

3GPP TR 23.843 V1.2.0 (2013-10)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Core Network Overload (CNO) solutions (Release 12)



The present document has been developed within the 3rd Generation Partnership Project (3GPPTM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Report is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPPTM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

3GPP, Architecture, Study, Core Network,
Overload

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2013, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword	6
1 Scope	7
2 References	8
3 Definitions and abbreviations.....	9
3.1 Definitions	9
3.2 Abbreviations.....	9
4 Scenarios and problem analysis for CNO	9
4.1 General.....	9
4.2 Scenario 1: Overlaid RATs and failure of RAN node	10
4.3 Scenario 2: CN overload due to flood of registrations and mobility management events	10
4.4 Scenario 3: CN overload due to flood of resource allocation for mobile originating services.....	11
4.5 Scenario 4: CN overload due to flood of mobile terminated events	11
4.6 Scenario 5: CN overload due to flood of User Location Information (ULI) reporting	12
4.7 Scenario 6: User Location Information (ULI) reporting scenarios with existing capabilities	13
4.8 Scenario 7: ULI reporting when user plane radio bearers are not established for the UE	13
4.9 Scenario 8: GTP-C overload due to flood of Mobility and Session Management messages	13
5 Architecture principles	15
6 Solutions targeting HLR/HSS overload handling	15
6.1 Improved control of user registration attempts	15
6.1.1 Introduction	15
6.1.2 Solution 1: Optimizing the periodic LAU/RAU/TAU signalling.....	15
6.1.3 Solution 2: NAS reject solution	16
6.1.3.1 Evaluation.....	16
6.1.4 Ideas for RAN node restart CN overload prevention	16
6.1.5 Signalling load reduction for TAU/RAU caused by UE mobility across mobility management entities	17
6.2 Solutions targeting at HSS/HLR overload prevention	19
6.2.1 Introduction	19
6.2.1.1 CN signalling description for HLR/HSS overload	19
6.2.2 Solution 1: Optimizing subscription data download from HSS	22
6.2.3 Solution 2: HLR/HSS overload notification.....	23
6.2.4 Solution 3: Prevent HLR/HSS from overload due to RAT-reselection in PS domain	25
6.2.4.1 General	25
6.2.4.2 Evaluation.....	25
6.2.5 Solution 4: Diameter application evaluation and improvement via existing mechanisms	26
6.2.5.1 Evaluation criteria	26
6.2.5.2 Solution description: Diameter Load Manager.....	26
6.2.5.2.1 Diameter charging interfaces	27
6.3 Solution: Optimizing control of mobile terminated services by CN node	28
7 Solutions targeting improved efficiency of User Location Information reporting.....	29
7.1 Solution 1: ULI reporting only when the UE is in "CONNECTED" state	29
7.1.1 Description	29
7.1.2 Impacts on existing nodes and functionality	29
7.1.3 Solution evaluation.....	29
7.2 Solution 2: ULI reporting at PCC area level.....	30
7.2.1 Overview of ULI reporting at PCC area level.....	30
7.2.2 More detailed description.....	31
7.2.3 Impacts on existing nodes and functionality	32
7.2.4 Solution evaluation.....	32
7.3 Solution 3: New "change of eNB" reporting event.....	33
7.3.1 Description	33

7.3.2	Impacts on existing nodes and functionality	33
7.3.3	Solution evaluation.....	33
7A.	Solutions targeting reporting list of users on the area(s) of interest.....	34
7A.1	Solution1: Perform ULI reporting using LCS procedures	34
7A.1.1	Problem description.....	34
7A.1.2	Overview of ULI reporting using LCS procedures	34
7A.1.3	Impacts on existing nodes and functionality	35
7A.1.3.1	General	35
7A.1.3.2	Impacts on existing procedures	35
7A.1.4	Solution evaluation.....	35
8	Solutions for GTP-c overload handling	36
8.1	Solutions targeting existing mechanism for GTP-C node overload prevention.....	36
8.1.1	Introduction.....	36
8.1.2	Mobility management signalling.....	36
8.1.3	Re-attach signalling.....	36
8.1.4	Service request signalling.....	36
8.1.5	UE requested PDN connectivity signalling.....	37
8.1.6	Network triggered Service Requests	37
8.2	Framework for solutions using modifications of GTP-c signalling	38
8.2.1	General.....	38
8.2.2	List of interfaces (and directions) where each of GTP-c load and overload control should apply	38
8.2.3	Scope of GTP-c load / overload control.....	39
8.2.4	Examples of actions GTP-c node may take when another node has advertised overload.....	39
8.2.5	Solution 1: Using load information for dynamic load balancing of GW nodes	40
8.2.5.1	Description	40
8.2.5.2	Applicability	40
8.2.5.3	Messages and inclusion period	40
8.2.5.4	Node selection using load information	40
8.2.5.5	Advertising support of this feature	41
8.2.5.6	Roaming consideration	42
8.2.5.7	Network sharing support	42
8.2.6	Solution 2: Using overload information for overload control of GTP-C nodes	42
8.2.6.1	Description	42
8.2.6.2	Applicability	42
8.2.6.3	Messages and inclusion period	43
8.2.6.4	Expected actions from involved nodes when overload information is received.....	43
8.2.6.5	Advertising support of this feature	43
8.2.6.6	Roaming consideration	43
8.2.6.7	Network sharing support	43
8.3	Solutions for preventing S-GW and P-GW overload.....	44
8.3.1	Solution 1: Use of Gateway Load Manager for DNS based load balancing.....	44
8.3.1.1	Description	44
8.3.1.2	Impacts on existing nodes and functionalities	45
9	Evaluation	46
9.1	Evaluation of SS7/ MAP interface.....	46
9.2	Enhancement of Diameter interface for overload prevention and control support	47
9.3	Evaluation related with the support of overload control and dynamic load control for GTP-C	48
9.4	Evaluation related with the support of User Location Information reporting improvements	50
9.5	Evaluation related with the support of reporting list of users on the area(s) of interest.....	51
10	Conclusions.....	52
10.1	Conclusions for MAP/SS7 and Diameter interfaces	52
10.1.1	MAP/SS7 interface.....	52
10.1.2	Diameter interface.....	52
10.2	Conclusions for GTP-C interfaces	53
10.3	Conclusions for User Location Information reporting improvements	54

Annex A: CN interfaces and services using Diameter as well as overload impact.....55

Annex B: Change history56

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present document investigates core network signalling overload scenarios and potential general handling solutions, in particular:

1. Identify and document events that have occurred and caused network disturbances due to signalling overload. In addition, identify and document scenarios that have high probability of occurrence in the 3GPP network, which may result in signalling overload for core network entities. Such scenarios/events may include HLR/HSS overload by RNC restart, denial of service attacks, and misbehaving/3GPP-non-compliant mobiles causing unpredictable system response;
2. Analyse the criticality of the scenarios and determine whether it is required to take actions for the identified scenarios;
3. Study ways to mitigate and/or eliminate the impact on the core network from signalling overload scenarios that are identified to be critical.

The information provided about the HSS/HLR overload will serve as a starting basis for the study. All currently deployed 3GPP networks should be covered in the study, including LTE

The study should avoid overlap with other parallel activities within 3GPP, and work in close cooperation with the specific WG needs to be maintained.

During the study, if potential security threats such as denial of service attack scenarios are identified, SA WG3 must then be informed to take appropriate measures.

2 References

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

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

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 41.101: "Technical Specifications and Technical Reports for a GERAN-based 3GPP system".
- [3] 3GPP TS 23.116: "Super-Charger technical realization; Stage 2".
- [4] IETF RFC 3588: "Diameter Base Protocol".
- [5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [6] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [7] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".
- [8] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [9] 3GPP TS 23.203: "Policy and charging control architecture".

3 Definitions and abbreviations

3.1 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].

<defined term>: <definition>.

example: text used to clarify abstract rules by applying them literally.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

CNO	Core Network Overload
ULI	User Location Information

4 Scenarios and problem analysis for CNO

4.1 General

The following clauses describe and analyse scenarios which may cause overload of core network entities due to high signalling load caused by, e.g.

1. Flood of registrations caused by special mobility events:

- Mass of mobile users attempting simultaneously to perform registration procedures such as Attach or location updating. Examples are scenarios where a train or bus is crossing LAI/RAI borders, or a big plane arrives at an airport.

NOTE 1: These scenarios and potential solutions may be similar to those that were addressed by the former "Registration in Densely-Populated Area (RED)" work item which are documented in TR 23.880.

2. Frequent RAT-reselection due to scattered 3G/4G coverage

- Frequent loss of broadband coverage may potentially cause extremely frequent intersystem change activities by e.g. smart phones.

3. Flood of registrations after O&M operations:

- Restart of RAN nodes (i.e. RNC and BSC) may cause a massive number of registration attempts, depending on the behaviour of the base stations controlled by the restarted RAN nodes. This is discussed in more detail in clause 4.2.
- Restart or failure of CN nodes which handle mobility management (MSC server/VLR, SGSN, MME)

NOTE 2: A related study item dealing with CN node failures in EPC is performed by CT4. The work is documented in TR 23.857.

4. Flood of resource allocation requests for mobile originating services:

- Massive number of mobile users attempt simultaneously to initiate signalling procedure in order to allocate resources for mobile originating services, such as establishing bearers.

5. Flood of mobile terminated events:

- A massive number of mobile terminated events simultaneously for specific users belonging to specific HLR/HSS (e.g. sending SMS to say Happy New Year in China Spring Festival) may cause excessive signalling load within the PLMN.
- A massive number of mobile terminated events simultaneously causing signalling towards the same SGSN/MME where a large number of receiving users are located (e.g. content pushed to every member of push type services) may cause excessive signalling load within the PLMN.

6. Flood of User Location Information (ULI) reporting when numerous users are subject to ULI subscription from PCRF/OCS:

- A mass of mobile users simultaneously inducing ULI update notifications may cause high signalling load within the PLMN. Examples are scenarios when the mobility of a large number of users is causing an high amount of signalling (e.g. train stations, business districts, or football stadium).

7. Flood of GTP Control Plane messages due to various Mobility Management and Session Management events:

- Frequent Idle-Connected, and Connected-Idle transitions cause due to e.g. eNB idle timer may result in a spike in SGW's load.
- Large number of TAUs/RAUs due to user mobility may result in a flood of GTP-C messages towards PGWs.

4.2 Scenario 1: Overlaid RATs and failure of RAN node

NOTE 1: While the following description focuses on GSM and UMTS, it may also be applicable to other combinations of RATs.

Many geographic areas are now covered by more than one radio technology (e.g. GSM and UMTS) and many of the customers in those areas have devices that support both GSM and UMTS.

Typically the GSM/UMTS cells are configured with (release 99) neighbour cell/cell reselection information that 'push' GSM/UMTS devices to UMTS whenever there is [reasonable] UMTS coverage. In Release 8, the adoption of "absolute priorities" for RAT re-selection, seems to mean that the GSM/UMTS/LTE device will change to the highest priority RAT whenever it has even minimal quality coverage of that RAT.

It seems that when some RNCs restart, they issue commands to the NodeBs that cause the NodeBs to themselves restart and/or to do 'something' to their control channels (e.g. perhaps to set the cell as "barred", or, to stop transmitting any power on the pilot channel -). In turn, it appears that this disruption of the control channels cause the mobiles to perform cell reselection. If all the NodeBs are in a similar, restarting, situation then the mobiles move to GSM.

Typically the GSM cells are in a different Routing Area and frequently a different Location Area to the 3G cells. Hence the mobile performs an LA and RA update. While camped on the GSM cells, the received neighbour cell information and cell reselection parameters encourage the mobiles to keep looking for UMTS cells. So, within seconds of the UMTS cells completing their restarts, the mobiles return to UMTS and perform another RA and LA update.

This can be the cause of a huge surge in Mobility Management signalling that can damage MSCs/SGSNs and/or HLRs.

NOTE 2: Currently the behaviour of GSM BSCs upon restart may be less of an issue. This is because, IF their BCCHs are switched off upon BSC restart, the 2G-only devices have no other RAT to select to, and, any GSM/UMTS/LTE devices will probably be already camped on UMTS/LTE if there is any coverage.

4.3 Scenario 2: CN overload due to flood of registrations and mobility management events

An HLR/HSS or core network node may be overloaded due to registration and mobility management events such as a massive number of Attach and default bearer requests in a short period of time. This may be triggered, for example, when a large number of M2M devices try to re-Attach as a result of failure of a core network node.

Attach (including CS LAU with IMSI attach) procedure and TAU/RAU/LAU procedures are typical registration messages from 3GPP network perspective. During Attach procedure (including CS LAU with IMSI attach) over

GERAN/UTRAN access, the SGSN, MSC/VLR and HLR/HSS may be overloaded due to a massive amount of registration related signalling. Sustained high levels of registration signalling can prevent the network from recovering gracefully.

Similarly, during Attach procedure over E-UTRAN access, the MME and HLR/HSS may be overloaded due to a massive amount of registration related signalling. Sustained high volume of Attach requests can prevent the network from recovering gracefully. In addition, the S-GW/P-GW, PCRF and TDF may also become overloaded due to a flood of default bearer establishment signalling, requests for policy control over Gx to PCRF, requests for policy counter status over Sy to OCS and request to establish TDF sessions over Sd. This flood may be extended beyond the S-GW/P-GW to the PCRF and OCS when PCC and online charging usage are predominant.

During registration procedure over non-3GPP access, the S-GW/P-GW and HLR/HSS (i.e. 3GPP node) may be overloaded due to massive amount of registered related signalling. The PCRF may also receive a massive amount of request for policy control over Gx. Other non-3GPP related nodes (e.g. ePDG) are not discussed in this TR.

4.4 Scenario 3: CN overload due to flood of resource allocation for mobile originating services

When massive numbers of mobile users attempt simultaneously to initiate mobile originating services (e.g. to establish an application session), UEs signal to allocate resources in core and serving networks, (e.g. Service Request procedure, UE requested PDN connectivity procedure). This massive number of requests may be triggered, for example during a catastrophic event.

During the process of setting up an application session, the UE may start signalling for establishing a dedicated bearer. This results in signalling to establish a bearer between SGSN/GGSN or MME/S-GW/P-GW/PCRF. An AF may also start signalling to request resource reservation over Rx. This results in signalling over Rx, Gx and Sy reference points as well. When a massive number of such signalling requests need to be handled in a short period of time, it may overload the network nodes. This flood may be extended beyond the S-GW/P-GW to the PCRF and OCS when PCC and online charging usage are predominant.

4.5 Scenario 4: CN overload due to flood of mobile terminated events

When a massive number of users attempts to initiate mobile terminating services simultaneously for specific users belonging to specific HLR/HSS, it causes an excessive signalling load within the network, e.g. to query for the routing information for next hop from the specific HLR/HSS. Similarly some automatic information services or advertisements by SMS or IP based calling servers/services could cause excessive load. In such cases, the HLR/HSS gets possibly overloaded due to massive number of queries.

For a typical mobile terminated service (e.g. SMS), a high level sequence is as follows:

- 1) Service request arrives at PLMN's gateway server [SMSC, G-MSC, IMS IP-SM-GW]. Server starts to process the request;
- 2) Gateway server queries HSS/HLR for profile/ routing information.
- 3) Gateway server performs any required processing and forwards the service to the serving network entity.

Step 2 in the sequence above can contribute to high load at the HLR/HSS when a massive number of requests for profile/ routing information have to be processed in a short period of time.

Push like services and applications generate mobile terminated data triggering signalling requests in the core network that may be also triggered via Rx reference point. Routing the IP packet data that is destined to mobile terminals may trigger SGSN or MME to initiate Paging followed by Service Request procedures. When a massive number of such mobile terminated signalling requests need to be handled by the same SGSN/MME in a short period of time, it may overload network nodes that handle these requests.

4.6 Scenario 5: CN overload due to flood of User Location Information (ULI) reporting

In some cases, ULI reporting does not imply a dedicated notification (e.g. at Attach, mobility with SGW change). In other cases the need to report ULI implies dedicated signalling within the PLMN.

In the latter cases, a massive number of users simultaneously inducing ULI update notifications may cause an excessive signalling load within the PLMN, i.e. within

- the MME/SGSN (source of the ULI update);
- the SGW, PGW, and possibly V-PCRF in roaming case (relay of the ULI update);
- the PCRF/OCS and TDF (consumer of the ULI update).

This massive number of ULI update notifications may be caused for example by massive mobility of users in a specific location (e.g. train stations or business districts during busy hours, football stadium, city centre during the weekend) or by the use for a greater number of users of ULI subscriptions at finer granularity (e.g. cell level).

Such risk has already been noted in TS 23.060 [6], clause 15.1.3.1, note 2 and in clause 6.1.4 ("Event Triggers") of TS 23.203 [9]

Location change (serving cell) (see note 10)	The serving cell of the UE has changed.	PCEF, BBERF	PCRF
Location change (serving area) (see notes 4 and 10)	The serving area of the UE has changed.	PCEF, BBERF	PCRF
NOTE 4: A change in the serving area may also result in a change in the serving cell, and a change in the serving CN node. NOTE 10: Due to the potential increase in signalling load, it is recommended that such event trigger subscription is only applied for a limited number of subscribers.			

As examples, for following service scenarios:

- Location based policy/location based charging by PCRF/OCS for a large number of subscribers in the network (which applies to potential overloading of GTP and Gx/Gxx/Gy/... interfaces).
- Subscriber/session statistics gathering for e.g. historical data and planning (which applies to potential overloading of GTP and Gx/Gxx/Sd/... interfaces).

Following optimization may be envisaged:

- reporting users within a specific area of interest (e.g. group of cells or LA/RA/TA) while there is no need to report ULI for mobility events not inducing the specific area of interest.
- tracking incoming and outgoing users from a specific area of interest (e.g. group of cells or LA/RA/TA) while there is no need to report ULI for mobility events not inducing the specific area of interest.
- tracking an individual user only within a specific area of interest (e.g. group of cells or LA/RA/TA) while there is no need to report ULI for mobility events not inducing the specific area of interest.

4.7 Scenario 6: User Location Information (ULI) reporting scenarios with existing capabilities

Scenario-A: A big airplane arriving at an airport:

This should not be an issue from ULI reporting point of view as the devices perform the Attach procedure and set up PDN connection in which the location reporting (ECGI) is carried in these session management signalling up to PGW as already defined today for Rel-10. If PCC is used for Attach and TAU procedure, this is not an issue from ULR reporting point of view for the same reason that ULI does not cause additional signalling load from the existing defined procedure.

Scenario-B: Emergency / LI requirement:

Location reporting is needed only during call establishment / release phase and the location reporting is already sent as part of the session management procedure. i.e. ULI does not cause additional signalling load from the existing defined procedure.

Ref: Table 5.4-2 from TR 23.842 "Study on network provided location information to the IP Multimedia Subsystem (IMS)" shows for each of the identified scenarios whether NPLI is required, or not, during the execution of the corresponding IMS events (i.e. before session establishment/modification can be committed).

Table 5.4-2: When NPLI is Needed

	Session Initiation (Offer)	Session Response (Offer Response)
Lawful Interception (LI)	If available	Must
Data Retention (DR)	If available	Must
Charging	If available (NOTE 4)	Must
Emergency	Must	-
Routing Localized Services	Must	-
Location Based Service Triggering	Must	-
NOTE 4: For on-line charging using location-based fees, it may be required to have NPLI in real time already at session setup.		

4.8 Scenario 7: ULI reporting when user plane radio bearers are not established for the UE

Per existing specifications, when ULI change notification is requested at the level of the RA (Routing Area) or TA (Tracking Area), the node serving the UE (e.g. MME, SGSN) immediately reports a change of RA/TA regardless of the CONNECTED / IDLE state of the UE. Immediately reporting a change of TA/RA upon a TA/RA update w/o the "active flag", i.e. when the UE is in IDLE state and does not have any radio and S1-M user plane bearers generates extra signalling and it may not be necessary depending on the specific PCC service, or because the UE may anyway move subsequently to another TA/RA before switching to CONNECTED state.

An example is that of a Home Zone subscription where the end-user is granted a specific QoS and tariff when using the PLMN for data services within the cell or the few cells that serve(s) or surrounds the home of the user. Clearly while the UE is not active, notifications to the PCRF and /or the OCS and/or the TDF (through PCRF) of TA or RA updates of the UE are not required.

The extra signalling involves the node serving the UE (e.g. MME, SGSN) but also the SGW, the PGW and the consumer of the information (e.g. the PCRF and/or the OCS and/or the TDF).

4.9 Scenario 8: GTP-C overload due to flood of Mobility and Session Management messages

The following different mobility and session management scenarios can cause GTP-C overload:

1. Frequent Idle -> Connected, and Connected -> Idle transitions cause due to e.g. eNB idle timer. Depending on the value of eNB idle timers (which may result in large # of e.g. SERVICE REQUESTs from UEs in a busy hour), session overload may occur in either an SGW managing TA/TAs or a set of SGWs managing TAs.

2. Large number of users performing TAU/RAU. In a typical network deployment, the number of MMEs and SGWs is considerably large(r) than the number of PGWs. In densely populated areas say North-Eastern USA e.g. metro New York, metro Boston, metro Philadelphia etc, mass transit systems transfer a large number of users on a daily basis. This results in large number of simultaneous TAUs/RAUs towards MMEs/SGSNs and corresponding Modify Bearer Requests towards SGWs. This may result in large number of MBRs towards a single or very few PGWs.
3. An overload of a downstream node (e.g. PGW) may also potentially cause overload of an upstream node (e.g. SGW) e.g. due to GTP-c signalling retransmissions.
4. At the failure of an EPC node (e.g. SGW) where the network would try to re-establish the GTP-c session via a new EPC node (SGW) that would replace the failing one. The risk is that the failure of a node (e.g. SGW) would trigger a spike in GTP-c signalling to restore within the shortest time the PDN connections affected by the failure. These attempts to restore PDN connections affected by the failure would overflow other nodes (e.g. other SGW, PGW) and transform a local failure (e.g. of an SGW) into a complete network issue via a snow ball effect. The same applies upon a failure of a PGW, MME or SGSN.
5. At overload or failure of a GTP-c node (e.g. SGW) where the network would need to establish subsequent (new) GTP-c sessions via a smaller number of GTP-c nodes (e.g. using only other SGW of the same cluster). The risk is that the overload / failure of a node (SGW) would trigger an increase of GTP-C signalling that would overflow other nodes (other SGW of the same cluster) and transform a local failure (of an SGW) into a complete network issue via a snow ball effect.
6. A GTP-c node (e.g. PGW) may encounter issues to handle traffic on a non-overloaded GTP-c interface (e.g. S5 interface) when another of its (possibly non GTP-c) interfaces (e.g. Gx) is overloaded.
7. Application signalling that induces creation of dedicated bearers served by a MME or pool of MME: A large number of users may start application related interactions (e.g. IMS SIP call) simultaneously when some exceptional event occurs, which leads to a large amount of almost simultaneous Create/Update Bearer Requests sent from PGW to MME.

Editor's note: Roaming impacts for GTP-based S8 are FFS.

Given the nature of GTP-C protocol in how it relies on retransmissions of unacknowledged requests, when a GTP-C Node experiences overload (or severe overload) the number of unacknowledged GTP-C messages compounds exponentially especially in case of congestion. The larger the number of users on an operator's network, the worse the problem becomes. Therefore, mechanisms to detect, and mitigate overload on GTP Control plane shall be investigated. Current GTP-c load balancing relies on the MME using DNS weights that are semi-static and "typically set according to the capacity of a GW node relative to other GW nodes" (see TS 23.401 [5]) but that do not take into account the instantaneous load or capacity of the GWs. Let's assume that all xGW have the same capacity (and are associated with the same semi-static load factors). When there is no network failure, such schema allows an even share of the PDN connections between the xGW.

- When a xGW node has a partial failure (e.g. one of its components has failed), or during certain maintenance operations, it may still be working but not with the full capacity. In this case the DNS weights associated with this node are becoming stale / wrong information.
- When an xGW has failed, all its traffic is "handed-over" to other xGW. Thus these other xGW support a higher amount of load than usual. When the failed xGW restarts / recovers, the traffic allocation, based on even DNS weights, allocates the same amount of traffic to the various xGW, even though the recovering xGW is not loaded at all while the other xGW support an higher amount of load than usual. The same applies during network extensions (e.g. when adding a new SGW to an SGW cluster).
- Once the load is un-balanced for any of the reason above, overload may be experienced in one or more nodes of a xGW cluster while there is still remaining capacity on other nodes of the same cluster, leading to GTP-C retransmissions, potential re-attempts via an alternative node, failures.

5 Architecture principles

The study should follow the principles as defined below:

1. Already specified overload control means as well as tools available to manage or handle the overload scenarios should be examined and preferred, if they are adequate, and these should be improved if possible, or if deemed necessary.
2. General overload handling solutions that work regardless of the cause are preferred.
3. The study will focus initially on providing a solution that does not require UE modifications. However the study does not preclude the possibility for improving UE behaviour.
4. Based on regional/national requirements and network operator policy, an MPS session shall be exempted from core network overload controls for a node, up to the point where further exemption would cause instability. Proposed solutions should be consistent with congestion control exemptions defined for MPS (TS 23.401 [5], clause 4.3.18) for EPC for E-UTRAN access.

6 Solutions targeting HLR/HSS overload handling

6.1 Improved control of user registration attempts

6.1.1 Introduction

This clause addresses solutions which provide improved control of user registration attempts in order to avoid unnecessary load of core network entities involved in mobility management, i.e. MSC/VLR, SGSN, MME and HSS/HLR, e.g.:

- Flexible network control of Attach and location updating procedures (LAU, RAU, TAU) to avoid overload of core network nodes,
- Avoiding frequent RAT reselection when ISR is not applicable.

The solution space includes:

- existing concepts, such as:
 - control of UE inter RAT-activities of the UE by appropriate setting of parameters impacting inter-RAT cell selection/reselection
 - selective RA update procedure
 - deployment of ISR functionality
- improvements to existing concepts and new concepts, such as, e.g.:
 - additional cause values in registration reject messages indicating core network overload
 - overload control functionality developed under the NIMTC work item

6.1.2 Solution 1: Optimizing the periodic LAU/RAU/TAU signalling

In Rel-10, TS 23.401 [5]/TS 23.060 [6] has specified mechanism for optimising the LAU/RAU/TAU signalling. The following solution describes how this mechanism can be used to improve the core network load conditions.

To prevent network from overload caused by unnecessary periodic LAU/RAU/TAU signalling, Core network entity, i.e. SGSN/MME, based on operator policy and/or subscription information received from HSS, may generate a longer periodic update timer, i.e. periodic LAU/RAU/TAU timer, for some specific UE, e.g. UE configured for MTC, and allocate it to the UE. Such UE then would not initiate too frequent a periodic update procedure which helps to reduce the interacting with core network entity and thus the possibility core network entity falls into overload.

6.1.3 Solution 2: NAS reject solution

This solution describes examples of behaviour to throttle requests from the UE when MME/SGSN or MSC/VLR are overloaded, or when these nodes determine overload conditions in the HLR/HSS or in the P-GW/GGSN. This solution can be applied to manage overload as a result of flood of resource allocation for mobile originating services as specified in clause 4.4.

When the MME or SGSN is overloaded and it receives the NAS request message for mobility management (e.g. Attach Request, TAU Request, RAU Request and etc), it performs General NAS level Mobility Management congestion control handling as specified in TS 23.401 [5] or TS 23.060 [6], by rejecting the NAS request with back-off timer and a dedicated cause for congestion.

When the MME or SGSN is overloaded and it receives the NAS request message for session management (e.g. PDN Connectivity Request, Activate PDP Context Request and etc), it performs APN based Session Management congestion control handling as specified in TS 23.401 [5] or TS 23.060 [6], by rejecting the NAS request with back-off timer and dedicated cause.

When the MSC/VLR is overloaded and it receives the NAS request message for mobility management (e.g. Location Updating Request), it rejects the NAS request indicating "congestion" with an optional timer (i.e. T3246) to the UE as specified in TS 23.012.

When the HLR/HSS is overloaded and the related MME, SGSN or MSC/VLR is aware of that (e.g. receiving the Overload Notification from the HLR/HSS as specified in clause 6.2.3 or based on implementation mechanism), it could perform General NAS level Mobility Management congestion control handling as specified in TS 23.401 [5] or TS 23.060 [6], or rejection mechanism as specified in TS 23.012. During the above congestion control procedure, the MME, SGSN or MSC/VLR applies the following principles to handle NAS requests from the UE:

- Only reject the mobility management request from those UEs whose subscriber profiles are in an overloaded HLR/HSS.
- If the request from the UE does not require HSS interaction, the MME should not reject the request due to HLR / HSS overload.
- The timer value for which the UE is requested to back off could be generated by the MME, SGSN or MSC/VLR or applied based on configuration. If the HLR/HSS provides explicit overload notification (refer to 6.2.3), the MME, SGSN or MSC/VLR should use it to derive the UE back off time period.

When P-GW or GGSN is overloaded, it performs PDN GW control of overload as specified in TS 23.401 [5] or GGSN control of overload as specified in TS 23.060 [6].

6.1.3.1 Evaluation

The principle of NAS Reject solutions (including General NAS level Mobility Management control, APN based congestion control) has been introduced into 3GPP specification from Rel-10 during NIMTC specification work. This solution reuses this specified principle of NAS reject solution from CNO perspective, and shows example of the procedures that may be applied by MME, SGSN or MSC/VLR to manage the HLR/HSS overload scenario.

6.1.4 Ideas for RAN node restart CN overload prevention

With the possible exception of O&M specifications, the following mechanisms are believed to be achievable with the existing 3GPP specifications.

When performing RNC/(e)NodeB restarts:

- a) use Access Class Barring bits on the (e) NodeB rather than Cell Barring. This is because ACB shall not trigger cell reselection while Cell Barring shall trigger reselection.
- b) do not restart all the nodeBs/UMTS cells at the same time. By staggering the time of NodeB restarts, most mobiles will perform intra-UMTS cell reselection and remain in the same LA/RA, rather than performing inter-RAT cell reselection.
- c) do NOT use GSM features that dynamically allocate extra SDCCH signalling channels. This is because GSM radio interface signalling channel congestion can be used to slow down the rate at which mobiles update to 2G.

This is particularly useful as, until 4 (CS domain) / 5 (PS domain) failed GSM access attempts, the mobile's temporary 3G core network IDs and registered 3G LA/RA are not deleted, thus, a return to 3G during this period does not lead to any update to the 3G nodes.

- d) activate ACB on GSM cells while performing a UMTS restart in that geographic area. (This can delay the 2G LA/RA update and hence avoid the deletion of the UMTS temporary IDs and registered LAI/RAI).
- e) on UMTS cells activate ACB for "mobility management events" while performing a GSM or LTE restart in that geographic area. . (This can delay the 3G LA/RA update and hence avoid the deletion of the other RAT's temporary IDs and registered LAI/RAI).
- f) configure GSM cells/BSC to reject/delay/ignore Channel Request messages that indicate mobility management events, (This can delay the 2G LA/RA update and hence avoid the deletion of the UMTS temporary IDs and registered LAI/RAI).
- g) configure GSM cells/BSC, to locally (from within the BSS) return Location Update Reject messages (e.g. with a cause value indicating "search for other LAs in this PLMN").

6.1.5 Signalling load reduction for TAU/RAU caused by UE mobility across mobility management entities

During the TAU/RAU procedure, the new MME/SGSN needs to send Update Location message to the HSS/HLR and retrieve the subscription data from the HSS/HLR. Frequent TAU/RAU may cause HSS/HLR or core network to be overloaded. For the 2G/3G system, one way of decreasing the Update Location message from the SGSN to the HSS/HLR is to increase the geographical coverage of the RAI, however this method will increase the signalling load of Paging in the radio interface, and there is no good method to avoid/suppress the Ping-Pong RAU between the borders of two RAIs/SGSNs/SGSN Pools. In the LTE system, the target MME includes the last visited TAI in the new TAI list allocated to the UE during the TAU procedure, and the Ping-Pong TAU within the same MME or the same MME pool can be avoided. The MME can dynamically change the TAI items of the TAI list assigned to the UE according to the mode of UE, e.g. if the UE moves quickly, a large TAI list is assigned to the UE. The TAU procedure is decreased and the Update Location message from the MME to the HSS is also decreased accordingly. However there is also no good method to avoid/suppress the Ping-Pong TAU between the border of two MMEs/MME Pools.

Combining a 2G SGSN and a 3G SGSN to one combined 2G/3G-SGSN and one RAI shared by the 2G and 3G RAT is defined in TS 23.060 [6] to avoid/suppress the RAU procedure when the UE in IDLE state moves between 2G and 3G system. This technology is the basic idea of the ISR function defined in the TS 23.401 [5]. ISR was designed to reduce the required inter-RAT TAU/RAU of the UE which moves between the border of S4-GSN and MME. To support ISR feature, one enhancement was introduced that HSS records the current MME/S4-SGSN and previous S4-SGSN/MME and will not execute Cancel Location procedures with previous S4-SGSN/MME, when receiving Update Location request from new S4-SGSN/MME even the HSS does not know whether the ISR is activated to the UE. The HSS also needs to send Insert Subscriber Data to both serving and previous S4-SGSNs/MMEs to keep their Subscriber Data up to date. When UE moves between serving and previous S4-SGSN/MME, its TAU/RAU signalling load can be saved a lot, since Update Location procedures are not required.

The feature of two CN nodes registration in the HSS/HLR was designed for ISR support so far, and not applicable to the following UE mobility scenarios with no ISR support:

- 1) MME <-> MME;
- 2) MME <-> Gn/Gp SGSN;
- 3) S4 SGSN <-> S4 SGSN;
- 4) Gn/Gp SGSN <-> Gn/Gp SGSN;
- 5) S4 SGSN <-> Gn/Gp SGSN.

But more benefits on signalling load reduction can be expected, if the feature of two CN nodes registration in the HSS/HLR can be extended to these scenarios, especially in case of Ping-Pong mobility happens simultaneously, which may increase the signalling load dramatically. See Figure 6.1.5.1.

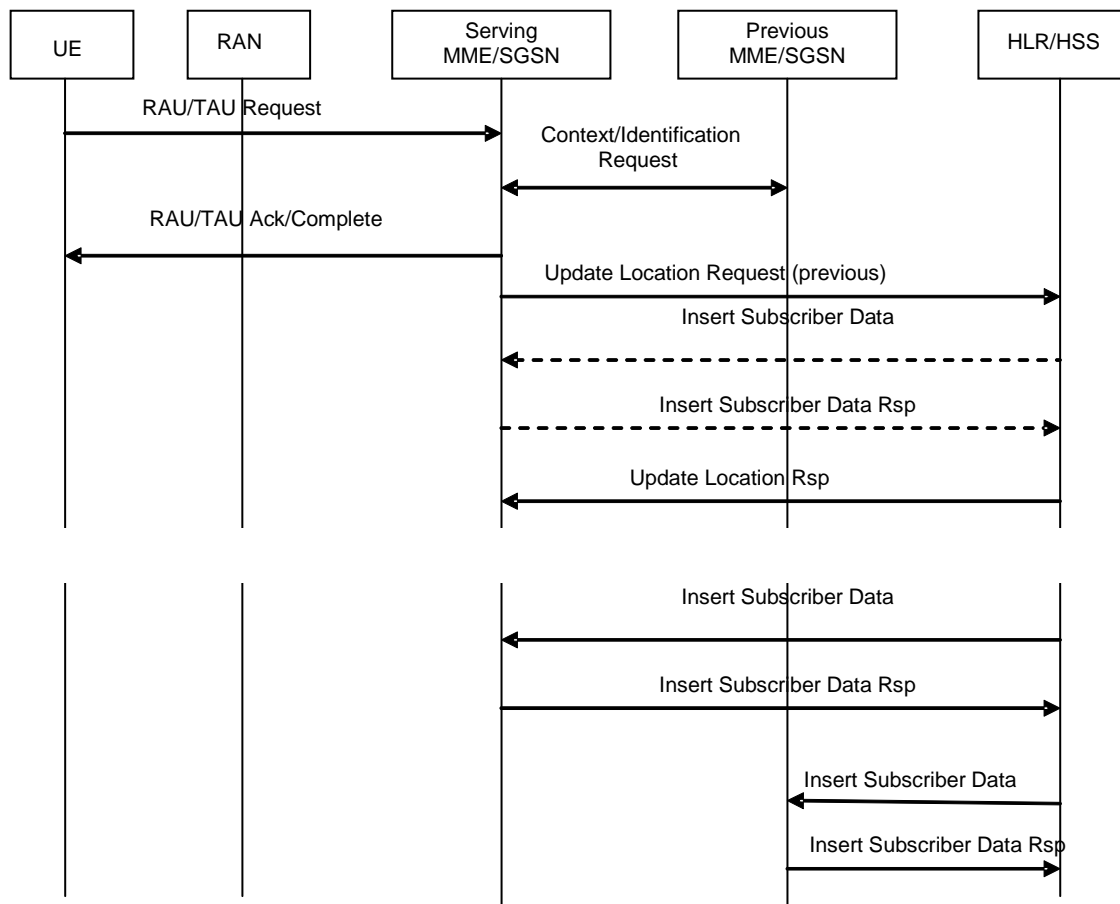


Figure 6.1.5.1 Optimized RAU/TAU Procedures

With this solution:

- When serving SGSN/MME sends Update Location Request to HSS, the previous SGSN/MME will also be notified to HSS. HSS records both Serving and Previous SGSNs/MMEs for this UE, but will not send Cancel Location Request to Previous SGSN/MME, since UE may move back in a short period time in case of Ping-Pong mobility;
- Without executing Cancel Location to previous SGSN/MME, the Subscriber Data of this UE in both Serving and Previous SGSNs/MMEs shall be updated simultaneously by HSS, if HSS needs to do so, to guarantee both Subscriber Data in both nodes are up to date;
- Every time receiving Update Location Request, HSS will use the Serving and Previous SGSNs/MMEs of this latest Update Location Request to update its local stored Serving and Previous SGSNs/MMEs, and send the Cancel Location Request to outdated local stored SGSNs/MMEs.
- The TAU/RAU procedure is performed without sending Update Location message from the two SGSNs/MMEs to the HSS/HLR if the two SGSNs/MMEs are registered in the HSS/HLR.

Since HSS rarely updates subscriber data actively, but the Update Location is executed per TAU/RAU procedure, signalling load to both HSS and MME/SGSN will be saved a lot, especially in case of UE mobility Ping-Pong scenario.

6.2 Solutions targeting at HSS/HLR overload prevention

6.2.1 Introduction

This clause addresses solutions aiming to prevent HSS/HLR overload, e.g:

- minimizing HSS/HLR interrogations in registration procedures,
- optimization of HSS/HLR message content,
- mechanisms to enable core network nodes (MSC/VLR, SGSN, MME) to obtain information on HSS/HLR load status.

The solution space includes:

- existing concepts, such as:
 - provision of Super-Charger functionality as defined in TS 23.116 [3]
 - overload protection function for HSS using Diameter (see e.g. RFC 3588 [4])
 - avoidance of unnecessary authentication procedures
- new concepts, such as, e.g.:
 - potential optimizations in user profile download from HSS
 - load indicators in messages sent by the HSS/HLR

6.2.1.1 CN signalling description for HLR/HSS overload

Generally, when the HLR/HSS detects overload, it discards the received messages (e.g. due to local buffer overflow), complete parts of the incoming dialogs, or rejects the request optionally with overload indication.

This clause intends to analyze most of all the procedures related with HLR/HSS and capture the solutions/behaviours targeting at procedure handling in case of HLR/HSS overload. The procedures below apply to both MAP and Diameter application signalling.

Update Location Procedure

This procedure is used by the MME/SGSN/MSC to update location information in the HLR/HSS and download subscription profile from the HLR/HSS.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

However, in some network scenarios, a lot of UEs register to the mobile network simultaneously, which makes it necessary for the HLR/HSS to process a lot of Update Location Request messages at the same time and cause HLR/HSS overload. This should be resolved, using solutions developed and evaluated in clause 6.2, e.g. providing overload indication to MME/SGSN/MSC.

If the HLR/HSS receives Update Location Request message when it is overloaded, it may ignore it, e.g. due to local buffer overflow. The MME/SGSN/MSC could delay the registration for this UE and the subsequent arriving UE (e.g. reject the attach request for certain periods) based on, e.g. the overload indication received before, or local configuration. It should be noted that following a timeout in SGSN/MME, the UE will retry the request requiring a new update location procedure or further throttling at SGSN/MME. These aspects should be addressed in the solutions developed and evaluated in clause 6.1 and 6.2.

Cancel Location Procedure

This procedure is used by the HLR/HSS to delete a subscriber record from the MME/SGSN/MSC.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If it is executed when the HLR/HSS is overloaded, the HLR/HSS can delay the process for some UEs. This is normal handling in case of HLR/HSS overload, and there is no problem for the core network.

Purge UE Procedure

This procedure is used by the MME/SGSN/MSC to indicate to the HLR/HSS that the subscriber's profile has been deleted in the MME/SGSN/MSC.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If the HLR/HSS receives the Purge message when it is overloaded, it may ignore it, e.g. due to local buffer overflow. In this case, the MME/SGSN/MSC could resend the Purge message later based on implementation solution. There is no problem for the core network.

Insert Subscriber Data Procedure

This procedure is mainly used by the HLR/HSS to download subscription profile to the MME/SGSN/MSC during the Update Location procedure or due to subscription update.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If there are a large number of such concurrent updates, the HLR/HSS is able to control the sequence of execution, e.g. controlling the message rate to outbound buffers such that it does not cause HLR/HSS overload.

If it is executed when the HLR/HSS is overloaded, the HLR/HSS can delay the process for certain UEs. This is the normal handling in case of HLR/HSS overload, and there is no problem for the core network.

Delete Subscriber Data Procedure

This procedure is mainly used by the HLR/HSS to remove some or data of the HLR/HSS user profile stored in the MME/SGSN/MSC.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If there are a large number of such concurrent updates, the HLR/HSS is able to control the sequence of execution, e.g. controlling the message rate to outbound buffers such that it does not cause HLR/HSS overload.

If it is executed when the HLR/HSS is overloaded, the HLR/HSS can delay the process for certain UEs. This is the normal handling in case of HLR/HSS overload, and there is no problem for the core network.

Authentication Procedure

This procedure is used by the MME/SGSN/MSC to request the authentication information from the HLR/HSS. It is common to be executed as part of UE registration procedure (e.g. Attach procedure).

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

However, in some network scenarios, a lot of UEs register to the mobile network simultaneously, which makes it necessary for the HLR/HSS to process a lot of Authentication Request messages at the same time during such registration procedures, causing HLR/HSS overload. It should be resolved, and the solutions are developed and evaluated in the clause 6.2, e.g. providing overload indication to the MME/SGSN/MSC.

If the HLR/HSS receives the Authentication Request message when it is overloaded, it may ignore it, e.g. due to local buffer overflow. In this case, the MME/SGSN/MSC could reject the request for this UE (due to failure of authentication in time) and the subsequent arriving UE (e.g. reject the attach request for certain periods) based on, e.g. the overload indication received before, or local configuration. This should be addressed in the solutions developed and evaluated in clauses 6.1 and 6.2.

Fault Recovery (Reset) Procedure

This procedure is used by the HLR/HSS, after a restart, to indicate to the MME and SGSN that a failure has occurred.

It will not cause HLR/HSS overload as it is sent by the HLR/HSS and the MME/SGSN/MSC will not trigger new Update Location procedure to the HLR/HSS immediately.

This procedure will not occur when the HLR/HSS is overload as it is executed after a restart.

Notification Procedure

This procedure is mainly used by the MME/SGSN/MSC to notify the HLR/HSS about the terminal information, APN-PGW pair, UE reachable or memory capacity and etc.

Normally, this procedure is performed per UE and it will not cause HLR/HSS overload.

If the HLR/HSS receives the Notify Request message when it is overloaded, it may ignore it, e.g. due to local buffer overflow. In this case, the MME/SGSN/MSC could resend the Notify Request message later based on implementation. There is no problem for the core network in most of the cases, e.g. for updating the terminal information, or updating the UE reachable or memory capacity, as they are not so urgent.

But there is a risk of breaking the seamless handover between 3GPP and non-3GPP if the MME fails to update the APN-PGW pair in time because it is possible that the UE performs handover before the MME succeeds to update the pair. So this problem should be resolved.

T-ADS Query Procedure

This procedure is for domain selection for mobile terminated voice and SMS procedure as defined in TS 23.221.

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If a lot of MT services for T-ADS arrive simultaneously, T-ADS could check the buffer information for redundant requests in order to reduce the signalling towards the HLR/HSS. If such MT services are for different UE, it could cause server overload (e.g. T-ADS, and HLR/HSS and etc). In this case, the T-ADS could terminate the mobile terminated service.

If the HLR/HSS receives the T-ADS Request when it is overloaded, it may ignore it, e.g. due to local buffer overflow. In this case, the T-ADS could select a target domain, e.g. based on default configuration, or terminate the mobile terminated service. The normal procedure, however is to retry the T-ADS request.

Sending Routing Information Procedure

This procedure is for mobile terminated services (e.g. MT SMS, MT LCS, etc).

Normally, this procedure is performed per UE and will not cause HLR/HSS overload.

If a lot of MT services for routing query arrive simultaneously, especially from different senders for different UEs, it could cause HLR/HSS overload. In this case, the sender could terminate the mobile terminated service.

If the HLR/HSS receives the routing query request when it is overloaded, it may ignore it, e.g. due to local buffer overflow. If the sender resends the request, the service is terminated, and the problem of overload is alleviated.

6.2.2 Solution 1: Optimizing subscription data download from HSS

The risk of overload on HSS/HLR interfaces is partially due to the fact that the size of messages sent from HSS/HLR to Core Network nodes (SGSN, MME, MSC/VLR) which include subscription data, is increasing with every release of the specifications.

When the MAP protocol is used, e.g. on the Gr interface, the bare size of certain MAP information elements (e.g. InsertSubscriberDataArg in the Insert Subscriber Data (ISD) message), causes message segmentation by the MAP layer. MAP segmentation requires acknowledgements for each message segment (see TS 29.002). This further increases the load on MAP-based HSS/HLR interfaces.

Subscription data consists of following three types of information:

- user identities (e.g. IMSI, MSISDN),
- dynamic data (e.g. SGSN number, SGSN address, MNRG),
- static data (e.g. APN subscriptions, ODB).

Static subscription data is highly duplicated among the individual user subscriptions. Even big network operators with more than 500 million subscribers typically offer less than 100 different tariffs. However, subscriptions for the same tariff type usually share the same static subscription data for all corresponding users.

The duplication property of static subscription data can be utilized by introducing the concept of Subscription Profile IDs on HSS/HLR interfaces.

The Subscription Profile ID serves as an identifier of a corresponding record of static subscription data stored in CN nodes (SGSN, MME and MSC/VLR) and in HLR/HSS. It can be used in messages indicating subscriber data from the HLR/HSS to the CN nodes instead of providing the entire data record itself.

Editor's note: The details of employing the Subscription Profile ID in the Insert Subscriber Data procedure are FFS. It needs to be studied further if there could be risks that subscription records stored in HLR/HSS and CN node can get unsynchronized.

6.2.3 Solution 2: HLR/HSS overload notification

Current HLR load control mechanisms use SS7 / MAP mechanisms for throttling traffic per IMSI. HLRs discard messages for MAP operations taking into account the priority of their application context, according to the overload control for MAP entities. However, prioritization is per MAP operation, e.g. the Update Location procedure has higher priority than Purge procedure, and the HLR may discard the Purge handling but process the Update Location procedure in case of overload.

For Diameter, load control mechanisms used are overload signal (3004 DIAMETER_TOO_BUSY) and message discards. These mechanisms are useful to handle transient HSS server overload by load balancing or discarding. However, no feedback is provided to the Diameter clients (SGSN, MME, MSC) to throttle traffic to the HSS to handle a sustained overload condition.

For both MAP and Diameter application, request throttling is applied per IMSI only and this is not sufficient to handle sustained HLR/HSS server overload. In addition, when the HLR/HSS has to handle a lot of Update Location procedures at the same time, e.g. thousands of UEs register into the network simultaneously; current mechanisms do not provide feedback to clients to slow down traffic. With retry mechanism in MME/SGSN/MSC for Update Location procedure (e.g. TC timer for MAP), the overload situation in the HLR/HSS will be worse if the HLR/HSS just discards messages in case of overload according to current principles. In this case, it will be better if the HLR/HSS can provide overload indication so that the MME/SGSN/MSC could reduce the Update Location request to the overload HLR/HSS.

This solution is limited to addressing overload due to signalling on Diameter based interfaces to HSS and MAP based interfaces to HLR. Network nodes like MME and SGSN can use feedback from HSS/HLR overload notification to limit overloading the HSS/HLR. This can be coupled with existing mechanisms in the core network to limit overall load in the system.

NOTE 1: Overload of the IP/SS7 transport network itself is not addressed here. This is handled by SCTP flow control for Diameter/SIGTRAN and TCAP/SCCP for SS7 networks.

When the HLR/HSS detects overload, it could provide the overload indication as follows:

- The HLR/HSS includes an overload indication in each response message to the MME/SGSN/MSC, e.g. Update Location Accept, Update Location Reject or Authentication Answer message. This overload indication is not a per IMSI indication.
- Overload indication can contain "status" information. Status information, for example, may include the level of congestion, validity period for back-off operation, or normal indication.

NOTE 2: For example, congestion level indication can be used to indicate to the serving network that the serving PLMN should begin some flow control mechanism in order to start limiting the amount of HSS interactions. A validity period for back-off operation can be used to indicate to the serving network that the serving PLMN should immediately start the flow control mechanism to prevent most or all interaction with HSS for a specific duration. Normal indication can be used to resume normal HSS interaction from the serving PLMN.

- Alternatively, the HLR/HSS sends a dedicated Overload Notification message to the MME/SGSN/MSC which has ongoing message exchange with the HLR/HSS (e.g. ongoing dialog for Update Location procedure).

Editor's note: This alternative could be valid for MAP, but not for diameter. In diameter, adding a new command to an existing application implies defining a completely new application, which should be out of the question. So, the only alternative would be adding optional IEs indicating the overload status inside existing messages.

- List of HLR/HSS Ids could also be provided together with the overload indication, so that the MME/SGSN/MSC can reduce the registration only for those UEs whose IMSI leading digits are equal to one of these HLR/HSS Ids.

Editor's note: If the IMSI corresponds to another (Home) PLMN how the VPLMN may associate a "List of HLR/HSS Ids" with "IMSI leading digits equal to one of these HLR/HSS Ids" is to be clarified (when an HPLMN opens a new IMSI range or adds a new HSS/HLR, this HPLMN operator should NOT have to warn all its roaming VPLMN partners).

- A back-off timer could also be provided by the HLR/HSS.

Editor's note: It is FFS how the receiving node (MME/SGSN/MSC/VLR) stops the overload notification mechanism.

This solution is mainly for the Update Location dialogue. In other words, the HLR/HSS can process other requests (e.g. Notify Request for update APN-PDN GW pair) without overload indication, or discard requests.

Editor's note: In Diameter, Update Location and Notify are two different messages; but not in MAP. The Notify Request message, as defined by SA2, has been implemented in MAP with the existing MAP Update Location message. So it may not be straightforward for the HLR/HSS to discard one and not the other based only in the type of message.

The above mechanism can also be applied in a node internal manner without HSS/HLR triggering based on implementation specific mechanism.

Editor's note: It is FFS how the MME/SGSN/MSC handles the UE registration request in this scenario.

6.2.4 Solution 3: Prevent HLR/HSS from overload due to RAT-reselection in PS domain

6.2.4.1 General

When inter RAT Routeing Area Update procedure or inter RAT Tracking Area Update procedure is performed as described in TS 23.060 [6] and TS 23.401 [5], the HSS/HLR will send the Cancel Location Message to the old SGSN/MME to delete the MM contexts and PDP/EPS bearer contexts for the UE and send the whole Subscription data to the new SGSN/MME.

In the scenario of frequent RAT-reselection due to scattered 3G/4G or 2G/3G coverage, the HSS will frequently send almost same Subscription data to the same SGSN or MME, which brings the risk of overload on HSS/HLR interfaces.

For this scenario, the HSS/HLR can generate a Timer according to the network condition, i.e. frequent RAT-reselection is detected, and sends it to the old SGSN/MME within the Cancel Location Message and then the SGSN/MME will not delete the stored MM contexts and PDP/EPS bearer contexts for the UE before Timer expires.

If the UE enters again into the coverage of the old SGSN/MME and the old SGSN/MME determine that the Timer is still running, the old SGSN/MME will include an indication in Update Location message to inform HLR/HSS that the original MM contexts and PDP/EPS bearer contexts for the UE is still available. So the HLR/HSS will not send the Subscription data to the old SGSN/MME anymore and the old SGSN/MME will perform the Location Update procedure according to the original MM contexts and PDP/EPS bearer contexts.

6.2.4.2 Evaluation

This solution is different from the now existing Super-charge mechanism in TS 23.116 [3], and can be regarded as the enhancement of it: In Super-charge mechanism, the MM contexts and PDP/EPS bearer contexts might be stored permanently in SGSN/MME once the procedure is triggered, and that would bring additional burden to the SGSN/MME. However in this solution, the stored MM contexts and PDP/EPS bearer contexts in SGSN/MME would be deleted when the timer is expired. Alternatively, this timer may also be internally configured in the SGSN/MME.

There is no strong relation between ISR and this solution: In ISR, UE needs to attach both in SGSN and MME, and when UE moves between the SGSN and MME, it does not need to initiate location update procedure. Paging should also be done both in the SGSN and MME. However, in this contribution, HLR/HSS knows exactly where the UE is, i.e. in SGSN or MME. Only when UE moves between SGSN/MME(s), the old SGSN or MME can keep the stored MM contexts and PDP/EPS bearer contexts until the timer expired.

6.2.5 Solution 4: Diameter application evaluation and improvement via existing mechanisms

6.2.5.1 Evaluation criteria

3GPP needs to take a proactive approach to addressing any possible shortcoming related to Diameter using existing mechanism in parallel while pursuing a longer term goal of updating Diameter base protocol.

3GPP should investigate further and document certain aspects of Diameter usage based on so far deployment experiences, network outage information, congestion and overload conditions that has been attributed to interfaces supporting Diameter. Some of these aspects to be further investigated are as follows:

1. Further clarify the use of Diameter Agent (DA) for interfaces that support Diameter but currently 3GPP specs are not explicitly clear on DA usage (e.g. exception is the PCC specification of DRA).
2. Further clarify "Diameter too Busy" and other similar error usage on a per 3GPP Diameter Application level for 3GPP Diameter nodes. For example, how should an MME/SGSN react when it receives this error from HSS routed via similar functional node like a Diameter Agent (DA) with functionalities that can support overload and congestion without Diameter protocol update and vice versa.

How the PCEF/TDF should react when it receives this error from PCRF via a Diameter Agent that does not support any Diameter protocol update and vice versa.

3. When node internal implementation detects conditions that could imply possible congestion or overload situation approaching, Diameter application specific action should be taken to prevent/reduce other procedures so that as a consequence it in turn reduces overall Diameter signalling on that specific application.

The node may detect conditions that imply overload either explicitly or implicitly (e.g. the client and the server have a TCP connection up but the server is not able to reply at all).

An example may be delaying UE Attach procedures by using various backoff timers to reduce S6a signalling between MME and HSS.

Another example may be using local policies in the PCEF or in the TDF or in the AF for that particular IP-CAN session or TDF session or AF session. To apply local policies to reduce the signalling sent to the PCRF or to prioritize those messages on application level that may help to reduce additional signalling and re-attempts over the Gx/Rx interfaces (e.g. IP-CAN session termination or AF session termination procedures are sent to a node that reported "Diameter too busy" or "Diameter out of space").

These types of scenarios require analysis of node behaviour related to specific 3GPP Diameter Application.

4. Identify other 3GPP procedures that are dependent on producing Diameter signalling and determine if there are tools available (e.g. other existing mechanism in 3GPP) to ensure certain actions can be taken by the system to help reduce load on the system based on e.g. preconfigured Diameter signalling load value or based on the knowledge in the client about the maximum number of requests that can be sent to a server that reported "Diameter too busy" or "Diameter out of space".

This requires analysis of node behaviour related to specific 3GPP Diameter Application.

5. Clarify in which scenarios, existing mechanisms provided by Diameter Base Protocol RFC can be used and are still a valid way to prevent signalling overload, e.g. a simple Diameter relationship with a client and server sharing a one to one peer to peer relationship, then when server becomes overloaded, the client just needs to reduce the amount of Diameter traffic it sends to the server.

The solution(s) for evaluation may include proposals, for example, scenarios documented in clause 6.

6.2.5.2 Solution description: Diameter Load Manager

Editor's note: In this clause, proposed solutions will be documented or referred to from clause 6 as appropriate, and analysed on the aspects described for investigation in clause 6.2.5.1.

In order to handle a large number of concurrent messages on S6 interface, a server like the HSS and a Diameter Agent function can selectively drop requests or answer with 3004 DIAMETER_TOO_BUSY to relieve the load on the HSS.

Answering with 3004 DIAMETER_TOO_BUSY is preferred to dropping requests when possible since it provides the client with some feedback. In this alternative, there is a Diameter Agent - DLM (Diameter Load Manager) that acts as a load handling proxy for the HSS and is one Diameter hop from the HSS. There may be more than one DLM in an operator network, however, an HSS is load balanced through a single DLM. The DLM can derive dynamic load of HSS based on initial configuration information, methods that use the aggregate number of DIAMETER_TOO_BUSY messages it receives, request message drops by HSS, as well as SCTP transport level indications of load on the DLM - HSS interface. The methods to derive load are implementation dependent and outside the scope of this study. When the HSS consists of a cluster of nodes / Front Ends (FE), the DLM distributes requests to FEs based on the estimated load levels of each FE. When the aggregate load on the HSS (or DLM) reaches a preconfigured threshold level, the DLM may rank the request messages via proprietary means dependent on an application basis and forward high priority messages to HSS while dropping or answering with 3004 DIAMETER_TOO_BUSY for lower priority messages. Answering with 3004 DIAMETER_TOO_BUSY for certain types of messages by DLM may be used as an early indication mechanism to contain the load on the HSS, and as a means to inform the Diameter client. The DLM function may be used in a similar manner for other interfaces that implement an implicitly terminated Diameter session (i.e. server does not maintain state of the session) that routes/selects the server as for S6 interface related function. The DLM function may be used in a similar manner for other interfaces that implement an implicitly terminated Diameter session model as for S6 interface related function.

Editor's note: Ranking of messages and Diameter application behaviour in DLM are FFS.

For the PCC architecture, DRA can contain functionality similar to DLM and apply it as additional operator policies during PCRF selection. In this case, the DRA takes the PCRF load into consideration for selecting within the set of PCRF servers that are applicable for an UE/ IP-CAN session. The DRA can use similar methods as DLM to get the load of the PCRF, e.g. methods that use the aggregate number of DIAMETER_TOO_BUSY messages it receives, related PCRF notification of its load to DRA, etc. With the load of the PCRF, the DRA can maintain a prioritized list of servers and use that information as selection criteria for PCRF. The DRA may estimate the PCRF server load with certain accuracy if it is on the path of signalling between PCC clients and PCRF (DRA in proxy mode) and additional logic is implemented for load estimation.

6.2.5.2.1 Diameter charging interfaces

Offline charging interfaces, based on the Rf protocol between a Charging Trigger Function and the Charging Data Function located in the Offline Charging System (OFCS), are used to convey charging information for network resource usage concurrently with the usage. When the OFCS is overloaded, then the Diameter messages may be discarded resulting in the collection of inaccurate data used for billing and resulting loss of revenue for services delivered. Procedures should be defined for the CTF to handle the overload condition of the destination OFCS that allow the OFCS to stabilize. Mechanisms should be studied and defined by SA Working Group 5.

Online charging interfaces, based on the Ro protocol between a Charging Trigger Function and the Online Charging Function located in the Online Charging System (OCS), are used to authorize usage of network resources in addition to conveying charging information for the network resource usage. When the OCS is overloaded, then Diameter messages may be discarded leading to indeterminate behaviour in the CTF nodes generating the requests. It is likely that different types of CTFs may be required to perform different actions in response to overload. For example, an SMSC may simply delay sending an SMS, whereas a PCEF may deny user session establishment. Common and application-specific procedures should be defined for the CTF to handle the overload condition of the destination OCS that allow the OCS to stabilize. Mechanisms should be studied and defined by SA Working Group 5.

6.3 Solution: Optimizing control of mobile terminated services by CN node

For the scenario where massive number of small downlink data to IDLE UEs, in order to avoid massive Paging message impacts to the network, the mechanism of optimizing the handling of abnormal conditions in UE triggered Service Request procedure (specified in TS 23.401 [5] clause 5.3.4.2) can be used to reduce the rate of Downlink Data Notifications to MME.

On receiving massive number of Downlink Data Notifications from Serving GW, the MME determines that the rate of the events has become significantly high and that its load exceeds the operator configured threshold. The MME indicates "Delay Downlink Packet Notification Request" with parameter D to the Serving GW. The Serving GW uses this delay value to reduce the rate of sending Downlink Data Notification messages. As a result the rate of Paging triggers will be reduced.

7 Solutions targeting improved efficiency of User Location Information reporting

7.1 Solution 1: ULI reporting only when the UE is in "CONNECTED" state

7.1.1 Description

For ULI reporting related with UE change of RA/TA, a new option is added to enable the PCRF/OCS to request ULI reporting to be sent only when the UE is in "CONNECTED" state: the Node serving the UE (MME/SGN) defers ULI reporting related with RA/TA change as long as the UE is without active radio and S1/Iu user plane bearers or is in 2G STAND-BY state.

7.1.2 Impacts on existing nodes and functionality

Mobility Management (Attach, RA/TA updates) procedures are not modified by this solution.

The signalling (e.g. GTP-c) used for actual reporting of ULI related with UE change of RA/TA is not modified by this solution.

The solution adds following modification in the signalling (e.g. GTP-c) carrying a request for ULI reporting related with UE change of RA/TA: the ULI request may indicate ULI reporting associated with this request is to be sent only when the UE is in "CONNECTED" state or at transition to "CONNECTED" state and the location has changed since the last report.

The MME needs to retain information on the last reported location to determine whether a location report shall be sent at transition to "CONNECTED" state.

7.1.3 Solution evaluation

Refer to clause 9.4.

7.2 Solution 2: ULI reporting at PCC area level

7.2.1 Overview of ULI reporting at PCC area level

In some use cases policy/charging decisions and also e.g. statistics gathering per specific IP-CAN session depend on whether the UE is inside or outside a specific set of cells and/or serving areas associated with the user subscription:

- PCRF and/or OCS should be notified when an individual UE enters or leaves a specific area of interest (e.g. group of cells or RA/TA) provided by the PCRF i.e. therefore avoiding notifications inside or outside the specific area of interest.
- PCRF and/or OCS should be notified when an individual UE enters or leaves a specific area of interest (e.g. group of cells or RA/TA) pre-configured in the MME/SGSN i.e. therefore avoiding notifications inside or outside the specific area of interest.

NOTE 1: This is e.g. to define suitable QoS and charging policies to apply to the data service of the user in that set of cells and/or serving areas.

Thus a (new) granularity of User Location Information reporting "at PCC area level" is defined.

The ULI reporting at PCC area level works the same way as ULI reporting defined in TS 23.203 [9] with the following modification: The PCRF may send via the PCEF towards the CN node serving the UE a Location change reporting request at "PCC area" level, telling it wants to be notified only when the UE enters or leaves a PCC area together with the definition of the PCC area(s), providing for each PCC area:

- Either a "UE-dedicated PCC area" i.e. a short list of [exact maximum TBD] cells and/or ENB and/or serving areas (TA/RA) comprising this PCC area in the request from PCRF. In this case, the actual Location report contains the PCC area identifier and a flag stating whether the UE is entering or leaving the area, or
- A pointer to a "Core Network predefined PCC area" that is predefined in the MME/SGSN serving the UE. In this case, the actual Location report contains the PCC area identifier and a flag stating whether the UE is entering or leaving the area.

To avoid a MME/SGSN to handle reporting for multiple PCC areas in parallel for any given UE, PCRF shall make sure that only one Location change reporting procedure is active at a time:

- either a "UE-dedicated PCC area", made of a single PCC area, or
- a pointer to an "Core Network predefined area".

Based on operator configuration, Core Network "predefined PCC areas" shall not overlap.

NOTE 2: For the PCRF, the determination of the PCC area may take into account the subscription of the user retrieved from the SPR.

NOTE 3: A PCC area does not span beyond a PLMN boundary.

NOTE 4: Solution 2 as well as the H-PCRF subscription to Location change reporting (serving cell) or to Location change reporting (serving area (i.e. RA / TA)) are not generally meant to apply to roaming cases not associated with Network sharing.

At IP-CAN session establishment and upon change of serving EPC node (MME, SGSN, SGW), the PCRF and/or OCS and/or TDF (through PCRF) is notified whether Location change at PCC area level is supported by the network. If Location change at PCC area level is not supported, then the fall-back to Location change reporting at cell and/or serving area and/or CSG levels should be performed.

In addition, rather than listing all the cells of an eNB as "cells of interest", it could be possible for the UE-dedicated PCC area to refer to eNBs of interest, using the Global eNB ID IE defined in 3GPP TS 36.413. This would

- save signalling on S1 interface as the MME would not need to request cell-level reporting to the eNB: without eNB granularity, the MME would need to request the eNB with cell-level reporting in the area of interest (the MME does not know how many cells the eNB has).

7.2.2 More detailed description

When ULI reporting at PCC area level is supported, the following capabilities are added to the 3gpp system:

1. Adding a change of PCC area as an Event Reporting Function trigger:

The Event Reporting Function (ERF) performs event trigger detection. When an event matching the event trigger occurs, the ERF shall report the occurred event to the PCRF.

When ULI reporting at PCC area level is supported, the following Event trigger is added to the list of existing Event triggers (TS 23.203 [9] clause 6.1.4 "Event Triggers"):

Event trigger	Description	Reported from	Condition for reporting
Location change (PCC area) (see note)	The UE has entered or left a PCC area	PCEF, BBERF	PCRF
NOTE: A change in the PCC area may be associated with a change in the serving cell, possibly a change in the serving area and possibly a change in the serving CN node. PCC areas are defined in clause 7.2.1.			

When the ULI reporting at PCC area level applies to EPC (TS 23.203 [9] Table A.4.3-2: EPS specific event triggers), this corresponds to:

Event trigger	Description	Reported from	Condition for reporting
Location change (PCC area)	<p>The UE has entered or left a PCC area. The PCC area is defined as a</p> <ul style="list-style-type: none"> • A pointer to a "Core Network predefined PCC area" that is predefined in the MME/SGSN serving the UE, or • A short collection of cells (CGI/SAI for GERAN/UTRAN accesses and/or ECGI or Global eNB ID for E-UTRAN access) and/or as a collection of serving areas (Routeing areas and/or Tracking Areas). 	PCEF, BBERF	PCRF

2. Adding PCC area entering/leaving event in ULI reporting request sent by PGW (e.g. Change Reporting Action) towards MME/SGSN.

Rel-11 specifications of subscription requests to ULI reporting sent by PGW (e.g. Change Reporting Action) towards MME/SGSN just allow the PGW to tell it wants ULI at RA/TA level (or ULI at cell level) i.e. any RA/TA (any cell) where the UE is camping shall be reported.

The solution proposes that the subscription request to ULI reporting sent by PGW (e.g. Change Reporting Action) towards MME/SGSN is modified to allow the PGW to tell it wants ULI at PCC level together with a PCC area identifier and with the list of cells and/or eNBs and/or serving areas (TA/RA) comprising this PCC area. i.e. ULI reporting is done only when the UE enters in the PCC area or leaves this PCC area. The actual reporting from MME/SGSN contains the same PCC area identifier as in the request from PGW and an indication on whether the UE is inside or outside the PCC area.

When ULI at PCC area has been activated, the PGW should be able to store in its CDR information about the UE entering or leaving a PCC area

Only PCRF can activate ULI at PCC area level on the PGW. Nevertheless, when on-line charging applies, the OCS can request the PCEF to report ULI at PCC area level activated by the PCRF, via the Credit Control procedure. When such reporting has been activated over Gy, the PGW notifies the OCS with information about the UE entering or leaving a PCC area (together with the PCC area identifier). This assumes co-ordination between the PCRF and the OCS about the configuration of the PCC areas in the SPR (similar PCRF-OCS co-ordination is needed for the configuration related with the rating , etc.).

- UE-dedicated PCC areas: the PCC area and its identifier for the UE is expected to be configured in the SPR. OCS is configured with the mapping between the PCC area identifier and the ratings inside and outside the PCC area.
- Core Network predefined PCC areas: the PCC area and PCC area identifier should be configured in MME/SGSN and OCS should be configured with the mapping between PCC area identifier and the ratings inside and outside the PCC area.

For both PCC area types, when PGW initiates Credit-Control procedure, its request contains the PCC area identifier and an indication on whether the UE is inside or outside the PCC area. This implies an initial actual PCC area reporting as a first response to the PCC area reporting request from the PGW whereby the PCC area identifier and whether the UE is inside or outside the PCC area are stored in the PGW. This stored information is updated at each actual PCC area reporting.

When PCRF sends a request for stopping PCC area reporting, the PGW shall:

- send a ULI reporting stop to the MME/SGSN;
- if OCS has subscribed to PCC area reporting, send a Credit-Control Request message to OCS with an indication that the PCC area reporting has stopped.

Editor's note: It is FFS if the solution can be optimized to allow that both PCRF and OCS can activate event triggers and credit management triggers as per current PCC procedures.

7.2.3 Impacts on existing nodes and functionality

Mobility Management (Attach, RA/TA updates) procedures and existing RA/TA etc. definition are not modified by this solution; this solution neither modifies the content nor the number of messages sent over S1/Iu/Gb. Existing mechanisms allowing the PCRF to request via the PGW related with "subscription" onto a MME/SGSN for ULI information are reused including the mechanisms used at mobility between MME/SGSN.

The solution adds following modification in the signalling (e.g. GTP-c) carrying a request for ULI reporting: the ULI request may indicate ULI reporting associated with a PCC area(s) together with the mapping from PCC area(s) to a list of cells / eNBs / RA / TA.

The signalling (e.g. GTP-c) used for actual reporting of ULI is only modified by adding the indication of the PCC area the UE has entered in or has left. This solution aims at reducing the number of messages sent for actual reporting of ULI due to the fact that notifications are generated only when the UE enters or leaves a PCC area.

The solution adds following modifications to Gy for on-line charging:

- in the Credit-Control-Request message from the PGW, the addition of the PCC area identifier (provided by PCRF), whether the UE is inside or outside the PCC area, and optionally whether the PCC area reporting has been stopped; and
- in the Credit-Control-Answer message from OCS, the addition of an indication on whether OCS subscribes to PCC area entering/leaving events reporting.

7.2.4 Solution evaluation

Refer to clause 9.4.

7.3 Solution 3: New "change of eNB" reporting event

7.3.1 Description

For ULI at cell ID level, the MME needs to request the eNB to report intra-eNB cell changes. This causes S1 interface and GTPv2 signalling load at every cell change in RRC Connected mode.

In this solution, when the user is known as distant from the "cell(s) of interest", a new granularity of ULI reporting at "change of eNB" is requested by the PGW/PCRF, whereas a ULI reporting at change of cell is requested when it is notified that the UE is in an eNB which contains cells of interest, i.e. the "cells of interest" are not known by the MME/SGSN.

In this case, the MME would not request that the eNB reported intra-eNB cell changes. Inter-eNB connected mode changes are already visible at the MME level, and these would still be reported to the PGW with the ECGI of the cell the UE entered the eNB.

7.3.2 Impacts on existing nodes and functionality

Mobility Management (Attach, RA/TA updates) procedures are not modified by this solution.

The signalling (e.g. GTP-c) used for actual reporting of ULI related with UE change of eNB/2G Cell/3G SAI/RA/TA is not modified by this solution.

The solution adds the following modification in the PGW-MME/SGSN signalling (e.g. GTP-c), in Gx and in Gy carrying a request for ULI reporting:

- the ULI request may indicate ULI reporting associated with this request is to be sent only when the eNB changes in LTE;
- the ULI reporting may indicate that this report is associated with an eNB change reporting, and whether the ECGI corresponds to a cell of a macro-eNB or an HeNB.

The solution adds the following modifications in the CDRs for charging:

- the addition of an indication whether the CDR contains an eNB level ULI, an HeNB level ULI or a cell level ULI.

Editor's note: It is FFS how the MME is aware whether the ECGI provided by the RAN corresponds to an HeNB or a cell of an eNB (including the case where HeNB-GW architecture is deployed).

When the UE moves in RRC connected mode within a single frequency layer of a regular grid of "3 sectorised cell eNBs", the number of ULI reports from the MME to PGW would be halved.

7.3.3 Solution evaluation

Refer to clause 9.4.

7A. Solutions targeting reporting list of users on the area(s) of interest

7A.1 Solution1: Perform ULI reporting using LCS procedures

7A.1.1 Problem description

The problem description aims to extend the existing LCS architecture in order to support tracking reporting on per area of interest (TA/RAs, cell ids) which allows to the PCRF as LCS client to retrieve identity of users within a specific area of interest and tracks incoming and outgoing users from this area, this addresses the following scenarios:

- reporting users within a specific area of interest (e.g. group of cells or LA/RA/TA) while there is no need to report ULI for mobility events not inducing the specific area of interest
- tracking incoming and outgoing users from a specific area of interest (e.g. group of cells or LA/RA/TA) while there is no need to report ULI for mobility events not inducing the specific area of interest

7A.1.2 Overview of ULI reporting using LCS procedures

The PCRF or OCS is only interested in knowing whether the user is inside or outside a specific area(s) rather than knowing user location during all the session at each location change in order to define QoS and charging policies to apply to data services of the user in a specific area(s).

A ULI reporting mechanism using the LCS procedures would save signalling traffic due to user location updates procedures in the GPRS/EPC core networks and control plane interfaces.

Instead of tracking reporting on a per user basis, defining areas of interest and tracking the identity of the users within these areas will reduce considerably the signalling traffic load in the core network and control plane interfaces.

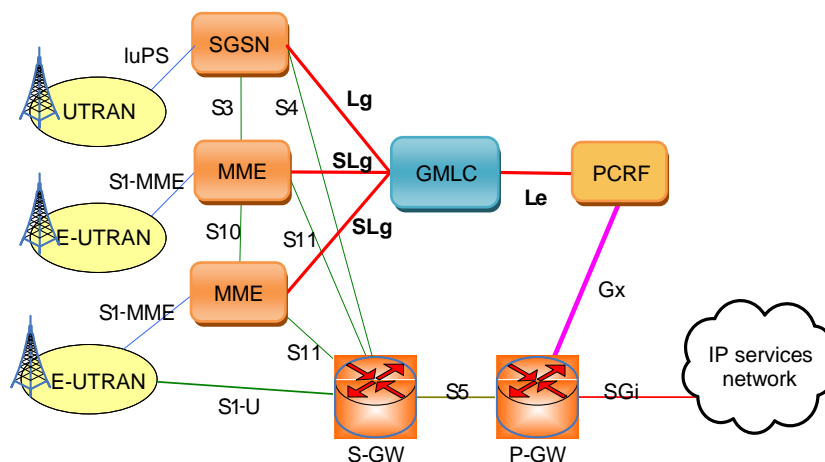


Figure 7.3.1: Overview of proposed solution for ULI reporting

The PCRF or OCS may send to GMLC the identities of area(s) of interest (TA/RA/LA) and subscribe to GMLC reporting of UE identities entering or leaving the areas of interest. The GMLC interacts with MME(s)/SGSN(s) to retrieve the required inputs.

The GMLC maps each area of interest (s) (TA/RA or Cell ids) received from the PCRF with the corresponding MME/SGSN or pools of MME/SGSN serving based on operator configuration.

NOTE 1: The determination of the area(s) of interest may be configured in the PCRF.

The PCRF may request the GMLC to aggregate ULI during a certain period before report it to the PCRF. This avoids reporting ULI to the PCRF systematically and generates the corresponding QoS and charging policies.

The existing mechanisms are appropriate to convey location information towards core network and control plane at session establishment since it does not generate additional signalling. However, the proposed solution aims at providing ULI updates, which would generate unsustainable additional signalling traffic using the existing mechanisms with the scenarios introduced in this TR.

7A.1.3 Impacts on existing nodes and functionality

7A.1.3.1 General

Mobility Management (Attach, RA/TA updates) procedures are not modified by this solution; this solution neither modifies the content nor the number of messages sent over S1/Iu/Gb.

The SLg/Lg reference points defined in TS 23.271 shall be enhanced to return users within the area(s) of interest (TA/RA/LA) results to the GMLC allowing tracking the status of area(s) of interest rather than users' location changes reduces considerably the signalling traffic compared to existing ULI reporting mechanisms.

The reference point between the PCRF or OCS and the GMLC could be based on Le interface defined in TS 23.271. In this case, Le interface shall be enhanced to convey location identifiers and return users' identity within the area(s) of interest.

7A.1.3.2 Impacts on existing procedures

PCRF:

- Define the PCRF as a new LCS client entity.
- The PCRF should be enhanced to request from the GMLC to start/stop reporting the list of UEs entering or leaving the area(s) of interest.
- The PCRF should be enhanced to collect UE identities entering or leaving the area(s) of interest and update related users' PCC rules.

GMLC:

- The GMLC should be enhanced to provide the PCRF list of UEs located in the area(s) of interest as requested by the PCRF. The GMLC may aggregate ULI during a certain period before report it to the PCRF

MME/SGSN:

- The MME/SGSN should be enhanced to provide the list of UEs entering/leaving the area(s) of interest as requested by the PCRF via the GMLC

Reference points:

- The reference point between MME and GMLC (SLg/Lg) should be enhanced to return the list of UEs rather than reports per user basis.
- The reference point between PCRF and GMLC (Le interface) should be enhanced to convey location identifiers (TA/RA, Cell ids) and return the list of users within the area(s) of interest.

7A.1.4 Solution evaluation

Refer to clause 9.5.

8 Solutions for GTP-c overload handling

8.1 Solutions targeting existing mechanism for GTP-C node overload prevention

8.1.1 Introduction

The GTP-C overload handling listed below looks at the resulting signalling from some of the scenarios given in clause 4. For each case it is proposed which existing functionality that can be used to reduce the effects of extensive signalling on the related interfaces and if any modification to existing functionality are needed it is FFS. The focus will be to get solutions giving a graceful resolution of possible overload situations.

8.1.2 Mobility management signalling

Extensive mobility management signalling can be a result from a RAN node restart as specified in Scenario 1 in clause 4.2.

The resulting S4 and S11 signalling will be Modify Bearer Request/Response. Existing solution for this can be to use Modify Access Bearers Request message sent per UE instead of Modify Bearer Request sent per UE and PDN connection, which may give reduced signalling over S11. This policy does not apply to cases when S5/S8 signalling is needed (e.g. RAT change, ULI notification change) and does not apply in case of legacy access as Modify Access Bearers Request is not supported over S4.

Support of the Modify Access Bearers Request procedure is optional for MME and SGW, and its use restricted to few scenarios when multiple conditions are fulfilled (see 3GPP TS 29.274 clause 7.2.24).

This procedure cannot help in particular in the case of overlaid RATs and failure of a RAN node (Scenario 1 in clause 4.2) for all UEs that reselect a different RAT after the node restart (see clause 4.2) due to the need to report the RAT change to the PGW.

Editor's note: It's FFS whether there are other solutions or enhancements can be made to existing solutions for this case.

8.1.3 Re-attach signalling

Extensive re-attach signalling can be a result from failure in a core network node as specified in Scenario 2 in clause 4.3).

The resulting S4, S11 and S5 signalling will be Create Session Request/Response or Modify Bearer Request/Response (e.g. SGW restoration procedure). Create Session Request/Response can be handled by the existing APN back-off timer function in the PDN GW. This mechanism cannot signal overload in case the PGW would nevertheless accept the Create session Request. Besides, this mechanism does not apply to Modify Bearer Request.

In case the SGW or PDN GW is severely overloaded and cannot indicate overload, the existing solution may result in the source node sending retransmissions of its requests to the overloaded node.

The APN back-off timer can be tuned by using different timer values depending on the overload level of a GTP-c node. The MME should reject PDN connection requests, for the specific APN related to that PDN GW during the "PDN GW back-off time".

Editor's note: It's FFS if the back-off timer mechanism can lead to oscillations with regard to network load.

Editor's note: It's FFS whether there are other solutions or enhancements can be made to existing solutions for this case.

8.1.4 Service request signalling

Extensive service request signalling can be a result from a catastrophic event as specified in Scenario 3 in clause 4.4.

Refer to clause 8.1.2,

Mechanisms related with APN back-off timer signalling cannot apply to mid-session signalling such as notifications sent on existing sessions over S5/S8.

Editor's note: Implications of this on the proposed solution are FFS.

8.1.5 UE requested PDN connectivity signalling

Extensive UE requested PDN connectivity signalling can be a result from a catastrophic event as specified in Scenario 3 in clause 4.4.

Refer to clause 8.1.3.

8.1.6 Network triggered Service Requests

Extensive network triggered service request signalling can be a result from push like services and applications as specified in Scenario 4 in clause 4.5. The resulting signalling over S4/S11 will be Downlink Data Notification (DDN) followed by Service Request. This can be handled by the existing Throttling of Downlink Data Notification Requests functionality (see clause 4.3.7.4.1a in TS 23.401 [5]).

This mechanism does not apply for network initiated signalling for dedicated bearer establishment/update/deletion, e.g. cannot protect the MME/SGSN against massive PGW initiated signalling requests resulting from application signalling that induces creation of dedicated bearers.

8.2 Framework for solutions using modifications of GTP-c signalling

8.2.1 General

Load information reflects the operating status of the resources of the originating GTP-c node.

This information when transmitted between GTP-c nodes may be used during SGW/PGW selection to support load balancing of the PDN connections for UEs.

Overload information reflects an indication of when the originating node is running above its nominal capacity which may cause severe issues in handling the incoming traffic.

This information when transmitted between GTP-c nodes may be used to reduce / throttle the amount of GTP-c signalling traffic between the GTP-c nodes.

GTP-C should support the option to signal load information for optional use by the receiver during node selection to enhance existing DNS-based node selection mechanisms (per TS 29.303) - possibly before overload occurs (preventive action). The mechanism for dynamic GTP-c node load control defined by 3GPP Rel12 CNO activities shall leverage existing (per TS 29.303) mechanisms.

NOTE 1: The exact format of load information is left to Stage 3.

GTP-C should support the option to signal overload information to enable the receiver to shed part of the control plane signalling towards an overloaded node when overload has occurred (reactive action).

NOTE 2: The exact format of overload information is left to Stage 3.

GTP-c overload mechanism(s) should continue to allow for preferential treatment of priority users (eMPS) and emergency services as per existing specifications.

SGW should not need to know via GTP-c signalling which PDN connections correspond to emergency services.

8.2.2 List of interfaces (and directions) where each of GTP-c load and overload control should apply

The GTP-c Load / Overload control mechanism should be generic in its definition. Thus, it should be applicable to all GTP-c interfaces defined by 3GPP system architecture.

- Dynamic GTP-c Load information is used to improve the existing GTP-C Node selection procedure. Load balancing related with GTP-c is employed during PDN connection creation (or at TAU/RAU/Handover with SGW relocation). Thus, it is used by nodes that need to allocate a PGW (and possibly a SGW) at PDN connection creation (or TAU/RAU/Handover with SGW relocation).

The candidate interfaces for Load Information exchange are:

1. (PGW load information) from PGW to MME/SGSN via the SGW.
2. (PGW load information) from PGW to GTP-c based Non 3GPP networks nodes (e.g. TWAN / ePDG / HSGW).
3. (SGW load information) from SGW to MME/SGSN.
4. (MME/SGSN load information) from MME/SGSN to other MMEs/SGSNs.

NOTE 1: The benefits of last interface/bullet need to be further evaluated.

NOTE 2: Interfaces related with Non 3GPP access are out of scope of FS-CNO.

- For Overload Information:

Similarly, transfer of Overload information may be useful when sent,

1. (PGW overload information) from PGW to MME/SGSN via the SGW
2. (SGW overload information) from SGW to MME/SGSN
3. (PGW overload information) from PGW to GTP-c based Non-3GPP Access Gateways (e.g. TWAN / ePDG / HSGW)
4. (MME/SGSN overload information) from MME/SGSN to SGW/PGW
5. (MME/SGSN overload information) from MME/SGSN may need to notify overload to other MMEs/SGSNs

NOTE 3: The benefits for the last interface/bullet needs to be further evaluated.

NOTE 4: Interfaces related with Non 3GPP access are out of scope of FS-CNO.

Based on local policies, a node may decide to send different values of Load / Overload information on inter-network (roaming) and on intra-network interfaces.

8.2.3 Scope of GTP-c load / overload control

The Overload information may be considered at 2 levels:

- GTP-c Node: It shall be possible to signal information about the load / overload of a full GTP-c node (i.e. information not restricted just to APN-level)
- APN: The PGW may detect overload for certain APNs, e.g. based on Diameter overload indication received from a PCRF or from an external AAA server, or e.g. based on shortage of resources for an APN (IP address pool). Stage 3 should investigate how to deal with PGW determining overload for some APN and needing to signal the overload level associated with that APN.

The Load information is only provided at the level of a GTP-c Node.

8.2.4 Examples of actions GTP-c node may take when another node has advertised overload

Editor's note: This clause is work in progress and exact handling/procedural impacts are FFS.

An MME/SGSN may use the GW load information for enhanced load balancing when selecting an SGW or PGW, e.g. in complement to the existing DNS weights mechanism (which takes into account relative capacities of nodes versus each others).

An MME/SGSN may take the following actions for GWs experiencing overload:

1. select an alternative GW during SGW/PGW selection;
2. reject EPS Session Management requests from the UE (e.g. PDN Connectivity, Bearer Resource Allocation or Bearer Resource Modification Requests) with a Session Management back-off timer;
3. reject Mobility Management signalling requests from UEs with a Mobility Management back-off timer (e.g. reject Service Request requiring to activate user plane bearers in an overloaded SGW);
4. relocating the SGW of the UE (e.g. to serve a Service Request requiring to activate user plane bearers in an overloaded SGW);
5. throttle certain GTP-c messages, e.g. ULI related notifications.

The MME/SGSN should not apply the above for high priority access and emergency services.

A SGW/PGW may take the following actions for MME/SGSN having indicated they experience overload:

1. Limit or completely block non-GBR dedicated bearer establishment.
2. Limit or completely block all Dedicated Bearer establishments or modification, except QCI=1 bearers.
3. Limit or completely block all Dedicated Bearer establishments, including the QCI=1 bearers.

4. Avoid a burst of Session Deletion procedures from the PGW, due to cleaning up the stale sessions.

The SGW/PGW should not apply the above for high priority access and emergency services.

8.2.5 Solution 1: Using load information for dynamic load balancing of GW nodes

8.2.5.1 Description

The solution complies to the framework described in this clause.

"Load Information" reflects the operating status of the resources of the originating GTP-c node. This information when transmitted between GTP-c nodes may be used during SGW/PGW selection to support load balancing of the PDN connections for UEs.

NOTE 1: How a node computes its Load Information is implementation dependent.

In one of realization, the value of Load Information could range from 0-100. Lower the value, lesser the load experienced by that node.

NOTE 2: The exact format of Load Information on GTP-c interfaces is left up to Stage 3.

8.2.5.2 Applicability

PGW should provide its "Load Information" to MME/SGSN via SGW i.e. when the SGW receives PGW's "Load Information" it shall forward it to the MME/SGSN.

SGW should provide its "Load Information" to MME/SGSN.

Editor's note: It is FFS whether in this version of the specification Load Information is included on S10 (between two MMEs), S3 (MME – SGSN) or S16 (between two SGSNs).

As the applicability of Load Information is to allow enhanced GW selection by GW selection function, Load Information is only transmitted in GW -> MME/SGSN direction.

8.2.5.3 Messages and inclusion period

For GTP-c nodes supporting this feature, Load Information can be included by piggybacking it over existing signalling messages:

- Any response messages by PDN GW and SGW AND
- Any SGW and PDN GW initiated requests.

In either PDN GW initiated messages (e.g. Update Bearer Request) or response messages to MME/SGSN (e.g. Create Session Response) PGW may include its Load Information towards peer SGW.

In either SGW initiated messages (e.g. Downlink Data Notification) or response messages to MME/SGSN (e.g. Create Session Response) SGW may include its Load Information towards peer MME/SGSN. If SGW had received Load Information from peer PGW, then it also includes PGW's Load Information towards peer MME/SGSN.

The transfer of the load Information shall not add significant additional load to each peer node. The calculation of Load Information should not severely impact the resource utilization of the node.

NOTE 1: It is up to stage 3 to define exact mechanism when the "Load Information" is to be transferred.

NOTE 2: The way for a node to compute its own Load information is implementation dependant.

8.2.5.4 Node selection using load information

When included, Load Information is used by SGW and PDN GW selection function i.e. MME and SGSN to perform node selection.

For SGW selection function, Load Information applies only to selection of SGW during the following procedures:

- Initial attach.
- Mobility procedures involving SGW change.
- SGW restoration.

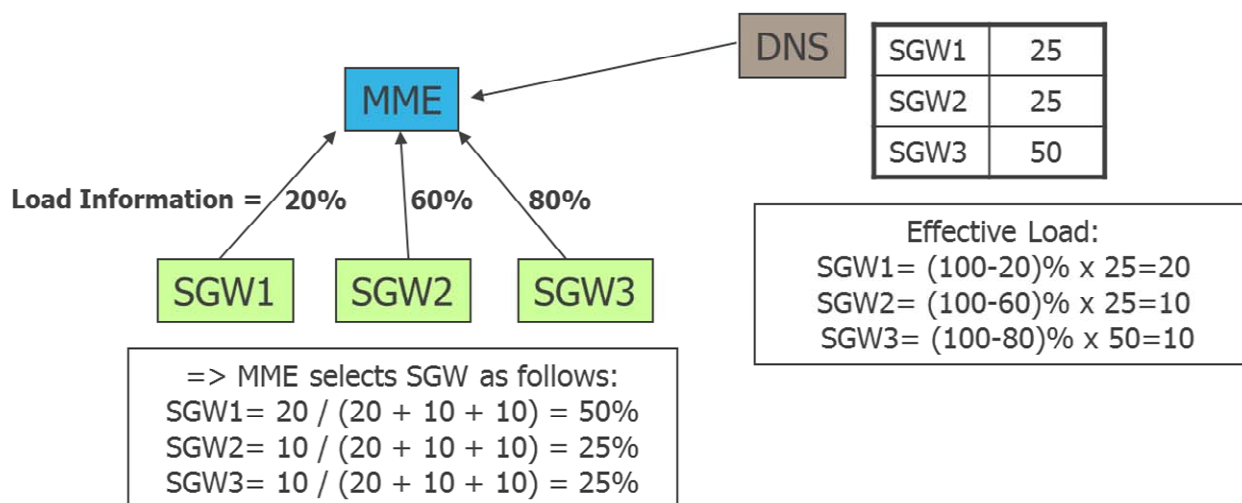
For PDN GW selection function, Load Information applies only to selection of PGW during the following procedures:

- Initial attach.
- UE requested PDN connectivity.
- PDN GW restoration.

During GW selection, if the GW IP Addresses returned from DNS server includes Weight Factors, and Load Information is also made available to the GW selection Function via Control plane signalling, then the GW selection takes both the information into account to perform appropriate GW node selection.

One example of realizing such capability would be for DNS SRV weights to be multiplied by Load Information to build Load balancing parameters as shown below:

- The "Load information" is a percentage of Load usage.
- Per candidate target GW Node for new GTP-c sessions:
 - the "Remaining load factor" is computed as $(100 - \text{"Load information"})$.
 - Then the "Effective load" is computed as $(\text{DNS weight} \times \text{"Remaining load factor"})$ to build a Load balancing parameter.
- New GTP sessions are allocated between candidate target GW Nodes with a rate proportional to their "Effective load".



NOTE: The exact algorithm of calculating weighted GW loads based on DNS SRV weights and Load Information is left up to Stage 3.

Figure 8.2.5.4-1

8.2.5.5 Advertising support of this feature

Since the feature "GTP-c augmented GW Selection" is optional, an explicit capability negotiation is not warranted to indicate support of this feature. GTP-c node is to send Load Information based on whether local configuration allows for it.

NOTE: Stage 3 is free to decide if explicit indication to advertise/negotiate support of this feature is needed or not.

8.2.5.6 Roaming consideration

Inter PLMN GTP-C load will be handled as part of advertisement of support for this feature i.e. clause 8.2.5.5.

8.2.5.7 Network sharing support

MOCN

No special considerations for MOCN are expected by this feature.

GWCN

No special considerations for GWCN are expected by this feature.

8.2.6 Solution 2: Using overload information for overload control of GTP-C nodes

8.2.6.1 Description

The solution complies to the framework described in this clause.

"Overload Information" reflects an indication of when the originating node is running above its nominal capacity which may cause severe issues in handling the incoming traffic. This information when transmitted between GTP-c nodes is used to reduce / throttle the amount of GTP-c signalling traffic between the GTP-c nodes. In other words, the "Overload Information" provides guidance to the receiving node to decide actions which leads to mitigation towards the sender of the information.

A GTP-c node is said to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic). At such point, the overloaded node includes "Overload Information" in existing GTP-c message(s) which assists the receiving node to take appropriate mitigation measures.

NOTE: Additional information (like validity-period, throttle rate, message scope etc) which may better assist in appropriate overload mitigation actions by receiving node may also be included. However, the exact content of Overload Information is left up to Stage 3 with the goal that when different GTP-C nodes supporting the same function receive the same "Overload Action", the same system level mitigation result should be achieved.

It shall be possible to run the node congestion control (added as part of Rel-12 CNO) in parallel and concurrently with existing congestion control mechanism (e.g. with PGW APN back-off timer related congestion control mechanism).

8.2.6.2 Applicability

When in overloaded state, PDN GW and SGW, depending on configuration, include Overload Information towards MME/SGSN. When the SGW receives PGW's Overload Information it shall forward it to the MME/SGSN.

When in overloaded state, MME/SGSN, depending on configuration, include Overload Information towards PDN GW and SGW. When the SGW receives MME/SGSN's Overload Information it shall forward it to the PGW.

NOTE 1: It is FFS whether in this release of the specifications Overload Information is included over S10 (between two MMEs), S3 (MME - SGSN) or S16 (between two SGSNs).

NOTE 2: If Overload Information is passed in MME/SGSN -> SGW -> PGW direction, then care should be taken that PDN GW acts on the correct serving MME for that PDN connection at any given point of time (e.g. during inter-MME TAU w/o SGW change procedure, address of new MME may not be conveyed to PDN GW. If old MME was overloaded, but new MME isn't then PDN GW should not act on the overload information).

The Node level overload Control may run independently from the APN overload control.

8.2.6.3 Messages and inclusion period

For GTP-c nodes supporting this feature, Overload Information can be included by piggybacking it over existing signalling messages:

- Any response messages by PDN GW and SGW;
- Any response messages by MME/SGSN;
- Any SGW and PDN GW initiated requests;
- Any MME/SGSN initiated requests.

If SGW had received overload Information from peer PGW, then it also includes PGW's Overload Information towards peer MME/SGSN.

If SGW had received overload Information from peer MME/SGSN, then it also includes MME/SGSN's Overload Information towards peer PGW.

The transfer of the overload Information shall not add significant additional load to each peer node. The calculation of overload Information should not severely impact the resource utilization of the node.

NOTE 1: It is up to stage 3 to define exact mechanism when the "Overload Information" is to be transferred.

NOTE 2: The way for a node to compute its overload information is implementation dependant.

8.2.6.4 Expected actions from involved nodes when overload information is received

Please refer to clause 8.2.4.

8.2.6.5 Advertising support of this feature

Since this feature is optional GTP-c node is to send Overload Information based on whether local configuration allows for it.

NOTE: Stage 3 is free to decide if explicit indication to advertise/negotiate support of this feature is needed or not.

If the peer node to the overloaded node does not support this feature, the received Overload Information is discarded by the peer node.

8.2.6.6 Roaming consideration

Inter PLMN GTP-C overload will be handled as part of advertisement of support for this feature i.e. clause 8.2.6.5.

8.2.6.7 Network sharing support

MOCN

No special considerations for MOCN are expected due to this feature.

GWCN

No special considerations for GWCN are expected due to this feature.

8.3 Solutions for preventing S-GW and P-GW overload

8.3.1 Solution 1: Use of Gateway Load Manager for DNS based load balancing

8.3.1.1 Description

This solution addresses only load control and relies on the existing overload mechanisms (e.g. backoff timer) to address load throttling".

In a sensible network deployment scenario the load of S-GW and P-GW should be equally distributed and each GW should be capable to handle the traffic load that it was engineered for and should have some reserve capacity to handle the event of a sudden traffic spike. Before the traffic spike event pushes the P-GW into an extreme overload territory, the P-GW can invoke a back-off timer to reject new connection requests in addition to any self-protection mechanism that it may have in order to keep itself operating in a stable manner (e.g. reject of new connections).

Currently, the S-GW and P-GW selection mechanism is based on DNS procedure as specified in TS 29.303. MME selects the S-GW and P-GW from a list of available addresses and weight factor provided by the DNS server. The selection process used by MME does not identify the actual load of S-GWs and P-GWs.

During initial selection procedure, if the selected S-GW is currently overloaded then it does not response to Create Session Request. As a consequence MME may reselect another S-GW. If S-GW determines that P-GW is overloaded or P-GW is not responding, S-GW includes an error cause code, (e.g., 'Remote peer is not responding' or 'All the dynamic addresses are occupied', etc) in Create Session Response message, so MME can try to reselect another P-GW. This kind of reactive approach can be minimized, if the DNS procedure can also take "current load factor" of S/P-GW into consideration.

NOTE: "Current load factor" does not necessarily imply real time sampling of S/P-GW load. It can represent a load condition for a certain period of time (e.g. 3 mins) to account for peak oscillations within small time intervals.

To allow the S-GW and P-GW selection procedure to also take into account their current load condition, a functional entity called "GW load Manager" (GLM) is introduced. It sits between MME/SGSN and the DNS server. GLM is informed about the load information from S-GW and P-GW.

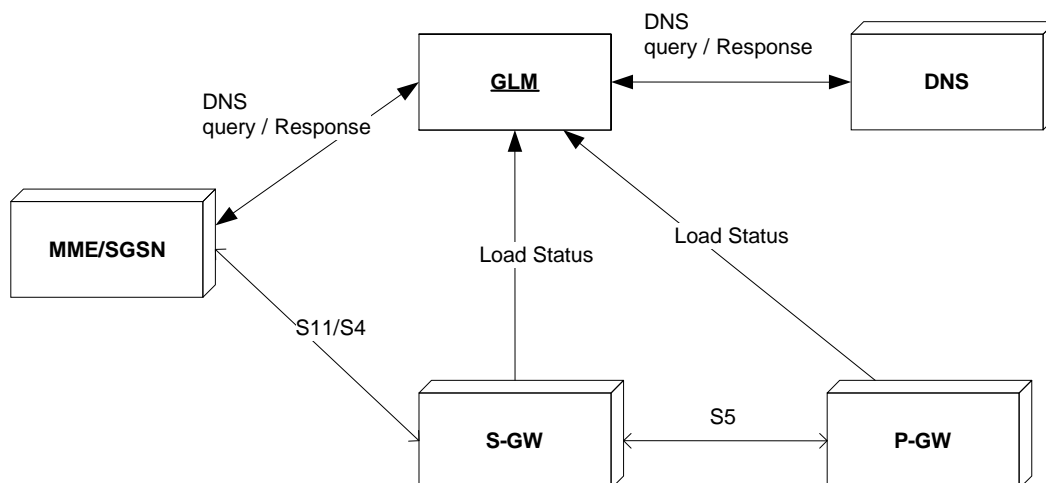


Figure 8.3.1.1: P/S GW selection with "GW Load Manager"

MME/SGSN are configured to send a DNS query to the GLM. GLM has current load status of S-GW/P-GW, and based on that it may change the weight factors in DNS responses received from DNS server before forwarding to MME/SGSN. This allows the P-GW and S-GW with lesser load to be selected by MME/SGSN.

In a scenario where all the S-GWs and P-GWs are heavily loaded, any one of them can go into overload condition with further spike of traffic. During this condition, the GLM may not be returning any S/P-GW address in the DNS response back to the MME/SGSN to prevent further increasing load in those gateways. MME/SGSN may then also invoke back-off timer to prevent UEs from creating more load towards the network.

Editor's note: It is FFS whether this solution supports roaming with home routed traffic, i.e. whether the MME/SGSN can take into account the load information from P-GWs pertaining to different PLMNs e.g. from the same operator group.

Editor's note: It is FFS with how the latency related to the change of S/P-GW load information would be taken into account by the MME/SGSN (considering DNS caching in MME/SGSN), and how much extra signalling the solution may imply between the MME/SGSN and the DNS.

Editor's note: The new GLM adds a new failure point. It is FFS how to address the failure of the GLM and provide redundancy of the GLM.

8.3.1.2 Impacts on existing nodes and functionalities

GLM queries the DNS like a MME/SGSN.

MME/SGSN is configured to use the GW Load Manager as contact for DNS queries and may need to adjust the TTL of DNS resource records to ensure the records are based on the most recent "current load factor" reported from P/S-GW.

GLM can retrieve load information from S/P-GW based on protocols like SNMP or via OA&M. Otherwise; standardizing an interface in 3GPP with a new reference point from the S/P-GW to the GLM is required, as the solution needs to work in multi-vendor and roaming environment. Furthermore it implies configuration to ensure that DNS requests from MME/SGSN are handled by the GLM.

9 Evaluation

9.1 Evaluation of SS7/ MAP interface

SS7 signalling - SCCP and TCAP defined by the ITU-T, has evolved as an international standard since 1980. SS7 has overload control mechanism for its links that are quite robust. SS7/TCAP does not have end to end overload control mechanisms. However, if the MAP entity is overloaded, HLR can discard lower priority signalling as described in TS 29.002 in order to relieve congestion. If this overload control mechanism is changed significantly, it may result in other instability. This is a mature system with deployments and experience that can be used to manage a network that has predictable overload control. Thus, the recommendation in this study is to use existing mechanisms of SS7 and TCAP in particular to handle congestion.

9.2 Enhancement of Diameter interface for overload prevention and control support

Diameter interface is defined for signalling between many core network nodes and services. An analysis table for these interfaces and service impact is shown in Annex A. Overload on these interfaces can lead to server congestion or even collapse. The impact to services can be:

- Denial of services, persistent access restriction,
- loss of IMS and broadband services,
- Loss of location information for emergency services and lawful intercept,
- Loss of ability to use policy control to provide service personalization,
- Loss of ability to use policy control to optimize network resources,
- Billing errors and loss of revenue.

Besides good network engineering, one of the measures for better traffic management on diameter interfaces is the deployment of Diameter Agent in network. This functional node plays important roles for load balancing and overload prevention/control over these interfaces using Diameter. Hence, the overall overload protection mechanism must take this aspect (i.e., Agent between client/server) into consideration.

In addition the Diameter interface shall be enhanced to support overload prevention and control, especially for core network entities. Currently it has very limited support in this aspect:

- 1) Cause code 3004 "DIAMETER_TOO_BUSY" for server to client in responses.
- 2) The transport layer may be unaware of the application layer and therefore cannot provide sufficient congestion control for congestion at the application layer.
- 3) Congestion collapse due to an overloaded Diameter server may occur because there is no way for a server to communicate its current overload level and coordinate actions with the client.
- 4) A Diameter server in overload will expend resources inspecting and rejecting messages. To preserve good throughput, a process is needed to offload this task to the Diameter client(s).
- 5) If diameter routing agents are deployed, the servers' load levels for efficiently load balancing/re-routing have to consider topology hiding and can at best be based on statistical estimation.

Overload signalling in Diameter is of coarse granularity and is deployed in a hop-by-hop manner. These mechanisms are not sufficient for Diameter applications to become aware of overload; this is more relevant in large scale deployments with multiple clients, servers and agents in the middle of the communication. Particular overload aspects to investigate relate to the difference between session oriented Diameter interactions and Diameter interactions relying on implicitly terminated Diameter sessions (i.e. the server does not maintain state of the session) and the effect of Diameter Agents between end points. Without standardized mechanisms at some layer (Diameter application, base protocol, transport, network, etc.) the Diameter-based protocol interfaces used by functional entities in the 3GPP architecture cannot obtain detailed or useful information to avoid overload or respond to congestion.

9.3 Evaluation related with the support of overload control and dynamic load control for GTP-C

GTP-C interface is defined for signalling between many core network nodes and services. Overload on these interfaces can lead to node congestion or even collapse. The impact to services can be e.g.:

- loss of PDN connectivity (IMS, Internet ...) and associated services
- loss of ability to setup and release radio and core network bearers necessary to support services e.g. GBR bearers for VoLTE;
- Loss of ability to report to the PGW/PCRF user information's changes, e.g; location information for emergency services and lawful intercept, changes in RAT or QoS;
- Billing errors and loss of revenue.

The GTP-C interface shall be enhanced to support overload prevention and dynamic load control as it has currently very limited support in this aspect:

- 1) no means exists in GTP-C to signal the dynamic load of a node. GTP-c load balancing based on semi-static DNS weights does not take into account the instantaneous load or capacities of the S/P-GW and may lead to overload in one or more nodes of a SGW or PGW cluster while there is still remaining capacity on other nodes of the same cluster. GTP-c load balancing based on Dynamic DNS updates requires a new standard interface to configure and test, implies modifications to the operator DNS infrastructure which is very sensitive for operators, and induce much shorter DNS cache timers which adds to the signalling load of nodes performing GTP-c load balancing.
- 2) a PGW can detect congestion for a specific APN and perform overload control for that APN. But:
 - this does not allow to report an overload at the node level;
 - this is an On/Off mechanism, when approaching congestion or during congestion, that can create oscillations in network signalling (e.g. sudden decrease or surge of signalling traffic when APN congestion controls starts/stops);
 - The On/Off nature of this mechanism may be mitigated by applying different values of the PGW Back-Off Time
 - this has effects only on subsequent Create Session Requests, not on GTP-C signalling exchanged for already established PDN connection;
 - this is only supported from the PGW to the MME/SGSN, but not supported e.g. from the SGW to MME/SGSN or from MME/SGSN to the SGW/PGW.
- 3) an MME/SGSN can request an SGW to throttle Downlink Data Notification message. But this has not effect e.g. on network initiated signalling for dedicated bearers establishment/update/deletion.
- 4) The Modify Bearers Access Request procedure may reduce in some scenarios the signalling over S11, but this does not allow to limit this signalling to what the SGW can actually receive, this is not usable over S4 nor when S5/S8 signalling is required to update the PGW, e.g. about RAT or ULI change, and so is not usable in certain scenarios possibly generating massive signalling, e.g. RAN failure with overlaid RATs.
- 5) Some GTP-C cause code (e.g. 'NoResourceAvailable') exists to signal temporary unavailability of resources to process a received request, but the receiver can continue to send requests for other UEs as this cause is not defined to mean node overload;
- 6) GTP-C retransmissions (upon lack of responses) amplify GTP-C overload;
- 7) A solution where a GTP-c sending node would rely on the size of its GTP-c sending queue would not allow a MME to determine whether a PGW (or the SGW) is congested and which PGW is congested (as the GTP-c sending queue would actually be per SGW and not per PGW).
- 8) Congestion collapse due to an overloaded GTP-C entity may occur because there is no way for a GTP-C entity to communicate its current overload level and coordinate actions with its GTP-C peer.

- 9) A GTP-C entity in overload will expend resources inspecting and rejecting messages. To preserve good throughput, a process is needed to offload this task to the GTP-C peer(s) as close as possible to the source of traffic.

9.4 Evaluation related with the support of User Location Information reporting improvements

This technical study has identified and discussed 3 solutions

Solution 1: ULI reporting only when the UE is in "CONNECTED" state (clause 7.1 of this TR):

This option does not add new messages and requires a flag to be added in the subscription to UE change of RA/TA.

This solution saves ULI signalling at RA/TA updates due to the UE moving between RA/TA while being IDLE when ULI reporting at RA/TA level has been requested by the PGW.

Solution 2: ULI reporting at PCC area level (clause 7.2 of this TR):

The solution introduces the PCC area, which is either a list of cells and/or eNBs or a list of TAs/RAs. A PCC area can either be defined as part of UE subscription (e.g. for Home Zones), or as a pre-configured area in MME/SGSN (e.g. for foreign PLMN overlapped coverage at country borders). This solution enhances the current ULI reporting per UE as follows:

- The solution adds following modification in the signalling (e.g. GTP-c) carrying a request for ULI reporting: the ULI reporting request from PCC may indicate ULI reporting associated with a single PCC area identified by a PCC area identifier together with the mapping from PCC area to a list of cells and/or eNBs and/or RAs and/or TAs.
- The signalling (e.g. GTP-c) used for actual reporting of ULI is modified by only adding the indication of the PCC area the UE has entered in or has left the PCC area, identified by its PCC area identifier. This solution aims at reducing the number of messages sent for actual reporting of ULI due to the fact that notifications are generated only when the UE enters or leaves a PCC area.
- Request to report Location Change on Sd, Gx, Gxx and Location Change reporting on Gx, Gxx and Sd are modified with the capability of reporting on PCC area level along with PCC area description.
- Addition of PCC area identifier, an inside/outside indication, and optionally a PCC area reporting stop indication in the Credit-Control-Request message from the PGW, and addition of an indication on whether OCS subscribes to PCC area entering/leaving events reporting in the Credit-Control-Answer message from OCS.

This solution saves a lot of useless signalling as very often ULI are requested not to track each cell or RA/TA where the UE is camping but to determine whether an UE is within an area of interest (e.g. subscriber Home Zone, coverage overlapping country border area)

Only a single PCC area ULI reporting procedure can be active at a time, but there is no PCC area limitation as a PCC area can be made of non contiguous coverage cells or TAs/RAs.

MME/SGSN is not required to handle reporting for multiple PCC areas in parallel, as only PCRF can request ULI reporting, only a single PCC area reporting procedure can be active at a time in this solution, and based on operator configuration, "Core Network predefined PCC areas" do not overlap.

Solution 3: New "change of eNB" reporting event (clause 7.3 of this TR):

This solution requires changes on GTP-c, on Gx, on Gy and in the SGW/PGW CDRs:

- a new flag in the cell change ULI reporting request from PGW, PCRF and OCS, indicating that reporting has to be done at change of eNB;
- two flags in the actual ULI reporting from MME to SGW/PGW, from PGW to PCRF, and from PGW to OCS: the first one indicating eNB granularity reporting, the second one indicating whether ECGI corresponds to a cell or an HeNB;
- similar two flags in the CDRs in SGW and in PGW.

This solution does not impact RAN, and saves S1 signalling.

9.5 Evaluation related with the support of reporting list of users on the area(s) of interest

Solution1: Perform ULI reporting using LCS procedures (clause 7A.1 of this TR):

This solution is "area-based" as it allows the PCRF to subscribe to reporting of UE identities entering or leaving an area of interest, so targets an area of interest and not a specific UE by extending existing LCS architecture. It is therefore addressing other use cases than the ULI reporting at PCC area level solution (clause 7.2 of this TR), which is UE based, (e.g. determining which UE are within a shopping mall in order to send ads to these UE).

It relies on the usage of LCS but still requires further studies as there is an impact on multiple nodes (PCRF, SGSN/MME and GMLC) and some related interfaces.

10 Conclusions

10.1 Conclusions for MAP/SS7 and Diameter interfaces

10.1.1 MAP/SS7 interface

As evaluated in clause 9.1, the recommendation in this study is to use existing mechanisms of SS7 and TCAP in particular to handle congestion.

10.1.2 Diameter interface

It has been identified as a problem that overload signalling in Diameter is of coarse granularity and is deployed in a hop-by-hop manner; this is more relevant in large scale deployments with multiple clients, servers and agents in the middle of the communication.. Diameter applications need to respond to overload. Without standardized mechanisms at some layer (Diameter application, base protocol, transport, network, etc.) the Diameter-based protocol interfaces used by functional entities in the 3GPP architecture cannot obtain detailed or useful information to avoid overload or respond to congestion in such large deployments. Mechanisms similar to the ones described in clause 6.2.5 for DLM (Diameter Load Manager) could be studied in stage-3 for potential benefits in server congestion management.

It is therefore proposed to find a standardized means to convey necessary congestion information between functional entities that use a Diameter-based protocol interface. IETF dime working group has recognized the limitation of the protocol and has started work to define suitable mechanisms to address this at the protocol layer. CT3, CT4 and SA5 should take into account the work done in IETF at Diameter protocol level and consider investigating Diameter protocol end points behaviour and any other changes needed in 3GPP Stage 3 specifications to support overload control mechanisms on Diameter interface for 3GPP applications. Particular overload aspects to investigate relate to the difference between session oriented Diameter interactions and Diameter interactions relying on implicitly terminated Diameter sessions (i.e. the server does not maintain state of the session) and the effect of Diameter Agents between end points when deployed.

10.2 Conclusions for GTP-C interfaces

It has been identified as a problem that GTP-c does not support overload signalling and that GTP-c retransmissions of unacknowledged requests amplify the overload. The larger the number of users on an operator's network, the worse the problem becomes.

GTP-c peers need to respond to overload. Without standardized mechanisms, the GTP-c based protocol interfaces used by functional entities in the 3GPP architecture cannot obtain detailed or useful information to avoid overload or respond to congestion.

Besides that, the current GTP-c load balancing based on semi-static DNS weights may lead to overload in one or more nodes of a SGW or PGW cluster while there is still remaining capacity on other nodes of the same cluster.

It is therefore proposed to study in stage-3 mechanisms fulfilling the requirements set in clause 8.2 with the aim to define means to convey in GTP-c necessary overload and load information between functional entities that use a GTP-c based protocol interface:

- This corresponds to Solutions as described in solution clause 8.2.5 (Solution 1: Using Load Information for Dynamic Load Balancing of GW nodes) and clause 8.2.6 (Solution 1: Using Overload Information for Overload Control of GTP-C Nodes).

The exact list of interfaces to which GTP-c load / overload control mechanism applies to is left up to Stage 3's evaluation. However, SA WG2 recommends the following interfaces to be investigated:

- For Load Information:
 1. (PGW load information) from PGW to MME/SGSN via the SGW
 2. (SGW load information) from SGW to MME/SGSN
 3. (PGW load information) from PGW to GTP-c based Non 3GPP networks nodes (i.e. TWAN / ePDG)

NOTE 1: The impacts of last interface/bullet need to be further evaluated.

- For Overload Information:
 1. (PGW overload information) from PGW to MME/SGSN via the SGW
 2. (SGW overload information) from SGW to MME/SGSN
 3. (MME/SGSN overload information) from MME/SGSN to SGW/PGW
 4. (PGW overload information) from PGW to GTP-c based Non-3GPP Access Gateways (i.e. TWAN / ePDG)

NOTE 2: The impacts for the last interface/bullet needs to be further evaluated.

CT WG4 should consider defining suitable mechanisms based on clause 8.2.5 and 8.2.6 of the TR to address this at the protocol layer and investigating GTP-c protocol end points behaviour and any other changes needed (e.g. to address various "Notes" specified in 8.2.5 and 8.2.6) in 3GPP Stage 3 specifications to support dynamic load control and overload control mechanisms on GTP-c interface for the 3GPP functional entities.

It is assumed that stage 3 will define the Load/Overload related information exchanged between GTP-c nodes with enough precision to guarantee a common multi-vendor interpretation of this information allowing inter-operability between various GTP-c nodes.

3GPP will recommend various potential overload mitigation actions (as e.g. in clause 8.2.4 of the TR) based on the reception of the Overload related information exchanged between GTP-c nodes. However, the exact internal processing logics of a node will not be standardized.

10.3 Conclusions for User Location Information reporting improvements

For User Location Information reporting improvements, FS-CNO concludes that

1. Solution 1 (ULI reporting only when the UE is in "CONNECTED" state) and solution 2 (ULI reporting at PCC area level) are recommended to be standardized within the scope of Rel12. Solution 3 (New "change of eNB" reporting event) is not recommended for standardization as eNB granularity has been added to solution 2.
2. Some further use cases (that cannot be fulfilled by existing procedures that target UE(s) and not areas of interest) such as determining the list of users entering a shopping mall (e.g. in order to send ads to these users), may require other solutions such as solutions described in 7A. Nevertheless solutions described in 7A would need further work and therefore cannot be concluded in the Rel12 timeframe. Thus solving these use cases would deserve a new standard activity to take place in the future.

Annex A: CN interfaces and services using Diameter as well as overload impact

This clause provides information on core network nodes, interfaces and services using Diameter and impact due to overload.

Editor's note: The following table is under development.

Table A.1: CN nodes and their related interfaces using Diameter

CN nodes	Defined interface	Services	overload impact
PCRF - PCEF/TDF	Gx, Sd	Policy control and DPI	Denial of services, loss of policy control for service personalization and network optimization, billing errors and revenue loss
PCRF/PCEF/AS/MRFC - OCS/OFCS	Sy, Gy/Ro, Ro, Gz/Rf, Ro	Online/offline charging, service authorization, policy control, charging information reporting	Denial of some services, billing errors and loss of revenue
PCRF - AF, P-CSCF	Rx	application and IMS services	Denial of IMS services
HPCRF--VPCRF	S9	Roaming authentication/authorization	Loss of roaming service
CDF/CGF - MRFC/MGCF/AS/S CC-AS/I-/S-CSCF, etc	Rf	Offline charging,	
HSS - MME/SGSN	S6a, S6d	Mobility management, registration, authentication and location services	Denial of Services, signalling storms leading to congestion collapse, and persistent inability to access the network,
HSS - GMLC/MME	SLg, SLh	UE location reporting	Unable to provide location information to core/IMS network, including emergency services, lawful interception and location services.
HSS/UDC - I-/S-CSCF	Cx/Dx	UE IMS registration, authentication, and domain management	Denial of IMS services, signalling storm leads to congestion collapse, reselection from LTE to 2/3G,
HSS - SCC-AS/AS	Sh/Dh	IMS services delivery	Denial of or unpredictable behaviour of certain services (e.g., voice call routed to voicemail, delayed messaging...)
HSS - BSF	Zh	Bootstrapping Server Function	
Note 1: Reference: 3GPP TS 23.203, TS 32.240. Note 2: If a DRA (Diameter Routing Agent) is deployed, it relays these interfaces between functional nodes to HSS and/or PCRF.			

Annex B:

Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2010-10	SA2#81	S2-104649			Initial Skelton		0.0.0
2010-10	SA2#81	S2-105088			Introduction	0.0.0	0.1.0
2010-10	SA2#81	S2-105089			Add CNO scope	0.0.0	0.1.0
2010-10	SA2#81	S2-105090			Add CNO architecture principles	0.0.0	0.1.0
2010-10	SA2#81	S2-105091			CNO general introduction of scenarios and some solutions.	0.0.0	0.1.0
2010-11	SA2#82	S2-105559			Editorial corrections	0.1.0	0.2.0
2010-11	SA2#82	S2-105941			NAS Reject solution for user registration attempts	0.1.0	0.2.0
2010-11	SA2#82	S2-105942			Optimizing the periodic update signalling	0.1.0	0.2.0
2010-11	SA2#82	S2-105943			RAN restart issues and CNO	0.1.0	0.2.0
2010-11					Editorial corrections	0.2.0	0.2.1
2011-02	SA2#83	S2-111135			Flood of Mobile Terminated Data	0.2.1	0.3.0
2011-02	SA2#83	S2-111136			Flood of registration and mobility management events	0.2.1	0.3.0
2011-02	SA2#83	S2-111137			Flood of resource allocation requests for mobile originating services	0.2.1	0.3.0
2011-02	SA2#83	S2-111138			Optimization of Subscription data for HSS/HLR overload protection	0.2.1	0.3.0
2011-02	SA2#84	S2-112087			Signalling Load Reduction for TAU/RAU caused by UE mobility across mobility management entities. Added in clause 6.1.5	0.3.0	0.4.0
2011-02	SA2#84	S2-112189			Optimizing control of mobile terminated services by CN node. Added in clause 6.3.	0.3.0	0.4.0
2011-02	SA2#84	S2-112190			Evaluation of Core Network Signalling in case of HLR/HSS Overload. Added in clause 6.2.1.1	0.3.0	0.4.0
2011-02	SA2#84	S2-112191			Prevent HLR/HSS from overload due to RAT reselection. Added in clause 6.2.4	0.3.0	0.4.0
2011-02	SA2#84	S2-112209		4	HLR/HSS Overload Notification Solution. Added in clause 6.2.3	0.3.0	0.4.0
2012-07	SA2#92	S2-123252			Addition of Evaluation clause (chapter 7)	0.4.0	0.5.0
2012-07	SA2#92	S2-123253			Diameter Application Evaluation and Improvement via existing mechanism. Added into 6.2.5	0.4.0	0.5.0
2012-07	SA2#92	S2-123254			Evaluation of SS7/MAP and Diameter overload. Added in sections 7, 8 and Annex A.	0.4.0	0.5.0
2012-07	SA2#92	S2-123257			Multi-level HSS Overload Indication. Added in 6.2.3.	0.4.0	0.5.0
2012-07	SA2#92	S2-123401			Update of NAS Reject Solution. Revision in 6.1.3.	0.4.0	0.5.0
2012-09					Editorial corrections. TSG numbers in Annex B.	0.5.0	0.5.1
2012-10	SA2#93	S2-123807			Update of CNO TR scope clause	0.5.1	0.6.0
2012-10	SA2#93	S2-124015			MPS considerations for Core Network Overload Control	0.5.1	0.6.0
2012-10	SA2#93	S2-124016			Additions to Diameter overload analysis related to policy	0.5.1	0.6.0
2012-10	SA2#93	S2-124017			Additions to Diameter overload analysis related to charging	0.5.1	0.6.0
2012-10	SA2#93	S2-124018			Diameter Load Balancing Agent	0.5.1	0.6.0
2012-10	SA2#93	S2-123502			Editorial Cleanups of TR23.843	0.5.1	0.6.0
2012-10	SA2#93	S2-124146			CN overload due to flood of User Location Information (ULI) reporting	0.5.1	0.6.0
2012-10	SA2#93	S2-124020			Use cases for overload due to Location Request	0.5.1	0.6.0
2012-11	SA2#94	S2-124859			Load Consideration in PCRF Selection	0.6.0	0.7.0
2012-11	SA2#94	S2-124741			Conclusion on Diameter Overload	0.6.0	0.7.0
2012-11	SA2#94	S2-124861			ULI Reporting at Policy Area Level	0.6.0	0.7.0
2012-11	SA2#94	S2-124748			only report a change of location when user plane radio bearers are actually established for the UE	0.6.0	0.7.0
2012-11	SA2#94	S2-124862			GTP-C Overload Scenarios	0.6.0	0.7.0
2012-11	SA2#94	S2-124863			perform ULI reporting using LCS procedures	0.6.0	0.7.0
2013-04	SA2#96	S2-131542			Additional use cases related with GTP-c Overload or related with the need to have a more dynamic GTP-c Load control	0.7.0	0.8.0
2013-04	SA2#96	S2-131543			General Requirements for GTP-c Load / Overload Control	0.7.0	0.8.0
2013-04	SA2#96	S2-131544			Overload on GTP-C interfaces	0.7.0	0.8.0
2013-04	SA2#96	S2-131547			S-GW/P-GW overload prevention	0.7.0	0.8.0
2013-05	SA2#97	S2-131831			TR23.843 chapter revision	0.8.0	0.9.0
2013-05	SA2#97	S2-132125			GTP-C load balancing Mechanism	0.8.0	0.9.0
2013-05	SA2#97	S2-132255			GTP-C Overload Control Mechanism	0.8.0	0.9.0
2013-05	SA2#97	S2-132124			Evaluation of GTP-C overload prevention and control	0.8.0	0.9.0

2013-05	SA2#97	S2-132194			Conclusion for GTP-C overload prevention and control	0.8.0	0.9.0
2013-06	SP-60	SP-130237	-	-	MCC editorial update for presentation to TSG SA for information	0.9.0	1.0.0
2013-07	SA2#98	S2-132763			Evaluation related with Solutions for User Location Information reporting improvements	1.0.0	1.1.0
2013-07	SA2#98	S2-132984			Reducing ULI signalling load in LTE	1.0.0	1.1.0
2013-07	SA2#98	S2-132985			CNO avoidance for ULI reporting	1.0.0	1.1.0
2013-07	SA2#98	S2-132986			Update of solution 3 performing ULI reporting using LCS procedures	1.0.0	1.1.0
2013-07	SA2#98	S2-133060			Update of solution 2 for User Location Information reporting improvements	1.0.0	1.1.0
2013-10	SA2#99	S2-133634			CNO_ULI solution 2 updates and evaluation	1.1.0	1.2.0
2013-10	SA2#99	S2-133635			CNO_ULI TR conclusions	1.1.0	1.2.0
2013-10	SA2#99	S2-133816			CNO_ULI solution 3 updates and evaluation	1.1.0	1.2.0
2013-10	-	-			Editorial corrections	1.1.0	1.2.0