3GPP TR 29.809 V0.3.0 (2013-06)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
Study on Diameter overload control mechanisms
(Release 12)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ^{TM}) 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 3GPP ^{TM} system should be obtained via the 3GPP Organizational Partners' Publications Offices.

MCC selects keywords from stock list.

Keywords

<keyword[, keyword]>

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

Contents

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 possible enhancements of the Diameter base protocol (IETF RFC 6733 [2] and existing Diameter applications to support overload control mechanisms in 3GPP core networks.

This work is based on the results of the feasibility study on Core Network Overload available in 3GPP TR 23.843 [3] and the related work done in the IETF Diameter Maintenance and Extensions (DiME) working group.

This study will cover:

- Identification of the set of requirements for an improved overload control mechanism over Diameter based signaling interfaces used in 3GPP core networks.
- Identification, evaluation and selection of candidate solutions for overload control mechanisms, including:
    - Mechanisms to detect overload situations e.g. notification of Diameter end-point signaling load;
    - Mechanisms to exchange overload control policies between Diameter end-points;
    - Details on the expected behaviour of 3GPP core network nodes supporting the defined overload control mechanism (Diameter end-points and Diameter agent);
    - Evaluation of the impacts of the proposed solution(s) on existing Diameter-based Technical Specifications and Diameter based signalling networks (internal operator networks, inter-operator network (e.g. IPX).
    - Recommendations on the solutions to select depending of the applicability context (interfaces, application, network, etc.)

The results of this study will contribute to the work done within the IETF DiME working group on Diameter overload control, through official liaison statement from 3GPP or company-driven individual contributions, which includes:

- Provide feedback from 3GPP on the requirements for Diameter overload control mechanisms defined in IETF Draft draft-ietf-dime-overload-reqs-06 [4]);
- Contribute to the specification of the IETF standard mechanism for overload control over Diameter.

The results of this study will be used to identify the changes required in the 3GPP specifications to support overload control mechanisms over Diameter-based 3GPP interfaces and applications.

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] IETF RFC 6733: "Diameter Base Protocol".

[3] 3GPP TR 23 843: "Study on Core Network Overload Solutions".

[4] IETF Draft draft-ietf-dime-overload-reqs-06: "Diameter Overload Control Requirements".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[5] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[6] 3GPP TS 29.272: "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[7] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[8] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[9] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[10] 3GPP TS 23.203: "Policy and charging control architecture".

[11] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[12] 3GPP TS 29.213: "Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping".

[13] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[14] 3GPP TS 29.215: "Policy and Charging Control (PCC) over S9 reference point; Stage 3".

[15] IETF Draft draft-ietf-dime-app-design-guide-15: "Diameter Applications Design Guidelines".

[16] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; protocol details".

[17] IETF Draft draft-campbell-dime-overload-data-analysis-00: "Diameter Overload Data Analysis".

[18] 3GPP TS 22.153: "Multimedia Priority Service".

[19] 3GPP TS 29.219: "Policy and charging control: Spending limit reporting over Sy reference point".

[20] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[21] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

[22] 3GPP TS 23.007: "Restoration procedures".

[23] IETF Draft draft-roach-dime-overload-ctrl-03: "A Mechanism for Diameter Overload Control".

[24] IETF Draft draft-korhonen-dime-ovl-01: "The Diameter Overload Control Application (DOCA)".

3 Definitions, symbols 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].

Definition format (Normal)

<defined term>: *<definition>.*

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

3.2 Symbols

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

Symbol format (EW)

<symbol>	<Explanation>

3.3 Abbreviations

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

BBAI	Broadband Access Interworking
DRA	Diameter Routing Agent
IPX	IP exchange
MPS	Multimedia Priority Service
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function

4 Introduction

The Diameter base protocol is widely adopted in 3GPP as protocol support of numerous signalling interfaces in IMS, EPC, PCC and charging architectures (e.g. S6a/S6d, Gx/Rx, Cx/Sh, Gz (only Diameter based reference point)/Gy, Rf/Ro).

Overload situations occur when the resources of a Diameter node are insufficient to process all the incoming. During this period of overload, the performances of the network are seriously degraded and cumulative effects can even lead to situation of congestion collapse.

As part of the study on Core Network Overload Solutions (3GPP TR 23.843 [3]), it has been investigated how the Diameter based interfaces were protected against signaling overload. The conclusion was that the existing overload control mechanisms in the Diameter base protocol defined in IETF RFC 6733 [2] were too limited to efficiently prevent and react to signaling overload. These limitations are even more critical in large scale networks in which multiple Diameter nodes, from various vendors, are in the signaling path.

Although vendor-specific solutions might be already available in some networks, a standardization effort is required to cope with a multi-vendor/operator environment in large scale networks and roaming cases.

The following sections describe the problem caused by Diameter overload in 3GPP networks and investigate the possible enhancements of the Diameter based interfaces to support adequate overload control mechanisms. These enhancements should have minimal impacts on existing infrastructures and be generic enough to be suitable for multiple Diameter based interfaces. However, the exact solution to implement will be decided per Diameter application, depending on the specific requirements of each interface.

5 Impacts of Diameter Overload in 3GPP Networks

5.1 Introduction

5.2 Diameter Overload

5.2.1 Introduction

The following subclauses provide an overview of the overload situation in Diameter and describe the mechanisms described in IETF RFC 6733 [2] to discover that a Diameter node is overloaded.

5.2.2 Diameter Overload Problem

Diameter (IETF RFC 6733 [2]) is protocol that enables the exchange of messages between Diameter nodes over TCP and SCTP connections. Communicating Diameter nodes can share a direct connection or be connected through other Diameter peers (Diameter agents). In normal conditions, any request sent by a Diameter client will be processed by a Diameter server in a given realm and the Diameter server will send back to the Diameter client a message indicating the result of the request (success/failure).

As described in the IETF Draft draft-ietf-dime-overload-reqs-06 [4], overload situations in a Diameter signaling network occur when the number of incoming requests exceeds the maximum request throughput supported by the receiving Diameter node. Reasons for these temporary overload cases are many and various in an operational network, including: insufficient internal resource capacity of a Diameter node faced with a sudden burst of requests e.g. after network failure/restart procedures affecting a large number of users, deficiency of a Diameter node component leading to a drastic reduction of the overall performances of the Diameter node, etc.

As a consequence of the overload situation, the answering Diameter node cannot successfully process the exceeding proportion of requests. These requests can be either simply dropped or extremely delayed in the processing. At best, the Diameter node may have enough internal resources to send back to the request initiator a message indicating that the requests cannot be successfully processed. Whatever the behavior of the overloaded Diameter nodes, the rate of successfully processed requests and consequently the overall performances of the network decrease.

5.2.3 Limitations of Existing Mechanisms in Diameter

The base Diameter protocol (IETF RFC 6733 [2]) provides two native mechanisms to explicitly indicate that a server is overloaded.

The first mechanism is to use of the Protocol Error "DIAMETER_TOO_BUSY" in the answer related to the request. This error is used by the Diameter node to indicate a specific server being requested might be busy and unable to provide the requested service. When receiving such an error code, the downstream Diameter node should attempt to send the message to an alternate peer, if available. Shedding of messages or redirection of messages if there are other servers available to take over the load may be implemented in the downstream Diameter node in this case. However, the Protocol Error "DIAMETER_TOO_BUSY does not provide detailed information of the severity of the overload state of the server. Furthermore, it can be imagined that in the case the server is already overloaded, it has to respond to each request with this error code, which may make things even worse. Although the recipient of the Protocol Error "DIAMETER_TOO_BUSY" could send further requests to alternate peers (if applicable) to offload the overloaded node, there is no existing explicit indication of when the overloaded node is not overloaded anymore. This results in implementation specific handling that is not deterministic or optimal.

The base Diameter protocol (IETF RFC 6733 [2]) enables also an overloaded server to inform a peer of its lack of internal resources for normal request processing by sending a request for transport layer disconnection (Disconnect-Peer-Request) with the disconnect cause set to "BUSY", as described in section 5.4 of the base Diameter protocol (IETF RFC 6733 [2]). This mechanism is only meaningful when client and server have a direct transport connection. If an agent is on the path between the client and the server, only this agent will receive the disconnection request the cause "BUSY". There is no way to propagate this information to the client that has initiated the request: the client behind the agent will only receive the Protocol Error "DIAMETER_UNABLE_TO_DELIVER" (see below). Moreover, the Diameter node receiving this disconnection reason is not expected to attempt reconnection "*unless it has a valid reason to do so (e.g., message to be forwarded)*", as stated in the base Diameter protocol (IETF RFC 6733 [2]), which provide very few guidance on when to reopen the connection after an overload situation. It seems to be assumed that the overloaded node should be able to reopen the connection after the end of the overload situation whereas Diameter servers in operational networks are usually configured as connection request responder-only, leading to a deadlock situation.

When a Diameter agent (Relay or Proxy) is on the path between the client and the server, the diameter client may receive from the agent the Protocol Error "DIAMETER_UNABLE_TO_DELIVER" as answer to the pending request if the server has terminated the connection with the agent due an overloaded state or if the server does not even respond because the additional requests are dropped. Besides the case the host is overloaded and cannot respond the request, which may fall into this error scope, this Protocol Error cause may be received by the client for other error cases (e.g. failure of the transport connection, no entry in the peer table of the Diameter agent), and there is no way for the Diameter client to clearly determine an overload situation using only Protocol Error "DIAMETER_UNABLE_TO_DELIVER".

As an alternative mechanism, a Diameter node might assume that a peer is overloaded when no responses to requests are received from the peer while the transport connection works well. However, this mechanism is neither reliable nor accurate and may take long time for the downstream Diameter node to realize overload might happen at the server.

Besides the limitation indicated above for each, a common limitation with all the existing mechanisms is that the downstream Diameter node can only react after overload happens, i.e. after overload is detected. A mechanism for overload protection is worth investigated.

As a conclusion, the base Diameter protocol (IETF RFC 6733 [2]) provides very limited mechanisms to detect and overcome overload situations. These mechanisms are based on specific error handling or transport connection management at the server side. The default behaviour of the client relies only on the availability of alternate peers to offload the requests when the primary server is offloaded. However, these mechanisms are too loosely standardized to predict a generic behaviour of all the Diameter nodes present in the same network in case of overload. For a more sophisticated overload control mechanism, the specification effort is required at the application level. This effort could further detail the use of existing mechanisms for a given Diameter application, by clarifying the expected behaviour of clients and servers in case of overload. Moreover, being at the application level would allow defining new mechanisms to enhance the existing Diameter overload control mechanism.

5.3 Overload Scenarios in 3GPP Networks

5.3.1 Introduction

3GPP TR 23.843 [3] describes a certain number of overload scenarios from which we retain the main following categories:

- a traffic flood resulting from the failure of a network element, inducing a signalling spike;
- a network element which is under dimensioned for the peak hour and thus entering overload conditions until it is upgraded;
- exceptional but predictable events (e.g. Christmas, New year, Mother’s day, promotional offers during a Short period);
- a catastrophic event locally generating a traffic spike including emergency traffic handling.

The characteristics of these overload scenarios are different and the overload control that will be defined by 3GPP should cover these different scenarios categories.

5.3.2 Overload of the HSS

5.3.2.1 Introduction

5.3.2.2 Causes of Overload

5.3.2.3 Impacts

5.3.2.3.1 Introduction

5.3.2.3.2 Overload impacts over S6a

Impacts vary according to the interfaces where overload occurs, hereafter are described some possible impacts of an overload over the S6a interface, in particular towards the UE.

As described in the subclause 5.2.3, when the HSS is overloaded over S6a, the MME can receive for a pending request:

- An Answer with the Result-Code set to"DIAMETER_TOO_BUSY";
- An Answer with the Result-Code set to "DIAMETER_UNABLE_TO_DELIVER" when interconnected to the HSS via Diameter agent(s);
- or no response at all when HSS and MME are peers sharing the same connection..

The table A.1 in the Annex A of 3GPP TS 29.272 [6] describes the mapping between the possible Diameter error codes received by the MME and the appropriate NAS cause codes to forward to the UE that has initiated an Attach, Tracking Area Update or Service Request procedures.

In this table, the Result-Code "DIAMETER_UNABLE_TO_DELIVER" is mapped to the NAS cause code #15 "No suitable cells in tracking area", which forces the UE to select another RAT and this will contribute to the overload. It would result in new attempts including those through the MAP protocol when Gr SGSNs are involved.

The mapping corresponding to the Result-Code "DIAMETER_TOO_BUSY"

is not described in the table A. It means that the default expected behaviour of the MME when receiving such a Result-Code is the one defined in the base Diameter protocol (IETF RFC 6733 [2]) with the limitations detailed in the section 5.2.3 above.

Moreover, in the table A.2 in the Annex A 3GPP TS 29.272 [6], which described the mapping to NAS cause code for other error conditions, it is not described what should do the MME when no response is received for a pending request. This implies that the normal behaviour described in the base Diameter protocol (IETF RFC 6733 [2]) applies i.e. the retransmission of the pending request.

Editor's Note: The table A.1 and table A.2 in the Annex A of the 3GPP TS 29.272 may be updated before completion of this study, in order to clarify the behaviour of the MME in such overload error cases.

As described above, the overload of the HSS triggers even more requests from the UE and consequently additional requests towards the HSS that contribute to worsen the overload state of the HSS. It is therefore critical to avoid as much as possible such overload scenario.

5.3.3 Overload of the PCRF/DRA

5.3.3.1 Introduction

This clause covers the overload of the PCRF and the DRA. The Policy and Charging Control architecture and stage 2 procedures are described in the 3GPP TS 23.203 [10]. Related stage 3 specifications are the 3GPP TS 29.212 [11], 3GPP TS 29.213 [12], 3GPP TS 29.214 [13], 3GPP TS 29.215[14] and 3GPP TS 29.219 [19].

5.3.3.2 Overload of the PCRF

5.3.3.2.1 Introduction

The PCRF is a functional entity managing a multitude of interfaces (intra and inter operator) to different functional entities. Most of the interfaces are Diameter based (e.g. Gx, Rx), while others aren’t (e.g. Ud).

All of the Diameter based interfaces are session stateful. The same PCRF must be used for the lifetime of a session. In addition, the same PCRF must be used for sessions established over the different reference points (Gx, S9, Gxa/Gxc, etc.) for the same UE or UE's IP CAN session, depending on the operator deployment configuration and scenario. For example, in the visited access case in roaming scenarios, all sessions for a UE have to be associated with the same V-PCRF/H-PCRF pair. The PCRF associates those sessions with session information related to the same UE obtained over the different reference points (e.g. Rx, Sd).

The PCRF serving a UE is selected when the first Diameter session related to the UE or UE’s IP-CAN session is established. It keeps state related to the UE as long as there is an ongoing IP-CAN session for the UE and cannot be changed for that duration. However, a new PCRF can be selected when a UE attaches to the network if the PCRF selection is on a UE basis, or when the UE sets up a new IP CAN session if the PCRF selection is performed on an IP-CAN session basis.

A specialized Diameter Routing Agent (DRA) can be deployed to assist in the PCRF selection, when new PCC related Diameter sessions are being set up (see subclause 5.3.3.3) and more than one PCRF exists in a Diameter realm.

5.3.3.2.2 Causes of Overload

See subclause 5.3.1.

5.3.3.2.3 Impacts

When the PCRF is overloaded, it may behave as follows:

- Reject requests with a DIAMETER_TOO_BUSY result code. When the scenario/configuration allows it (as specified in clause 5.3.3.2.1), a recipient of such error (e.g. DRA) may try alternate PCRFs, reject the triggering procedure (e.g. PCEF rejects a resource modification request due to a CCA with this error), or possibly in certain cases retry the failed request when it deems the PCRF not busy anymore. As specified in 5.2.3, such determination is not currently defined in the standards, is implementation specific and is not deterministic.

- Drop requests. The request initiator/intermediary typically times out the outstanding request and depending on the scenario/configuration, may have options such as retrying the request, rejecting the triggering request or sending the request to an alternate PCRF if applicable.

- Drop existing transport connections/not accept incoming connections. The behaviour of elements interacting with the PCRF in this case will depend on whether they are peers of the PCRF (i.e. have a direct connection to it) or are communicating to the PCRF via intermediaries (e.g. a PCEF communicating to the PCRF via a DRA). In general, this case, like the "dropping of requests", is not an explicit indication of overload to elements interacting with the PCRF. The options available to the node trying to communicate with the PCRF are to reject the triggering procedure, send the request to an alternate PCRF if applicable, or retry/send the request when the connection to the PCRF is restored.

In all of the above cases, retrying the request should be only performed if it doesn't exceed the time budget the retrying node is allowed to use to complete the interaction with the PCRF, based on operator policies and configuration. As an example, if a PGW is configured to time out Gx requests after 2 seconds and has 5 seconds to respond back to a resource modification request from the SGW over S5, it has room to retry a timed out Gx request once without exceeding its time budget of 5 seconds. If however the PGW only had 3 seconds to respond to the SGW, it cannot retry a timed out Gx request without risking the timeout of the S5 procedure initiated by the SGW.

When a request cannot be routed to an alternate PCRF or retried to the same PCRF, the request initiator will need to deal with the failure by either handling it locally if policies/scenario allow it (e.g. Gx CCR-I rejected but PGW has local operator policies to not reject the corresponding IP-CAN session establishment), or reject the triggering procedure (e.g. reject the IP-CAN session establishment). In the latter case, if the triggering procedure is retried, it could exacerbate the overload condition and/or cause additional load/overload in the RAN, IMS, etc.

More detailed impacts are specified in Annex X.

For supporting BBAI, following additionally impacts shall be considered:

- For WLAN scenario, the PCRF shall additionally be able to associate sessions established over the S9a and Gxb* for the same UE or UE's IP-CAN session.

- For H(e)NB PS service, the PCRF shall additionally be able to associate session established over the S9a with all the Gx sessions which have same H(e)NB Local IP address.

- For WLAN scenario and NSWO traffic case, the PCRF shall be able to associate session established over the S9a, S9, Rx and Sd interfaces for the same UE or UE's IP-CAN session.

- For HNB CS service, a new PCRF can be selected when the HNB performs the registration to the HNB GW and an S15 session is initiated by the HNB GW. The PCRF shall able to associate the S9a session with the S15 session.

5.3.3.3 Overload of the DRA used for the PCRF selection

5.3.3.3.1 Introduction

The Policy and Charging Control architecture and procedures related to the Diameter Routeing Agent (DRA) are described in the 3GPP TS 23.203 [10] and 3GPP TS 29.213 [12].

5.3.3.3.2 Causes of Overload

See sub clause 5.3.1.

5.3.3.3.3 Impacts

5.3.3.3.3.1 Introduction

In order to ensure that all Diameter sessions for Gx, S9, Gxa/Gxc, Rx and Sd (when the unsolicited application reporting applies) for a certain IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm, an optional logical "Diameter Routing Agent (DRA)" function is enabled. The DRA acts as a proxy agent or a redirect agent. In addition the DRA stores information about the assigned PCRF for a UE and IP CAN session. The DRA selects the PCRF at IP CAN session or Gateway Control session establishment and stores the PCRF address. After IP CAN session or Gateway Control Session establishment, the DRA ensures that the same PCRF is contacted for all related Rx, Gxa/Gxc, Gx, S9 and Sd Diameter Sessions.

It is assumed in the 3GPP TS 23. 203 [10] that there is a single logical DRA serving a Diameter realm.

As described in Annex A, a DRA can be deployed in three different modes: PA1, PA2 and redirect agent.

When a DRA node is overloaded, like any other node, it may reject requests with a DIAMETER_TOO_BUSY result code or simply drop messages/connections as specified in 5.3.3.2.3.

For supporting BBAI, following additionally impacts shall be considered:

- For WLAN scenario and EPC-routed traffic case, the DRA shall additionally ensures that the same PCRF is selected for related S9a, Gxb* Diameter sessions for the same UE or UE’s IP-CAN session.
- For H(e)NB PS service, the DRA shall additionally ensure that the same PCRF is selected for the related S9a Diameter sessions.
- For WLAN scenario and NSWO traffic case, the DRA shall ensure that the same PCRF is selected for the related S9a*, S9, Rx and Sd Diameter Sessions.
- For HNB CS service, the DRA shall ensure that the same PCRF is selected for the related S9a and S15Diameter sessions.

5.3.3.3.3.2 Proxy Agent 1 (PA1)

When a DRA running as PA1 is overloaded, its impacts on clients of the PCRF (e.g. PCEF, BBERF, AF) is similar to a deployment with no DRA when the PCRF is overloaded. This is because all messages between the clients of the PCRF and the PCRF go through the DRA.

Additionally, when the DRA is overloaded, the PCRF is impacted as well, as messages from the PCRF may be rejected or dropped before they reach the client. There are two categories of messages originated by the PCRF that are impacted:

- Answers that are dropped by the DRA will result in timeouts at the client, without the knowledge of the PCRF. The client will detect that no answer was received for its request and may retry the request (possibly causing further overload) or fail the triggering procedure (e.g. resource modification request). If the request is not eventually successfully retried, this can cause a session state mismatch between the PCRF and its clients (e.g. Gx CCA dropped by the DRA). Depending on the application and message contents, this can have impacts from charging, usage monitoring, to QoS (e.g. no dedicated bearers are setup for an IMS call, charging information not conveyed to PCEF, etc.).
- Requests can be rejected or dropped. They will need to be handled by the PCRF similarly to how its clients, i.e. retry later or fail the procedure. If the procedure is failed, this could cause calls to be dropped (e.g. if Gx RAR is

triggered by Rx, the corresponding Rx session may need to be aborted), charging to not be applied properly, usage monitoring, etc.

5.3.3.3.3.3 Proxy Agent 2 (PA2)

When a DRA running as PA2 is overloaded, its impacts on clients of the PCRF (e.g. PCEF, BBERF, AF) is different from a DRA running as PA1. The main difference is that not all messages go through the DRA. Instead, only session establishment requests as well as termination requests for certain applications (Gx, Gxx, S9).

Session establishment requests are impacted in the same way as PA1. Session update requests are not impacted as they go directly to the destination bypassing the DRA. Session termination requests for certain applications (ones that modify the binding) are impacted as they are supposed to go through the DRA. As opposed to the PA1 case if the DRA rejects the termination request with a DIAMETER_TOO_BUSY result-code or drops the request, the client could try to send it directly to the PCRF. This will ensure that the PCRF cleans up the corresponding state and related sessions (e.g. if Gx is terminated, Rx would need to be aborted, etc.). However, the drawback is that the DRA will end up with a stale binding, as it would think that the session is still active.

5.3.3.3.3.4 Redirect Agent

When a DRA is running as a redirect agent, its overload impacts are similar to the PA2 case for requests initiated by clients of the PCRF. The difference though with PA2 is that the redirect agent is never in the path of messages between the PCRF and its clients.

5.3.4 Overload of the 3GPP AAA Server

5.3.4.1 Introduction

The 3GPP AAA Server is a functional entity in the EPC architecture, which exposes many different diameter interfaces towards other network nodes, both internal and external to the operator’s domain. Those interfaces include:

- STa, SWa: towards external access networks (trusted, STa, and untrusted, SWa)
- SWm: towards ePDG
- S6b: towards PDN-GW (it can be internal for home-routed traffic, or external, for local-breakout traffic)
- SWx: towards HSS (internal)

Those interfaces follow a stateful mode of operation (session-oriented), except SWx which is stateless (non-session oriented).

It should be noted that, typically, it is expected to find a number of 3GPP AAA Servers deployed in an operator’s network, which can work in a load-sharing model; each AAA server in that pool can initially handle any incoming user, but once a user is handled in a certain AAA, this server is registered in the HSS, and from that moment, subsequent interactions for that user must be handled by the originally assigned AAA server. This means that no traffic balancing can take place for interactions past the initial user assignment to a server.

5.3.4.2 Causes of Overload

Similar causes of overload to those described in clause 5.3.1 are also applicable to the 3GPP AAA Server.

In particular, failure and restart of network elements such as the PDN-GW may impose a big traffic load on some 3GPP AAA Servers over the S6b interface, given that a diameter session is maintained for each PDN-Connection, and also considering that the S6b interactions must always be redirected to a previously assigned AAA server which is already handling the user.

Each 3GPP AAA Server keeps access session information for a given user, initiated typically via STa/SWa reference points. For this reason, in comparison with S6b messages, STa/SWa messages are more prone to be load balanced to a less loaded 3GPP AAA Server since they are used to setup an initial access session; this is not so feasible over the S6b interface, which is typically used once the access session is already ongoing.

5.3.4.3 Impacts

Given the big number of diameter interfaces on the 3GPP AAA Server, and their dependencies, it is particularly important to prevent unavailability of this network entity as a result of peaks of traffic.

It should be noted that, prior to Release 11, the unavailability of a specific 3GPP AAA Server which had already been assigned to a user, resulted on that user being unable to get access/service from the network (even if the external access network decided to allocate a new AAA server), because the HSS kept re-directing back to the former 3GPP AAA Server all traffic addressed to that user. This was solved by including a new indication (AAA-Failure-Indication AVP) from the access network, over STa and SWx, to let the HSS override a former user/server assignment.

Therefore, as a consequence of the above, when an access network determines that a certain 3GPP AAA Server is undergoing a certain level of unavailability due to overload, it should not simply send traffic to a non-overloaded server; instead, it must take into account that users already handled by that server should either remain in that server (with the restriction of a potential temporary service unavailability), or they should be re-allocated to a new server, by making use of the mechanism defined in Release 11 that allows the HSS to override previous 3GPP AAA Server allocations.

Additionally, other impacts related to the overload on specific interfaces include, for instance, the scenario in which a severe overload of the HSS could imply to stop accepting new incoming users to the system, and therefore it would have an impact on interfaces towards the external access networks (i.e., to start rejecting incoming traffic over STa/SWa).

5.3.5 Overload of the Offline Charging System (OFCS)

Editor's note: The initial input is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, which would be solved by future company contributions.

5.3.5.1 Introduction

The Offline Charging System terminates the Rf reference point as defined in 3GPP TS 32.240 [20]. Other 3GPP specifications define additional reference points that are functionally equivalent to the Rf reference point. These are the Gz reference point in the Evolved PS domain and the Wf reference point for WLAN offline charging.

The Offline Charging System (OFCS) may be decomposed into Charging Data Function (CDF) and the Charging Gateway Function (CGF) in which case, the CDF provides the Diameter Accounting Application.

As defined in 3GPP TS 32.240 [20], the following network elements are connected to the OFCS by the Rf reference point: P-GW, MME, S-GW, ePDG, SGSN, WLAN, S-CSCF, MGCF, BGCF, IBCF, P-CSCF, I-CSCF, MRFC, SIP AS, Service-NE, and CS-NE.

The Rf interface utilizes the Diameter Accounting Application as defined in 3GPP TS 32.299 [21].

This clause considers different Overload scenarios over Reference Points associated to 3GPP Diameter Charging Application for Offline Charging (Rf), and captures existing defined mechanisms intended to prevent them, if any.

5.3.5.2 Causes

5.3.5.2.1 Network Causes

The different Network Overload scenarios depicted in 3GPP TR 23.843 [3] (scenario 1 to 5 and 8), are also causes for Overload situations over Rf due to:

- Huge surge in Mobility Management signalling: Flood of new Rf charging sessions from new SGW, Rf closing sessions on old SGW, update Rf sessions from SGW/PGW on "RAT Change/SGW change" from PGW

- Flood of Attach over E-UTRAN access resulting in flood of default bearer establishment signalling, requests extended beyond the S-GW/P-GW to OFCS (Rf) for associated charging sessions establishment.

- Flood of resources allocations for Mobile Originating services: dedicated bearers (over E-UTRAN) or PDP ctxs (over GSM/UMTS), application sessions, extended beyond the S-GW/P-GW/SGSN/GGSN/AF to OFCS (Rf), associated charging sessions establishment.

- Flood of signalling for Mobile Terminating services: SMS-MT resulting in flood of signalling Rf for MME/SMS-SC, and Push-Application with flood of signalling for resources allocation (bearers..) extended beyond the S-GW/P-GW/SGSN/GGSN/AF to OFCS(Rf), associated charging sessions establishment.

- Flood of ULI update extended beyond the S-GW/P-GW/GGSN to OFCS(Rf) associated charging sessions update.

3GPP Diameter Charging Interfaces Rf may also experience overload when specific Network Nodes fail:

- Failure of SGW/SGSN/MME/IMS Nodes

- Restoration procedures as described in 3GPP TS 23.007 [22]

Editor's Note: It is FFS what the specific impacts of node failures is on the offline charging system.

5.3.5.2.2 Multiple Interfaces for the Same Bearer/Session/Service

The different Overload causes described above, have increased effects on Charging Nodes Overload (CDF) since these Charging Nodes handle multiple interfaces for the same session for a UE.

- In IMS, IMS Nodes combined with a set of AS, may each have an Rf sessions established with a single CDF for a given IMS session.

- In EPC, SGWs and PGW may each have an Rf session with a single CDF for a given IP-CAN bearer.

- For an IMS session over EPC (e.g., VoLTE), the combination of the above IMS and EPC nodes may each have an Rf session with a single CDF.

As noted above, changes associated with a single session trigger multiple Diameter interactions with a single CDF. Extending this to a large number of users in a short period has a multiplicative impact on the CDF.

5.3.5.2.4 Multiple Interfaces for the Same User

A CDF may run offline charging for different services in parallel for the same UE: Voice, data, SMS..., therefore several Rf interfaces may be active at the same time for this purpose.

Some Network Nodes failure may lead to several services being affected by the failure, therefore CDF will face storm of signalling for multiple Rf interfaces at the same time.

5.3.5.2.5 Tariff SwitchTime

Predictable event such as Tariff Switch Time may also be one cause of burst of traffic over Rf interface due to mass simultaneous charging change condition trigger at the time the Tariff switches: this affects all active bearers/sessions and services per user (i.e multiple Rf), and all the users with ongoing Rf sessions.

5.3.5.2.6 Overload of the CTF

One aspect of the Overload to be considered is also Network Node/Network Overload due to interaction with Charging domain.

CDF Failure, after unsuccessful failover mechanism, may cause Network Nodes Overload due to buffering of Accounting data.

5.3.5.3 Impacts

Editor's note: The initial input is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, which would be solved by future company contributions

5.3.5.3.1 Existing Mechanisms used on 3GPP Diameter Charging Interfaces

All these Overload Situations described above causing storm of Traffic over Ro and Rf are currently mainly handled through failure handling procedures based on DIAMETER_TOO_BUSY.

5.3.5.3.1.1 Failure Handling

Sending DIAMETER_TOO_BUSY is one standard possibility for the Server to inform the CTFs that it is overloaded and cannot process any additional request. When receiving such error, CTF behaviour is specified for rejecting new requests (e.g new IMS-session, new IP-CAN bearer/ session) and/or closing ongoing services (e.g. IMS-session, IP-CAN bearer/session) depending on the cases.

1) Online Charging (Ro)

   DIAMETER_TOO_BUSY received by the CTF from the Overloaded server side (i.e. OCS) is processed by the CTF as specified in RFC 3588 and RFC 4006, mainly:

   - For event-based and new session-based requests, attempt sending to an alternate OCF.

   - For requests associated to existing charging sessions, attempt sending to an alternate OCF when the server indicated FAILOVER_SUPPORTED, otherwise follows instructions provided by the server in Credit-Control-Failure-Handling AVP (e.g terminate, continue..).

2) Offline Charging (Rf)

   DIAMETER_TOO_BUSY received by the CTF from the Overloaded server side (i.e CDF) is processed by the CTF as specified in RFC 3588, i.e attempt sending to an alternate CDF. In case backup to alternate CDF is not possible, buffering may be done by the CTF per 3GPP TS 32.299 [21].

   In RFC 3588, an Accounting-Realtime-Required AVP (not used in 3GPP) may be used by a Diameter Server in ACA to control the behavior of the client associated to this DIAMETER_TOO_BUSY, e.g. deliver the service even if records cannot be stored.

5.3.5.3.1.2 Tariff SwitchTime

For Online Charging, a mechanism is defined in 3GPP TS 32.299 [21] in order to avoid mass simultaneous quota refresh request from the CTFs: both usages (before and after Tariff Switch Time), are maintained by the CTF and reported at the next CCR opportunity to the OCS.

5.3.5.3.1.3 Limitations

These mechanisms still lack of guidance for the CTFs to throttle the traffic before the server is Overloaded and cannot process anymore request. Also the CTF is not able to resume dialog with the server when it recovers from Overload.

5.3.5.3.2 Impact of Overload of the CTF

When a Network Node becomes Overloaded due to CTF functions, this may impact all other Interfaces handled by the Node towards the different elements within the Network. The per-Interface Overload mechanim is therefore expected to take place: e.g SIP-overload, GTPc-Overload, Diameter Overload, etc.

5.3.6 Overload of the Online Charging System (OCS)

Editor’s note: The initial input is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, which would be solved by future company contributions.

5.3.6.1 Introduction

The Online Charging System terminates the Ro reference point as defined in 3GPP TS 32.240 [20]. Other 3GPP specifications define additional reference points that are functionally equivalent to the Ro reference point. These are the Gy reference point in the Evolved PS domain and the Wo reference point for WLAN offline charging.

As defined in 3GPP TS 32.240 [20], the following network elements are connected to the OCS by the Ro reference point: P-GW, WLAN, IMS-GWF, MRFC, SIP AS, and Service-NE.

The Ro interface utilizes the Diameter Credit Control Application as defined in 3GPP TS 32.299 [21].

This clause considers different Overload scenarios over Reference Points associated to 3GPP Diameter Credit-Control Application for Online Charging (Ro), and captures existing defined mechanisms intended to prevent them, if any.

5.3.6.2 Causes

5.3.6.2.1 Network causes

The different Network Overload scenarios depicted in 3GPP TR 23.843 [3] (scenario 1 to 5 and 8), are also causes for Overload situations over Ro due to:

- Huge surge in Mobility Management signalling: Flood of Ro sub-sessions signalling on “RAT Change/SGW change” from PGW
- Flood of Attach over E-UTRAN access resulting in flood of default bearer establishment signalling, requests extended beyond the P-GW to OCS (Ro) for associated charging sessions establishment.
- Flood of resources allocations for Mobile Originating services: dedicated bearers (over E-UTRAN) or PDP ctxs (over GSM/UMTS), application sessions, extended beyond the P-GW/GGSN/AF to OCS(Ro), associated charging sessions establishment.
- Flood of signalling for Mobile Terminating services: SMS-MT resulting in flood of signalling over Ro to SMS-SC, and Push-Application with flood of signalling for resources allocation (bearers..) extended beyond the P-GW/ GGSN/AF to OCS(Ro) associated charging sessions establishment.
- Flood of ULI update extended beyond the P-GW/GGSN to OCS(Ro) associated charging sessions update.

NOTE: There is a separate study activity in SA2 for ULI update overload problem.

3GPP Diameter Credit-Control Interfaces Ro may also experience overload when specific Network Nodes fail:

- Failure of SGW/SGSN/MME
- Restoration procedures as described in 3GPP TS 23.007 [22]
- Failure of IMS Nodes

Editor’s Note: It is FFS what the specific impacts of node failures is on the online charging system.

5.3.6.2.2 Multiple Interfaces for the Same Bearer/Session/Service

The different Overload causes described above have increased effects on OCS since these Charging Nodes handle multiple interfaces for the same session for a UE.

For IMS session over E-UTRAN/GPRS/UMTS, IMS (AS or IMS-GWF) and PGW having Ro interface towards the OCS: storm of closing/establishment of IMS sessions and IP CAN bearers/sessions extended to storm of multiple charging Ro sessions closing/establishment to OCS.

5.3.6.2.3 Multiple Interfaces for the Same User

The OCS (owning UE’s account) may run online charging for different services in parallel for the same UE: Voice, data, SMS..., therefore several Ro interfaces may be active at the same time for this purpose.

Some Network Nodes failure may lead to several services being affected by the failure, therefore OCS will face storm of signalling for multiple Ro interfaces at the same time.

5.3.6.2.4 Tariff SwitchTime

Predictable event such as Tariff Switch Time may also be one cause of burst of traffic over Ro interface due to mass simultaneous quota refresh with new Tariff at the time the Tariff switches: this affects all active bearers/sessions and services per user (i.e. multiple Ro), and all the users with ongoing Ro sessions.

5.3.6.2.5 OCS Sy Application

In addition to 3GPP Online Diameter Application, the OCS also processes Sy Application using the same resources (i.e counters) that are used by the Credit-Control Application for the same user and bearers/sessions, therefore OCS overload due to excessive Ro traffic would affect the Sy interface.

5.3.6.2.6 Overload of the CTF

One aspect of the Overload to be considered is also Network Node/Network Overload due to interaction with Charging domain. OCS Failure, after unsuccessful failover mechanism, may cause a storm of closing IP-CAN bearers/sessions/IMS sessions/services inducing a Network overload situation in case this OCS owns a huge number of UEs.

5.3.6.2.7 Simultaneous Online/Offline Sessions

Both online (Ro) and offline (Rf) Charging can be active at the same time for a CTF, therefore Network Nodes embedding such CTF may experience Overload due to simultaneous charging sessions, in addition to other process performed by the Node.

Such Nodes are: PGW, IMS-AS/IMS-GWF, Poc Server, BM-SC...

6 Requirements for Diameter Overload Control

6.1 Introduction

[This section will highlight a set of design considerations and key requirements for 3GPP. An analysis of the gap between 3GPP and IETF requirements will also be provided in this section]

6.2 Design Considerations

6.2.1 Introduction

Particular design considerations for the 3GPP use of Diameter overload control are addressed in the following subclauses.

Editor's Note: The particular points addressed in the hereafter specified subclauses need further confirmation to justify any additional requirement for the overload solution.

6.2.2 Impacts on Existing Applications used in 3GPP

6.2.2.1 Introduction

6.2.2.2 Overload and Applications

A key topic is on how to address the traffic overload associated to a given Diameter application (e.g. Diameter S6a/S6d application) versus traffic for other applications.

Distinction should be made between:

- the overload information;
- the way (algorithm) a node will handle the traffic reduction for a given application.

- It may be application agnostic, e.g. a percentage of reduction applies to the total number of the Diameter messages for this application and messages to be dropped are selected on a random basis. The same way to process the traffic applies to other applications with an overloaded traffic;
- or it may be application aware e.g. a percentage of reduction applies to the total number of the Diameter messages for this application, and messages to be dropped are selected according to an application specific priority order (as discussed in subclause 6.4.5). For instance, a MME may act differently towards its UEs for an overload over S6a than for an overload over SGd for SMS.

For a client, although an agnostic application behaviour may be applied, it may be more relevant to have traffic reduction handling dependent on the application, e.g. in order to:

- minimize the impacts on the delivered service and so improve the user experience;
- or achieve a sustainable traffic reduction possibly at the expense of bad user experience for a limited number of users.

There may not be the need to standardize an application specific order of priority; this may be left to implementations.

When a server is overloaded, its Diameter identity may be given back to the clients and to the Diameter agents in the path, so that traffic may be reduced for this server and not for others. There are a number of other scenarios and potential scopes to which overload control information may apply discussed in IETF Draft draft-ietf-dime-overload-reqs-06 [4]. Additionally, 3GPP specific scenarios will need to be studied.

Considering from a Client's perspective, there is a one to one mapping between Application and server, when a Node serves as a client for multiple Applications in parallel, which is the case for Network Nodes running Charging Applications, the server identity could be sufficient to derive the application (e.g. OCS identity relates to Online Charging Application, i.e. Ro). However it might be worth considering the Client Node to apply different behaviour depending on the server (i.e. Application) experiencing overload, i.e. different whether Charging Interfaces or other Application interfaces (see subclause 6.2.2.4.3).

Editor's note: The initial input of the above paragraph relating to Charging application is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, which would be solved by future company contributions.

6.2.2.3 Complexity

Overload handling may become quite complex as it implies a trade-off between the efficiency to quickly reduce the overload conditions and the accuracy in the handling of traffic reduction to minimize the impacts on the delivered service and on the user experience.

Overcomplicating the solution may represent a danger to the consistent behaviour between the different involved actors and this may create additional problems.

In their work, IETF DiME is analysing the content of a default overload algorithm, which shall be supported by Diameter nodes when no other overload algorithms are available between the Diameter nodes. 3GPP should try to agree the use of this default algorithm for its own usage for which 3GPP could indicate IETF DiME some generic points needed for 3GPP applications. However, specific 3GPP client and application behaviour needs to be investigation so 3GPP's own overload specific algorithms can be provided in addition.

6.2.2.4 3GPP Diameter Charging Applications

Editor's note: The initial input is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, which would be solved by future company contributions.

6.2.2.4.1 3GPP Use of Diameter for Charging

According to 3GPP Charging architecture, as defined in 3GPP TS 32.240 [20], Rf/Ro are generic Reference Points from the Charging Trigger Function (CTF) residing in the different Network Elements (IMS, EPC, AS, SMS-SC…) to the Charging Data Function (CDF)/ Online Charging Function (OCF) respectively.

3GPP Offline Charging application over Rf Reference Point is specified from basic functionalities of IETF Diameter RFC 3588, re-using Diameter accounting.

3GPP Online Charging application over Ro Reference Point is specified as re-using IETF Diameter Credit Control application IETF RFC 4006 with appropriate functionalities.

In addition, when used within a specific domain/subsystem/service (e.g. IMS, EPC...), the Ro/Rf Reference Points are specified with service-context specific behaviors and information.

Therefore, from 3GPP Charging Applications perspective (i.e. Ro/Rf), there may be different levels to be considered for an overload control mechanism to be defined:

- At Diameter protocol level
- At Diameter Application level, i.e. "Accounting Application" and "Credit-Control Application"
- At 3GPP Charging Application level, i.e. Ro/Rf
- At "3GPP-service-Context" level, i.e. PS-Charging, IMS-Charging, SMS-Charging…

Considering that OCS/CDF Overload situations currently rely on "DIAMETER_TOO_BUSY" mechanism, it can be noted the Client side associated behaviour is defined:

- At Diameter Protocol level (IETF RFC 3588), as a protocol error, and used as such by "Accounting Application" and by "3GPP Offline Charging Application (Rf)" level.
- At Credit-Control Application level (IETF RFC 4006), within failure procedures, and used as such by 3GPP Online Charging Application level (Ro).
- At "3GPP-service-Context" level, within service-context dedicated failure procedures for Rf and Ro. As an example PS-Charging, support of failure situations by the PGW for Ro: CCR-I, Tx expiry, Session Failover enabled => sending to alternate OCS.

Based on this, for a new Overload mechanism to be defined, two levels may be worth considering:

- 3GPP Charging Application level, i.e. 3GPP adaptation of "Accounting Application" Rf and "Credit-Control-Application" Ro

  As examples:

  - on Rf: traffic to be throttled on a Node in order to prevent new charging session ACR(start) and interim ACR(Interim).
  - on Ro: traffic to be throttled in order to prevent new charging session (CCR-I).

- "3GPP-service-Context" level (i.e. PS, IMS…) for both Ro and Rf, this one would have a finest granularity and would have the advantage of a finest per-domain tuning allowing a better user experience.

  As examples:

    - for IMS on Rf: traffic to be throttled on an IMS Node in order to prevent interim ACR(Interim) for Re-Invite.
    - for PGW on Ro: traffic to be throttled in order to prevent update existing charging session (CCR-U) for specific APNs.

- "3GPP-service-Context" level (i.e PS, IMS…) for both Ro and Rf, this one would have a finest granularity and would have the advantage of a finest per-domain tuning allowing a better user experience.

  As examples:

  - for IMS on Rf: traffic to be throttled on an IMS Node in order to prevent interim ACR(Interim) for Re-Invite.
  - for PGW on Ro: traffic to be throttled in order to prevent update existing charging session (CCR-U) for specific APNs.

6.2.2.4.2 Server Connected to Multiple Clients

A key point to be considered by the mechanism is that Server for Charging applications may have multiple Clients in parallel: several Rf instances from CDF, and several Ro instances from OCS.

A server may be considered as Overloaded as a whole, but this Overload may be caused by a sub-set of active Charging sessions, resulting in all Charging sessions to be impacted by this overload.

It may be interesting from the server's perspective for the overload mechanism to allow targetting the appropriate charging session(s) so the accurate behaviour can take place on Client Side. This would not be possible to be addressed with a "3GPP Charging Application" level solution, granularity of "3GPP-service-Context" would be needed instead, and would allow to select between e.g. IMS and PS.

As examples:

- CDF is overloaded: IMS traffic to be throttled whereas PGW can continue
- OCS is overloaded: MMS traffic to be throttled whereas MMTel-AS(IMS) can continue

6.2.2.4.3 Client connected Multiple Servers

Another key point to be considered by the mechanism is that a Network Node acting as a Client may run several Diameter Applications in parallel, in addition to Charging applications (Offline Rf and Online Ro).

Although, when a Node serves as a client for multiple Applications, each application is served by a different server, when a server enters in Overload, it may be interesting for the Node to apply a differentiated overload e.g throttling depending on whether the server is a CDF or HSS (e.g. for a S-CSCF).

Granularity of a "Diameter Applications" overload mechanism would be needed for this.

6.2.2.4.4 Intermediate Nodes Consideration

Intermediate Nodes (Diameter Agent) may exist between Client side (i.e. CTF) and Server side (i.e. CDF or OCS).

These Diameter Agents may act as Diameter Relay or Diameter Redirect: as such they are transparent to any Charging Application specific overload mechanism. In addition, they are assumed not to apply any overload mechanism unknown from the Charging Applications.

When acting as Diameter Proxy, the Diameter Agent, as such, may apply local policies, however such policies are expected to be transparent to any Charging Application specific overload mechanism, and also not related to any other overload mechanism unknown from the Charging Applications.

Except for the specific case of a "Diameter credit-control proxy" referred-to in IETF RFC 4006 which supports Diameter Credit-Control Application (statement: "*If Diameter credit-control proxies exist between the credit-control-client and the credit-control server, they MUST advertise the Diameter credit-control application support*"), and would need to be considered for Overload mechanism over Ro.

6.2.3 Extensibility and Interoperability

6.2.3.1 General

The specifications of Diameter interfaces and applications, as any other specification defined in 3GPP, are defined per "Release". A given release is characterized by a finite set of functionalities achieved at a given milestone. Features can be implemented as soon as completion of the release. After freezing of the release (i.e. no new feature can be added after the completion of the release), work related to the addition of new features will be part of on a new release. This work is often started before completion of the current release but new features will only be implemented after completion of the new release.

As it is not expected that all the 3GPP nodes in the networks can be upgraded at the same time to support the latest release, several releases usually coexist in 3GPP networks. To ensure constant interoperability and continuous end-to-end network service, there is therefore a major requirement to ensure backward and onward compatibility between releases in the system, guaranteeing optimal interoperability between nodes supporting the new features backward and the nodes not already upgraded in the network. In this context, a specific effort has been made to apply this compatibility requirement to the design of Diameter applications in 3GPP.

The notion of release is absent from the base Diameter protocol. Extensibility of the base Diameter protocol and Diameter applications is defined in the IETF RFC 6733 [2] and further detailed in the IETF Draft "Diameter Applications Design Guidelines" (IETF Draft draft-ietf-dime-app-design-guide-15 [15]). However, following these guidelines, addition of a new feature to an existing application may often lead to the creation of a new application. From a 3GPP point of view, defining a new application is equivalent to define a new version of an interface protocol and this does not allow interoperability between nodes. To avoid this issue, 3GPP has defined an alternative mechanism that allows further extension of exiting applications without requiring the creation of a new application. This mechanism was initially defined for the Diameter Cx application in the 3GPP TS 29.229 [16] and is now reused in most of the 3GPP defined Diameter applications using the vendor ID of 3GPP (10415). It relies on the special handling of optional AVPs at the application level and advertising the support of new functionalities in the Supported-Features AVP, ensuring interoperability between nodes supporting different features over the same Diameter application.

This specific interoperability aspect in 3GPP networks is an important requirement for any new solution when considering the definition of a new Diameter overload control mechanism. In particular, if it is decided that one key requirement is to enable the support of load/overload information using AVPs exchanged between Diameter clients and servers over any existing Diameter application using the Supported-Features AVP as defined in 3GPP, this would imply that:

- New functionalities related to overload control will have to be introduced as a new feature of the existing application;
- Support of new feature related to overload control will be advertised with the Supported-Features AVP;
- Any new AVP introduced in the existing 3GPP defined Diameter application to convey load/overload information will have to be optional AVPs with the M-bit cleared.

In the context of Diameter overload control over 3GPP interfaces, this specific compatibility mechanism would enable end-to-end capabilities exchange between diameter client and server. However, this mechanism has some limitations, as for example:

- Some Diameter applications used in 3GPP do not support the Supported-Features AVP;
- This mechanism is only specified for dialogue between client and server and the specific use of the Supported-Features AVP by Diameter agents is not described;
- Support of a feature is defined as a Boolean state (supported/not supported) and does not allow indicating different levels of functionality supported without defining new feature;
- This mechanism is 3GPP-specific and the use of this mechanism by non-3GPP Diameter nodes is undefined.

Therefore, if the use of the Supported-Features AVP provides some degrees of flexibility for the extensibility of Diameter applications and end-to-end exchange of capabilities in 3GPP networks, further investigations are needed to assess this mechanism against the specific requirements for support of a generic overload control solution over existing 3GPP Diameter applications. As a result, additional or alternative solutions may have to be defined.

Whatever the solution selected to ensure backward and onward compatibility in 3GPP networks, the Diameter overload control mechanism will have to be designed to be extensible without requiring the definition of new application when introducing future related functionalities. Therefore, the design consideration for extensibility given in IETF RFC 6733 [2] and 3GPP TS 29.229 [16] should also be considered when defining this new mechanism.

6.2.4 Diameter Session Management in 3GPP networks

6.2.4.1 General

In the 3GPP Diameter applications, two main cases exist:

- Diameters sessions established on a per UE basis for a long duration, which may last some hours or days. This is the case for PCC and Charging related Diameter applications or between access entities and 3GPP AAA server for non 3GPP access (see subclauses 5.3.3 and 5.3.4 and 5.3.5).

- Diameter sessions which are implicitly terminated, so with no state maintained in the server. This is the case for HSS Diameter applications

When handling overload conditions or to prevent overload, a solution could be to use load balancing to other servers which are not overloaded, but this may not be so straightforward:

- a user is configured in one HSS, and if this HSS is overloaded, it is not possible to transfer the traffic of the user to another HSS;
- when establishing a new IP CAN bearer/session for a user and related Diameter sessions to a PCRF, an OCS or a 3GPP AAA server, it may be possible to select a PCRF, an OCS or 3GPP AAA server, but when a user has established IP CAN bearer/sessions, they cannot be moved to another server. The network could terminate IP CAN bearers/sessions and select a new PCRF, OCS or AAA server when the UE re-establishes them, but this would impact the user's experience and also cause extra signalling load.

These considerations may not impact the protocol for load and overload but are more related to behaviour of the Diameter nodes, which would therefore be application or session dependent. These examples also raise questions to which extent the node behaviours for overload handling enter into the scope of 3GPP standardisation or may be better left to implementation.

Note that for 3GPP Charging Applications, Node behaviour related to Diameter Charging sessions has a minimum solution described (see chapter 5.3.5.3.1).

Editor's note: The initial input of the above paragraph relating to Charging application is based on a Liaison from 3GPP SA5. Some concerns, not directly related to specific charging issues but to overload mechanism under analysis, have been raised by several companies, that would be solved by future company contributions.

6.2.5 Network Architecture Considerations

6.2.5.1 Introduction

Several scenarios are discussed in IETF Draft draft-ietf-dime-overload-reqs-06 [4]. Additional considerations for 3GPP networks are discussed below.

6.2.5.2 Network Topologies

6.2.5.2.1 Introduction

There are different topologies used in 3GPP networks. Some examples are shown in the following:

Possible topology 1:

As shown in the Figure 6.2.5-1, in Diameter LTE non-roaming case, both the clients (e.g. MME or S4-SGSN or PCEF), and the servers (e.g. HSS or PCRF) are in the home PMN. There may be DA (Diameter Agent) or DRA (Diameter Routing Agent) deployed to support user identity resolution or session correlation for the HSS or the PCRF if there are more than one HSS or PCRF serving the same users. These Diameter Agents may be deployed separately to support load balancing and overload control for the HSS or the PCRF respectively, and it is also possible they are collocated in the deployment.

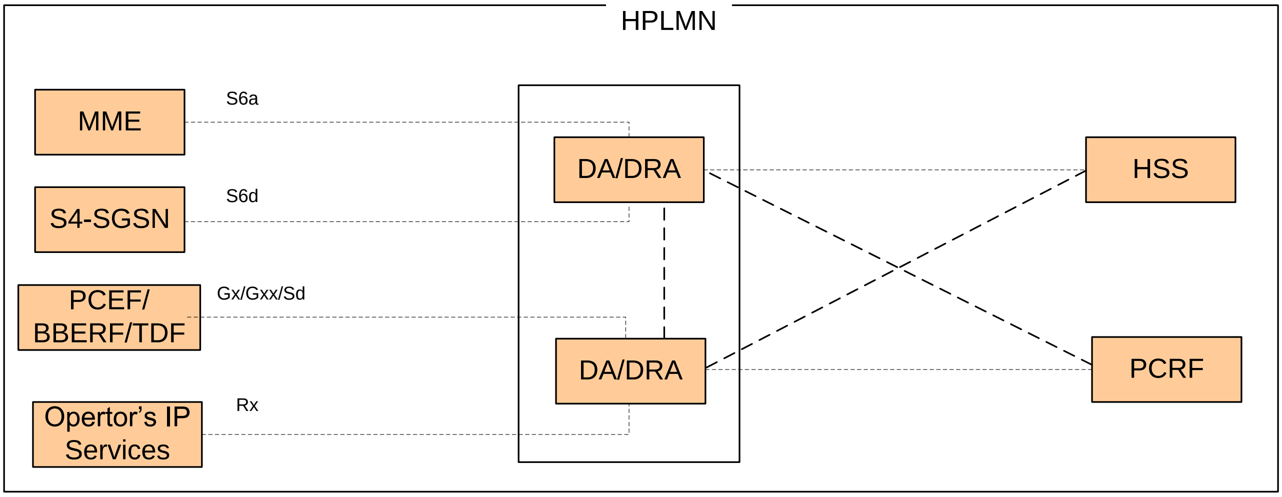

Figure 6.2.5-1: Diameter LTE non-roaming Implementation Architecture

Possible topology 2:

As shown in the figure 6.2.5-2, which is proposed in the GSMA IR88 for LTE roaming guidelines, there are DEA (Diameter Edge Agent) deployed in each PMN for load balancing and topology hiding, which are the Diameter flow point of ingress to the PMN. The DEA may support overload control to protect the HSS and PCRF. Besides the DEA, it is possible to deploy other Diameter Agents or Diameter Routing Agents to support load balancing and overload control for the HSS or the PCRF, as shown in Figure 6.2.5-1 for non-roaming case.

For supporting BBAI, following additionally impacts shall be considered:

- During the S9a/S9a* session establishment procedure, the BPCF acts as the client and the (v)PCRF acts as the server as shown in the Figure 6.2.5-3.
- During the S9a session establishment trigger procedure, the (v)PCRF acts as the client and BPCF acts as the server as shown in the Figure 6.2.5-4.
- During the S9a session establishment procedure, DRA only can select the (v)PCRF which sent the S9a session establishment trigger message.
- During the S9 session establishment trigger procedure, the hPCRF acts as the client and vPCRF acts as the server as shown in the Figure 6.2.5-5.
- If the S9 session establishment procedure is triggered by the hPCRF, the DRA only can select the hPCRF which sent the S9 session establishment trigger message.
- S9/S9a session establishment trigger procedure (i.e. TER/TEA command) does not maintain the state.

Editor's Note: Whether the BPCF supports the Diameter overload control needs to be confirmed by the BBF.

The interconnection between PMN can be implemented in two modes:

- Bilateral mode with direct peer connections between DEAs and no IPX agent in between,
- Transit mode with PMN interconnection by IPX Agents.

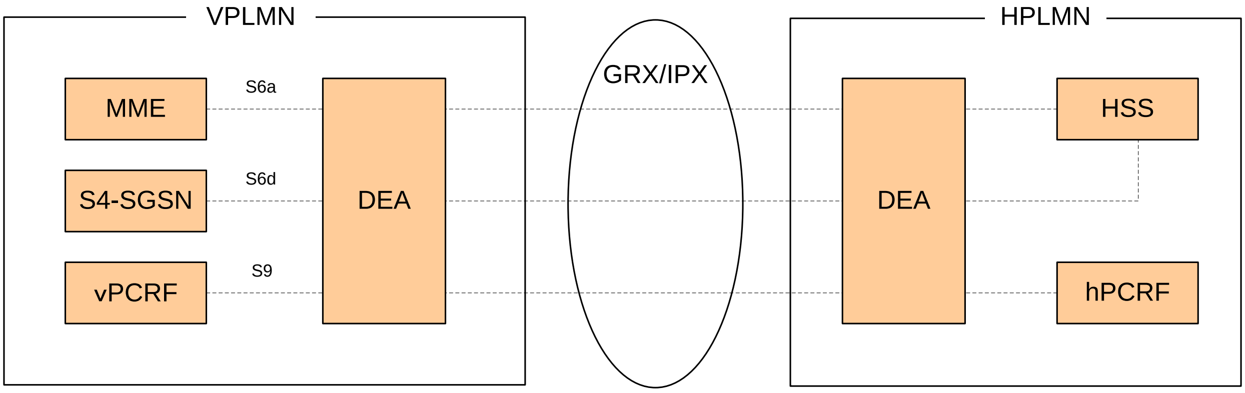

Figure 6.2.5-2: Diameter LTE Roaming Implementation Architecture

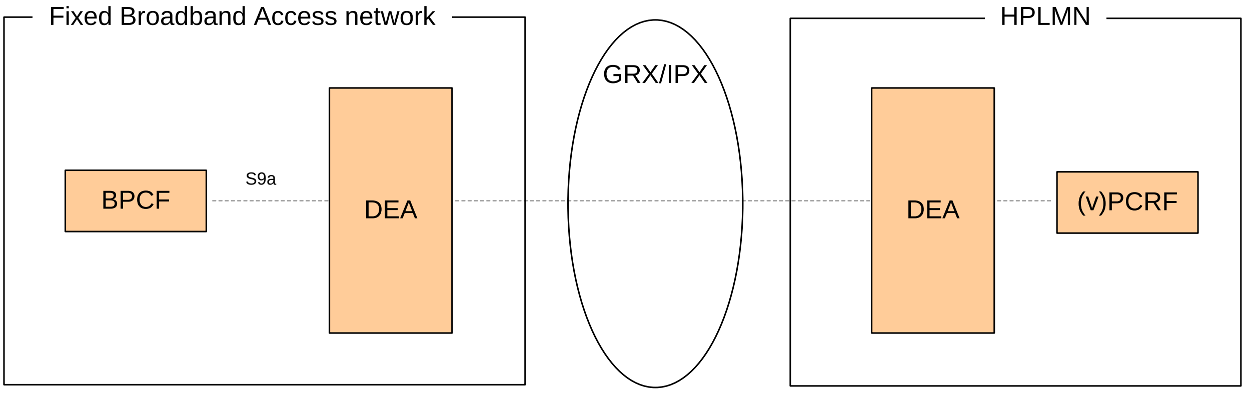

Figure 6.2.5-3: Diameter Implementation Architecture for BBAI

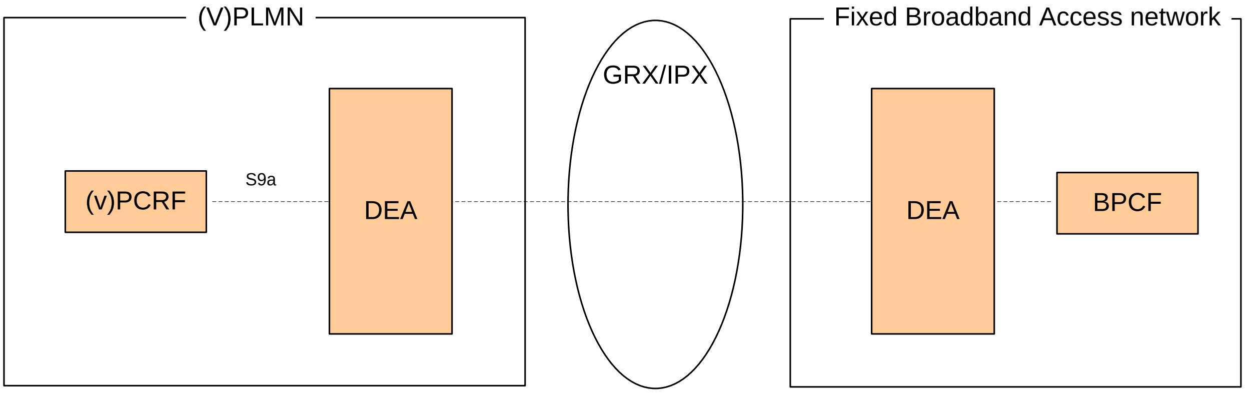

Figure 6.2.5-4: Diameter Implementation Architecture for BBAI during the S9a session trigger procedure

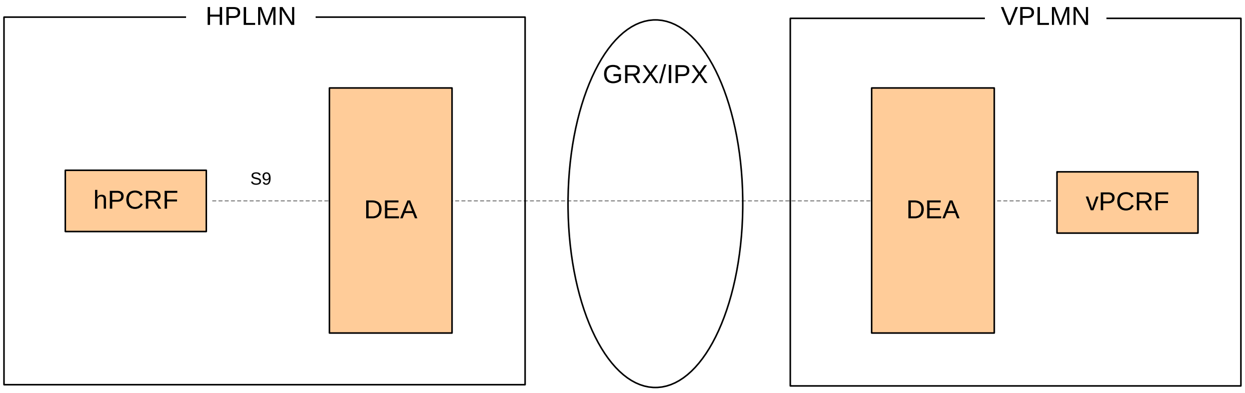

Figure 6.2.5-5: Diameter Roaming Implementation Architecture for BBAI during the S9 session trigger procedure

Possible topology 3:

In the IMS network, as shown in the figure 6.2.5-6, I/S-CSCFs, Application Server and HSS are all located in the same domain. There may be SLF or Diameter Agents deployed for user identity to HSS resolution, which may support load balancing and overload control at the same time.

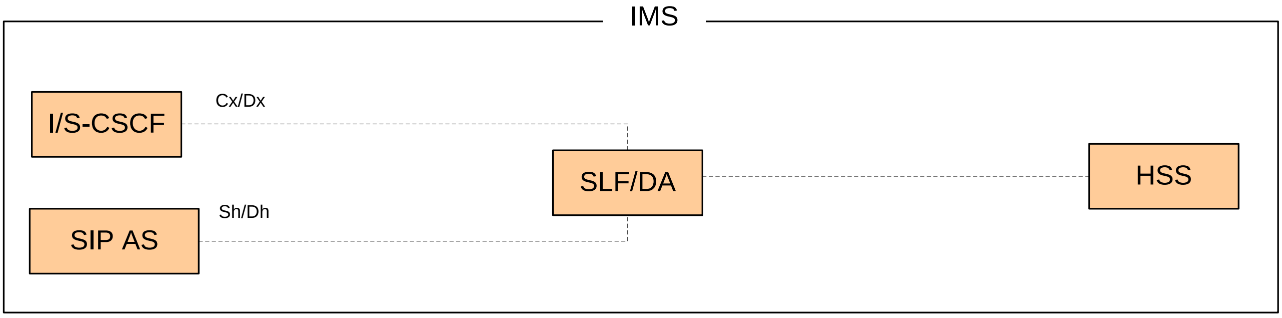

Figure 6.2.5-6: Diameter IMS Implementation Architecture

6.2.5.2.2 Types of Network Topologies

For this study, the following network topologies are identified:

- Topology without DAs:

  Diameter clients and servers are directly connected with SCTP/TCP transport connections. Clients and servers are meshed.

- Topology with DAs handling "no topology hiding":

  Diameter clients and servers are connected through DAs without topology hiding. This topology contains variants, which will be considered the same way, unless otherwise stated:

  - There may be one or several DAs in a path between a client and a server;
  - The DAs may be relay agents, proxy or redirect agents;
  - DAs may be in a meshed network;
  - A client may be connected to one or more DAs;
  - A server may be connected to one or more DAs.

- Topology with DAs handling "topology hiding":

Behind the "hiding topology" wording, the following case is identified:

- The DA is associated with several servers (a server farm) which are equivalent for handling the client requests. Clients do not know the identity of the server that will serve a particular UE. The DA can apply load balancing between the servers.

Editor's note: Topology hiding requires further investigation.

- Other DA topology cases:
  - The case where a DA is associated with several servers which are not equivalent for handling the client requests, and so without a load balancing possibility, and where the client does not know the identity of the server that will serve a UE at least for an initial request (c.f. the user identity to HSS resolution in 3GPP specifications).
  - The case where clients behind a DA do not support the overload control feature. In this case, the DA handles the overload control feature instead of the clients (e.g. in a PLMN interconnection).

6.2.5.2.3 Network Topologies with HSS

The HSS supports Diameter interfaces with a variety of network elements:

- S6a / S6d with MME / SGSN;
- Cx, with I, S-CSCFs;
- Sh with ASs;
- SWx with AAA server;
- Zh with BSF
- S6m / S6n with MTC IWF / MTC AAA;
- SLh with GMLC;
- S6c with SMS central functions.

HSS topologies are various:

- one HSS;
- multiple separated and independent HSSs, which require a user identity to HSS resolution mechanism as the subscription data of a user is stored in only one of the HSSs;
- a distributed HSS, following the UDC architecture, with one UDR and several front-ends which could be geographically distributed, but allowing access to any user subscription data;
- several distributed HSSs, which also require a user identity to HSS resolution mechanism, as the subscription data of a user is stored in only one of the distributed HSSs.

Another characteristic is that the Diameter sessions are implicitly terminated (limited to a request answer exchange).

Load sharing is not applicable between separated and independent HSS, or between distributed HSS.

Load sharing may be applied with distributed HSSs between the different front-ends. It may help to solve the overload of a front end when traffic is not equally balanced between all the front ends. Nevertheless, if the overload is due to the UDR within the UDC architecture, the fact to choose another front-end may not solve the overload.

Regarding the user identity to HSS resolution mechanism, 3GPP specifications describe the possible use of a Redirect or Proxy DAs without excluding other possibilities. They are here recapitulated, as they will have impacts on how overload will be handled according to the different solutions:

- When a redirect server is deployed, a client which has to send a request to a HSS of which it does not know the identity, will only provide the Diameter realm and send its request to the Redirect DA, that will return the identity of the HSS to the client The client then forwards the request with the HSS identity in the Diameter Host AVP.

- When a proxy DA is used, the client which does not know the identity of the HSS, only provides the Diameter realm and sends the request to the proxy DA which will determine the HSS identity and forward the request to the HSS. The client is informed of this HSS identity in the answer it gets from this HSS.

In both cases, for further requests related to the same UEs, the client reuses the HSS identity it has stored.

3GPP specifications do not exclude other implementation dependent resolution mechanisms, without specifying them. For example, a practical one for MME or SGSN, consists in local configured tables mapping an IMSI range to a HSS identity.

6.2.5.2.4 Network Topologies with PCRF

In 3GPP TS 23.203 [10] subclause 7.6.2, it is written:

> "In order to ensure that all Diameter sessions for Gx, S9, Gxa/Gxc, Rx and Sd (when the unsolicited application reporting applies) for a certain IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm, an optional logical "Diameter Routing Agent (DRA)" function is enabled. This resolution mechanism is not required in networks that utilise a single PCRF per Diameter realm."

The fact of deploying several PCRFs introduces the use of a logical DA handling resolution mechanism to find the right PCRF where a UE session is being handled. This mechanism is different to those already explained for the HSS case and has also consequences on the overload handling.

Editor’s note: this subclause has to be reviewed by CT3.

6.2.5.3 Heterogeneous Networks

In a heterogeneous network, the functional entities may support different level of functionalities, thus some of them may not support Diameter overload control, or may not support extra functionalities defined for Diameter overload control in future releases. A mechanism is needed for the entities to exchange their capabilities.

6.2.5.4 Interconnected Networks

[This section should highlight the fact that the overload control mechanism should support roaming scenarios, including the use of IPX as interconnection network between PLMNs.]

6.2.6 Network Performances

[This section should highlight key criteria regarding impacts of overload on network performances (e.g. traffic throughput, processed requests per second, etc.)]

6.3 Diameter Overload Prevention and Detection

6.3.1 Introduction

6.3.2 Explicit Overload Indication

6.3.2.1 Introduction

6.3.2.2 Overload information propagation

An overloaded Diameter node (e.g. HSS), when transferring overload information, requests a reduction of traffic sent by the downstream Diameter nodes.

A key question is where this traffic reduction is performed, as it can be done by intermediate Diameter agents or by the Diameter clients at the source of the traffic.

For 3GPP applications, an approach is to consider that the overload control actions should in general be done by the elements that make the most sense for any given 3GPP applications. The request initiator may have a better knowledge of the application environment to accurately reduce the traffic, e.g. an MME, when informed of an overload from a HSS, it may accurately react towards the UEs and not simply drop messages.

Nevertheless, it does not preclude intermediate nodes to take actions to reduce traffic when relevant, e.g. when the clients are not supporting the overload control mechanism, in case of a notification of an extreme congestion from a Diameter node, or when an intermediate node has sufficient information to handle an overload situation effectively. As a general principle, Diameter agents in front of a server have to "protect" the server.

When the Diameter path between a client and a server supporting an overload control mechanism goes through intermediate Diameter agents which do not support the overload control mechanism, these intermediate nodes should nevertheless relay the overload information even if they don't process or understand it. This has security implications that are much more impactful than existing Diameter end-to-end security concerns as one maliciously constructed message carrying Diameter overload control information could shut down an entire Diameter network. As such, sending overload control information through non-supporting elements shall not be done without adequate protection of the overload control information.

6.3.2.3 Overload status information to be carried

IETF Draft draft-campbell-dime-overload-data-analysis-00 [17] has considerations of information to be included based on existing proposed mechanisms. It is suggested to continue this effort and produce a data model supporting core overload control information such as overload level/status, load level, scoping, and algorithm to be applied. Additional extensions to this base set of information may be needed for specific 3GPP Diameter applications.

6.3.2.4 Transfer of Load/Overload Information

There are several optional ways to transfer the load/overload information:

- Dedicated Diameter messages with a new Diameter application;
- Piggybacking of the load/overload information on existing messages independent of Diameter applications;
- Piggybacking of the load/overload information on existing Diameter applications messages.

With use of a new Diameter application, some points need to be taken into account:

- In the Diameter nodes, e.g. client and server, a correlation between a specific Diameter application which contributes to the load/overload and the new Diameter application for transfer of load/overload information needs to be created, thus the client of the specific Diameter application may be informed of the overload status of the server and start traffic reduction in case overload happens in the server, e.g. prioritize messages to be sent or to be skipped/shedded;
- The server needs to decide the Diameter nodes to which the load/overload information needs to be informed, e.g. to retrieve the identities of the clients of specific Diameter applications;
- Since new messages or commands are introduced, the new Diameter application itself may contribute to the overload.

With use of piggybacking of the overload information on existing messages independent of Diameter applications, e.g. Device-Watchdog-Request/Answer messages which are only exchanged between two peers, one point needs to be taken into account:

- If there are intermediate Diameter Agents being deployed between the client and server for a specific Diameter application, the overload information of the server may not be able to reach the clients, if any of the intermediate Diameter Agents does not support this overload control mechanism and may not be able to forward this information.

With use of piggybacking of the overload information on existing Diameter applications messages, some points need to be taken into account:

- The overload information may be per Diameter application;
- Impacts on existing Diameter applications are expected.

Editor's note: Further investigation of the load/overload transfer mechanism is needed.

6.3.3 Implicit Overload Indication

6.3.3.1 Introduction

IETF Draft draft-ietf-dime-overload-reqs-06 [4] talks about the use of implicit indications and the inadequacy of this approach for large, diverse networks.

However, a Diameter client may receive some overload indications as defined in Diameter base specification IETF RFC 6733 [2] and then it is recommended that the client uses them to mitigate overload situation. This may happen even if involved server and client support the new CN Overload mechanism under definition, but client handling of such indications is even more important when the new mechanism is not supported by either client or server.

At least the following indications may be considered:

- DIAMETER_TOO_BUSY protocol error:

  Diameter base specification IETF RFC 6733 [2] does not suggest that the receipt of a protocol error DIAMETER_TOO_BUSY response should affect future Diameter messages in any way, then it may be relevant for some applications to define the behavior that best mitigate the overload situation, taking into account application specifics, operator deployments.... For example, MME may implement a mitigation procedure based on the rate of received DIAMETER_TOO_BUSY protocol error from HSS.

- Lack of response:

  In case of overload the server may react dropping the requests without any Diameter error message being returned, what may imply retransmissions in the client side, negatively impacting overload. Therefore, for each application, it should be analyzed how to mitigate overload in this situation. For example, the client may consider avoiding retransmissions when a number of messages have not been answered.

6.4 Diameter Node Behavior for Overload Mitigation

6.4.1 Introduction

This section describes the behaviour of the Diameter clients (e.g. MME, PCEF, etc.), Diameter agents (e.g. DRA, DEA, etc.) and Diameter servers (e.g. HSS, PCRF, OCF/CDF) in overload situations with use of explicit or implicit overload indication for overload mitigation.

6.4.2 Load-balancing

6.4.2.1 General

In the case there are more than one server which can serve for the same users and same Diameter application, a logical Diameter Agent may be deployed before the servers for load balancing. Load balancing allows the distribution of the traffic towards different servers in order to even out the traffic handling between them and provide a distributed reliability. The load information transmitted by servers can be used in order to provide a dynamic load balancing.

The Diameter Agent can hide the overload situation of a specific server to other Diameter nodes, including clients, if the requests can be handled by other servers. In this way, to other Diameter nodes, the Diameter Agent aggregates the load of all the servers, and if possible may aggregate the overload severity of all the servers, e.g. if any request from the client can be handled by any of the servers.

The Diameter Agent may allocate load to different servers based on an algorithm or configuration, to avoid the case most or all traffic reaching to one specific server, resulting in overload of the server, while other servers are kept idle. The assumption is that the Diameter Agent can get the load status of each server by some means, e.g. by explicit or implicit indication from the servers. When one or more servers behind a Diameter agent are overloaded, if the remaining servers are not overloaded, the Diameter agent may be able to divert traffic to these servers without propagating the overload information downstream. However, in cases where the servers behind an agent cannot handle the offered load, the Diameter agent may need to propagate the overload information downstream.

When applying load balancing, the Diameter Agent needs to take different Diameter session management in 3GPP networks into account. For a request which has to be handled by a specific server, e.g. a PCC related request for which a PCRF has been selected for the UE or UE’s IP-CAN session involved in a previous procedure and some related Diameter sessions have been established on the PCRF for the UE or UE’s IP-CAN session, the Diameter Routing Agent needs to route the request to the specific server, load balancing cannot be applied. In case overload of the specific server happens, the subsequent request to the specific server cannot be re-routed to other servers.

6.4.3 Message Retransmission

6.4.3.1 General

Message Retransmission is not a means for overload mitigation.

In the case a Diameter Agent for load balancing and overload control is deployed, if one of the server behind the Diameter Agent cannot handle a request due to overload, the Diameter Agent can re-route the current request to an available server. If all the servers cannot handle a request, an error or a response with overload indication has to be returned to the client. The client can retransmit the request to an alternative server if available or retransmit the request later when the overload situation of the servers is improved.

In the case there is no intermediate Diameter Agent for load balancing and overload control deployed before the servers, if the server cannot handle a request, an error or a response with overload indication can be returned to the client. The client can retransmit the request to an alternative server if available or retransmit the request later when the overload situation of the server is improved.

6.4.4 Message Throttling

6.4.4.1 General

Message throttling consists of adapting the rate of messages sent to an overloaded server by relying on the obtained overload information.

Several considerations should be taken into account when doing message throttling:

- On which type of messages the throttling is to be applied with possible priorities:
  - the various request commands used in a Diameter application have not all the same importance, so a priority can be introduced when throttling. MAP allows operators to define priorities among MAP procedures;

  - some Diameter messages may be related to emergency situations or to high priority users and should not be throttled;
  - above behaviours are Diameter application dependent but it remains compatible with the objective to have a mechanism for transferring overload information (AVPs) which can be applied to any Diameter application.
- Where the throttling is to be applied:
  - applying throttling as close to the source as possible can avoid spreading the problem inside the network and using resources of intermediate nodes in the network for signalling that would anyhow be discarded by the overloaded server node;
  - Intermediate nodes may have a broader view of the network, or more specific information about servers, than do clients. In these cases, intermediaries may be the most effective place to apply overload control actions, including throttling e.g. by dropping, rejecting, delaying messages.
  - when taking into account other behaviour regarding which messages to throttle, the Diameter client may be well placed to take appropriate actions, as it may have the knowledge specific to the application that intermediaries may not have. In these cases, the client may most effectively decide which messages to throttle and also to react towards sources of the request traffic e.g. by dropping, rejecting, delaying messages;
  - the client throttling will remain compatible with intermediate DAs which do throttling according to operator policies, taking into account that the traffic delivered to the server should be close to the optimal maximum;
  - when clients do not support the overload control feature, throttling may be applied by an intermediate node supporting the overload control feature.

6.4.4.2 Throttling by Throttling Factor

When a Diameter server reports overload to clients, the Overload Information received by the clients may be converted (e.g. based on a negotiated algorithm) into a throttling factor if not explicitly received. A throttling factor of e.g. 10% indicates that the clients will not send every tenth request message on average that would have otherwise been sent to the server. This means that future traffic will be 10% less than would have been without throttling. It does not necessarily mean that future traffic will be 10% less than past traffic. Traffic can still increase although throttling is in place. Similarly, when a client takes additional actions (e.g. an MME asks the UE not to retry before a certain delay), it may not be possible for the client to calculate how much traffic reduction the additional action causes; the client will simply reject (i.e. not send to the server) every tenth request message it becomes aware of. This may result in less future traffic than expected. Overloaded Diameter Servers are expected to adjust the reported Overload Information when the resulting throttling is too high or too low.

6.4.4.3 Throttling by maximum Rate

When a Diameter server reports overload to clients, the Overload Information received by the clients may be converted (e.g. based on a negotiated algorithm) into a maximum rate if not explicitly received. A maximum rate of e.g. 500 requests per second indicates that the client will reduce future traffic (i.e. treat as many requests as failed) so that the maximum of 500 requests per second sent to the server is not exceeded.

6.4.4.4 Throttling by window of unanswered messages

When a Diameter server reports overload condition to its clients, it may indicate a maximum number of unanswered messages (window) that the client must not exceed. If this window limit is not explicitly received, the client may calculate it base on Overload Information received from the server.

When the number of unanswered messages reaches the specified limit, the client should stop sending further request messages to the server; then, as soon as the server answers some of the pending messages, the client may continue sending further request messages to the server until the window limit is reached again.

It should be noted that, in order for the window mechanism to work properly, those messages that timeout on the client due to being answered very late by the server, or simply discarded, should count as answered by the window mechanism on the client (i.e. they should decrease the number of pending messages to be answered).

The server should be able to indicate to the client that a higher window limit applies as soon as the overload condition disappears. If the server does not support window advertisement, the client should use a locally configured window size.

The server could indicate different window sizes depending on the nature of the overload condition. For instance, if the server detects peaks of traffic coming from only one source, it may apply a bigger window size to that client; on the other hand, if the server gets heavy traffic from many different sources, it may apply a smaller window size to each individual source of overload).

This mechanism may be combined with other criteria, such as application-dependent message priority (see clause 6.4.5). In that case, the client may be able to exceed the window of pending messages but only for those messages with very high priority (e.g. MPS or emergency related traffic). Note that those high-priority messages should still increase the number of unanswered messages (i.e., normal window handling) when the window limit is not reached, and only get a special handling once the window has been filled.

In addition, a more advanced handling of priority messages could be to have separate throttling windows per message category.

6.4.5 Message Prioritization

6.4.5.1 General

Message prioritization applies at the overloaded server or Diameter Agent. In this case, the server/agent needs to decide which requests to process (high priority requests), and which requests to reject, simply discard, or delay (low priority requests).

Message prioritization also applies at the client when performing message throttling.

A first priority case is when a different priority is allocated to the different procedures of a Diameter application. In MAP (cf. 3GPP TS 29.002 [5] subclause 5.1.2), MAP messages can be ignored according to a priority list of application contexts which is defined by the operator. Diameter messages could get different priority depending on the applicable procedure. For example, in PCC, the same Diameter command could be prioritized or not depending on whether it corresponds to either the establishment or the termination of a Gx session.

There are other priority cases to analyze: for example, there is a strong requirement, for some Diameter applications, that a Diameter node applying traffic reduction due to Diameter overload control should be able to provide priority treatment for emergency and high priority users.

Based on regional/national requirements and network operator policy, it shall be possible to exempt MPS (cf. 3GPP TS 22.153 [18]) from Diameter overload controls up to the point where further exemption would cause network instability. Therefore, Diameter messages related to MPS have the highest priority, and are last to be dropped or rejected, when a Diameter node decides it is necessary to apply traffic reduction. Diameter overload controls should not adversely impact MPS.

On the contrary, if messages are related to low priority cases, it is necessary to drop or reject such low priority messages before the messages with a normal priority.

Message prioritization should also take into account its effect on sustainable load reduction; e.g. for the client (MME) not sending S6a CLA or PUR messages may not really result in a sustainable load reduction in the server (HSS) since CLR must then be repeated or non receipt of PUR may result in unnecessary follow up traffic (ISR, CLR) that would not be sent when PUR was successfully performed.

Apart from that, in an application there may be dependencies among different messages from a functional point of view, in a way that several messages have to be received (sometimes even in a specific order) to complete some procedures.

For example, an IMS registration requires multiple HSS interactions (e.g. multiple Cx and Sh messages). In case of overload, if any of these messages is throttled, then the user would not be able to finally register, in fact, success probability would decrease as the congestion increases. Another consequence is that the amount of unnecesary signalling is increased.

Therefore, messages throttling should take into account that some messages are required as a group to achieve a unique result, and for some applications it may be relevant to attempt to throttle initial messages.

Prioritization can be based on other criteria, for example, messages related to existent users (e.g. already registered, attached or with a session already created) could be prioritized, e.g. PCRF would benefit from prioritizing users with a session, being able to keep the consumer quota for subscribers that are already using some services. Even, since multiple network elements may work together (e.g. for user attach or registration), it could be beneficial that this priority applies (i.e. existent users are prioritized) in all related applications.

For Diameter applications where there are requirements for differential handling of messages according to priority, the overload information may need to indicate:

- the kind of requests that the server prioritizes (e.g. from now on, send me only requests for emergency and EMPS users or Update location);
- an overload metric, leaving the source client to decide which kind of messages to actually send to the overloaded node.

Indicating the kind of requests that the server would accept to receive in its current overload status may require the transport of some complex information (e.g. in this overload status an HSS would accept no Purge, any message for eMPS user, only 50% of notifications for normal users, no message at all for normal users,…). An overload metric may allow the support of a simpler protocol.

Editor’s note: 3GPP needs to confirm which kind of overload metric 3GPP is in favor of.

It should then be noted that priority cases handling is not part of the mechanism for transferring the overload information, but is a behavior applied by a node according to the overload conditions it has received. This requires the node to be aware if a message has a high priority or not and this is currently dependent on the Diameter application (e.g. through an AVP indicating a priority, such as the Priority-Session AVP over Cx) or through some internal configuration of a node (e.g. the MME knowing that a user benefits from eMPS).

Message prioritization (per Diameter application) may not need to be standardized and can be left to implementations.

6.4.6 Application Prioritization

6.4.6.1 General

A 3GPP Diameter server (e.g. HSS) may support various Diameter applications (e.g. S6a/d, Cx, Sh, etc.). Typically a successful S6a/d authentication/registration for a UE will be followed by more traffic (S6a/d traffic, Cx traffic, Sh traffic, etc.) for that UE while a dropped S6a/d authentication/registration will not. Consequently, a successful traffic reduction on S6a/d may automatically result in less follow up traffic on other interfaces. It may therefore be worth for the server to prioritize among 3GPP Diameter Applications when requesting load reduction, e.g. request S6a load reduction before requesting Sh load reduction.

Editor's Note: Further study is needed to identify consequences of successful load reduction on one application for other applications.

6.4.7 Overload Mitigation Differentiation per Client

6.4.7.1 General

A 3GPP Diameter server (e.g. HSS) or agent when going into overload may detect that the overload is caused by request flooding from a single client node (e.g. MME), or a limited set of client nodes, while other client nodes are sending reasonably few requests only. It may therefore be worth for the server/agent to differentiate among client nodes when requesting load reduction, e.g. request more reduction from flooding clients, and less reduction or no reduction at all from other clients.

Another use case for the server/agent to differentiate among client nodes is when different client nodes are statically configured in the server/agent with different priorities and less load reduction or no reduction at all is requested from high priority clients.

Overload Mitigation Differentiation per Client is especially useful when throttling by a throttling factor is requested (see clause 6.4.4.2), but should also be considered when throttling by maximum rate (see clause 6.4.4.3) is requested. Otherwise normal/low load generating clients will unfairly suffer from the high load generated by other clients: They need to process the received overload information even when this will not result in load reduction (e.g. because the sending rate is already lower than the maximum rate).

It may be up to server/agent implementations to decide when and whether overload mitigation differentiation per client is used.

6.5 3GPP-IETF Requirements Gap Analysis

6.5.1 Introduction

6.5.2 General 3GPP requirements

6.5.2.1 General

Requirements for Diameter overload in the context of the 3GPP applications using Diameter based interfaces refer to the requirements that are described in IETF Draft draft-ietf-dime-overload-reqs-06 [4].

The mechanism shall allow distinguishing between:

- Load information which allows upstream Diameter nodes to instigate actions to prevent overload such as load balancing. This should allow a more dynamic load balancing than relying on pre-configured weights, especially when a node restarts (and is thus not loaded at all);
- Overload information which, when transferred, allows upstream Diameter nodes to take overload control actions.

3GPP has the following requirements for the mechanism to convey the load/overload information between nodes:

- Be the same whatever the Diameter applications;
- Not to require a redefinition of existing Diameter applications (protocol), even though the application SW will have to be modified;
- Involve Diameter end points and agents where relevant;
- Support different overload scopes, e.g. traffic overload for a node, a realm, an application;
- Negotiate an overload control algorithm with a default;
- Allow some control on which load/overload information may be sent outside a PLMN;
- To allow exchange of load /overload information between nodes that are connected by intermediaries that do not support the mechanism;
- To allow extensibility.

Editor's note: 3GPP acceptance of the above requirements and of the existing requirement list of IETF Draft draft-ietf-dime-overload-reqs-06 [4] is to be confirmed. Pending cases as well as possible new requirements need to be addressed.

6.5.3 Review of IETF Requirements

6.5.3.1 General

The IETF Draft draft-ietf-dime-overload-reqs-06 [4] provides a set of normative requirements for an improved overload control mechanism over Diameter. The aim of this subclause is to review this set of requirements from a 3GPP point of view, considering that 3GPP will be a major consumer of this foreseen overload mechanism.

The list of requirements is ordered as currently defined in the IETF Draft draft-ietf-dime-overload-reqs-06 [4]. And for each requirement, a status (Y/N) is given to indicate whether the requirement is relevant from a 3GPP point of view. When required, further clarifications are provided in the "Comments" column.

Table 6.5.3/1: IETF Requirements Review

#	Existing Requirement	Y/N	Comments
REQ1	The overload control mechanism MUST provide a communication method for Diameter nodes to exchange load and overload information	Y	
REQ2	The mechanism MUST allow Diameter nodes to support overload control regardless of which Diameter applications they support.	Y	This requirement is OK if it aims to recommend that the overload control mechanism must be supported by any node supporting any Diameter application. It must be understood that this requirement does not imply that the overload control mechanism must be "transparent" for application (that would contradict other requirements). There has been concern expressed that this requirement should also ensure that Diameter clients receive sufficient information to behave gracefully. . It is recommended that the following sentence be added: "Diameter clients must be able to use the received load and/or overload information to support graceful behavior during an overload condition. Graceful behavior under overload conditions is best described by REQ 3."
REQ3	The overload control mechanism MUST limit the impact of overload on the overall useful throughput of a Diameter server, even when the incoming load on the network is far in excess of its capacity. The overall useful throughput under load is the ultimate measure of the value of an overload control mechanism	Y	
REQ4	Diameter allows requests to be sent from either side of a connection and either side of a connection may have need to provide its overload status. The mechanism MUST allow each side of a connection to independently inform the other of its overload status	Y	
REQ5	Diameter allows nodes to determine their peers via dynamic discovery or manual configuration. The mechanism MUST work consistently without regard to how peers are determined	N	This requirement is out of scope as it considers procedures that take place before the Diameter connection establishment
REQ6	The mechanism designers SHOULD seek to minimize the amount of new configuration required in order to work. For example, it is better to allow peers to advertise or negotiate support for the mechanism, rather than to require this knowledge to be configured at each node	N	The “SHOULD” is likely too strong here. This requirement is difficult to enforce/verify and for some configurations it could even be better to rely on pre-configured information for instance.
REQ7	The overload control mechanism and any associated default algorithm(s) MUST ensure that the system remains stable. At some point after an overload condition has ended, the mechanism MUST enable capacity to stabilize and become equal to what it would be in the absence of an overload condition. Note that this also requires that the mechanism MUST allow nodes to shed load without introducing non converging oscillations during or after an overload condition.	Y	This requirement is valid whatever the type of environment, i.e. mixed or homogeneous environment.
REQ8	Supporting nodes MUST be able to distinguish current overload information from stale information, and SHOULD make decisions using the most currently available information.	Y	
REQ9	The mechanism MUST function across fully loaded as well as quiescent transport connections. This is partially derived from the requirement for stability in REQ 7.	Y	

#	Existing Requirement	Y/N	Comments
REQ10	Consumers of overload information MUST be able to determine when the overload condition improves or ends.	Y	The consumer of overload information could be also interested to determine when an overload starts. It is also commented that multiple overload degrees must be considered when considering "improvement" of overload condition (cf. REQ 22)
REQ11	The overload control mechanism MUST be able to operate in networks of different sizes	Y	
REQ12	When a single network node fails, goes into overload, or suffers from reduced processing capacity, the mechanism MUST make it possible to limit the impact of this on other nodes in the network. This helps to prevent a small-scale failure from becoming a widespread outage	Y	This requirement is true for one or several nodes
REQ13	The mechanism MUST NOT introduce substantial additional work for node in an overloaded state. For example, a requirement for an overloaded node to send overload information every time it received a new request would introduce substantial work. Existing messaging is likely to have the characteristic of increasing as an overload condition approaches, allowing for the possibility of increased feedback for information piggybacked on it.	Y	It is commented that this requirement seems useless when defining requirements for overload control mechanism.
REQ14	Some scenarios that result in overload involve a rapid increase of traffic with little time between normal levels and overload inducing levels. The mechanism SHOULD provide for rapid feedback when traffic levels increase	Y	
REQ15	The mechanism MUST NOT interfere with the congestion control mechanisms of underlying transport protocols. For example, a mechanism that opened additional TCP connections when the network is congested would reduce the effectiveness of the underlying congestion control mechanisms	Y	
REQ16	The overload control mechanism is likely to be deployed incrementally. The mechanism MUST support a mixed environment where some, but not all, nodes implement it.	Y	
REQ17	In a mixed environment with nodes that support the overload control mechanism and that do not, the mechanism MUST result in at least as much useful throughput as would have resulted if the mechanism were not present. It SHOULD result in less severe congestion in this environment.	Y	
REQ18	In a mixed environment of nodes that support the overload control mechanism and that do not, the mechanism MUST NOT preclude elements that support overload control from treating elements that do not support overload control in a equitable fashion relative to those that do. users and operators of nodes that do not support the mechanism MUST NOT unfairly benefit from the mechanism. The mechanism specification SHOULD provide guidance to implementors for dealing with elements not supporting overload control.	Y	
REQ19	It MUST be possible to use the mechanism between nodes in different realms and in different administrative domains.	Y	
REQ20	Any explicit overload indication MUST be clearly distinguishable from other errors reported via Diameter.	Y	

#	Existing Requirement	Y/N	Comments
REQ21	In cases where a network node fails, is so overloaded that it cannot process messages, or cannot communicate due to a network failure, it may not be able to provide explicit indications of the nature of the failure or its levels of congestion. The mechanism MUST result in at least as much useful throughput as would have resulted if the overload control mechanism was not in place.	Y	It was commented the mechanism should support implicit mechanism to quickly react in real-time to overload situations or network failure and not only "properly function in these cases"
REQ22	The mechanism MUST provide a way for an node to throttle the amount of traffic it receives from an peer node. This throttling SHOULD be graded so that it can be applied gradually as offered load increases. Overload is not a binary state; there may be degrees of overload.	Y	
REQ23	REMOVED	n/a	
REQ24	The mechanism MUST provide sufficient information to enable a load balancing node to divert messages that are rejected or otherwise throttled by an overloaded upstream node to other upstream nodes that are the most likely to have sufficient capacity to process them.	Y	Ok with the principle but it is important to note that load balancing for session-related requests may not be possible.
REQ25	The mechanism MUST provide a mechanism for indicating load levels even when not in an overloaded condition, to assist nodes making decisions to prevent overload conditions from occurring	Y	
REQ26	The base specification for the overload control mechanism SHOULD offer general guidance on which message types might be desirable to send or process over others during times of overload, based on application-specific considerations. For example, it may be more beneficial to process messages for existing sessions ahead of new sessions. Some networks may have a requirement to give priority to requests associated with emergency sessions. Any normative or otherwise detailed definition of the relative priorities of message types during an overload condition will be the responsibility of the application specification.	Y	As it stands, it could be OK. But the requirement could only be "the mechanism SHOULD allow message prioritization in case of overload". The rest is irrelevant as message prioritization will have to be anyway defined per application. Moreover, it is also commented that message prioritization is valid for emergency but also high priority sessions (e.g. MPS) and this should be highlighted in the TR.
REQ27	The mechanism MUST NOT prevent a node from prioritizing requests based on any local policy, so that certain requests are given preferential treatment, given additional retransmission, not throttled, or processed ahead of others	N	Useless as it is impossible to enforce this requirement.
REQ28	The overload control mechanism MUST NOT provide new vulnerabilities to malicious attack, or increase the severity of any existing vulnerabilities. This includes vulnerabilities to DoS and DDoS attacks as well as replay and man-in-the middle attacks. Note that the Diameter base specification [RFC6733] lacks end to end security and this must be considered	Y	
REQ29	REMOVED	n/a	
REQ30	The mechanism MUST NOT depend on being deployed in environments where all Diameter nodes are completely trusted. It SHOULD operate as effectively as possible in environments where other nodes are malicious; this includes preventing malicious nodes from obtaining more than a fair share of service. Note that this does not imply any responsibility on the mechanism to detect, or take countermeasures against, malicious nodes	N	The first sentence could be kept but the rest is useless without stating that E2E security is mandatory to support, that is not the case.
REQ31	It MUST be possible for a supporting node to make authorization decisions about what information will be sent to peer nodes based on the identity of those nodes. This allows a domain administrator who considers the load of their nodes to be sensitive information to restrict access to that information. Of course, in such cases, there is no expectation that the overload control mechanism itself will help prevent overload from that peer node	Y	

#	Existing Requirement	Y/N	Comments
REQ32	The mechanism MUST NOT interfere with any Diameter compliant method that a node may use to protect itself from overload from non-supporting nodes, or from denial of service attacks	Y	
REQ33	There are multiple situations where a Diameter node may be overloaded for some purposes but not others. For example, this can happen to an agent or server that supports multiple applications, or when a server depends on multiple external resources, some of which may become overloaded while others are fully available. The mechanism MUST allow Diameter nodes to indicate overload with sufficient granularity to allow clients to take action based on the overloaded resources without unreasonably forcing available capacity to go unused. The mechanism MUST support specification of overload information with granularities of at least "Diameter node", "realm", and "Diameter application", and MUST allow extensibility for others to be added in the future	Y	The extensibility could become a "MUST" when considering the solution to deploy in 3GPP environment.
REQ34	The mechanism MUST provide a method for extending the information communicated and the algorithms used for overload control	Y	
REQ35	The mechanism SHOULD provide a method for exchanging overload and load information between elements that are connected by intermediaries that do not support the mechanism	Y	The "SHOULD" has to seen as a strong recommendation for solution design and a key criteria for selection of the preferred solution.
REQ36	The mechanism MUST provide a default algorithm that is mandatory to implement	Y	

Editor's note: 3GPP acceptance of the above requirements and of the existing requirement list of IETF Draft draft-ietf-dime-overload-reqs-06 [4] is to be confirmed. Pending cases as well as possible new requirements need to be addressed.

7 Solutions for Diameter overload control

7.1 Introduction

This section presents and compares the different solutions proposed to fulfill the requirements for Diameter overload control defined in IETF Draft draft-ietf-dime-overload-reqs-06 [4]. The evaluation will take also the requirements specific to the 3GPP networks. As an output of this analysis, a solution should be selected as preferred solution for implementation of a Diameter overload control mechanism in 3GPP networks.

7.2 Solution 1: MDOC

7.2.1 Solution overview

"The Mechanism for Diameter Overload Control" (MDOC) (IETF Draft draft-roach-dime-overload-ctrl-03 [23]) defines a mechanism for communicating the load and overload information among Diameter nodes on a hop-by-hop basis.

Because this mechanism is meant to be used on a hop-by-hop basis, load and overload information is exchanged only between adjacent nodes. This means that any Diameter agent that forwards a Diameter message must remove any load/overload information received from the previous hop, act upon it as necessary/possible and aggregate their own load/overload information to the existing one in the message before forwarding to the next hop.

The key information transmitted between adjacent Diameter peers is the current server load as well as an indication of overload state and severity (overload information). Both information parts are conveyed as a new Grouped AVP (Load-Info AVP), included into CER/CEA, DWR/DWA and any Diameter messages in which the Grouped AVP Load-Info can be included.

The Load-Info AVP is defined as follow:

```
< Load-Info > ::= < AVP Header: 1600 >
                  < Overload-Metric >
                  * { Overload-Info-Scope }
                  [ Supported-Scopes ]
                  * [ Overload-Algorithm ]
                  [ Period-Of-Validity ]
                  [ Session-Group ]
                  [ Load ]
                  * [ AVP ]
```

The Overload-Metric AVP is used as input to the load mitigation algorithm. Its definition and interpretation is left up to each individual algorithm, with the exception that an Overload-Metric of "0" always indicates that the node is not in overload (that is, no load abatement procedures are in effect) for the indicated scope.

The Overload-Info-Scope AVP is used to indicate to which scope the Overload-Metric applies. The indication of scopes for overload information allows a node to indicate a subset of requests to which overload information is to be applied. Seven scopes are defined in the IETF draft but only "Connection" scope is mandatory to implement for all the nodes supporting this overload control mechanism.

The Supported-Scopes AVP contains a bitmap that indicates the scope(s) that a given node can receive on the connection. This AVP is only used in CER/CEA.

The Overload-Algorithm AVP may be used only in CER/CEA to negotiate the algorithm that will be used for load abatement. If absent of this AVP in CER/CEA, the default Overload Algorithm (Loss) is used.

The Period-Of-Validity AVP is used to indicate the length of time, in seconds, the Overload-Metric is to be considered valid (unless overridden by a subsequent Overload-Metric in the same scope).

The Session-Group AVP is used to assign a new session to the session group that it names. This AVP may appear only once, in the answer to a session-creating request. This AVP will may allow to apply the overload algorithm to a group of session if the "Session-Group" scope is applied.

The Load AVP is used to indicate the load level of the scope in which it appears. The load level is indicated as a linear scale, from 0 (least loaded) to 65535 (most loaded).

The IETF draft also defines a default overload algorithm for shedding traffic under overload circumstances. Identified by the indicator "Loss" (1) in Overload-Algorithm AVP and meant to be implemented by all the Diameter nodes supporting the overload control mechanism, this algorithm allows a Diameter peer to ask its peers to reduce the number of requests they would ordinarily send by a specified percentage. In this algorithm, a range from 0 to 100 is used as possible values of Overload-Metric AVP to indicate the requested percentage of traffic reduction. For example, if a peer requests to another peer a reduction of 10% of the traffic currently sent, then that peer will redirect, reject, or treat as failed, 10% of the traffic that would have otherwise been sent to this Diameter node. When the requests have to be treated as failed by a Diameter agent, the Diameter agent indicates to the peer who originated the request by sending a new error code "DIAMETER_PEER_IN_OVERLOAD" in the response.

The design of the mechanism described in this document allows for the definition of alternate load abatement algorithms as well and the algorithm to apply is negotiated during the capabilities exchange phase between the peer.

7.3 Solution 2: DOCA

7.3.1 Solution Overview

"The Diameter Overload Control Application (DOCA)" (IETF Draft draft-korhonen-dime-ovl-01 [24]) describes a new application, the Diameter Overload Control Application (DOCA), to convey overload information between Diameter nodes.

This new session-stateless Diameter application defines a command pair, DOCA-Report-Request/Answer (DRR/DRA), and a set of AVPs to convey the related overload control information. Any the DOCA capable Diameter node can initiate a DOCA-Report-Request at any given time. The receiver of the request acknowledges with a DOCA-Report-Answer and includes the Result-Code AVP indicating whether it could honor the action/report in the request. The DOCA-Report-Answer can also piggyback overload control information related the node sending the answer.

A Diameter proxy supporting the DOCA application can inspect the DOCA related AVPs in the DRR/DRA message pair and, depending on the value of the OC-Scope AVP, it can inject its own information in the messages.

The DOCA-Report-Request (DRR) message is used to report overload condition information. The message can be originated as a result of emerging overload condition or as a periodic unsolicited report.

The DOCA-Report-Answer (DRA) message is used as an acknowledge response to the DOCA-Report-Request. The message can also piggyback overload condition information in order to avoid unnecessary DOCA-Report-Request messages to the reverse direction.

The IETF draft defines the following AVPs related to the overload control mechanism:

The OC-Scope AVP indicates in a bitmask the scope where and concerning what the overload control information contained in OC-Information can be injected. The following scopes are supported:

- "Host": OC-Information AVP concerns only a single host within a realm (which internally MAY represent of pool).
- "Realm": OC-Information AVP concerns a realm. No specific hosts are identified.
- "Only origin realm": OC-Information AVP can only be included by a Diameter node on the path that has the same Origin-Realm as the DOCA client.
- "Application information": OC-Information AVP contains application related information (the OC-Applications AVP).
- "Node utilization information": OC-Information AVP contains node wide load related information (the OC-Utilization AVP).
- "Application priorities": OC-Information AVP contains priority information (the OC-Priority AVP) so when the overload condition is on, Diameter nodes are able to prioritize between different applications, for example, when dropping or throttling messages.

The OC-Algorithm AVP, used only in the DRR message, is a bitmask that indicates the supported algorithms to mitigate the overload condition. The following algorithms are supported:

- "Drop": Messages are plain dropped. It is RECOMMENDED to drop messages selectively based, for example, on application priorities. This is the default algorithm.
- "Throttle": The message sending rate is according to the OC-Sending-Rate AVP.
- "Prioritize": Apply priorities among applications and the other used means for holding traffic.

The OC-Action AVP indicates three different states: the start, the end or the update of the overload condition. The interim is the default value and can be sent during the overload condition or during the normal condition.

The OC-Tocl AVP, used only in the DRR message, indicates in a DRR a timer in milliseconds that defines the requested interval for sending periodic DOCA-Report-Request messages with the OC-Action AVP set to 'Interim'. The value of zero (0) means no periodic DOCA-Report-Request messages are sent or desired. The default value is 120000.

The OC-Applications AVP is a Grouped AVP that contains a list of Application-IDs of interest and meant to be used during the initialization state to agree on the common set of supported applications of monitoring interest when found in the DOCA-Report-Request/Answer command main level. When used within the OC-Information AVP, the OC-Applications AVP identifies those applications the overload information concerns.

The OC-Information AVP is a Grouped AVP that contains a set AVPs that identify the source of the overload control information, the overload information itself and which applications the information concerns.

7.4 Solution x

[Brief description of solution X]

7.5 Comparison

[Comparison of the solutions based on set of objective criteria and 3GPP requirements]

7.6 Conclusions

8 Conclusions and Recommendations

8.1 Introduction

8.2 Solution for Diameter Overload Control in 3GPP Networks

[This section should indicate how the selected overload mechanism is foreseen to be implemented in 3GPP networks. For instance, if possible options are available in the standard mechanism, a recommendation for 3GPP can be provided.]

8.3 Impacts on Existing 3GPP Specifications

[Based on the selected mechanism, this section should provide an overview of the foreseen impacts on existing 3GPP specifications. The required changes will not be detailed in this TR.]

8.3 Recommendations for New Diameter Applications

[This section should provide generic guidelines regarding the support of overload control in new Diameter applications defined in 3GPP.]

Annex A: PCRF Overload Impacts per Interface

This annex describes the impact of the PCRF overload on different interfaces. It is meant to serve as a complement to clause 5.3.3.

A.1 Impacts due to the overload of the PCRF

A.1.1 Impacts when a DRA is not deployed

A.1.1.1 Impacts on the Gx interface

The following requests may be impacted:

- CCR with CC-Request-Type set to INITIAL_REQUEST: these requests are used to set up an IP-CAN session.
    - If the PCRF explicitly rejects such a request with DIAMETER_TOO_BUSY, the PCEF may either:
        - Send the request to another PCRF if possible, i.e. if the PCEF is connected to multiple PCRFs and the scenario/configuration allows it. This isn't possible for example if the corresponding Gxx session has already been established with the "busy" PCRF as sending the Gx request to a different PCRF will result in Gx and Gxx sessions not being linked, causing the gateway control session to not get the proper QoS rules and as such, potentially impacting the end user's traffic.
        - Reject the IP-CAN session establishment towards the UE if the above is not possible. This would cause the PDN connection establishment to fail and potentially cause the UE to retry, causing additional load on the network.
        - Apply local policy without rejecting the PDN connection establishment. This would not cause further load on the network; however, the services provided to the UE could be limited and potentially have charging impacts. In this case, the PCEF could re-attempt the Gx session establishment at a later point when the PCRF is deemed not busy (see section 5.2.3 for limitations related to this procedure).
    - If the PCRF drops the request, the PCEF will eventually time out the CCR transaction and may behave as follows:
        - Retry the request at a later time; this would cause delays in the PDN connection setup. If the PCRF is still busy then and drops the request, the PCEF will need to resort to one of the options specified above in the handling of the DIAMTER_TOO_BUSY result-code.
        - Apply one of the behaviours defined in the DIAMETER_TOO_BUSY handling.
    - If the connection to the PCRF is dropped or unavailable, the PCEF may behave as follows:
        - Send the request to an alternate PCRF if applicable and possible given the scenario/configuration.
        - Send/Retry the request when the connection to the PCRF is restored. This option should be only used if the above option isn't possible and the time budget is not exceeded as explained in 5.3.3.2.3.
        - Reject the IP-CAN session establishment as specified in the DIAMETER_TOO_BUSY handling.
        - Apply local policy without rejecting the PDN connection establishment.
- CCR update requests: these requests are used to update an IP-CAN session. Such updates can be due to various reasons, e.g. RAT change, location update, request of bearer modification, , usage reporting, etc. In this case, update requests cannot be sent to another PCRF.
    - If the PCRF explicitly rejects such a request with DIAMETER_TOO_BUSY, the PCEF may either:

        - Reject the PDN connection update procedure. This can have a number of impacts, depending on the reason for the update. For example, a RAT change could cause the handoff to the new access to fail. If the target access is the only one available, this could cause service interruption.
        - Deactivate the PDN connection. Although this is a drastic measure, if the PCEF can communicate with multiple PCRFs, it may allow the PDN connection re-establishment to be sent to an available and non-busy PCRF, as such potentially restoring service to the end user.
        - Apply local policy without rejecting the PDN connection update. This has similar implications as the ones specified for the IP-CAN session establishment case. Additionally, this could have impact on other existing sessions, such as Rx for instance. If the IP-CAN session update was related to information relevant to the Rx session (e.g. associated rule failure, loss of bearer, etc.), the AF would not be informed of such events.
    - If the PCRF drops the request, the PCEF will eventually time out the CCR transaction and may behave as follows;
        - Retry the request, which would cause further load on the busy PCRF.
        - Apply one of the behaviours specified for the DIAMETER_TOO_BUSY case.
    - If the connection to the PCRF is dropped or unavailable, the PCEF may behave as follows:
        - Send/Retry the request when the connection to the PCRF is restored.
        - Apply one of the behaviours specified for the DIAMETER_TOO_BUSY case.
- CCR termination requests: these requests are used to terminate an IP-CAN session. The PCEF should either re-attempt the Gx session termination at a later time or simply clean up its session context locally. The impacts in case the session isn't properly cleaned up at the PCRF is that other related sessions (e.g. Rx, S9, etc.) will not be properly aborted or updated.

A.1.1.2 Impacts on the Gxx interface

The following Gxx requests may be impacted:

- CCR with CC-Request-Type set to INITIAL_REQUEST: these requests are used to set up a gateway control session. This request can be initiated based on different events: PDN connection establishment or BBERF relocation for case 2b (as defined in 3GPP TS 29.213 [12]) and local IP address assignment for case 2a (as defined in 3GPP TS 29.213 [12]).
    - If the PCRF explicitly rejects such a request with DIAMETER_TOO_BUSY, the BBERF may behave as follows:
        - Send the request to a different PCRF in case 2a if such PCRF is available, or in case 2b if this request was due to an IP-CAN session establishment, assuming the scenario (non-roaming)/configuration allows for it.
        - In case 2b and BBERF relocation, sending the request to an alternate PCRF is not possible as the Gxx session has to be linked with the previously set up Gx session. As such, the handling of this case is similar to a session update where the BBERF cannot choose another PCRF to handle the request.
        - Reject the triggering request to establish the gateway control session. This can lead to the PDN connection establishment to fail in case 2b or for the UE not to potentially not be able to attach in case 2a.
        - Apply local policies and accept the request. The implications here are that the Gxx and corresponding Gx session will not be linked, causing a potential mismatch in QoS rules.
    - If the PCRF drops the request or the connection or the connection isn't available, in addition to the above options, the BBERF can retry the request again to the same PCRF (when and if the connection is available), which could cause further load on the PCRF and a delay in the gateway control session establishment.
- CCR update requests: these requests are used to update a gateway control session. Such updates are usually sent due to either a resource modification request or a QoS rule failure notification. Such requests cannot be sent to alternate PCRFs; the impact and possible behaviors of the BBERF are similar to the Gx case and PCEF.

- CCR termination requests: these requests are used to terminate a gateway control session. The behaviour of the BBERF is similar to the PCEF handling in the case of Gx.

A.1.1.3 Impacts on the Rx interface

Rx sessions are dependent on the existence of the corresponding Gx session. As such, the impact of PCRF overload on Rx is different from the other applications.

The following are Rx requests initiated by an AF:

- AAR to setup a session: These requests are sent to either perform the initial provisioning of session information related to media flows or to establish a session associated with the AF signalling session.
    - If the PCRF explicitly rejects such a request with DIAMETER_TOO_BUSY, the AF may behave as follows:
        - Reject the corresponding procedure that triggered the Rx AAR. Depending on the AF and procedure, the impact would vary. For example, in the case of IMS and Rx AAR triggered by a SIP REGISTER, rejecting the SIP registration will not allow the user to establish or receive calls. On the other hand, if the Rx AAR is triggered by a SIP INVITE, rejecting it would impact the call being established. In both cases, the likelihood is that the UE will re-attempt the failed procedure and as such, further contributing to the PCRF and potentially P-CSCF/SIP load.
        - Allow the AF procedure to complete and apply local policy. The drawback in this approach is that it could have charging and QoS impacts. The AF could in addition retry the Rx request at a later time.
    - If the PCRF drops the AAR or if the connection is dropped/not available, the AF can retry the request at a later time. In this case, the AF procedure can be allowed (e.g. in the case of IMS, the SIP procedure), so no delay is incurred while waiting to retry the Rx request. Eventually, if enough retries fail, the AF would need to resort to one of the options above.
- AAR to update an existing session. The AF may behave similarly to session establishment. The impact on the UE may differ here as rejecting a session modification may not be as impactful as rejecting a session establishment. For example, in the case of IMS, if a SIP re-INVITE is sent to add video to an audio only call, the video may not be added, but the audio call can continue without being impacted.
- STR to terminate a session. The AF may behave similarly to the PCEF on session termination, i.e. clean up session state locally or retry the request at a later time. The impact of simply cleaning up state locally is that the corresponding Gx session would end up with “stale” PCC rules, possibly causing dedicated resources to be held up in the RAN and possibly having charging impacts.

A.1.1.4 Impacts on the S9 interface

A.1.1.4.1 Introduction

The S9 interface is used between a V-PCRF and an H-PCRF. It carries both S9 and Rx application messages. There are different cases that need to be analysed:

- Overload of the V-PCRF
- Overload of the H-PCRF

Additionally, we need to consider the home routed case as well as the visited access case.

One of the main differences with the non-roaming case is that S9 is an inter-operator interface and as such, corresponding traffic goes through IPX and traverses multiple Diameter agents (e.g. DEA, etc.). Additionally, operators typically hide their internal topology from other operators. As such, if the H/V-PCRF is overloaded and responds back to an S9 request with DIAMETER_TOO_BUSY, the error the V/H-PCRF will receive may be DIAMETER_TOO_BUSY or other errors as intermediaries may modify the original result code especially that the responding PCRF’s identity is not typically included in the answer seen by the requesting PCRF. As such, properly handling the overload of the H/V-PCRF with the current standard procedures will be challenging.

A.1.1.4.2 Overload of the H-PCRF

In the home routed case, all the interfaces go to the H-PCRF except for Gxx which terminates on the V-PCRF in case 2a and case 2b as defined in 3GPP TS 29.213 [12]. If the H-PCRF is overloaded, the impact on Gx, Sd, Rx is similar to the non-roaming case. The impact on S9 is similar to the impact on Gxx in the non-roaming case. Specifically because S9 in this case is only used to convey gateway control session related procedures. Note that although the impact to S9 is similar to Gxx, it does differ due to the multitude of agents and IPX it needs to traverse as explained in 5.3.3.2.3.a.d.

In the visited access case, all the interfaces go to the V-PCRF except for certain cases where the AF is in the H-PLMN, in which case Rx goes to the H-PCRF. In this case, the impact of the H-PCRF overload on the V-PCRF is similar to the impact of the PCRF overload on the PCEF in the non-roaming case. The V-PCRF may be unable to request PCC rules from the H-PCRF or report events happening in the V-PLMN. In these cases, the V-PCRF would need to act based on operator policies and roaming agreements and either reject the requests that triggered S9 (e.g. Gx, Gxx) or respond successfully back to its clients if the scenario and roaming agreements allow it.

A.1.1.4.3 Overload of the V-PCRF

The V-PCRF acts as the client over the S9 interface. However, it acts as a server to locally connected clients (e.g. BBERF). From the H-PCRF perspective, the V-PCRF acts as its point of contact to provision decision rules and information on the corresponding BBERF/PCEF/TDF in the V-PLMN. With regards to Rx messages, the V-PCRF may act as a proxy or as a client/server when sending these messages over the S9 reference point. When the V-PCRF is overloaded, its impacts to the H-PCRF are similar to impacts of an overloaded DRA. The impact of the V-PCRF overload to other entities (e.g. BBERF) are similar to the overload of a PCRF in the non-roaming case.

A.1.1.5 Impacts on the Sd interface

The Sd interface can be used in two ways: solicited and unsolicited. The impacts of overload of the PCRF vary depending on the mode and procedure.

The following messages may be impacted:

- CCR with CC-Request-Type set to INITIAL_REQUEST: this request is sent by the TDF to establish an Sd session with the PCRF in the unsolicited reporting case. Given that the Sd session has to be bound to an existing Gx session, the TDF cannot send this request to a different PCRF. The impact on the TDF in this case is that the session establishment will have to be delayed and retried at a later time. The impact is simply that the PCRF isn't informed of the potentially detected applications on the TDF until the session establishment can succeed.

- CCR with CC-Request-Type set to UPDATE_REQUEST: this request is sent by the TDF for various reasons, including application detection, usage reporting, etc. Whether the PCRF responds with DIAMETER_TOO_BUSY or drops the request, the TDF should retry the request later if it's still applicable (e.g. application that was detected is still running). This is especially critical in cases of usage reporting as their impacts go beyond the IP-CAN session.

- CCR with CC-Request-Type set to TERMINATION_REQUEST: this request is initiated by the TDF based on a request from the PCRF to release the session. In this case, if accumulated usage has not been reported to the PCRF, the TDF should attempt to retry the request at a later time. Otherwise, the TDF can clean up its session context locally.

A.2 Impacts when a DRA is deployed

When a DRA is deployed between the clients and the PCRF, the impact of PCRF overload may be different than the deployment with no DRA. In this section, we will only analyse additional impacts due to the DRA.

A DRA can be deployed in three different modes as defined in 3GPP TS 29.213 [12]:

- Proxy agent always in the path, also referred to as PA1

- Proxy agent in the path on session establishment and certain session termination messages, also referred to as PA2

- Redirect agent

The redirect DRA is not in the path of messages from/to the PCRF. As such, it cannot intercept error responses, realize that requests were dropped, connections lost, etc. For this reason, the only DRA modes that are analysed in this section are PA1 and PA2.

A.2.1 Impacts on the Gx interface

Below are the impacts of the PCRF overload on Gx when a DRA is deployed:

- CCR with CC-Request-Type set to INITIAL_REQUEST. If the PCRF returns a DIAMETER_TOO_BUSY response and if the scenario/configuration allows the DRA to select another PCRF, the DRA can select another PCRF that is available and not busy. In the case where the request is dropped by the PCRF, the DRA may be able to retry the request to the same PCRF or select an alternate PCRF if the scenario/configuration allows it. Similarly, when the connection to the PCRF is dropped/unavailable, the DRA may be able to select an alternate PCRF if applicable to send/retry the request when the connection is restored. If the DRA is unable to select a PCRF to successfully process the request, it should respond back to the PCEF with an error. The error should be carefully chosen to properly convey the error to the PCEF without causing unnecessary retransmissions (e.g. DIAMETER_UNABLE_TO_DELIVER when the PCRF is busy) or misrepresentations (e.g. sending DIAMETER_TOO_BUSY when the DRA itself is not busy and the request was not directed to a specific PCRF). There aren't very appropriate result codes that are currently available in the IETF or 3GPP specs for this case.

- CCR with CC-Request-Type set to UPDATE_REQUEST. The DRA cannot send this request to other PCRFs. As such, it can retry the request before responding to the client or simply respond back to the client with an error. If the PCRF had returned a DIAMETER_TOO_BUSY, the DRA may relay this error code. Otherwise, if the request was dropped, the DRA may respond with DIAMETER_UNABLE_TO_DELIVER.

- CCR with CC-Request-Type set to TERMINATION_REQUEST. The DRA can:

  - Respond successfully to the PCEF and retry the termination request to the overloaded PCRF later.

  - Alternatively update its binding by removing the corresponding session. This could impact all associated sessions (e.g. Rx) as the DRA may not be able to route such requests to the corresponding PCRF. In this case, the DRA can respond back to the PCEF either successfully or with a permanent error to avoid further retransmissions of the termination request from the client.

A.2.2 Impacts on the Gxx interface

The impacts when a DRA is deployed are similar to the Gx interface.

A.2.3 Impacts on the Rx interface

Rx requests have to be routed to the same PCRF that handled the corresponding Gx session. As such, if that PCRF is overloaded, the DRA will not be able to re-route the requests to other PCRFs. As such, its behaviour with regards to Rx requests will be similar to the handling of Gx update messages.

A.2.4 Impacts on the S9 interface

In the home routed case in cases 2a and 2b, the impact on S9 based on H-PCRF overload is similar to impacts on Gxx in the non-roaming case. Conversely, the impact on S9 based on V-PCRF overload is similar to the overload of a DRA in the non-roaming case as explained in clause 5.3.3.2.3.a.d.b.

A.2.5 Impacts on the Sd interface

The impact is similar to Rx as Sd requests need to be sent to the same PCRF that handled the corresponding Gx session.

Annex <X>:Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2013-02	C4#60	C4-130420			TR Skeleton		0.0.0
2013-02	C4#60	C4-130223			Scope and Introduction Sections	0.0.0	0.1.0
2013-02	C4#60	C4-130419			Diameter Overload requirements and study points	0.0.0	0.1.0
2013-04	C4#60ah	C4-130491			Limitations of Existing Mechanisms in Diameter for Overload Control	0.1.0	0.2.0
2013-04	C4#60ah	C4-130505			Overload scenarios	0.1.0	0.2.0
2013-04	C4#60ah	C4-130506			PCC specific considerations for overload control	0.1.0	0.2.0
2013-04	C4#60ah	C4-130507			Clarifications and Updates to TR 29.809	0.1.0	0.2.0
2013-04	C4#60ah	C4-130477			3GPP-IETF Requirements Gap Analysis	0.1.0	0.2.0
2013-04	C4#60ah	C4-130494			Extensibility and Interoperability	0.1.0	0.2.0
2013-04	C4#60ah	C4-130495			Application Prioritization	0.1.0	0.2.0
2013-04	C4#60ah	C4-130496			Diameter Applications	0.1.0	0.2.0
2013-04	C4#60ah	C4-130498			Overload mitigation	0.1.0	0.2.0
2013-04	C4#60ah	C4-130508			Message Throttling	0.1.0	0.2.0
2013-04	C4#60ah	C4-130499			Overload Information Propagation	0.1.0	0.2.0
2013-04	C4#60ah	C4-130500			Diameter Node Behavior for Overload Mitigation	0.1.0	0.2.0
2013-04	C4#60ah	C4-130501			Network Topologies	0.1.0	0.2.0
2013-04	C4#60ah	C4-130502			Overload Control in Heterogeneous Network	0.1.0	0.2.0
2013-04	C4#60ah	C4-130489			Transfer of Overload Information	0.1.0	0.2.0
2013-04	C4#60ah	C4-130503			Network topologies	0.1.0	0.2.0
2013-06	C4#61	C4-130847			Client Prioritization	0.2.0	0.3.0
2013-06	C4#61	C4-130851			Message dependencies for message prioritization	0.2.0	0.3.0
2013-06	C4#61	C4-130844			Diameter overload control support for BBAI	0.2.0	0.3.0
2013-06	C4#61	C4-130848			Message Throttling by Window Limit	0.2.0	0.3.0
2013-06	C4#61	C4-130849			3GPP AAA Server Overload Aspects	0.2.0	0.3.0
2013-06	C4#61	C4-130850			Implicit Overload Indication	0.2.0	0.3.0
2013-06	C4#61	C4-130852			3GPP Charging Applications	0.2.0	0.3.0
2013-06	C4#61	C4-130878			Causes of Overload for 3GPP Charging Applications Interfaces	0.2.0	0.3.0
2013-06	C4#61	C4-130880			Overview of the proposed solutions	0.2.0	0.3.0
2013-06	C4#61	C4-130881			Details on disconnection with "BUSY" cause	0.2.0	0.3.0
2013-06	C4#61	C4-130990			Clarifications on Overload impacts over S6a	0.2.0	0.3.0
2013-06	C4#61	C4-130991			PCRF/DRA overload impacts	0.2.0	0.3.0