME to release its MBMS bearer context locally, without sending any message to the MCE(s).

- if the MBMS GW has not yet moved the control of the MBMS session to an alternative MME (e.g. if the MBMS restoration procedures are not supported in the network),
- if the Sm path failure is transient from the perspective of the MBMS GW, the MBMS GW shall consider that MBMS session is still controlled by the related MME and proceed as if there had been no Sm path failure;
- if the Sm path failure is non transient from the perspective of the MBMS GW, the MBMS GW shall send an MBMS Session Start Request to the MME for the session and encode it as specified above (for a message sent to an alternative MME).

NOTE 7: The MBMS GW cannot know whether the MME will see the Sm path failure as transient or non transient if the Sm path recovers in the period between the maximum path failure timer of the MME plus and minus the period between two Echo Request messages sent by the MME. This can possibly lead the MBMS GW to send an MBMS Session Stop request to the MME for a session that has already been terminated by the MME (if the MME determined the failure is non transient) or to send an MBMS Session Start request (with the "MBMS session re-establishment indication" flag) to the MME for a session that is still alive at the MME (if the MME determined the failure is transient).

20.2.3.2 Sn path failure

The MBMS GW may be provisioned with the list (or a sub list) of the SGSNs belonging to the SGSN pool.

NOTE: The MBMS GW expects only one SGSN of the SGSN pool in BM-SC requests received across the SGmb interface.

An MBMS GW and SGSN shall handle Sn path failure similar to the Sm path failure as described in subclause 20.2.3.1 For IP Unicast over Sn/Iu when the SGSN changes the MBMS GW has to move the user plane which is affected by the Sn-path failure additionally.

20.2.3.3 SGmb path failure

In deployments without a Diameter Agent between the BM-SC and the MBMS GW, the MBMS GW shall detect an SGmb path failure using either:

- mechanisms as specified in the Diameter Base Protocol (e.g. transport connection failure, BM-SC peer not responding, Diameter Device-Watchdog-Request and Device-Watchdog-Answer messages during periods when there is no need for other MBMS signalling); or
- the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the MBMS GW, the MBMS GW shall detect an SGmb path failure using the MBMS Heartbeat procedure (see clause 29).

NOTE 1: A transport connection failure does not allow to identify a failure of the remote MBMS peer. Likewise, it is not possible to rely on Diameter Device-Watchdog-Request / Answer messages to test the responsiveness of the remote MBMS node during periods when there is no need for other MBMS signalling as these messages are only exchanged between Diameter peers with a direct transport connection.

Upon detecting an SGmb path failure, the MBMS GW should maintain the MBMS bearer contexts associated with the peer's BM-SC during an operator configurable maximum path failure duration.

If the SGmb path to the BM-SC is down for a duration exceeding the maximum path failure duration, the MBMS GW should deactivate all the related MBMS Bearer contexts locally and send MBMS Session Stop Requests towards all MME/SGSNs in which the MBMS bearer services are active.

NOTE 2: This enables to free corresponding radio resources in E-UTRAN/UTRAN for MBMS services if the BM-SC has failed without restart.

The MBMS GW shall pass on the "MBMS session re-establishment indication" flag in the MBMS Session Start Request it sends to MME/SGSNs if received from the BM-SC.

The MBMS GW shall pass on the "Local MBMS bearer context release" indication in the MBMS Session Stop Request it sends to MME/SGSNs if received from the BM-SC.

The MBMS GW shall accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from the same BM-SC that currently controls the MBMS session if the message includes the "MBMS session re-establishment indication" flag. The MBMS GW shall replace the SGmb related resources for this MBMS service by those received in the MBMS Session Start Request (if different). The MBMS GW should not send MBMS Session Start Request message(s) towards the involved MME/SGSN(s) if no parameters other than the estimated duration and relative start time have changed.

20.2.4 MME functionality

20.2.4.1 Sm path failure

Upon detecting an Sm path failure, the MME should maintain the MBMS bearer contexts associated with the peer's MBMS GW IP address during an operator configurable maximum path failure duration.

The MME should behave as specified for the case of an MBMS GW restart (see subclause 17A.1) if the Sm path to the MBMS GW is down for a duration exceeding the maximum path failure.

NOTE 1: This enables to free corresponding radio resources in E-UTRAN for MBMS services if the MBMS GW has failed without restart.

The MME shall pass on the "MBMS session re-establishment indication" flag in the MBMS Session Start Request it sends to MCEs if received from the MBMS GW.

The MME should accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from a different MBMS GW than the MBMS GW that currently controls the MBMS session if the message includes the "MBMS session re-establishment indication" flag. If it accepts the request from the new MBMS GW, the MME shall replace the Sm related resources (i.e. TEID-C) for this MBMS service associated to the previous MBMS GW by those associated to the new MBMS GW and consider that the MBMS session is now being controlled by the new MBMS GW. The MME shall then send an MBMS Session Start Request message including the "MBMS session re-establishment" flag (and the new M1 transport parameters) towards all involved MCE(s).

The MME may accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from a different MBMS GW than the MBMS GW that currently controls the MBMS session even if the message does not include the "MBMS session re-establishment indication" flag. If it accepts the request from the new MBMS GW, the MME shall replace the Sm related resources (i.e. TEID-C) for this MBMS service associated to the previous MBMS GW by those associated to the new MBMS GW and consider that the MBMS session is now being controlled by the new MBMS GW; the MME shall then either:

- stop the on-going MBMS bearer service and then start the new MBMS bearer service (without including the "MBMS session re-establishment indication" flag in the MBMS Session Start Request sent to the MCE(s)); or
- behave as if it had received an MBMS Session Start Request including the "MBMS session re-establishment indication" flag (i.e. include the "MBMS session re-establishment indication" flag in the MBMS Session Start Request sent to the MCE(s)).

The MME shall accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from the same MBMS GW that currently controls the MBMS session if the message includes the "MBMS session re-establishment indication" flag. The MME shall replace the Sm related resources (i.e. TEID-C) for this MBMS service by those received in the MBMS Session Start Request (if different). The MME should not send MBMS Session Start Request message(s) towards the involved MCE(s) if no parameters other than the estimated duration and relative start time have changed.

The MME shall reject an MBMS Session Stop Request received for an on-going MBMS bearer service from a different MBMS GW than the MBMS GW that currently controls the MBMS session.

NOTE 2: Upon a non-transient SGmb path failure, if the BM-SC moves the control of an MBMS session to an alternative MBMS GW, the same MME can receive an MBMS Session Stop Request from the old MBMS GW after an MBMS Session Start Request from the new MBMS GW.

The MME shall release the MBMS bearer context resources locally without sending any message to the MCE(s) if it receives a MBMS Session Stop Request with a "Local MBMS bearer context release" indication for an on-going MBMS bearer service from the MBMS GW currently controlling the MBMS session.

20.2.4.2 S5 path failure

The MME may support invoking the PGW triggered SGW restoration (see subclause 27.2.3) upon receiving a PGW Downlink Triggering Notification message when the S11 path for the related UE is still available (see subclause 20.2.1). If so, upon receiving a PGW Downlink Triggering Notification while the S11 path for the related UE is still available, the MME should proceed with the PGW triggered SGW restoration procedure (see subclauses 27.2.3.2 and 27.3.2.2) with the following modifications:

- if the PGW F-TEID or PGW IP address and GRE key for control plane received in the PGW Downlink Triggering Notification message does not match the stored PGW F-TEID or PGW IP address and GRE key for control plane of any PDN connection(s) for that UE, the MME shall not proceed with the PGW triggered SGW restoration procedure but just respond to the SGW with a PGW Downlink Triggering Acknowledge message with an acceptance cause code;

NOTE 1: This can happen e.g. if the PDN connection has already been restored by the MME upon receipt of a preceding PGW Restart Notification message. In this case, the PDN connection remains hanging in the PGW until the timer monitoring the maximum duration to restore the PDN connection expires in the PGW.

- if the PGW F-TEID or PGW IP address and GRE key for control plane received in the PGW Downlink Triggering Notification message matches the stored PGW F-TEID or PGW IP address and GRE key for control plane of any PDN connection(s) for that UE, the MME shall proceed with the PGW triggered SGW restoration procedure.
- if the related UE is in connected mode, the MME may restore the PDN connection(s) of that UE by performing the MME triggered Serving GW relocation procedure as defined in subclause 5.10.4 of 3GPP TS 23.401 [15].

NOTE 2: This avoids to tear down the S1 connection of the UE and thus to negatively affect other PDN connections of that UE that would not be impacted by the S5 path failure.

20.2.5 SGSN functionality

20.2.5.1 Sn path failure

Upon detecting an Sn path failure, the S4-SGSN should maintain the MBMS bearer contexts associated with the peer's MBMS GW IP address during an operator configurable maximum path failure duration.

The S4-SGSN should behave as specified for the case of an MBMS GW restart (see subclause 17A.1) if the Sn path to the MBMS GW is down for a duration exceeding the maximum path failure.

NOTE 1: This enables to free corresponding radio resources in UTRAN for MBMS services if the MBMS GW has failed without restart.

The S4-SGSN shall pass on the "MBMS session re-establishment indication" flag in the MBMS Session Start Request it sends to RNCs if received from the MBMS GW.

The S4-SGSN should accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from a different MBMS GW than the MBMS GW that currently controls the MBMS session if the message includes the "MBMS session re-establishment indication" flag. If it accepts the request from the new MBMS GW, the S4-SGSN shall replace the Sn related resources (i.e. TEID-C) for this MBMS service associated to the previous MBMS GW by those associated to the new MBMS GW and consider that the MBMS session is now being controlled by the new MBMS GW. The S4-SGSN shall then send an MBMS Session Start Request message including the "MBMS session re-establishment" flag (and the new M1 transport parameters) towards all involved RNC(s).

The S4-SGSN may accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from a different MBMS GW than the MBMS GW that currently controls the MBMS session even if the message does not include the "MBMS session re-establishment indication" flag. If it accepts the request from the new MBMS GW, the S4-SGSN shall replace the Sn related resources (i.e. TEID-C) for this MBMS service associated to the previous MBMS GW by those associated to the new MBMS GW and consider that the MBMS session is now being controlled by the new MBMS GW; the S4-SGSN shall then either:

- stop the on-going MBMS bearer service and then start the new MBMS bearer service (without including the "MBMS session re-establishment indication" flag in the MBMS Session Start Request sent to the RNC(s)); or
- behave as if it had received an MBMS Session Start Request including the "MBMS session re-establishment indication" flag (i.e. include the "MBMS session re-establishment indication" flag in the MBMS Session Start Request sent to the RNC(s)).

The S4-SGSN shall accept an MBMS Session Start Request received for an on-going MBMS bearer service (i.e. with the same TMGI and, if provided, MBMS Flow Identifier) from the same MBMS GW that currently controls the MBMS session if the message includes the "MBMS session re-establishment indication" flag. The S4-SGSN shall replace the Sn related resources (i.e. TEID-C) for this MBMS service by those received in the MBMS Session Start Request (if different). The S4-SGSN should not send MBMS Session Start Request message(s) towards the involved RNC(s) if no parameters other than the estimated duration and relative start time have changed.

The S4-SGSN shall reject an MBMS Session Stop Request received for an on-going MBMS bearer service from a different MBMS GW than the MBMS GW that currently controls the MBMS session.

NOTE 2: Upon a non-transient SGmb path failure, if the BM-SC moves the control of an MBMS session to an alternative MBMS GW, the same S4-SGSN can receive an MBMS Session Stop Request from the old MBMS GW after an MBMS Session Start Request from the new MBMS GW.

The S4-SGSN shall release the MBMS bearer context resources locally without sending any message to the RNC(s) if it receives a MBMS Session Stop Request with a "Local MBMS bearer context release" indication for an on-going MBMS bearer service from the MBMS GW currently controlling the MBMS session.

20.2.5.2 S5 path failure

The S4-SGSN may support invoking the PGW triggered SGW restoration (see subclause 27.2.3) upon receiving a PGW Downlink Triggering Notification and the S4 path of the related UE is still available (see subclause 20.2.1). If so, S4-SGSN shall proceed as defined for the MME in subclause 20.2.4.2, with the following modification:

- if the related UE is in connected mode, the S4-SGSN may restore the PDN connection(s) of that UE by performing the S4-SGSN triggered Serving GW relocation procedure as defined in subclause 9.2.2.4 of 3GPP TS 23.060 [5].

20.2.6 BM-SC functionality

20.2.6.1 SGmb path failure

In deployments without a Diameter Agent between the BM-SC and the MBMS GW, the BM-SC shall detect an SGmb path failure using either:

- mechanisms as specified in the Diameter Base Protocol (e.g. transport connection failure, MBMS GW peer not responding, Diameter Device-Watchdog-Request and Device-Watchdog-Answer messages during periods when there is no need for other MBMS signalling); or
- the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the MBMS GW, the BM-SC shall detect an SGmb path failure using the MBMS Heartbeat procedure (see clause 29).

NOTE 1: A transport connection failure does not allow to identify a failure of the remote MBMS peer. Likewise, it is not possible to rely on Diameter Device-Watchdog-Request / Answer messages to test the responsiveness of the remote MBMS node during periods when there is no need for other MBMS signalling as these messages are only exchanged between Diameter peers with a direct transport connection.

Upon detecting an SGmb path failure, the BM-SC should maintain the related MBMS bearer contexts.

During a transient SGmb path failure (e.g. before the maximum path failure duration timer expires), the BM-SC should consider all related MBMS bearer contexts as active in the MBMS GW. The BM-SC may initiate new MBMS sessions via an alternative MBMS GW (if available). The BM-SC should defer any MBMS session update or stop procedure for on-going MBMS sessions in the MBMS GW affected by the SGmb path failure until the transient path failure ends.

NOTE 2: Re-establishing an MBMS session via an alternative MBMS GW can generate network signalling over many interfaces and interrupt transiently the delivery of the MBMS data stream due to the need for related eNB/RNCs to switch to the new IP multicast group over M1. Thus during a transient SGmb path failure it is recommended to defer any MBMS session update or stop procedure for on-going MBMS sessions in the MBMS GW affected by the SGmb path failure. However if the MBMS session update or stop procedure is for time critical services, the BM-SC can immediately re-establish the active MBMS bearer services affected by the SGmb path failure by initiating MBMS Session Start procedure(s) towards an alternative MBMS GW (if available) as specified below, and subsequently send the MBMS Session Update or Stop message.

When detecting a non-transient SGmb path failure (e.g. the maximum path failure duration timer of the BM-SC expires), the BM-SC should re-establish the active MBMS bearer services affected by the SGmb path failure by initiating MBMS Session Start procedure(s) towards an alternative MBMS GW (if available) or towards the same MBMS GW (once the SGmb path is recovered).

NOTE 3: This enables to re-establish the MBMS sessions when a MBMS GW fails without restart.

The maximum path failure duration of the BM-SC should be configured with a shorter value than the maximum path failure duration timer of the MBMS GW to minimize the interruption of the active MBMS sessions upon a non-transient SGmb path failure. The BM-SC timer should be shorter than the MBMS GW timer by at least the period between two Diameter Device-Watchdog-Request messages or MBMS Heartbeat Request messages sent by the MBMS GW, to avoid that the MBMS GW timer expires before the BM-SC timer if the MBMS GW starts its timer before the BM-SC.

NOTE 4: This enables the MCE/RNC to receive a MBMS Session Start request from the new MME/SGSN (and MBMS GW) controlling the MBMS session before the MCE/RNC receives a request to stop the MBMS service from the previous controlling MME/SGSN (and MBMS GW).

When re-establishing the active MBMS bearer services affected by the SGmb path failure, the BM-SC shall encode the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request sent by the BM-SC if the original parameters were updated) with the following exceptions:

- the BM-SC shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- if no absolute start time ("MBMS data transfer start" parameter) has been sent, the BM-SC may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the BM-SC should set the estimated session duration to a value corresponding to the remaining duration of the session.

NOTE 5: If the BM-SC is instructed to modify an MBMS Session during the SGmb path failure, the contents of the MBMS Session Start Request sent to the MBMS GW after the SGmb path failure can also differ from the parameters sent to the MBMS GW before the SGmb path failure for the parameters that can be modified by the MBMS session update procedure (i.e. MBMS Session Area, MBMS Time to Data Transfer, MBMS Data Transfer Start).

After detecting an SGmb path failure, the BM-SC shall determine whether the failure is transient or non transient from the perspective of the MBMS GW (e.g. the BM-SC is provisioned with the maximum path failure timer of the MBMS GW). The BM-SC shall assume that the failure is non transient from the perspective of the MBMS GW if the SGmb path recovers after a period longer than the maximum path failure timer of the MBMS GW plus the period between two Diameter Device-Watchdog-Request messages or MBMS Heartbeat Request messages sent by the MBMS GW, to ensure that the MBMS GW also determines this is a non transient path failure if the BM-SC starts its timer before the MBMS GW. The BM-SC shall consider that the MBMS session has been released by the MBMS GW if the SGmb path failure is non transient for the MBMS GW. If the SGmb path failure remains transient for the MBMS GW, the BM-SC shall behave as follows upon detecting the SGmb path recovery:

- if the BM-SC has already moved the control of the MBMS session to an alternative MBMS GW, the BM-SC shall send an MBMS Session Stop Request message to the MBMS GW previously controlling the MBMS session with a "Local MBMS bearer context release" indication to instruct that MBMS GW to release the MBMS bearer context locally in the MBMS GW and in the associated MME/SGSN(s) without sending any message to the MCE/RNC(s).

- if the BM-SC has not yet moved the control of the MBMS session to an alternative MBMS GW (e.g. if the MBMS restoration procedures are not supported in the network),
 - if the SGmb path failure is transient from the perspective of the BM-SC, the BM-SC shall consider that the MBMS session is still controlled by the related MBMS GW and proceed as if there had been no SGmb path failure;
 - if the SGmb path failure is non transient from the perspective of the BM-SC, the BM-SC shall send an MBMS Session Start Request to the MBMS GW for the session and encode it as specified above (for a message sent to an alternative MBMS GW).

NOTE 6: The BM-SC cannot know whether the MBMS GW will see the SGmb path failure as transient or non transient if the SGmb path recovers in the period between the maximum path failure timer of the MBMS GW plus and minus the period between two Diameter Device-Watchdog-Request messages or MBMS Heartbeat Request messages sent by the MBMS GW. This can possibly lead the BM-SC to send an MBMS Session Stop request to the MBMS GW for a session that has already been terminated by the MBMS GW (if the MBMS GW determined the failure is non transient) or to send an MBMS Session Start request (with the "MBMS session re-establishment indication" flag) to the MBMS GW for a session that is still alive at the MBMS GW (if the MBMS GW determined the failure is transient).

20.2.6.2 MB2-C path failure

In deployments without a Diameter Agent between the BM-SC and the GCS AS, the BM-SC shall detect an MB2-C path failure using either:

- mechanisms as specified in the Diameter Base Protocol (e.g. transport connection failure, GCS AS peer not responding, Diameter Device-Watchdog-Request and Device-Watchdog-Answer messages during periods when there is no need for other MB2 signalling); or
- the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the GCS AS, the BM-SC shall detect an MB2-C path failure using the MBMS Heartbeat procedure (see clause 29).

NOTE 1: A transport connection failure does not allow to identify a failure of the remote MBMS peer. Likewise, it is not possible to rely on Diameter Device-Watchdog-Request / Answer messages to test the responsiveness of the remote MBMS node during periods when there is no need for other MB2 signalling as these messages are only exchanged between Diameter peers with a direct transport connection.

Upon detecting a non-transient MB2-C path failure, the BM-SC shall deallocate (locally) all the TMGIs that had been assigned to the GCS AS and the BM-SC shall stop all the related MBMS bearers to free the corresponding resources in E-UTRAN.

20.2.7 PGW functionality

20.2.7.1 S5 path failure

The PGW may support invoking the PGW triggered SGW restoration procedure (see clause 27.2.3) when detecting a path failure to an SGW (see subclause 20.2.1). If so, after detecting a path failure to an SGW, the PGW should maintain the S5 bearer contexts eligible for restoration and proceed with the PGW triggered SGW restoration procedure with the following modifications:

- for GTP-based S5, the PGW shall include the PGW F-TEID for control plane in the PGW Downlink Triggering Notification message;
- for PMIP-based S5, the PGW shall include the PGW IP address and uplink GRE key for control plane in the PMIP Update Notification message;

20.2.8 GCS AS functionality

20.2.8.1 MB2-C path failure

In deployments without a Diameter Agent between the BM-SC and the GCS AS, the GCS AS shall detect an MB2-C path failure using either:

- mechanisms as specified in the Diameter Base Protocol (e.g. transport connection failure, BM-SC peer not responding, Diameter Device-Watchdog-Request and Device-Watchdog-Answer messages during periods when there is no need for other MB2 signalling); or
- the MBMS Heartbeat procedure (see clause 29), if this procedure is supported.

In deployments with a Diameter Agent between the BM-SC and the GCS AS, the GCS AS shall detect an MB2-C path failure using the MBMS Heartbeat procedure (see clause 29).

NOTE 1: A transport connection failure does not allow to identify a failure of the remote MBMS peer. Likewise, it is not possible to rely on Diameter Device-Watchdog-Request / Answer messages to test the responsiveness of the remote MBMS node during periods when there is no need for other MB2 signalling as these messages are only exchanged between Diameter peers with a direct transport connection.

Upon detecting a non-transient MB2-C path failure, the GCS AS shall assume that all the TMGIs that had been assigned by the BM-SC have been de-allocated and that all the related MBMS bearers have been deactivated.

The GCS AS may restore the MBMS delivery e.g. via a different BM-SC using the MB2-C procedures specified in 3GPP TS 29.468 [36].

20.2.9 Sx interface functionality

20.2.9.1 Sxa path failure

If the path to the SGW-U is down, the SGW-C should handle this as SGW-U Failure without Restart, see clause 16.1a.1.

If the path to the SGW-C is down, the SGW-U should handle this as SGW-C Failure without Restart, see clause 16.1b.1.

20.2.9.2 Sxb path failure

If the path to the PGW-U is down, the PGW-C should handle this as PGW-U Failure without Restart, see subclause 17.1a.1.

If the path to the PGW-C is down, the PGW-U should handle this as PGW-C Failure without Restart, see subclause 17.1b.1.

20.3 User plane path failure detection and handling

20.3.1 General

GTP-U entities shall support detection of path failure by using Echo Request / Echo Response messages in the following way. A path counter shall be reset each time an Echo Response is received on the path and incremented when the T3-RESPONSE timer expires for any Echo Request message sent on the path. The path shall be considered to be down if the counter exceeds N3-REQUESTS.

Upon detecting a path failure, the network node should notify the failure via the Operation and Maintenance system and may either

- delete the bearer contexts associated with the path in failure; or

- maintain the bearer contexts associated with the path in failure during an operator configurable maximum path failure duration. The network node shall delete the maintained resources if the path is still down when this duration expires.

NOTE 1: During transient path failures (e.g. path failures not exceeding few minutes at most), maintaining the bearer contexts associated with the peer's IP address enables the delivery of end user services (when the path is reestablished again) and also avoids unnecessary signalling in the network for restoring those bearers.

NOTE 2: It is not intended to maintain bearer contexts during long path failures (e.g. exceeding few minutes at most) as this would imply undesirable effects like undue charging.

20.3.2 MBMS GW functionality

20.3.2.1 SGi-mb path failure

An MBMS GW may support the detection of an SGi-mb path failure.

NOTE 1: How an MBMS GW detects an SGi-mb path failure is implementation specific. E.g. an MBMS GW can monitor the receipt of downlink user plane from the BM-SC (synchronization sequences are transmitted continuously e.g. in case of MBSFN transmissions, even if there is no MBMS user data to be sent).

Upon detecting a non-transient SGi-mb path failure (operator configurable maximum path failure duration), based on operator's policy, the MBMS GW may tear down the affected MBMS sessions by sending MBMS Session Stop Request message(s) to the MME/SGSN(s) serving the MBMS sessions and Session Termination Request message(s) to the BM-SC with a terminating cause signalling a user plane failure.

NOTE 2: This enables to free corresponding radio resources in E-UTRAN/UTRAN and to attempt to re-establish the MBMS session(s).

20.3.3 BM-SC functionality

20.3.3.1 SGi-mb path failure

Upon receipt of a Session Termination Request message from an MBMS GW with a terminating cause signalling a user plane failure, the BM-SC may attempt to re-establish the MBMS session via the same MBMS GW (using different user plane resources over SGi-mb) or an alternative MBMS GW.

When re-establishing the MBMS session, the BM-SC shall encode the MBMS Session Start Request with the same contents as in the original MBMS Session Start Request (or per the last MBMS Session Update Request sent by the BM-SC if the original parameters were updated) with the following exceptions:

- the BM-SC shall set the "MBMS session re-establishment indication" flag to signal that this message is used to re-establish an MBMS session;
- if no absolute start time ("MBMS data transfer start" parameter) has been sent, the BM-SC may change the relative start time ("time to MBMS data transfer" parameter) to fasten the restoration of the MBMS service in E-UTRAN;
- the BM-SC should set the estimated session duration to a value corresponding to the remaining duration of the session;
- the BM-SC shall provide the new user plane resources assigned to the MBMS session over SGi-mb.

If the MBMS session is not re-established and if it was activated by a Group Communication Service Application Server(s) (GCS AS), the BM-SC shall notify the GCS AS that the MBMS session has been deactivated.

20.3.4 With Control and User plane Separation of SGW or PGW nodes

With a split SGW or PGW (see 3GPP TS 23.214 [42]), user plane path failure detection and handling shall be supported as specified in subclause 20.3.1 with the following additional requirements:

- upon detecting a GTP-U user plane path failure, the SGW-U or PGW-U shall report the user plane path failure to the SGW-C or PGW-C respectively, by sending an Sx Node Report Request (see 3GPP TS 29.244 [43]) including a User Plane Path Failure Report with the IP address of the remote GTP-U peer(s) towards which a failure has been detected;
- upon being notified about the user plane path failure, when deciding to delete the bearer contexts associated with the path in failure, the SGW-C or PGW-C shall modify or delete the affected Sx sessions in the SGW-U or PGW-U.

NOTE: The SGW-C and PGW-C need to take care to smooth the signalling load towards the SGW-U and PGW-U if a large number of Sx sessions are affected by the user plane path failure.

21 Error Indication handling

21.1 General

The following subclauses specify a network element behaviour, if it receives a GTPv1-U Error Indication message. The reception of the message triggers a node internal procedure and/or a Control Plane procedure (GTPv1-C, GTPv2, RANAP, S1-AP).

For the PMIP based S5/S8 interface, an error in the form of an ICMP message is used instead of a GTPv1-U Error Indication message for the Error Indication handling.

21.2 GGSN

GTP error indication message shall be handled as follows:

- If the GGSN receives a GTP error indication for a PDP context that has the DTI flag set (i.e. from an RNC), the GGSN should not delete the associated PDP context but mark it as invalid. Any subsequent packets arriving for an invalid PDP context should be discarded. The GGSN shall inform the SGSN that the GGSN received a GTP error indication from RNC. The SGSN shall re-establish the tunnel between the SGSN and GGSN as specified in 3GPP TS 29.060 [8], which sets the related PDP context as valid again in the GGSN. The GGSN then forwards any subsequent downlink packets to the SGSN.
- If the GGSN receives a GTP error indication for a PDP context that has the no DTI flag set (i.e. from an SGSN), the GGSN shall delete its PDP context and may notify the Operation and Maintenance network element.

21.3 Gn/Gp SGSN

GTP error indication message shall be handled as follows:

- If the SGSN receives a GTP error indication from a GGSN, the SGSN shall delete its PDP context and may notify the Operation and Maintenance network element. Additionally it shall send a Deactivate PDP Context Request message to the MS with cause "re-activation required"
- If the SGSN receives a GTP error indication from the RNC it shall locally release the RAB. The SGSN should preserve the associated PDP context. The SGSN may initiate the RAB Assignment procedure in order to re-establish the RAB.
- For MBMS, when an Error Indication is received from an SGSN, the receiving GGSN shall delete all information associated with the relevant SGSN in its MBMS Bearer Context and the GGSN may notify the Operation and Maintenance network element. In addition, for broadcast mode the GGSN may request the re-establishment of the MBMS Bearer Context by sending an MBMS Session Start Request message (see subclause 7.5A.2.5 of 3GPP TS 29.060 [8]). Furthermore, if the GGSN serves only one downstream SGSN for MBMS data transfer and the GGSN does not support the re-establishment procedure, the GGSN shall delete its MBMS Bearer Context together with the affected MBMS UE Context(s).

21.4 S4 SGSN

GTP error indication message shall be handled as follows:

- If the S4-SGSN receives a GTP error indication from a SGW, the S4-SGSN shall delete its Bearer context and may notify the Operation and Maintenance network element. Additionally it shall send a Deactivate PDP Context Request message to the MS with cause "re-activation required"
- If the S4-SGSN receives a GTP error indication from the RNC it shall locally release the RAB. The S4-SGSN should preserve the associated Bearer context. The S4-SGSN may initiate the RAB Assignment procedure in order to re-establish the RAB.

21.5 RNC or NodeB

GTP error indication message shall be handled as follows:

- When the RNC receives GTP error indication from the SGSN, it shall initiate the RAB Release procedure with the error cause "GTP Resources Unavailable" and shall immediately locally release the RAB (i.e. without waiting for a response from the SGSN).
- If the RNC receives a GTP error indication from the GGSN (i.e. if Direct Tunnel is established), it shall initiate the RAB Release procedure with the error cause "GTP Resources Unavailable" and immediately locally release the RAB (i.e. without waiting for a response from the SGSN). The SGSN shall delete the related PDP context at the SGSN and send a Deactivate PDP Context Request message to the MS with cause "re-activation required".
- If the RNC receives a GTP error indication from the SGW (i.e. if Direct Tunnel is established), it shall initiate the RAB Release procedure with the error cause "GTP Resources Unavailable" and immediately locally release the RAB (i.e. without waiting for a response from the SGSN). The SGSN shall delete the related PDP context and send a Deactivate PDP Context Request message to the MS with the cause "re-activation required". If the deleted PDP context is a primary PDP context, the SGSN shall set the "Tear down indicator" bit in the Deactivate PDP Context Request message. The SGSN may also optionally send a Delete Bearer Command or a Delete Session Request message to the SGW if the deleted PDP context is a secondary PDP context or a primary PDP context respectively.

NOTE: Sending a Delete Bearer Command or a Delete Session Request message to the SGW can help the SGSN to determine whether the GTP error indication was due to the release of the bearer context or the release of the UE context in the SGW.

21.6 eNodeB

GTP error indication message shall be handled as follows:

- If the eNodeB receives a GTP error indication from the SGW over an S1-U tunnel not doing indirect forwarding, it shall initiate the E-RAB Release procedure and immediately locally release the E-RAB (i.e. without waiting for a response from the MME). If the MME receives the E-RAB Release Indication for a default bearer that is not the last default bearer of a UE or that the UE has a SCEF PDN connection or that the UE supports Attach without PDN connectivity as specified in clause 5.3.8.3 of 3GPP TS 23.401 [15], the MME should send a Delete Session Request to the SGW. Additionally the MME may also send a Deactivate EPS Bearer Context Request to the UE with the ESM cause set to "Reactivation Requested" if the MME has decided to restore the PDN connection based on operator policy, QCI and/or ARP and/or APN. If the MME receives the E-RAB Release Indication for the last default bearer of a UE and the UE does not have a SCEF PDN connection and the UE does not support Attach without PDN connectivity as specified in clause 5.3.8.3 of 3GPP TS 23.401 [15], the MME shall initiate a MME initiated Detach procedure with the detach type "re-attach required". If the MME receives the UE Context Release Request from the eNB, the MME shall send a Release Access Bearers Request to the SGW but if the SGW responds with a "context not found" cause and the UE does not have a SCEF PDN connection and the UE does not support Attach without PDN connectivity, then the MME shall initiate a MME initiated Detach procedure with the detach type "re-attach required".

- If the eNodeB receives a GTP error indication from a peer eNodeB over an X2-U direct forwarding tunnel or from an SGW over an S1-U indirect forwarding tunnel, the eNodeB may ignore the error indication received over the forwarding tunnels or delete the forwarding tunnel context locally without deleting the EPS bearers.
- For dual connectivity case as specified in 3GPP TS 36.300 [32]:
 - If the MeNodeB receives a GTP error indication from the SGW over an S1-U tunnel, it shall initiate the E-RAB Release procedure and immediately locally release the E-RAB (i.e. without waiting for a response from the MME);
 - If the MeNodeB/SeNodeB receives a GTP error indication from the peer SeNodeB/MeNodeB, the MeNodeB/SeNodeB shall delete the X2-U tunnel locally;
 - If the SeNodeB receives a GTP error indication from the SGW over an S1-U tunnel, it shall delete the S1-U tunnel locally;
 - The MeNodeB and SeNodeB may initiate an additional dual connectivity procedure(s) as specified in 3GPP TS 36.300 [32].

21.7 SGW

GTP error indication message shall be handled as follows:

- For an 'Active' mode UE having a user plane connection with an RNC, i.e. SGW has F-TEIDs assigned by RNC for user plane for the UE, when the SGW receives a GTP Error Indication for a Bearer Context that has the DTI flag set (i.e. from an RNC), the SGW should not delete the associated Bearer Context but delete all the RNC GTP-U tunnel TEIDs for this MS and sends a Downlink Data Notification message to the SGSN (the complete behaviour is specified in clause 22). Then the SGW starts buffering downlink packets received for this MS.
- For an 'Active' mode UE having a user plane connection with an eNB, i.e. SGW has F-TEIDs assigned by eNB for user plane for the UE, when the SGW receives a GTP Error Indication for a Bearer Context from an eNodeB, the SGW should not delete the associated Bearer Context but delete all the eNodeB GTP-U tunnel TEIDs for this UE and sends a Downlink Data Notification message to the MME (the complete behaviour is specified in clause 22). Then the SGW starts buffering downlink packets received for this UE.
- For a UE having an S11 user plane connection with an MME, i.e. SGW has S11-U F-TEIDs assigned by MME for user plane for the UE, when the SGW receives a GTP Error Indication for a Bearer Context from an MME, the SGW may:
 - delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and notify the Operation and Maintenance network element, or as an alternative,
 - delete the MME GTP-U tunnel TEID for this UE and send a Downlink Data Notification message to the MME to re-establish the user plane path without deleting the PDN connection (the complete behaviour is specified in clause 22). Then the SGW starts buffering downlink packets received for this UE.
- If the SGW receives a GTP error indication from S4-SGSN for a Bearer Context other than the default bearer when S4-U is used, the SGW may delete its Bearer context and may notify the Operation and Maintenance network element, or as an alternative, the SGW may send Downlink Data Notification message to the S4-SGSN to re-establish the user plane path without deleting the bearer context.
- If the SGW receives a GTP error indication from S4-SGSN for the default bearer when S4-U is used, the SGW may delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and may notify the Operation and Maintenance network element, or as an alternative, the SGW may send Downlink Data Notification message to the S4-SGSN to re-establish the user plane path without deleting the PDN connection.
- If the SGW receives a GTP error indication from a PGW for the bearer other than the default bearer, the SGW shall delete its Bearer context and may notify the Operation and Maintenance network element.
- If the SGW receives a GTP error indication from a PGW for the default bearer, the SGW shall delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and may notify the Operation and Maintenance network element. The SGW may send the Delete Bearer Request for the default bearer to the MME/S4 SGSN to delete the associated PDN connection.

PMIP error indication message shall be handled as follows:

- If the SGW receives an ICMP message from a PGW that indicates the UE specific error indication, as specified in the 3GPP TS 29.275 [16], the SGW may delete the associated PDN connection (identified by the GRE key included in the ICMP message) and may notify the Operation and Maintenance network element. In this case, the SGW may also:
 - send the Delete Bearer Request for the default bearer to the MME/S4 SGSN to delete the associated PDN connection, and/or,
 - perform other implementation specific actions, such as: sending messages to release other external resources (e.g. PCC messages).

21.8 PGW

GTP error indication message shall be handled as follows:

- If the PGW receives a GTP error indication from a SGW/a TWAN /an ePDG for the bearer other than the default bearer, the PGW shall delete its Bearer context and may notify the Operation and Maintenance network element.
- If the PGW receives a GTP error indication from a SGW/a TWAN /an ePDG for the default bearer, the PGW shall delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and may notify the Operation and Maintenance network element.

PMIP error indication message shall be handled as follows:

- If the PGW receives an ICMP message from an SGW/an ePDG/a Trusted Non-3GPP IP access node that indicates the UE specific error indication as specified in the 3GPP TS 29.275 [16], the PGW may delete the associated PDN connection (identified by the GRE key included in the ICMP message) and may notify the Operation and Maintenance network element.

21.9 MBMS GW

GTP Error Indication message shall be handled as follows:

- If the MBMS GW receives a GTP Error Indication from a SGSN, the MBMS GW shall delete its Bearer context and may notify the Operation and Maintenance network element.

21.10 ePDG

GTP error indication message shall be handled as follows:

- If the ePDG receives a GTP error indication from a PGW for the bearer other than the default bearer, the ePDG shall delete its Bearer context and may notify the Operation and Maintenance network element.
- If the ePDG receives a GTP error indication from a PGW for the default bearer, the ePDG shall delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and initiate the release of the corresponding SWu instance (i.e. IKEv2 tunnel). The ePDG may notify the Operation and Maintenance network element.

PMIP error indication message shall be handled as follows:

- If the ePDG receives an ICMP message from a PGW that indicates the UE specific error indication as specified in the 3GPP TS 29.275 [16], the ePDG may delete the associated PDN connection (identified by the GRE key included in the ICMP message) and initiate the release of the corresponding SWu instance (i.e. IKEv2 tunnel) . The ePDG may notify the Operation and Maintenance network element.

21.11 TWAN

GTP error indication message shall be handled as follows:

- If the TWAN receives a GTP error indication from a PGW for the bearer other than the default bearer, the TWAN shall delete its Bearer context and may notify the Operation and Maintenance network element.
- If the TWAN receives a GTP error indication from a PGW for the default bearer, the TWAN shall delete all the Bearer contexts associated with the PDN connection (identified by the default bearer) and may initiate the release of the corresponding WLAN specific resource. The TWAN may notify the Operation and Maintenance network element.

PMIP error indication message shall be handled as follows:

- If the TWAN receives an ICMP message from a PGW that indicates the UE specific error indication as specified in the 3GPP TS 29.275 [16], the TWAN may delete the associated PDN connection (identified by the GRE key included in the ICMP message) and may initiate the release of the corresponding WLAN specific resource. The TWAN may notify the Operation and Maintenance network element.

21.12 MME

GTP error indication message shall be handled as follows:

- If the MME receives a GTP error indication from an SGW, the MME shall delete its Bearer context and may notify the Operation and Maintenance network element. Additionally the MME shall deactivate the corresponding PDN connection towards the UE with the cause "re-activation required", or initiate an explicit detach with reattached required procedure, as appropriate, see 3GPP TS 24.301 [19].

22 Downlink Data Notification Handling at MME/S4 SGSN

If the MME/S4 SGSN receives a Downlink Data Notification message from the SGW as a result of the SGW having received an Error Indication message from the eNodeB/RNC or S4-SGSN over S4 User Plane, the MME/S4 SGSN should perform the following:

- If the UE is in IDLE state, upon receipt of the Downlink Data Notification message, the MME/S4 SGSN shall perform the Network Triggered Service Request procedure as specified in 3GPP TS 23.060 [5] and 3GPP TS 23.401 [15].
- If the UE is in CONNECTED state, upon receipt of the Downlink Data Notification message, the MME shall perform S1 Release procedure and perform Network Triggered Service Request procedure as specified in 3GPP TS 23.401 [15].
- If the UE is in CONNECTED state, upon receipt of the Downlink Data Notification message and Direct Tunnel is used, the S4-SGSN shall perform Iu Release procedure and perform Network Triggered Service Request procedure as specified in 3GPP TS 23.060 [5] if the cause value included in Downlink Data Notification is "Error Indication received from RNC/eNodeB/S4-SGSN",
- If the UE is in CONNECTED state, upon receipt of the Downlink Data Notification message and Direct Tunnel is not used, the S4-SGSN should re-establish all of the S4-U bearers of this UE if the cause value included in Downlink Data Notification is "Error Indication received from RNC/eNodeB/S4-SGSN".

Upon receipt of a Downlink Data Notification message from the SGW, caused by an Error Indication message received from the MME over the S11 User Plane, the MME should perform the following if the UE is known by the MME:

- If the UE is in IDLE state, the MME shall perform the Network Triggered Service Request procedure as specified in 3GPP TS 23.401 [15].
- If the UE is in CONNECTED state, the MME may perform an S1 Release procedure and a Network Triggered Service Request procedure as specified in 3GPP TS 23.401 [15], or as an alternative, the MME may keep the existing S1 signalling connection and just send a Modify Bearer Request message to the SGW to re-establish the S11-U tunnel.

23 General partial failure handling procedures

The partial failure handling is an optional feature for MME, SGW, ePDG, TWAN and PGW. Partial failure handling is an optional feature between SGW-C, PGW-C, SGW-U and PGW-U for split SGW and PGW (see 3GPP TS 23.214 [42]).

For split SGW and PGW, the description in this clause related to SGW applies to SGW-C and PGW applies to PGW-C as well.

A partial failure handling feature may be used when a hardware or software failure affects a significant number of PDN connections while a significant number of PDN connections are unaffected. This feature may also be used for the degenerate case of a full/complete failure of a remote node (MME or PGW) in order to cleanup hanging PDN connections associated with the failed node. When it is impossible to recover the affected PDN connections (for example, using implementation-specific session redundancy procedures), it is useful to inform the peer nodes about the affected PDN connections for recovery on the peer nodes. Such a notification could be performed using an identifier that represents a large set of PDN connections rather than on individual PDN connection basis.

NOTE 1: If a hardware or software failure happens to impact only an insignificant number of PDN connections the node experiencing the fault need not treat the failure as a partial fault but may tear down connections one by one.

For the purposes of partial fault handling the term "node" refers to an entity that takes the role of an MME, PGW, ePDG, TWAN or SGW as defined in an SAE network.

A PDN Connection Set Identifier (CSID) shall identify a set of PDN connections within a node that may belong to an arbitrary number of UEs. A CSID is an opaque parameter local to a node. Each node that supports the feature maintains a local mapping of CSID to its internal resources. When one or more of those resources fail, the corresponding one or more fully qualified CSIDs are signalled to the peer nodes.

The fully qualified CSID (FQ-CSID) is the combination of the node identity and the CSID assigned by the node which together globally identifies a set of PDN connections.

NOTE 2: The node identifier in the FQ-CSID is required since two different nodes may use the same CSID value. A partial fault in one node should not cause completely unrelated PDN connections to be removed accidentally.

The node identifier shall be globally unique across all 3GPP EPS networks. Its format is defined in 3GPP TS 29.274 [13]

For the purposes of partial fault handling the term peer is used as follows: For a particular PDN connection two nodes are peers if both nodes are used for that PDN connection. For a PDN Connection Set the nodes are peers if they have at least one PDN connection in the PDN Connection Set where both nodes are used for that PDN connection. In particular PGW and MME are generally peers for the purposes of partial fault handling.

An FQ-CSID is established in a node and stored in peer nodes in the PDN connection at the time of PDN connection establishment, or during a node relocation, and used later during partial failure handling in messages defined in 3GPP TS 29.274 [13] and 3GPP TS 29.275 [16]. Each node that support the feature, including the MME, SGW, ePDG, TWAN and the PGW, shall maintain the FQ-CSID provided by every other peer node for a PDN connection. The FQ-CSIDs stored by PDN connection are later used to find the matching PDN connections when a FQ-CSID is received from a node reporting a partial fault for that FQ-CSID.

With the exception of the GTPv2 Delete PDN Connection Set Request and PMIPv6 Binding Revocation Indication BRI messages, each feature supporting MME, SGW, ePDG, TWAN or PGW shall assign only one FQ-CSID for itself in messages and each FQ-CSID shall have exactly one CSID within the FQ-CSID.

Following rules shall apply for all the nodes:

- 1) If a node (MME, SGW, ePDG, TWAN or PGW) supports the partial failure handling feature, it shall generate and include its own FQ-CSID during the PDN connection establishment, node relocation procedures. Explicit list of the relevant GTPv2 messages is given in the respective subclauses (14.3 "Partial Failure Handling at MME", 16.2 "Partial Failure Handling at SGW", 17B.2 "Partial Failure Handling at ePDG", 17C.2 "Partial Failure Handling at TWAN" and 17.2 "Partial Failure Handling at PGW"). A node that supports partial failure handling feature shall also store peers' FQ-CSIDs.

- 2) Additionally, if an SGW supports partial failure handling feature, it shall forward the peer node's (of an MME or of a PGW, depending on the direction) FQ-CSID and also Delete Connection Set Request/Response messages. Also, if the SGW detects the full/complete failure of an MME or PGW, e.g., through the Echo Request/Echo Response procedure, it may send a Delete PDN Connection Set Request (or PMIPv6 Binding Revocation Indication with G bit set) message containing all of the FQ-CSIDs of the associated hanging PDN connections of the failed node to the corresponding remote node (MME or PGW) .
- 3) If a node that supports partial failure handling feature receives peer node's FQ-CSID during the procedures, which are specified in Rule 1, it shall conclude that the peer node supports the feature. Subsequently, the node shall store the peer node's FQ-CSID and shall send appropriate partial failure handling messages to the peer.
- 4) If a node that supports partial failure handling feature does not receive the peer's FQ-CSID during the procedures, which are specified in Rule 1, it shall conclude that the peer node does not support the feature.
- 5) A node that supports partial failure handling feature shall not send any FQ-CSID IE or any partial failure handling specific messages to the peer node if the sender is aware (see Rule 4) that the receiver does not support the feature.
- 6) If a node does not support the partial failure handling feature, it shall ignore any received FQ-CSID IE or any partial failure handling specific message.
- 7) During session management procedures as specified in 3GPP TS 23.401 [15] and 3GPP TS 23.402 [18] (such as a dedicated bearer activation/deactivation/update), a node supporting the partial failure handling feature may update its FQ-CSID to the supporting peer node(s) in the Create Bearer Request/Response, Delete Bearer Request/Response or Update Bearer Request/Response.

NOTE 3: FQ-CSID handling for the Initial Attach and various handover cases are addressed in clauses 14, 16 and 17.

In addition to the above requirements, for split SGW and PGW, the following applies:

- 1) If a node (SGW-C, SGW-U, PGW-C or PGW-U) supports the partial failure handling feature, it shall generate and include its own FQ-CSID during the Sx Session Establishment procedure.
- 2) The SGW-C shall initiate Sx Session Modification procedure to update the SGW-U with the MME FQ-CSID, PGW-C FQ-CSID if changed;
- 3) The PGW-C shall initiate Sx Session Modification procedure to update the PGW-U with the MME FQ-CSID, SGW-C FQ-CSID, TWAN FQ-CSID, or ePDG FQ-CSID if changed;
- 4) The SGW-C and the PGW-C may change its FQ-CSID during a Sx Session Modification procedure if its SEID is changed;
- 5) When the node (SGW-C, SGW-U, PGW-C or PGW-U) detects that it has undergone a partial failure, it shall send a Sx Session Set Deletion Request message containing all the its CSIDs of the component(s) failing to its peer node;
- 6) For a SGW-C or a PGW-C, it shall also send Sx Session Set Deletion Request to the SGW-U or PGW-U respectively containing MME FQ-CSID, ePDG FQ-CSID, TWAN FQ-CSID, PGW-C FQ-CSID or SGW-C FQ-CSID if it receives the corresponding GTPv2 message Delete PDN Connection Set Request message containing those FQ-CSID.
- 7) The SGW-C and the PGW-C shall initiate the restoration procedure to restore the Sx Sessions affected by the partial failure in the SGW-U or the PGW-U in the same way as specified in the subclause 16.1A.3 for the SGW-U failure and 17.1A.3 for the PGW-U failure respectively, when receiving an Sx Session Set Deletion Request message including a SGW-U or a PGW-U FQ-CSID(s) which is associated with the partial failure from the SGW-U or the PGW-U.

Figure 23-1 illustrates FQ-CSID establishment during the Attach or PDN connection establishment procedures for 3GPP E-UTRAN access as specified in the above rules.

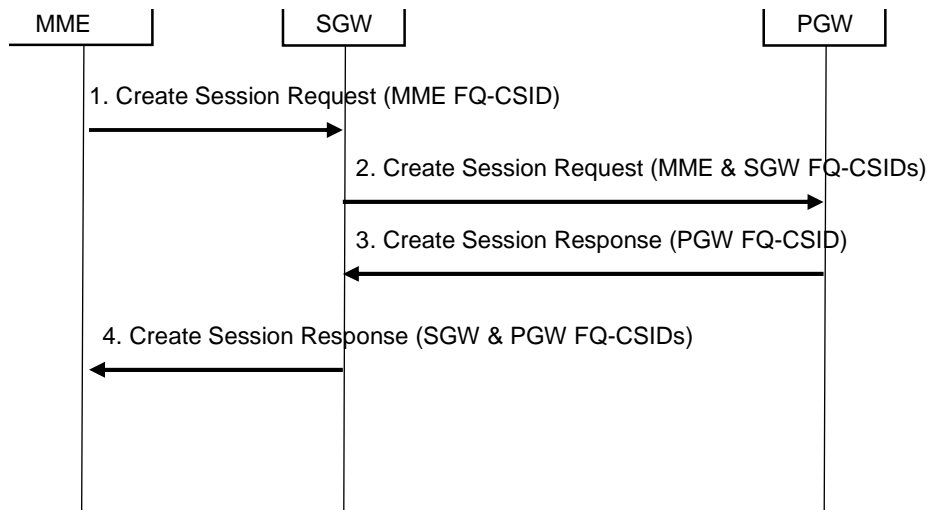


Figure 23-1: FQ-CSID establishment during the Attach or PDN establishment procedure for 3GPP E-UTRAN access

1. If an MME supports partial failure handling, the MME shall send own FQ-CSID to SGW with a Create Session Request message across S11 interface.

The MME's FQ-CSID indicates to the SGW that MME supports partial failure handling. If the SGW does not receive MME's FQ-CSID, then the SGW shall never send partial failure handling related messages or IEs to the MME.

If the SGW does not support partial failure handling, then the SGW shall silently discard MME's FQ-CSID.

If the SGW does support partial fault handling it shall store the MME's FQ-CSID in it's PDN connection table.

2. If the SGW supports partial failure handling, the SGW shall forward MME's FQ-CSID to PGW with a Create Session Request message or a Proxy Binding Update message across S5/S8 interface. The SGW shall also include own FQ-CSID into the message.

The SGW's FQ-CSID indicates to the PGW that the SGW supports partial failure handling.

If the PGW does not support partial failure handling, then the PGW shall silently discard both FQ-CSIDs.

3. If the SGW has indicated the support for partial failure handling to PGW, then the PGW, which supports the feature shall send own FQ-CSID back to the SGW with a Create Session Response message or a Proxy Binding Acknowledgement message across S5/S8 interface. PGW's FQ-CSIDs in the S5/S8 Create Session Response or a Proxy Binding Acknowledgement message indicates to the SGW that PGW supports partial failure handling.

If the SGW has not indicated support for partial failure handling, then PGW shall never send partial failure handling related messages or IEs to the SGW.

4. If the MME has indicated the support for partial failure handling to SGW, then the SGW, which supports the feature, shall forward PGW's FQ-CSID to MME with a Create Session Response message across S11 interface. The SGW shall also include own FQ-CSID into the message.

Figure 23-2 illustrates FQ-CSID establishment during the Attach or PDN connection establishment procedures for untrusted non-3GPP access as specified in the above rules.

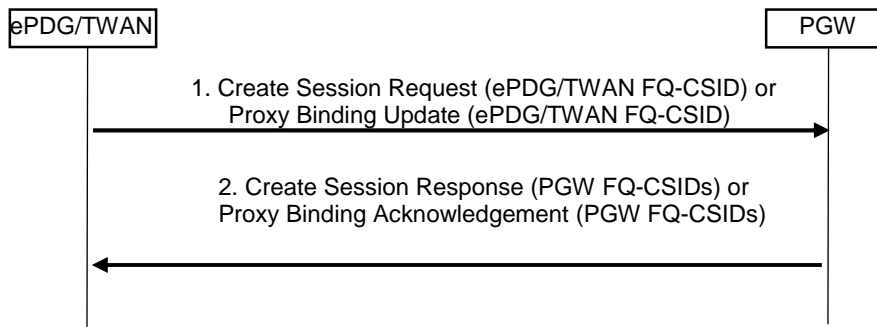


Figure 23-2: FQ-CSID establishment during the Attach or PDN establishment procedure for non-3GPP access

1. If an ePDG/TWAN supports partial failure handling, the ePDG/TWAN shall send own FQ-CSID to PGW with a Create Session Request message across GTPv2 based S2b/S2a interface or a Proxy Binding Update message across PMIPv6 based S2b/S2a interface.

The ePDG's/TWAN's FQ-CSID indicates to the PGW that ePDG/TWAN supports partial failure handling. If the PGW does not receive ePDG's/TWAN's FQ-CSID, then the PGW shall never send partial failure handling related messages or IEs to the ePDG/TWAN.

2. If the PGW supports partial failure handling, it shall store the ePDG's/TWAN's FQ-CSID in its PDN connection table and it shall send own FQ-CSID back to the ePDG/TWAN with a Create Session Response message across GTPv2 based S2b/S2a interface or a Proxy Binding Acknowledgement message across PMIPv6 based S2b/S2a interface. PGW's FQ-CSIDs in the Create Session Response or Proxy Binding Acknowledgement indicates to the ePDG/TWAN that PGW supports partial failure handling. The ePDG/TWAN shall then store the PGW's FQ-CSID in its PDN connection table.

If the PGW does not support partial failure handling, then the PGW shall silently discard ePDG's/TWAN's FQ-CSID.

Figure 23-3 illustrates FQ-CSID establishment during the Sx Session Establishment procedure for 3GPP access, with a split SGW, as specified in the above rules.

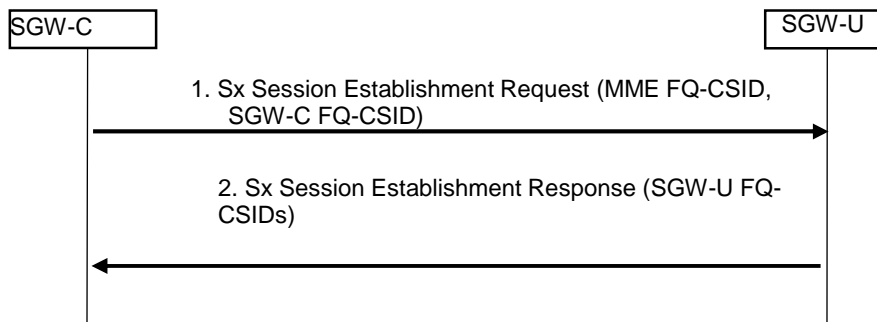


Figure 23-3: FQ-CSID establishment during the Sx Session Establishment procedure

1. If an SGW-C supports partial failure handling, the SGW-C shall send its own FQ-CSID and MME FQ-CSID to the SGW-U in the Sx Session Establishment Request.
2. If the SGW-U supports partial failure handling, it shall store the SGW-C FQ-CSID and MME FQ-CSID for the related Sx Session and it shall send its own FQ-CSID back to the SGW-C in the Sx Session Establishment Response message. The SGW-U's FQ-CSID in the Create Session Establishment Response implicitly indicates to the SGW-C that SGW-U supports partial failure handling. The SGW-C shall then store the SGW-U's FQ-CSID for the related Sx Session. If the SGW-C does not receive an SGW-U FQ-CSID from the SGW-U, then the SGW-C shall not further send partial failure handling related messages or IEs to the SGW-U.

If the SGW-U does not support partial failure handling, then the SGW-U shall silently discard the SGW-C's FQ-CSID and MME FQ-CSID.

Figure 23-4 illustrates FQ-CSID establishment during the Sx session Establishment procedure with a split PGW as specified in the above rules.

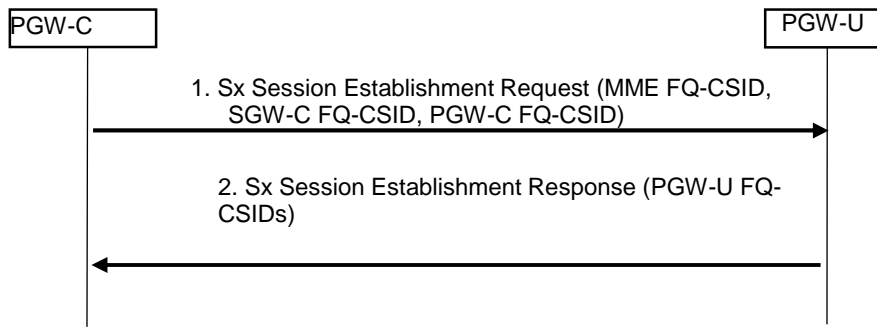


Figure 23-4: FQ-CSID establishment during the Sx session establishment procedure

1. If a PGW-C supports partial failure handling, the PGW-C shall send its own FQ-CSID, SGW-C FQ-CSID, TWAN FQ-CSID, ePDG FQ-CSID and MME FQ-CSID to PGW-U in the Sx Session Establishment Request.
2. If the PGW-U supports partial failure handling, it shall store the PGW-C FQ-CSID, SGW-C FQ-CSID, TWAN FQ-CSID, ePDG FQ-CSID and MME FQ-CSID for the related Sx Session and it shall send its own FQ-CSID back to the PGW-C in the Sx Session Establishment Response message. The PGW-U's FQ-CSIDs in the Sx Session Establishment Response implicitly indicates to the PGW-C that PGW-U supports partial failure handling. The PGW-C shall then store the PGW-U's FQ-CSID for the related Sx Session. If the PGW-C does not receive a PGW-U FQ-CSID from the PGW-U, then the PGW-C shall not further send partial failure handling related messages or IEs to the PGW-U.

If the PGW-U does not support partial failure handling, then the PGW-U shall silently discard PGW-C's FQ-CSID.

Figure 23-5 illustrates FQ-CSID establishment during the Sx Session Establishment procedures to provide the PGW-C FQ-CSID to the SGW-U after receiving a PGW-C FQ-CSID in Create Session Response from PGW-C on the S5/S8 interface.

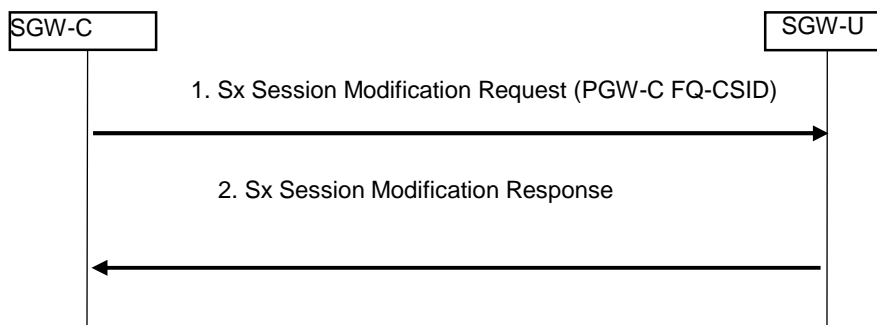


Figure 23-5: FQ-CSID establishment to provide a PGW-C FQ-CSID to the PGW-U

1. If an SGW-C supports partial failure handling and the SGW-U has indicated its support of partial failure in the Sx Session Establishment Response, the SGW-C shall send PGW-C FQ-CSID received on S5/S8 interface to the SGW-U in an Sx Session Modification Request.
2. If the SGW-U supports partial failure handling, it shall store the PGW-C FQ-CSID for the related Sx Session and send a reply to the SGW-C.

If the SGW-U does not support partial failure handling, then the SGW-U shall silently discard the PGW-C's FQ-CSID.

24 Restoration of data in the PCRF

24.1 Restart of the PCRF

24.1.0 PCRF Restart

PCRF storage of PCC contexts is volatile. When a PCRF fails, the PCC contexts and Diameter sessions affected by the failure are lost in the PCRF.

When a PCRF receives a non-initial message for which no Diameter session exists, it shall discard the message and return a Diameter error indication to the originating PCRF client.

25 Network triggered service restoration procedure

25.1 General

The network triggered service restoration procedure is an optional feature for the MME, S4-SGSN and SGW. A node that supports this feature shall support the network triggered service restoration procedure without ISR as specified in subclause 25.2 and the network triggered service restoration procedure with ISR as specified in subclause 25.3 if it supports Idle mode Signalling Reduction (ISR) (see 3GPP TS 23.401 [15] and 3GPP TS 23.060 [5]).

The network triggered restoration procedure without ISR shall apply to UEs for which ISR is not active at the time the ISR associated node fails. The network triggered restoration procedure with ISR shall apply to UEs for which ISR is active at the time the ISR associated node fails. Both procedures may run in parallel if there is a mix of UEs with ISR and without ISR at the time the ISR associated node fails.

For the PMIP based S5/S8 case, the terminology "S5/S8 bearer" used through clause 25 shall be read as "S5/S8 IP traffic flow" within the GRE tunnel. The detailed concepts of the "IP traffic flow" are specified in 3GPP TS 23.402 [18].

25.2 Network triggered service restoration procedure without ISR

25.2.1 General

The following requirements shall apply if the MME or S4-SGSN and the SGW support this feature.

If an SGW detects that an MME or S4-SGSN has restarted (see clause 18 "GTP-C based restart procedures"), instead of removing all the resources associated with the peer node, the SGW shall maintain the PDN connection table data and MM bearer contexts for some specific S5/S8 bearer contexts eligible for network initiated service restoration, and initiate the deletion of the resources associated with all the other S5/S8 bearers.

NOTE 1: This enables the SGW to still receive downlink user plane or control plane data from the PGW or from a PCRF (PMIP based S5/S8) for the maintained S5/S8 bearers.

The S5/S8 bearers eligible for network initiated service restoration are determined based on operator's policy, e.g. based on the QCI and/or ARP and/or APN, and such operator's policy shall be applicable for both the SGW and the MME/SGSN. The Delay Tolerant Connection Indication (DTCI), if set, may also be used to determine that the S5/S8 bearer is not eligible for network initiated service restoration, based on operator's policy when using QCI and/or ARP and/or APN is not sufficient, e.g. for Home routed roaming scenario.

Emergency PDN connections for users without authenticated IMSI do not need to be maintained by the SGW and cannot be restored at the initiative of the network.

NOTE 2: Users with an emergency call in progress can re-attach and re-establish the emergency PDN connection after detecting the loss of the signalling connection with the RAN. IMS Emergency PSAP callback is not supported for unauthenticated users with an emergency registration but without an emergency call in progress.

If at least one S5/S8 bearer needs to be maintained, the SGW shall also start a timer controlling the maximum duration during which those bearers shall be maintained. There is one operator configurable timer per SGW. The timer value may be equal to the periodic tracking area update timer (timer T3412) as specified in 3GPP TS 24.301 [19] or the periodic routing area update timer (timer T3312) as specified in 3GPP TS 24.008 [20]. This timer ensures that the S5/S8 bearers eligible for network initiated service restoration are maintained until the corresponding UE reattaches to the network. If the timer expires, the maintained resources shall be locally deleted assuming that the corresponding UE might have reattached to the network via a different SGW.

The SGW shall not release the default bearer of a PDN connection for which one or more dedicated bearers are maintained. Any downlink user plane or control plane packet received on a default bearer which is not eligible for network initiated service restoration but which is maintained for dedicated bearer(s) eligible for such procedure shall be silently discarded by the SGW.

When releasing the maintained S5/S8 bearers, the SGW may optionally perform other implementation specific actions such as messages to clear other external resources (e.g. PCC messages to clear the resources in the PCRF or GTP/PMIP messages to release the corresponding PDN connection in the PGW).

If the SGW receives a Create Session Request message for a UE for which some S5/S8 bearers are maintained, the SGW shall delete all the bearers for this UE and proceed with the Create Session Request message handling as specified in 3GPP TS 29.274 [13].

25.2.2 SGW procedure

Upon receipt of the first downlink user plane or control plane packet on a maintained S5/S8 bearer or PCC signalling from PCRF, the SGW shall immediately send a Downlink Data Notification message including the IMSI to the respective MME or S4-SGSN. In addition, depending on the received downlink packet type the SGW shall proceed as follows:

- if the received downlink packet contains user plane data, the SGW shall silently discard it but the SGW shall continue maintaining the corresponding bearers. If the SGW receives another downlink user plane packet for an ARP value other than the ARP included in the Downlink Data Notification sent before, it shall proceed as specified in subclause 5.3.4.3 "Network Triggered Service Request" of 3GPP TS 23.401 [15] with the exception that the packet shall be discarded by the SGW.
- For the S5/S8 GTP case:
 - if the received downlink packet contains a control plane message other than a Delete Bearer Request message then the SGW may reject the message and shall continue maintaining the corresponding bearers. If the SGW receives another control plane message for an ARP value other than the ARP included in the Downlink Data Notification sent before, it shall proceed as specified in subclause 5.3.4.3 "Network Triggered Service Request" of 3GPP TS 23.401 [15] with the exception that the message may be rejected by the SGW.
 - if the received downlink packet contains the Delete Bearer Request message, the SGW shall accept the message, and shall release the corresponding S5/S8 bearer(s) immediately.
- For the S5/S8 PMIP case:
 - if the received packet contains a control plane message other than the message of the Gateway Control and QoS Rules Provision procedure as specified in 3GPP TS 29.213 [21] subclause 4.4.3 which results in the SGW to decide to deactivate an existing dedicated bearer, then the SGW may reject the message and shall continue maintaining the corresponding bearers. If the SGW receives another control plane message for an ARP value other than the ARP included in the Downlink Data Notification sent before, it shall proceed as specified in subclause 5.3.4.3 "Network Triggered Service Request" of 3GPP TS 23.401 [15] with the exception that the message may be rejected by the SGW.
 - if the received downlink packet contains the message of the Gateway Control and QoS Rules Provision procedure as specified in 3GPP TS 29.213 [21] subclause 4.4.3 which results in the SGW to decide to deactivate an existing dedicated bearer, the SGW shall accept the message, and shall release the corresponding S5/S8 bearer(s) immediately.

The SGW may send the Downlink Data Notification message including the IMSI to the respective MME or S4-SGSN, if there is some DL data buffered for a UE when detecting the MME or S4-SGSN restart.

NOTE: For a UE using a power saving feature, DL data can be buffered for an extended duration in the SGW. The above requirement can allow the MME or S4-SGSN to restore the service to such a UE at the next occasion the UE becomes reachable. The SGW needs to pace the sending of Downlink Data Notification to the MME or S4-SGSN to avoid signalling storms over S11 and S4.

The SGW may send the Downlink Data Notification message to another MME or S4-SGSN (the same type of mobility node as the failed one) located in the same pool as the failed node if the SGW can not send it to the failed MME or S4-SGSN (e.g. because it did not restart). It is an implementation/deployment matter how an SGW becomes aware that an MME/S4-SGSN has failed and has not restarted.

25.2.3 MME/SGSN procedure

Upon receipt of a Downlink Data Notification message including the IMSI, the MME or S4-SGSN shall respond to the SGW with a Downlink Data Notification Acknowledge message and should page and force the UE to re-attach to the network. The paging area and subscriber's identity i.e. IMSI or S-TMSI/P-TMSI used during the paging procedure is implementation dependent. The MME or S4-SGSN may support and apply this procedure to a UE using extended idle mode DRX, and if so, they shall page the UE with the S-TMSI/P-TMSI.

NOTE 1: Upon receiving a page message with

- the IMSI, the UE starts the reattach procedure as specified in subclause 5.6.2.2.2 of 3GPP TS 24.301 [19] and subclause 4.7.9.1.2 of 3GPP TS 24.008 [20];
- the S-TMSI, the UE starts the service request procedure which is rejected by the MME with Cause #10 – Implicitly detached; the UE then re-attaches to the network as specified in subclause 5.6.2.2.1 of 3GPP TS 24.301 [19];
- the P-TMSI, in case of Iu mode, the UE starts the service request procedure which is rejected by the S4-SGSN with Cause #10 – Implicitly detached; the UE then re-attaches as specified in subclauses 4.7.9.1.1 and 4.7.13 of 3GPP TS 24.008 [20];
- the P-TMSI, in case of A/Gb mode, the UE sends any LLC frame and subsequently re-attaches to the network as specified in subclause 8.1.4 of 3GPP TS 23.060 [5].

NOTE 2: Paging in the MME or S4-SGSN serving area will cause excessive use of radio resources. How to reduce the paging area is implementation dependent.

NOTE 3: It is the responsibility of the MME/S4 SGSN to avoid unnecessary IMSI Paging.

NOTE 4: How the restarted or alternative MME/S4-SGSN knows the UE's DRX parameter or the extended DRX parameters to page the UE is implementation dependent.

NOTE 5: A restarted MME will not receive S1AP UE Context Active message as part of UE initiated Connection Resume procedure, since the eNB would have deleted the AS context for all UEs associated with this MME after detecting the MME restart.

The MME or S4-SGSN may request the SGW to immediately release the maintained S5/S8 bearers by sending the "Downlink Data Notification Acknowledge" message or a "Downlink Data Notification Failure Indication" message with the specific cause "UE already re-attached", e.g. if the UE has already re-attached to the network. The Downlink Data Notification Acknowledge and Downlink Data Notification Failure Indication shall include the IMSI to identify the UE context in the SGW.

25.3 Network triggered service restoration procedure with ISR

25.3.1 General

The following requirements shall apply if the involved MME, S4-SGSN and SGW support the ISR feature and the network triggered service restoration feature.

NOTE: The procedure in this clause does not consider the case where one of ISR associated nodes, i.e. the MME or the S4-SGSN, does not support the network triggered service restoration procedure.

In the rest of this clause, the term "non-failed" node refers to the CN node (MME or S4-SGSN) that remains in normal operation during this procedure, as opposed to the "restarted" node which refers to the CN node (MME or S4-SGSN) that has failed and restarted.

The procedure in the SGW towards the restarted node differs from the procedure towards the non-failed ISR associated node (see subclause 25.3.2).

25.3.2 SGW procedure

If an SGW detects that an ISR associated CN node (i.e. MME or S4-SGSN) has restarted (see clause 18), the SGW shall maintain all the PDN connection table data and MM bearer contexts associated with the non-failed and the restarted ISR associated nodes, and start a timer controlling the maximum duration during which the SGW shall consider that ISR is still active. There is one operator configurable timer per SGW. The timer value may be set to a value that is the greater value of the periodic tracking area update timer (timer T3412) as specified in 3GPP TS 24.301 [19] and the periodic routing area update timer (timer T3312) as specified in 3GPP TS 24.008 [20]. This timer ensures that the SGW can still send Downlink Data Notification messages to the restarted MME or S4-SGSN until the corresponding UE learns that ISR is deactivated. If the timer expires, the SGW shall deactivate ISR by locally releasing the resources for the maintained restarted CN node (i.e. restarted CN node control plane F-TEID).

Upon receipt of the downlink user plane or control plane packet on a maintained S5/S8 bearer for a UE in idle mode or in connected state with the failed CN node, the SGW shall initiate the network triggered service request procedure towards the non-failed CN node as specified in 3GPP TS 23.401 [15] subclause 5.3.4.3. In addition, if the S5/S8 bearer is eligible for network initiated service restoration, the SGW shall also immediately send a Downlink Data Notification message including the IMSI towards the restarted CN node as specified in subclause 25.2.2. The SGW shall continue to forward downlink user plane or control plane packet for a UE in connected state in the non-failed ISR associated node.

The S5/S8 bearers eligible for network initiated service restoration are determined by the SGW based on operator's policy e.g. based on the QCI and/or ARP and/or APN.

Emergency PDN connections for users without authenticated IMSI do not need to be maintained by the SGW and cannot be restored at the initiative of the network.

NOTE 0: Users with an emergency call in progress can re-attach and re-establish the emergency PDN connection after detecting the loss of the signalling connection with the RAN. IMS Emergency PSAP callback is not supported for unauthenticated users with an emergency registration but without an emergency call in progress.

The SGW may send the Downlink Data Notification message with the IMSI to another MME or S4-SGSN (the same type of mobility node as the failed one) in the same MME or S4-SGSN pool if the SGW can not send it to the failed MME or S4-SGSN (e.g. because it did not restart). It is an implementation/deployment matter how an SGW becomes aware that an MME/S4-SGSN has failed and has not restarted.

Upon receipt of a Downlink Data Notification message including the IMSI, the restarted CN node shall respond to the SGW with a Downlink Data Notification Acknowledge message and should page the UE and force it to re-attach to the network as specified in subclause 25.2.

NOTE 1: If the UE camps under the service area of the restarted CN node, then the UE re-attaches to the network (see NOTE 1 in subclause 25.2.3).

If the paging is successful (i.e. Modify Bearer Request is received) for the non-failed ISR associated CN node, the SGW may send a Stop Paging Indication message including the IMSI to the restarted CN node (or the alternative node in the same pool to which the Downlink Data Notification message with the IMSI has been sent before) to stop the paging procedure.

If the SGW receives a Create Session Request message as part of Initial Attach procedure for a UE for which the PDN connections, MM bearer context and ISR state have been maintained, the SGW shall stop the timer, deactivate ISR, and delete the maintained resources associated to the restarted CN node (i.e. CN node control plane F-TEID). The SGW may additionally send a Stop Paging Indication message to the non-failed ISR associated CN node to stop the paging procedure.

NOTE 2: The SGW may have already deleted the restarted CN node resources since Delete Session Request from non-failed ISR associated CN node may arrive earlier than the Create Session Request message.

If the non-failed ISR associated CN node received a Cancel Location message from HSS/HLR with "Initial Attach procedure" Cancellation Type, the non-failed CN node shall delete all the bearer contexts and send Delete Session Request message(s) to SGW. The SGW shall then release all the resources for this UE and sends one of the following messages to PGWs involved to release all the resources maintained in the PGWs as specified in 3GPP TS 23.401 [15] and 3GPP TS 23.402[18].

- For the GTP based S5/S8 case, Delete Session Request message(s)
- For the PMIP based S5/S8 case, PBU message(s) with Lifetime set to "0"

The SGW shall stop the timer and delete the resources for the maintained restarted CN node (i.e. restarted CN node control plane F-TEID) if it receives one of the following messages while the timer is running:

- a Modify Bearer Request message indicating that ISR is not active, e.g. from the non-failed CN node during a TAU/RAU procedure; or
- a Modify Bearer Request message indicating that ISR is active from another mobility management node with the same type as the restarted node.

25.3.3 MME/S4-SGSN procedure

If an MME/S4-SGSN detects a restart of an ISR associated counterpart (see clause 18), the MME/S4-SGSN shall wait for the next RAU/TAU procedure to deactivate ISR.

NOTE: As an implementation option, an MME/S4-SGSN may internally mark the ISR as not active, but this should not be visible in messages sent to the SGW.

The non-failed CN node may initiate the GUTI Relocation or P-TMSI Relocation Procedure with a non-broadcast TAI or RAI to force the UE to perform the TAU/RAU procedure for ISR deactivation, e.g. if a signalling connection is established with the UE following receipt of a Downlink Data Notification message.

If afterwards the non-failed MME/S4-SGSN receives TAU/RAU Request, then the MME/S4-SGSN shall inform the UE in the TAU/RAU Accept message to disable ISR as specified in 3GPP TS 23.401[15] and 3GPP TS 23.060 [5]. The non-failed CN node shall send a Modify Bearer Request message to the SGW, even if the MME/S4-SGSN did not change during the TAU/RAU, to request the SGW to disable ISR and to update the SGW with the latest RAT Type and Serving Network values. Upon receipt of that message, the SGW shall disable ISR and shall stop sending Downlink Data Notification message with IMSI to the restarted CN node.

26 Mobile terminated CS service delivery via an alternative MME in MME pool

This procedure is an optional feature for VLR and MME. It enables the network to continue delivering mobile terminated CS services to UEs via an alternative MME in the MME pool where the UE is located when the MME to which the UE was registered fails without restart or fails for a long duration.

NOTE 1: UEs in idle mode are not aware of an MME failure until they need to send some uplink data or signalling (e.g. a periodic Tracking Area Update) or until they are forced to re-attach e.g. via the network triggered service restoration procedure. Without support of the procedure defined in this clause, UEs that remain under LTE may not be able to receive mobile terminated CS services for a long duration after an MME failure without restart or a long MME failure.

The following requirements shall apply if the VLR and MME support this feature.

When the VLR has to page the UE for a mobile terminated CS service (e.g. upon receipt of an incoming CS call), if the VLR detects that the MME serving the UE is no longer in service, the VLR should send an SGs paging request with a CS restoration indicator to one alternative MME in the same MME pool. The VLR should load-balance the paging requests among the available MMEs in the pool during the restoration procedure.

The VLR may know the set of MMEs pertaining to the same MME pool by local configuration or by checking the MME Group ID within the MME name that MMEs signal to the VLR in the SGsAP-LOCATION-UPDATE-REQUEST,

SGsAP-RESET-INDICATION or SGsAP-RESET-ACK messages. The MME should send an SGsAP-RESET-INDICATION message to the VLR after restart.

The VLR may detect that an MME is no longer in service if there are no more SCTP associations in service with that MME.

NOTE 2: Semi-permanent SCTP associations are established between the MME and VLR, i.e. the SCTP associations remain up under normal circumstances.

The VLR should adjust its paging retransmission delay to avoid requesting again the UE to re-attach before the restoration procedure completes.

The MME shall behave as specified in subclause 14.1.3 upon receipt of an SGs paging request not including the CS restoration indicator.

The MME shall accept the SGs paging request and proceed as follows upon receipt of an SGs paging request including the CS restoration indicator:

- if the IMSI is unknown by the MME, or if the IMSI is known and the UE is marked as EMM-DEREGISTERED, the MME shall send the paging request with the location information provided by the VLR, regardless of the value of the "MME-Reset" indicator. If no such location information is provided, the MME may either page the UE in all the tracking areas corresponding to that MME or in the tracking areas served by the MME and by the VLR, or reject the paging request per operator policy. The paging request shall include the IMSI and the CN domain indicator set to "PS" to request the UE to re-attach;
- if the IMSI is known by the MME and the UE is considered to be attached to both EPS and non-EPS services or for SMS only (for an SGs paging request with an 'SMS indicator'), the MME shall page the UE based on the location information stored in the MME.

The MME may support and apply this procedure to a UE using extended idle mode DRX for MT-SMS service, and if so, the MME shall page the UE with the S-TMSI.

NOTE 3: How the alternative MME knows the UE's DRX parameter or the extended DRX parameters to page the UE is implementation dependent.

Upon receipt of a paging request including the IMSI and the CN domain indicator set to "PS", or upon receipt of a Service Reject with Cause #10 – Implicitly detached (when using S-TMSI paging), the UE re-attaches to one MME of the pool (that may not be necessarily the MME that initiated the paging procedure towards the UE) and a new SGs association is established with the VLR. This may be a different VLR than the VLR that initiated the SGs paging procedure, e.g. if Intra Domain Connection of RAN Nodes to Multiple CN Nodes is deployed for GERAN or UTRAN (see 3GPP TS 23.236 [24]).

NOTE 4: The UE can receive a Service Reject with Cause #10 – "Implicitly detached" upon being paged by an alternative MME with the S-TMSI assigned by the MME that has failed. The UE then re-attaches to the network as specified in subclause 5.6.2.2.1 of 3GPP TS 24.301 [19].

If the new SGs association is established towards the same VLR, the VLR should repeat the SGs paging request after the UE has re-attached to non-EPS services. The MT CS service or SMS is then delivered according to normal procedures.

If the new SGs association is established towards a different VLR, the MT CS service may be delivered via the new VLR using Mobile Terminating Roaming Retry or Mobile Terminating Roaming Forwarding (see 3GPP TS 23.018 [23]); the on-going MT SMS is retransmitted by the SMS-SC using the existing SMS procedures (SMS alert).

Subsequent MT CS services are delivered as per normal procedures.

NOTE 5: A UE with ISR active before the MME failure and using GERAN or UTRAN radio access will not receive the paging request sent by the alternative MME. The VLR can deliver the MT CS service by paging the UE on the A/Iu interface as per existing principles of 3GPP TS 29.118 [14] when the UE does not respond to a first paging on the SGs interface. Paging the UE on the A interface fails if the network operates in NMO I and the UE is in PS connected mode in GERAN.

See 3GPP TS 29.118 [14] for a comprehensive description.

27 Restoration of PDN connections after an SGW failure

27.1 General

The procedures specified in this clause enable to restore in the EPC the PDN connections affected by an SGW failure with or without restart, and thus to resume delivery of downlink data towards the UE with minimum service interruption and with minimal signalling in the network.

All the procedures specified in this clause are optional to support.

The procedures specified in subclause 27.2 apply to UEs for which ISR is not active when the SGW fails. The procedures specified in subclause 27.3 apply to UEs for which ISR is active when SGW fails. The procedures specified in these clauses only apply to PDN connections established between MME/S4-SGSN and PGW pertaining to the same operator, i.e. for non-roaming and roaming scenarios with local breakout. The MME/S4-SGSN and the PGW shall behave as per the restoration requirements specified in subclauses 14.1A.1 and 17.1A.1 for PDN connections established between nodes pertaining to different operators, i.e. as if the remote peer node does not support these SGW restoration procedures.

The procedures specified for an SGW in subclauses 27.2 and 27.3 apply as well to an SGW-C. An SGW-C shall always apply in addition the related PFCP procedures towards the SGW-U.

NOTE 1: The applicability of these procedures is restricted to PDN connections established between MME/S4-SGSN and PGW pertaining to the same operator to ensure, simply by local configuration, that MME/S4-SGSN and PGWs apply the same logic i.e. same operator's policies when determining whether and which PDN connections should be restored. This enables to restore in particular IMS PDN connections (even in roaming scenarios, for which local break out is used).

NOTE 2: The use of these SGW restoration procedures may be extended by Service Level Agreements to PDN connections established between MME/S4-SGSN and PGW pertaining to different operators, i.e. for roaming scenarios with home routed traffic, but this is not further considered in 3GPP specifications.

27.2 Restoration of PDN connections after an SGW failure for UEs without ISR

27.2.1 General

The PGW triggered SGW restoration procedure is an optional add-on feature for the MME/S4-SGSN, SGW and PGW on top of the MME/S4-SGSN triggered SGW restoration procedure as specified in subclause 27.2.2. A node that supports the PGW triggered SGW restoration procedure shall support the requirements specified in subclause 27.2.2 and in subclause 27.2.3.

27.2.2 MME/S4-SGSN triggered SGW restoration

27.2.2.1 General

The following requirements shall apply if the MME/S4-SGSN, the SGW, the PGW, and the PCRF support this feature.

The MME/S4-SGSN, PGW, and PCRF for PMIP based S5, shall know by local configuration whether this MME/S4-SGSN triggered SGW restoration procedure is supported in the PLMN, i.e. by peer PGWs, PCRFs and MME/S4-SGSNs. The PGW shall assume that either all or none of the MMEs/S4-SGSNs in the PLMN support this procedure. Upon detecting an SGW failure with or without restart (relying on restart counter as specified in clause 18 "GTP-C based restart procedures" and clause 19 "PMIP based restart procedures", or implementation e.g. preconfigured path failure timer), the MME/S4-SGSN and PGW shall maintain the bearers and MM contexts of the PDN connections affected by the SGW failure and eligible for restoration, instead of removing associated resources as per procedures specified in subclauses 14.1A.1 and 17.1A.1.

For PMIP based S5, when the PCRF detects an SGW failure or restart, the PCRF shall maintain the IP-CAN sessions and delete locally the Gxc sessions affected by the SGW failure.

NOTE 1: The PGW notifies the PCRF about the termination of IP-CAN sessions associated to PDN connections that are not restored by the MME/S4-SGSN within an operator configurable period.

The PDN connections eligible for restoration are determined by the MME/S4-SGSN and PGW based on same operator's policies, e.g. based on QCI, ARP and/or APN.

NOTE 2: The PCRF is not aware of which PDN connections are eligible for restoration. When the PGW detects an SGW failure, the PGW requests the PCRF to terminate IP-CAN sessions associated to PDN connections affected by the SGW failure and not eligible for restoration.

Maintaining the PDN connections affected by the SGW failure enables the MME/S4-SGSN to restore the corresponding bearers of the UE by selecting a new SGW or the restarted SGW. These PDN connections are maintained for an operator configurable period (T-Release-PDN timer), which is locally provisioned on MME/S4-SGSN and PGW, that by default should cover the periodic tracking area update timer (timer T3412) as specified in 3GPP TS 24.301 [19] or the periodic routing area update timer (timer T3312) as specified in 3GPP TS 24.008 [20]. After the expiry of the T-Release-PDN timer the MME/S4-SGSN and the PGW should delete any EPS bearer contexts that have not been restored via a new or the restarted SGW.

NOTE 3: The PGW's capability of supporting this SGW restoration procedure is stored per PDN and per UE by the serving MME/S4-SGSN. For a UE with multiple active PDN connections, some PGWs may support the SGW restoration procedure while others do not support the same. E.g. SGW restoration procedure may be supported for a PDN connection with local breakout while not supported for another PDN connection with home routed traffic. The restoration procedures upon SGW failure specified in subclauses 14.1A.1 and 17.1A.1 apply to the PDN connections for which the SGW restoration procedure is not supported or not applicable.

27.2.2.2 MME/S4-SGSN procedure

After detecting an SGW failure, the MME/S4-SGSN should attempt to restore the PDN connections eligible for restoration for all the UEs affected by the SGW failure, i.e. including UEs in ECM_IDLE / PMM-IDLE / GPRS STANDBY not engaged in any Service Request, or Connection Resume procedure or other mobility procedure. The MME/S4-SGSN shall control the pace of the SGW relocations to avoid core network node overload. The MME/S4-SGSN should prioritize the SGW relocation for UEs engaged in a Service Request, or a Connection Resume, or RAU/TAU procedures or having GBR bearers over UEs which are not engaged in any mobility procedure and that do not have a signaling connection to the MME/S4-SGSN nor GBR bearers. The MME/S4-SGSN should also prioritize the SGW relocation for UEs with an emergency PDN connection.

The MME/S4-SGSN may further prioritize the PDN connections to restore, e.g. for UEs ECM_IDLE / PMM-IDLE / GPRS STANDBY not engaged in any Service Request or Connection Resume procedure, based on operator's policy e.g. based on the QCI and/or APN. Besides, the MME/S4-SGSN may use the subscribed Restoration Priority per APN, if received from the HSS, and if permitted per service level agreements for in-bound roamers, to determine the relative restoration priority among PDN connections to the same APN. The MME/S4-SGSN may use a locally configured value as default restoration priority if the restoration priority for a user's PDN connection is not received from the HSS or not permitted by service level agreement for in-bound roamers.

NOTE 1: This is to allow all the affected UEs to be reconnected to the network in a relatively short time (that is function of the speed of the SGW relocations that the MME/S4-SGSN performs, based on implementation and the network load) so that downlink packets may be delivered to the UEs with minimum service interruption.

NOTE 2: Prioritizing the restoration of emergency PDN connections can enable to preserve emergency calls in progress for authenticated and unauthenticated users, and enable PSAP to call back authenticated users with an emergency registration but without an emergency call in progress.

NOTE 3: The Restoration Priority can e.g. allow to restore with a higher priority users with an IMS voice subscription over IMS users without an IMS voice subscription.

To restore the PDN connection(s) of a UE, the MME/S4-SGSN shall perform an SGW relocation procedure by sending a Create Session Request message (per PDN connection to restore) to the new or restarted SGW as per the steps 8-11 of a Tracking Area Update procedure with Serving GW change in subclause 5.3.3.1 in 3GPP TS 23.401[15]. For PDN connections with GBR bearers existing before the SGW failure, the MME/S4-SGSN may either request to restore or remove the GBR bearers in the Create Session Request (e.g. depending on how quickly the PDN connection is

restored). The MME/S4-SGSN shall restore the PDN connections of the affected UEs after the SGW failure as follows:

- 1) for UEs in ECM_IDLE/PMM-IDLE/GPRS STANDBY state:
 - the MME/S4-SGSN shall select a new SGW or the restarted SGW based on the last visited TAI/RAI. When Dedicated Core Networks are deployed, the UE Usage Type shall also be used for the SGW selection as specified in 3GPP TS 29.303 [37];
 - the MME/S4-SGSN shall then perform an SGW relocation procedure as specified above.
- 2) for UEs in ECM_CONNECTED/PMM-CONNECTED/GPRS READY state not engaged in any mobility procedure (TAU/RAU, Handover):
 - the MME/S4-SGSN shall release the S1/Iu/radio resources; if the eNodeB/RNC detects the SGW failure, the eNodeB/RNC may request the MME/S4-SGSN to release the S1/Iu resources;
 - the MME/S4-SGSN shall then handle these UEs as specified for UEs in ECM_IDLE/PMM-IDLE/GPRS STANDBY state, or for UEs performing a mobility procedure if the UE performs subsequently such a mobility procedure (e.g. a Service Request to re-establish the S1/Iu/radio bearers);
 - as an exception to these rules, for UTRAN without direct tunnel and GERAN, the S4-SGSN may perform SGW relocation while keeping the UEs in PMM-CONNECTED/GPRS READY state (i.e. without tearing down the Iu/radio resources) because S4 user plane is used and the SGW failure remains not visible to the radio network.

NOTE 4: An SGW failure with restart may be visible to the radio network and cause bearers to be released for bearers with on-going uplink traffic if an Error Indication is received from the SGW before the S4-SGSN detects the SGW restart.

- 3) for UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY state initiating a Service Request procedure or a Connection Resume procedure:
 - the MME/S4-SGSN shall first perform the SGW relocation procedure as specified above and then continue with the Service Request or the Connection Resume procedure since the MME/S4-SGSN has no valid SGW F-TEID to send in the S1-AP Initial Context Setup Request towards the eNodeB or in the Iu RAB Assignment Request message towards the RNC if Direct Tunnel is used.
- 4) for UEs initiating an intra-MME or intra-S4-SGSN TAU/RAU procedure:
 - the MME/S4-SGSN shall perform the SGW relocation procedure as specified above before the TAU/RAU procedure;
- 5) for UEs initiating an inter-MME/SGSN TAU/RAU procedure:
 - If both the source and target MME/S4-SGSNs support this SGW restoration procedure, the source MME/S4-SGSN should indicate to the target MME/S4-SGSN in the GTPv2 Context Response message that an SGW relocation procedure is needed due to an earlier SGW failure. Upon reception of such indication, the target MME/S4-SGSN shall perform the SGW relocation procedure as specified above and then proceed with the TAU/RAU procedure. The source MME/S4-SGSN may perform the SGW relocation procedure as specified above before responding to the GTPv2 Context Request message if the target MME/S4-SGSN does not support the SGW restoration procedure, e.g. during inter-PLMN RAU/TAU procedures when the target PLMN does not support the SGW restoration procedure.
- 6) for UEs in ECM-CONNECTED/PMM-CONNECTED/GPRS READY state for which a handover procedure is initiated:
 - The source MME/S4-SGSN should reject the Handover Required / Relocation Required message received from the RAN (for UEs with PDN connection(s) affected by an earlier SGW failure that have not been restored yet); the MME/S4-SGSN should then release the S1/Iu/radio resources of these UEs to force them to enter idle mode. The MME/S4-SGSN shall then proceed with the procedures specified above for UEs in ECM_IDLE/PMM-IDLE/GPRS STANDBY state, or for UEs performing a mobility procedure if the UE performs subsequently such a mobility procedure (e.g. a Service Request to re-establish the S1/Iu/radio bearers).

NOTE 5: S1/Iu/radio resources of UEs in ECM-CONNECTED/PMM-CONNECTED/GPRS READY state affected by an SGW failure are released very shortly after the SGW failure. Therefore only very few UEs affected an SGW failure and with PDN connections not restored yet may be subject to a handover, e.g. handovers taking place just after the SGW failure before the eNodeB/RNC or the MME/S4-SGSN release the S1/Iu/radio resources. This is why it is not necessary to support SGW relocation during Intra/Inter-CN handover procedures.

27.2.2.3 PGW procedure

The PGW shall maintain the PDN connections affected by the SGW failure and eligible for restoration for an operator configurable period (T-Release-PDN timer), as specified in subclause 27.2.2.1.

The PGW should maintain the GBR bearers of the PDN connections eligible for restoration for an operator configurable period (T-Release-GBR), which should be much shorter than the T-Release-PDN timer. Upon expiry of the T-Release-GBR timer, the PGW shall release GBR bearers that have not been restored yet and inform the PCRF about the corresponding PCC rule inactivation, with a cause as specified in 3GPP TS 29.212 [25].

NOTE: This is a safeguard mechanism to avoid e.g. overcharging the user in IMS for sessions not already terminated by IMS (e.g. by the far end user of a VoIP call).

The PGW shall discard downlink packets received for a PDN connection maintained after an SGW failure that has not been restored yet.

The PGW shall stop charging for PDN connections maintained after an SGW failure which have not been restored yet.

If the IP-CAN Session Modification Request is received for a PDN connection maintained after an SGW failure but not restored yet, the PGW shall reject the request if the request contains the installation/modification of PCC rules and other policy decisions (e.g. change of APN-AMBR), however the P-GW shall accept to remove the PCC rule if the removal of PCC rules is included in the request. The PGW shall accept an IP-CAN Session Modification Request if it only includes the removal of PCC rules. Refer to 3GPP TS 29.212 [25] subclause B.3.14 for the detail. For these IP-CAN sessions for which an IP-CAN session modification has been rejected, the PGW shall subsequently inform the PCRF when the PDN connection is restored as specified in subclause B.3.14 of 3GPP TS 29.212 [25]. This would enable the PCRF to update the PCC rules in the PGW if necessary. After the PDN connection is restored, the PGW shall initiate the bearer modification/deactivation procedure if necessary to modify or remove the resources associated with the PCC rules that were removed during the SGW failure.

The PGW shall accept an IP-CAN Session Termination Request received for a PDN connection maintained after an SGW failure but not restored yet, with an acceptance cause as specified in 3GPP TS 29.212 [25] and release the affected PDN connection locally. If subsequently the MME/S4-SGSN attempts to restore the PDN connection, the PGW shall reject the Modify Bearer Request (for GTP based S5) or the Proxy Binding Update (for PMIP based S5) with the cause "Context Not Found" as specified in 3GPP TS 29.274 [13] and 3GPP TS 29.275 [16] after the corresponding PDN connection has been released locally.

27.2.2.4 PCRF procedure

If the PGW rejects an IP-CAN session modification procedure with the rejection cause as specified in subclause 27.2.2.3, the PCRF should maintain the corresponding IP-CAN session and refrain from sending any further IP-CAN session modification request to the PGW until being notified by the PGW that the PDN connection is restored.

For PMIP based S5, the PCRF can not send any message to the SGW once the Gxc session in the PCRF is removed. The PCRF may however behave as for GTP based S5, e.g. send signaling to the PGW via the Gx interface. The Gxc session is restored when the PCRF receives Gateway Control Session Establishment from the SGW as specified in 3GPP TS 29.212 [25].

27.2.2.5 SGW procedure

After the SGW restarts, the SGW shall not send Error indication message for a configurable period when the SGW receives a GTP-U PDU for which no Bearer context exists.

NOTE: The period needs to be longer than the time required for the peer node to detect the restart of the SGW, e.g. the interval between two echo request messages. This ensures that the MME/SGSN or PGW does not deactivate the bearers before it detects the SGW failure and triggers the restoration procedure.

27.2.3 PGW triggered SGW restoration

27.2.3.1 General

The following requirements shall apply if the MME/S4-SGSN, the SGW and the PGW support this feature.

NOTE: The PGW triggered SGW restoration procedure does not require any further requirements from the PCRF than those already specified for the MME/S4-SGSN triggered SGW restoration procedure in subclause 27.2.2.1.

The PGW shall know by local configuration whether this PGW triggered SGW restoration procedure is supported in the PLMN. The MME/S4-SGSN/SGW may know the same by local configuration. When supported in the PLMN, the PGW supporting this procedure should be configured with the address of alternative(s) SGW(s) also supporting this procedure. The PGW shall assume that either all or none of the MMEs/S4-SGSNs in the PLMN support the procedure. All MMEs/S4-SGSNs in an MME/S4-SGSN pool should support this procedure when it is deployed.

The PGW triggered SGW restoration procedure does not apply to emergency PDN connections for users without authenticated IMSI.

NOTE: The MME/S4-SGSN can prioritize the restoration of emergency PDN connections (see subclause 27.2.2.2). IMS Emergency PSAP callback is not supported for unauthenticated users with an emergency registration but without an emergency call in progress.

27.2.3.2 MME/S4-SGSN procedure

During normal mode of operation (i.e. before SGW failure with/without restart):

The MME/S4-SGSN supporting the PGW triggered SGW restoration procedure shall include the MME/S4-SGSN identifier IE in existing signalling over the S11/S4 interface, i.e. in

- Create Session Request messages during an E-UTRAN Initial Attach, a UE requested PDN connectivity, and a PDP Context Activation procedure;
- Create Session Request message during TAU/RAU procedures with a SGW change;
- Create Session Request message during X2 based handover/Enhanced SRNS Relocation procedure with a SGW change;
- Modify Bearer Request message during Inter-RAT Handover procedures with/without a SGW change;
- Modify Bearer Request message during Intra-RAT handover procedure with a SGW change;
- Modify Bearer Request message during Inter-RAT TAU/RAU procedures without a SGW change;
- Modify Bearer Request message over S11/S4 if the message is deemed to be sent to the PGW due to other reasons, e.g. reporting ULI, time zone.

During SGW restoration procedure:

Upon receipt of a PGW Downlink Triggering Notification message for which it can not find a UE context corresponding to the received IMSI, the MME/S4-SGSN shall send a PGW Downlink Triggering Acknowledge message with the rejection cause code "Context Not Found" to the SGW to inform the SGW that the PGW Downlink Triggering Notification message has been received by the MME/S4-SGSN. If the PGW Downlink Triggering Notification message contains an MME/S4-SGSN identifier, the MME/S4-SGSN shall also include the IMSI and the MME/S4-SGSN identifier in the PGW Downlink Triggering Acknowledge message.

Upon receipt of a PGW Downlink Triggering Notification message for which it can find a UE context corresponding to the received IMSI, the MME/S4-SGSN shall send a PGW Downlink Triggering Acknowledge message back to the SGW with an acceptance cause code, and perform S-TMSI/P-TMSI paging as part of Network Initiated Service Request procedure as specified in subclause 5.3.4.3 of 3GPP TS 23.401 [15] and in subclause 6.12.1A of 3GPP TS 23.060 [5].

When receiving a Service Request message from the UE, the MME/S4-SGSN shall perform the SGW restoration procedure as specified in the subclause 27.2.2 with the addition that the MME/S4-SGSN shall include the MME/S4-SGSN identifier IE in the create session request message.

27.2.3.3 SGW procedure

During normal mode of operation (i.e. before SGW failure with/without restart):

The SGW shall forward the MME/S4-SGSN identifier IE to the PGW in existing signalling over the S5 interface if it is received over S11/S4 interface.

During SGW restoration procedure:

Upon receipt of a PGW Downlink Triggering Notification message (or a PMIP Update Notification message with the Notification Reason set to "PGW Downlink Trigger Notification") from a PGW, the SGW shall send the PGW Downlink Triggering Notification message to the MME/S4-SGSN identified by the MME/S4-SGSN identifier if present in the message. If no MME/S4-SGSN identifier is received from the PGW, the SGW shall send the PGW Downlink Triggering Notification message to all the MME/S4-SGSN within the MME/S4-SGSN pool as known by local configuration. The SGW shall then send a PGW Downlink Triggering Acknowledge message (or a PMIP Update Notification Acknowledgement message) back to the PGW with an acceptance cause code.

If the SGW receives a PGW Downlink Triggering Acknowledge message from an MME/S4-SGSN with the rejection cause code "Context Not Found" and with an IMSI and an MME/S4-SGSN identifier, the SGW shall then send a PGW Downlink Triggering Notification message, including the IMSI (as received in the PGW Downlink Triggering Acknowledge message), to all the MME/S4-SGSN within the MME/S4-SGSN pool as known by local configuration, except to the MME/S4-SGSN identified by the MME/S4-SGSN identifier received in the Downlink Triggering Acknowledge message.

The MME/S4-SGSN may have more than one IP address on the S11/S4 interface configured, but the PGW Downlink Triggering Notification should be sent only once per MME/S4-SGSN per local configuration in the SGW.

27.2.3.4 PGW procedure

During normal mode of operation (i.e. before SGW failure with/without restart):

The PGW shall store the MME/S4-SGSN identifier received in the last Create Session Request or Modify Bearer Request message (for GTP based S5) or Proxy Binding Update (for PMIP based S5) per PDN connection. If the PGW receives a Modify Bearer Request without MME/S4-SGSN identifier, it shall delete the stored MME/S4-SGSN identifier.

NOTE 1: This allows the PGW to have the serving MME/S4-SGSN address whenever there is S5 signalling message. However this cannot ensure that the PGW is always aware of the current serving MME/S4-SGSN address. E.g. during an inter-MME HO without SGW change, the current serving MME/S4-SGSN address will not be propagated to the PGW if there is no S5 signalling.

During SGW restoration procedure:

When downlink data packets or signalling other than an IP-CAN Session Termination Request arrives at the PGW, for a PDN connection associated with a failed SGW and that has not been restored yet (as specified in subclause 27.2.2), and the PDN connection is eligible for PGW initiated Downlink triggering based on operator's policies, e.g. for IMS PDN connection, the PGW shall proceed as follows:

- the PGW shall select a SGW (i.e. the restarted or an alternative SGW) which supports the PGW triggered SGW restoration procedure, based on local configuration;
- for GTP-based S5, the PGW shall then send a PGW Downlink Triggering Notification message including the IMSI and the MME/S4-SGSN identifier if available;
- for PMIP-based S5, the PGW shall then send a PMIP Update Notification message as specified in IETF RFC 7077 [26] to indicate it is a PGW initiated downlink triggering notification, including the IMSI and the MME/S4-SGSN Identifier when it is available;
- the PGW should not send a new PGW Downlink Triggering Notification message (for GTP-based S5) or Update Notification message (for PMIP-based S5) in very short time if it continues to receive subsequent downlink data or signaling for the same PDN connection. It is an implementation option how many times/how frequently the

PGW should send subsequent PGW Downlink Triggering Notification message (for GTP-based S5) or Update Notification message (for PMIP-based S5) before discarding the downlink packets or rejecting signalling.

- the PGW shall handle an IP-CAN Session Modification Request received from the PCRF as specified in subclause B.3.14 of 3GPP TS 29.212 [25] as if the PDN connection had not been affected by the SGW failure i.e. was in a normal state. After accepting an IP-CAN session modification request, if the MME/S4-SGSN does not restore the PDN connection shortly after the PGW initiated triggering, the PGW shall report the modification failure to the PCRF with a cause as specified in subclause B.3.14 of 3GPP TS 29.212 [25].

The PGW shall behave as specified in subclause 27.2.2.3 if the PGW receives an IP-CAN Session Termination Request for a PDN connection associated with a failed SGW and that has not been restored yet.

NOTE 2: To ensure the delivery of downlink data, it is implementation specific whether the PGW buffers or not the downlink data until the PDN connection is restored. The application functions e.g. P-CSCF for IMS, may also retransmit the data packets.

NOTE 3: The operator policies for PDN connections eligible for restoration (i.e. to be maintained upon SGW failure as per subclause 27.2.2) and PDN connections eligible for PGW initiated downlink triggering may differ, i.e. the PDN connections eligible for PGW initiated downlink triggering may be a subset of the PDN connections eligible for restoration.

27.3 Restoration of PDN connections after an SGW failure for UEs with ISR

27.3.1 MME/S4-SGSN triggered SGW restoration for UEs with ISR

27.3.1.1 General

The requirement specified in subclause 27.3.1.2 shall apply on top of the MME/S4-SGSN triggered SGW restoration procedure specified in subclause 27.2.2 and the involved MME and S4-SGSN additionally support the ISR feature.

NOTE: The procedure in this subclause does not consider the case where one of ISR associated nodes, i.e. the MME or the S4-SGSN, does not support the MME/S4-SGSN triggered SGW restoration procedure.

27.3.1.2 MME/S4-SGSN procedure

The MME/S4-SGSN shall restore the PDN connections of the affected UEs after the SGW failure as follows:

- 1) for UEs initiating an intra MME/S4-SGSN TAU/RAU procedure:
 - the MME/S4 SGSN shall perform the SGW relocation procedure as specified in subclause 27.2.2, and inform the UE in the related TAU/RAU Accept message to disable ISR as specified in 3GPP TS 23.401[15] and 3GPP TS 23.060 [5].
- 2) for UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY state initiating a Service Request procedure:
 - the MME/S4 SGSN shall perform the SGW relocation procedure as specified in subclause 27.2.2 and initiate the GUTI Relocation or P-TMSI Relocation procedure with a non-broadcast TAI or RAI to force the UE to perform the TAU/RAU procedure for ISR deactivation.
- 3) for UEs in ECM-CONNECTED/PMM-CONNECTED/GPRS READY state engaged in any handover or inter MME/S4-SGSN TAU/RAU procedure:
 - it shall be handled as specified in subclause 27.2.2.
- 4) for UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY state which are not engaged in any Service Request or other mobility procedure:
 - In networks supporting PGW triggered SGW restoration proactive paging of UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY state shall not be initiated.

The MME/S4-SGSN shall page the UE to bring the UE to ECM-CONNECTED/PMM-CONNECTED. If the paging is successful and the UE initiates the Service Request procedure, the MME/S4-SGSN shall perform the SGW relocation procedure as specified in subclause 27.2.2 and initiate the GUTI Relocation or P-TMSI Relocation Procedure with a non-broadcast TAI or RAI to force the UE to perform the TAU/RAU procedure for ISR deactivation as specified in subclause 5.3.4.3 of 3GPP TS 23.401[15]. If paging the UE fails, the MME or S4-SGSN should adjust its paging retransmission strategy (e.g. limit the number of short spaced retransmissions) to take into account the fact that the UE might be in GERAN/UTRAN or E-UTRAN coverage. If the associated MME/S4-SGSN receives ISR Status Indication with "deactivation Indication" from S4-SGSN/MME, the MME/S4-SGSN shall release the UE session locally. Otherwise after retrying the paging procedure, the MME/S4-SGSN may release locally the PDN connection context and UE MM context assuming the UE is in GERAN/UTRAN or E-UTRAN coverage area.

MME/S4-SGSN should handle UEs in ECM-CONNECTED/PMM-CONNECTED and involved in any handover or inter MME/S4-SGSN TAU/RAU procedure first before paging of UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY to minimise paging of UEs. Furthermore the sequence on how UEs in ECM-IDLE/PMM-IDLE/GPRS STANDBY can be paged to avoid overload are implementation dependent.

The MME/S4-SGSN which initiates the SGW restoration procedure should send ISR Status Indication with "ISR deactivation Indication" to the ISR associated S4-SGSN/MME to release the PDN connection context and UE MM context.

NOTE 1: The PDN connection context and UE MM context can be released after the timer (T-Release-PDN timer), which is used for maintaining the context, expires, as specified in subclause 27.2.2.1.

NOTE 2: The MME will only perform the SGW reselection for the UEs camping on the LTE, ISR activated UEs can camp in the GERAN/UTRAN, so paging is needed.

The S4-SGSN will only perform the SGW reselection for the UEs camping on the GERAN/UTRAN, ISR activated UEs can camp in the LTE, so paging is needed.

NOTE 3: It is the responsibility of the MME/S4-SGSN to avoid Paging Overload.

27.3.2 PGW triggered SGW restoration for UEs with ISR

27.3.2.1 General

The requirement specified in subclause 27.3.2.2 shall apply on top of the PGW triggered SGW restoration procedure specified in subclause 27.2.3 and the involved MME and S4-SGSN additionally support the ISR feature.

NOTE: The procedure in this subclause does not consider the case where one of ISR associated nodes, i.e. the MME or the S4-SGSN, does not support the PGW triggered SGW restoration procedure.

27.3.2.2 MME/S4-SGSN procedure

If the MME/S4-SGSN receives a PGW Downlink Triggering Notification message containing MME/S4-SGSN Identifier from the SGW for those UEs affected by the failed SGW, the MME/S4-SGSN shall behave as specified in subclause 27.2.3.2 and additionally send ISR Status Indication message with "Paging Indication" over the S3 interface to the ISR associated S4-SGSN/MME over the existing GTP-C tunnel between the S4-SGSN and the MME.

The ISR associated S4-SGSN/MME, which receives ISR Status Indication message with "Paging Indication", shall perform P-TMSI/S-TMSI paging as part of the Network Initiated Service Request procedure as specified in subclause 27.3.1.2.

After the MME/S4-SGSN receiving NAS message Service Request, the MME/S4-SGSN shall behave as specified in the subclause 27.3.1.2.

28 Restoration of data in the CSS

28.1 Restart of the CSS

The periodic backup of CSS data to non-volatile storage is mandatory.

When a CSS restarts after failure it shall perform the following actions for the subscriber data records that have been affected by the CSS fault:

- reload all data from the non-volatile back-up;
- send a "Reset" message to each VLR where one or more of its MSs may be registered to the CSS. This causes each VLR concerned to mark each relevant roaming user record "Location Information Not Confirmed by CSS", and
- send a "Reset" message to each SGSN where one or more of its MSs may be registered to the CSS. This causes each SGSN to mark each relevant MM context "Location Information Not Confirmed by CSS".
- send a "Reset" message to each MME where one or more of its UEs may be registered to the CSS.

29 MBMS Heartbeat procedure

The BM-SC, MBMS GW and GCS AS may support the MBMS Heartbeat procedure over the SGmb or MB2-C reference point to probe the liveness and detect the restart of a peer MBMS node.

This procedure is optional to support and use for MBMS deployments without an intermediate Diameter Agent between the BM-SC and the MBMS GW or GCS AS. A BM-SC, MBMS GW or GCS AS which support the MBMS restoration procedures as specified in this specification shall support and use the MBMS Heartbeat procedure for MBMS deployments with an intermediate Diameter Agent between the BM-SC and MBMS GW or GCS AS.

The restart of a peer MBMS node is detected using a Restart-Counter AVP. The Restart-Counter AVP contains a value that is incremented monotonically whenever the MBMS node restarts with loss of previous states.

The MBMS Heartbeat Request and Answer messages shall contain the Restart-Counter AVP set to the local restart counter of the sending node. Other MBMS messages sent over the SGmb or MB2-C reference point may also contain the Restart-Counter AVP if contacting the peer node for the first time or if the local restart counter has been incremented.

Upon receipt of a Restart-Counter AVP in a MBMS Heartbeat Request or Answer or in any other SGmb or MB2-C signalling message, the receiving node shall compare the value of the received Restart-Counter AVP with the previous Restart counter value stored for this peer entity and

- if no previous value was stored, the Restart counter value received in the SGmb or MB2-C signalling message shall be stored for the peer;
- if the value of the received Restart-Counter AVP is greater than the Restart-Counter previously received from the same MBMS node, the receiver shall consider that the peer MBMS node has restarted.

An intermediate Diameter Agent shall not modify the Restart-Counter AVP when proxying SGmb or MB2-C signalling between the BM-SC and MBMS GW or GCS AS.

The BM-SC, MBMS GW and GCS AS shall support the detection of an SGmb or MB2-C path failure by sending an MBMS Heartbeat Request message periodically when no other signalling is exchanged over those interfaces between those nodes. The MBMS Heartbeat Request message shall be repeated one or more times if no MBMS Heartbeat Answer is received. The SGmb or MB2-C path shall be considered to be down if the peer MBMS node does not respond to a configured number of consecutive MBMS Heartbeat Requests. MBMS Heartbeat Requests shall only be sent on a per node basis (i.e. not on a per MBMS session basis).

See 3GPP TS 29.061 [31] and 3GPP TS 29.468 [35] for further details.

30 Restoration of the SCEF

30.1 Restart of the SCEF

When an SCEF restarts after failure and has lost all or parts of his data, it shall reply to a report from MME, SGSN or HSS containing a SCEF reference ID for which it has no data with an error cause "SCEF_REFERENCE_ID_UNKNOWN" in the reply indicating that the SCEF reference ID provided in the message does not exist in the SCEF.

If an HSS receives a reply message with error cause set to "SCEF_REFERENCE_ID_UNKNOWN", it shall stop reporting and delete the event locally.

If an MME/SGSN receives reply message with error cause set to "SCEF_REFERENCE_ID_UNKNOWN", it shall stop reporting, initiate a notification to the HSS with cause "SCEF_REFERENCE_ID_UNKNOWN" and delete the event.

An HSS receiving a notification with cause "SCEF_REFERENCE_ID_UNKNOWN", it shall delete the event locally.

30.1.1 Mobile Originated NIDD procedure

During the Mobile Originated NIDD procedure, if the MME receives a MO-Data-Answer from the SCEF with a failure cause that UE cannot be found, the MME shall deactivate the corresponding PDN connection towards the UE with the cause "re-activation required", or initiate an explicit detach procedure with reattached required procedure, as appropriate, see 3GPP TS 24.301 [19].

Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
Apr 1999					Transferred to 3GPP CN1	6.1.0	
CN#03					Approved at CN#03		3.0.0
CN#04			001		GPRS restoration procedures	3.0.0	3.1.0
CN#06			002r2		Authentication Enhancements	3.1.0	3.2.0
CN#06			003		Support of VLR and HLR Data Restoration procedures with LCS	3.1.0	3.2.0
CN#07			004		Support of VLR and HLR Data Restoration procedures with LCS	3.2.0	3.3.0
CN#08			005		Clarifications on GSM vs. UMTS specific parts	3.3.0	3.4.0
CN#11					Release 4 after CN#11	3.4.0	4.0.0
CN#16			007		Removal of an optional IMSI paging after SGSN restart	4.0.0	4.1.0
CN#16					Release 5 after CN#16	4.1.0	5.0.0
CN#22			011r1		Restoration of data in RA update	5.0.0	5.1.0
CN#23			008r3		Change of Restart Counter definition for enhanced GTP	5.1.0	6.0.0
CN#25			012		Error Indication during an ongoing MBMS data transfer	6.0.0	6.1.0
CN#25			013		Restoration of GSNs in MBMS	6.0.0	6.1.0
CT#30			0014		Incorrect References	6.1.0	6.2.0
CT#32			0019r1		Correction for Usage of Cancel Location for Supercharger	6.2.0	7.0.0
CT#40			0020r2		EPS Restoration	7.0.0	8.0.0
CT#41			0021r3		Moving restoration procedures from TS 23.060 into TS 23.007	8.0.0	8.1.0
CT#41			0023r2		Node Restart Restoration Procedures for PGW, SGW and MME	8.0.0	8.1.0
CT#42			0027r2		RNC failure aligns with TS23.060	8.1.0	8.2.0
CT#42			0028		Restoration procedures for SGs interface	8.1.0	8.2.0
CT#42			0033r5		Partial Failure Handling	8.1.0	8.2.0
CT#42			0037r1		PMIP Path management / Restoration Clean-up	8.1.0	8.2.0
CT#43			0030r5		Moving the description of the restoration procedures (from 29.274) to 23.007	8.2.0	8.3.0
CT#43			0038r4		Partial fault handling finalization	8.2.0	8.3.0
CT#44			0043r1		FQ-CSID corrections	8.3.0	8.4.0
CT#44			0047r1		SGSN and SGW handling in case RNC/BSC Failure (lu mode) using S4	8.3.0	8.4.0
CT#44			0045r1		General on PMIP based restart procedure	8.4.0	9.0.0
CT#45			0065r1		Essential corrections to the partial failure support	9.0.0	9.1.0
			0051		Removal of Editor's note		
			0053r1		Restoration of data in MBMS GW		
			0058r1		Echo usage for GTPv2		
			0063r3		Error Indication cleanup		
			0064r4		Restoration of data in E-UTRAN		
CT#46			0066		Paging signalling optimization after SGSN failure	9.1.0	9.2.0
			0067		Paging signalling optimization after MME failure		
			0068		Error Indication for MBMS		
			0072r1		Removal of Editor's Notes for Partial Failure		
			0078r1		Error Indication Handling for MBMS		
			0080		Alignment of eNodeB failure sub-clause		
			0082r3		Alignment of RNC/BSC failure sub-clause		

CT#47			0091	Bulk Binding Revocation Indication	9.2.0	9.3.0
			0082r 2	Clarifications to eNodeB failure		
			0092r 1	Reference corrections		
			0095r 1	Restart counter correction		
CT#48			0100r 1	Essential correction to Error Indication message handling for the default bearer	9.3.0	9.4.0
			0076r 4	Cleanup of hanging PDN connections/bearers		
			0097r 1	Failure of remote nodes		
			0107r 1	Optimization on hanging PDN connection cleanup	9.4.0	10.0.0
CT#49			0115	Data Restoration for SMS	10.0.0	10.1.0
			0117	GTP-C based restart procedures		
			0121	Partial Failure handling		
CT#50			0135r 1	Heartbeat Request	10.1.0	10.2.0
			0129r 1	ePDG Partial Failure		
			0133r 1	Restoration of data in the ePDG		
			0131r 1	Error Indication handling in PGW and ePDG		
			0132	ePDG/PGW restart and restoration		
			0130r 1	PGW Restart Notification		
			0124	Essential correction to the MME and PGW restoration procedure		
CT#51			0142r 2	Timing for sending Downlink Data Notification as a result of the SGW having received an Error Indication message from the eNodeB/RNC	10.2.0	10.3.0
			0151r 1	Unclearness of Downlink Data Notification Handling at MME/S4 SGSN as a result of the SGW having received an Error Indication message from the eNodeB/RNC		
			0155	eNodeB failure		
			0154r 1	RNC failure		
			0148r 2	Error Indication in SGW		
			0145r 1	Error Indication for SGW		
			0146r 5	PCRF Failure and Restoration		
			0152r 2	Handling of UE specific Error Indication over the PMIP		
			0156r 5	MME/SGSN restart and restoration procedure		
CT#52			0166r 2	SGW behavior when it receives GTP error indication from S4-SGSN	10.3.0	10.4.0
			0160r 1	Fix wrong statement for the IMSI page in the Network triggered service restoration procedure		
			0164r 2	Clarification on Network triggered service restoration procedure		
			0167r 2	Gateway Control and QoS Policy Rules Provision Procedure handling at SGW		
			0161r 1	Moving PCRF Restoration text under appropriate heading		
			0162	eNB Error Indication Handling		
			0163r 3	MME/SGSN restart with ISR		
CT#53			0169r 2	Signalling path failure handling	10.4.0	10.5.0

			0175r 1	Downlink Data Notification Handling at MME/S4 SGSN		
			0170r 1	User plane path failure handling		
			0171r 1	PMIP alignment for the network triggered service restoration procedure		
CT#54			0183	Inter MME and intra SGW HO/TAU procedures	10.5.0	10.6.0
			0176	NTSR with ISR active		
			0190	DDN message in the service restoration procedure		
			0185r 2	Essential correction to Partial failure		
CT#54			0178	FQ-CSID Reporting	10.6.0	11.0.0
			0168r 5	CS service restoration after MME failure		
			0177r 1	PGW restoration		
CT#55			0193r 1	Error Indication Handling on S2a	11.0.0	11.1.0
			0194r 2	Restoration of data in the TWAN for S2a		
			0195r 2	TWAN partial failure		
			0196r 1	Restoration of data in the PGW for S2a		
			0198r 1	Correction on the S4-SGSN failure		
			0199r 1	S1 path failure handling		
			0201r 2	IP Address of the node sending the recovery IE		
CT#56			0191r 1	SGW Restoration procedure	11.1.0	11.2.0
			0204r 1	Missing SGSN behavior in the PGW failure		
			0206r 1	PGW triggered SGW restoration procedure		
			0208	Corrections to external resources cleanup upon SGW failure		
CT#57			0210r 2	Restoration of Data for VCSG	11.2.0	11.3.0
			0211r 1	Downlink Data Notification message handling in S4 SGSN		
CT#58			0209r 3	PCC and PMIP impacts for the SGW restoration procedure	11.3.0	11.4.0
			0212	Corrections to reference titles		
			0215r 1	Handling of emergency PDN connections during EPC node restoration		
			0216	Corrections to reference errors		
			0217r 3	SGW failure when ISR is active		
			0214r 4	Handling of VLR Failure without Restart		
CT#58			0224r 1	SGSN handling of VLR restart	11.4.0	11.5.0
			0225r 1	Fixing editor's notes in SGW restoration procedure		
			0226r 1	The inclusion of the MME/S4-SGSN identifier IE		
CT#59			0218r 1	Corrections to reference error for periodic location update timer	11.5.0	12.0.0
			0220r 1	MME/SGSN behaviour upon MBMS-GW restart		
			0221r 1	eMBMS service restoration upon MCE failure or M3AP path failure		
			0222r 1	eMBMS service restoration upon MME/SGSN restart		

			0223r 2	Sm path failure handling		
CT#60			0228	Trigger for re-establishing MBMS sessions upon an M3AP path recovery	12.0.0	12.1.0
			0239r 1	MME behaviour upon MBMS GW restart		
			0240r	SGSN behaviour upon MBMS GW restart		
			0237r 1	BM-SC failure		
			0238r 1	MBMS GW behaviour upon MME/SGSN restart		
			0236r 2	MCE behavior on MME restart and MME behavior on MCE restart		
			0232r 1	Contents of MBMS Session Start Request when re-establishing MBMS sessions		
			0231r 2	SGmb path failure		
			0230r 1	BM-SC behaviour upon MBMS GW restart		
			0229r 1	Moving the control of an MBMS session to another MME		
			0241r 2	Sn-path failure		
			0245r 1	SGSN behaviour upon SGW restart		
			0234	Restoration Priority during SGW and PGW restoration procedures		
			0243r 2	Delete Bearer Request triggered by PMIP error indication message		
			0242r 1	Stop Paging Indication in service restoration procedure with ISR		
CT#61			0246r 1	MBMS Session Start Request received for an on-going MBMS bearer service	12.1.0	12.2.0
			0247r 1	MBMS Session duration		
			0248r 1	BM-SC behaviour during SGmb path failure		
			0249r 1	MCE behavior on MME restart		
			0250r 1	Release of resources at old MME/SGSN during transient Sm path failure		
			0251r 1	Separate Subclause for MCE and RNC restoration functionality		
			0252r 2	Correct S-GW behaviors when a peer P-GW failed		
			0253r 1	Correct wrong NOTE reference		
			0255r 2	Handling of VLR Failure without Restart for MO SMS		
Sep 2013				Subclause numbers corrected in clause 17A.2. Style correction also in clause 27.2.2.2.	12.2.0	12.2.1
Dec 2013			0265r 2	Correction of reference to Update Notifications for Proxy Mobile IPv6	12.2.1	12.3.0
			0271r 2	Error handling when the PCC rule is removed due to the S-GW restoration support		
			0256r 1	Cause "GTP Resources Unavailable" handling at the SGSN		
			0258r 6	Restoration of warning message delivery upon eNB failure/restart		
			0259	M3AP path recovery		
			0261r 2	S4-SGSN procedure upon RNC and lu path failure		
			0266r 2	Non transient SGmb path failure		
			0267r 2	Detection of peer MBMS node restart and SGmb path failure/recovery		

			0268r 2	Non-transient SGI-mb path failure		
Mar 2014			0263r 6	SGW behaviour upon GTP Error indication	12.3.0	12.4.0
			0277r 1	Correct the PCRF procedure during the SGW restoration		
			0273r 1	Update the reference of IETF draft Update Notifications for Proxy Mobile IPv6 to RFC 7077		
			0282r 2	Handling of "GTP Resources Unavailable" cause in S4-SGSN		
			0275r 1	PWS Restart Indication parameters		
Jun 2014			0274r 3	Sm path failure recovery	12.4.0	12.5.0
			0283r 1	SGmb path failure recovery		
			0288r 1	M1 and/or M3/lu resources modification during MBMS session re-establishment		
			0289	MCE Failure		
			0291r 1	SGmb path failure		
			0284r 1	Handling of E-RAB Release due to GTPU error indication for default bearer at MME		
			0296r 2	Update SGW behaviours after receiving PMIP error indication		
			0285	PWS Restart Indication parameters		
			0286r 2	HeNB ID verification in the PWS Restart Indication message		
			0287r 2	Routing of PWS messages to HeNBs		
			0298r 2	SGW restoration when S5 path failure occurs		
			0290	Restoring the (S)Gs associations during tracking/routing area update procedures		
Sep 2014			0300r 2	Correct procedure name for PDN connection deactivation	12.5.0	12.6.0
			0301r 3	Handling of GTP Error Indication for Dual connectivity		
			0302r 2	Restoration for HSS Reset		
			0304r 1	Remove Editor's note for S5 path failure		
Dec 2014			0307	Warning Area List in Write-Replace Warning Request during PWS restoration	12.6.0	12.7.0
			0308r 1	Serial Number in Write-Replace Warning Request during PWS restoration		
			0309	GCSE restoration procedures upon BM-SC restart		
			0310r 1	GCSE restoration procedures upon GCS AS restart		
			0311r 1	GCSE restoration procedures upon MB2-C path failure		
			0312	GCSE restoration procedures upon SGI-mb path failure		
			0314r 1	GTP-C based restart procedures for HRPD		
Mar 2015			0316r 2	SGW restoration procedure in PMIP case	12.7.0	12.8.0
Mar 2015			0317r 1	Deferring GBR bearers deactivation upon S1 Reset or S1AP path failure	12.8.0	13.0.0
Jun 2015			0318r 1	MCE configuration update after an MBMS restoration	13.0.0	13.1.0
Sep 2015			0320r 1	HSS Reset	13.1.0	13.2.0
Dec 2015			0321r 2	Services restoration for UEs using extended idle mode DRX	13.2.0	13.3.0
			0326r 2	DTCI for restoration procedure		

			0323r 1		Implementation mistake of CR 0309 and CR 0310		
			0324r 2		HSS restart MONTE impacts		
			0325r 2		SCEF restart and MONTE impacts		
			0327r 2		SGW Restoration in Dedicated Core Network		
Mar 2016			0329r 2		HSS restart and resultant MONTE impacts	13.3.0	13.4.0
			0330r 2		Restart of SCEF		
			0331r 1		Correct the partial failure handling on SGW		
			0332r 1		S11-U Error Indication handling		
			0334r 3		Behaviours upon receipt of unknown NIDD		
			0335r 3		Enhance restoration procedure to be compatible with SCEF PDN connection and Attach without PDN connectivity		
			0336r 2		Connection Resume procedure used during restoration		
2016-06	CT#72	CP-160228	0337	3	MME handling of GTP Error Indication and MO-Data-Answer (failure)	13.4.0	13.5.0
2016-06	CT#72	CP-160231	0338	2	PGW restoration in NBIFOM case	13.4.0	13.5.0
2016-06	CT#72	CP-160234	0340	3	Restoration impact on the introduction of UE context retention at SCTP recovery	13.4.0	13.5.0
2016-06	CT#72	CP-160217	0341	1	Behaviours upon receipt of unknown NIDD (SGSN case)	13.5.0	14.0.0
2016-09	CT#73	CP-160422	0343	1	Failure case for NBIFOM	14.0.0	14.1.0
2017-03	CT#75	CP-170043	0344	1	Restoration Support for V2X Service	14.1.0	14.2.0
2017-03	CT#75	CP-170040	0345	1	Network triggered service restoration for PSM UE	14.1.0	14.2.0
2017-06	CT#76	CP-171036	0348	1	User Plane Path Failure with Control and User Plane Separation of SGW and PGW	14.2.0	14.3.0
2017-06	CT#76	CP-171023	0350	1	Service Restoration for UEs in extended DRX mode	14.2.0	14.3.0
2017-06	CT#76	CP-171036	0351	3	CUPS restoration procedures in SGW-C and SGW-U	14.2.0	14.3.0
2017-06	CT#76	CP-171036	0352	2	Partial failure handling for CUPS	14.2.0	14.3.0
2017-06	CT#76	CP-171036	0353	2	CUPS restoration procedures PGW-C and PGW-U	14.2.0	14.3.0
2017-06	CT#76	CP-171036	0354	1	CUPS restoration procedures	14.2.0	14.3.0

History

Document history		
V14.2.0	May 2017	Publication
V14.3.0	July 2017	Publication