3GPP TR 29.816 V10.0.0 (2010-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study on PCRF failure and restoration (Release 10)

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

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 contains the results of the study on PCRF failure and restoration.

Target failure and recovery scenarios are detailed; the following scenarios are addressed (incl. roaming):

- Single PCRF deployment (covering also the equivalent scenario of multiple PCRFs with a fixed assignment of PCRFs);
- Multiple PCRFs and the DRA is used;

PCRF node failures of different type (e.g. complete outage, loss of dynamic data) and the aspect of reliability in signaling connections will be studied.

Functional requirements for solutions to handle such cases in a standardized way are defined, considering the network elements PCRF, PCEF, BBERF, AF and DRA and taking operators' preferences into account (e.g. minimal impact on user experience versus maximal control/minimum risk for the operator).

The study describes the potential solutions, which include procedures and signalling between PCRF and other PCC related network nodes, and procedures and signalling between Diameter clients (i.e. PCEF/BBERF/AF) and the DRA.

Per solution the impacted 3GPP specifications and the necessary changes therein are listed.

The study report finally evaluates the solutions and draws conclusions with respect to the type of solutions and their feasibility in terms of implementation effort/complexity.

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.203: "Policy and charging control architecture".

[3] IETF RFC 4960: "Stream Control Transmission Protocol".

[4] IETF RFC 3588: "Diameter Base Protocol".

[5] 3GPP TS 23.401: "GPRS Enhancements for E-UTRAN Access".

[6] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[7] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] IETF RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile".

[10] 3GPP TS 29.212: "Policy and Charging Control over Gx reference point".

[11] 3GPP TS 29.213: " Policy and Charging Control signalling flows and QoS parameter mapping".

[12] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[13] 3GPP TS 29.215: "Policy and Charging Control (PCC) over S9 reference point; (Stage 3) ".

[14] 3GPP TS 22.153: "Multimedia priority service ".

[15] 3GPP TS 23.007: "Restoration procedures".

[16] 3GPP TS 29.274: "Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

3 Definitions and abbreviations

3.1 Definitions

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

failure handling: procdures on other nodes except the failed PCRF node, necessary due to the failure. No specific recovery and failure handling procedures are assumed, but as examples they could include data restoration, dropping of sessions or - as a special case - also null activity.

partial PCRF failure: failure of a PCRF node during or after which at least some PCRF session state is assumed to be valid and PCRF related signaling is still functional. The amount of remaining, valid PCRF session state is in principle not relevant. Two important categories of partial failures are (1) loss of memory and (2) loss of processing power. It remains an implementation issue, and an estimation of gain versus effort, to treat a failure as a total one, even though there exists still some amount of valid PCRF session state.

recovery: applies for a failed PCRF and is used to denote the point in the time where the failure condition is over.

recovery handling: encompasses procedures on the (previously) failed PCRF node, necessary due to the failure. No specific recovery and failure handling procedures are assumed, but as examples they could include data restoration, dropping of sessions or - as a special case - also null activity.

total PCRF failure: failure of a PCRF node during and after which no PCRF session state is assumed to be valid. The time duration of the failure is in principle not relevant.

3.2 Abbreviations

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

AF	Application Function
AVP	Attribute-Value Pair
BBERF	Bearer Binding and Event Reporting Function
CCA/CCR	Credit Control Answer/Request
DRA	DIAMETER Routing Agent
FQ-PSSID	Fully Qualified PSSID
H-PCRF	PCRF in the HPLMN
IP-CAN	IP Connectivity Access Network
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
RAA/RAR	Re-Auth-Answer/Request
PSSID	PCRF Session Set ID
SPR	Subscriber Profile Repository
TMN	Telecommunication Management Network
V-PCRF	PCRF in the VPLMN

4 Failure and restoration scenarios

4.1 Baseline architecture

4.1.1 Non-roaming case

The baseline for the study on PCRF failure and restoration in the non-roaming case is given by the architecture derived from 3GPP TS 23.203 [2], as shown in figure 4.1.1.1.

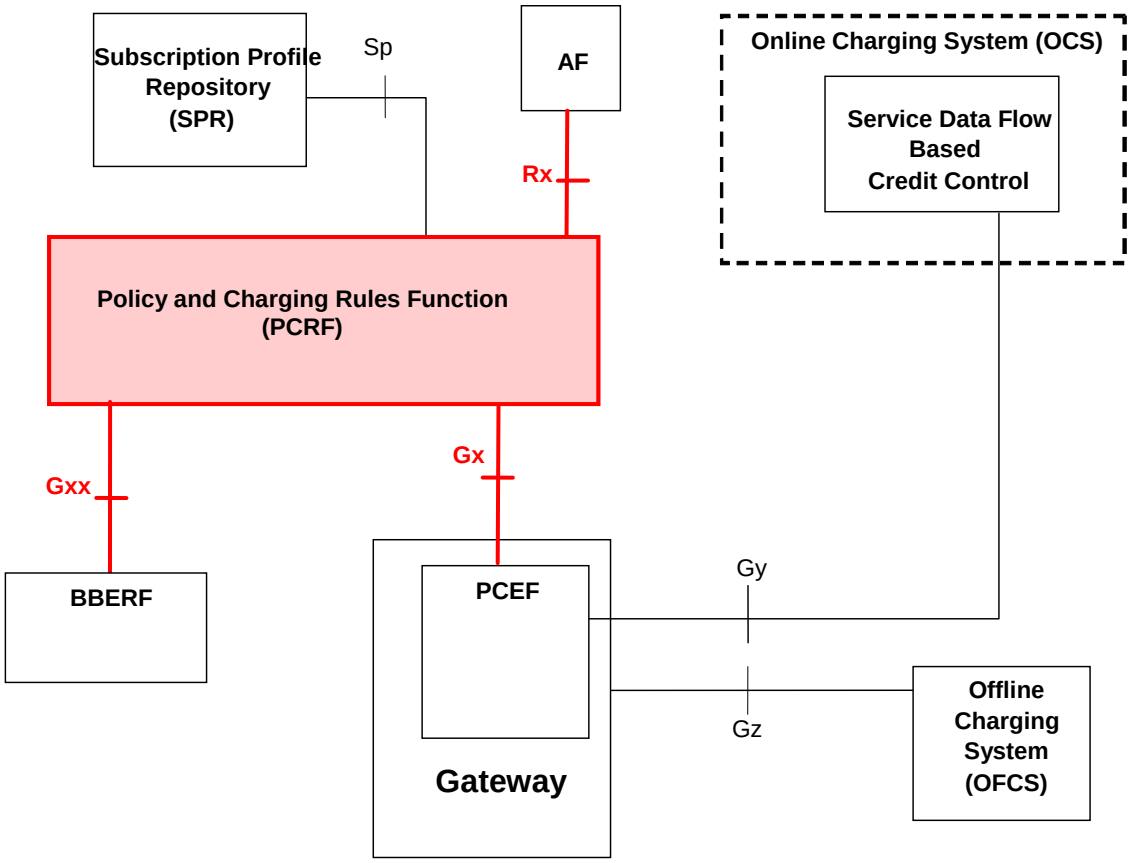

Figure 4.1.1.1: Baseline architecture for study on PCRF failure and restoration (non-roaming)

4.1.2 Roaming case

For the study of roaming aspects the two architectures in figure 4.1.2.1 and figure 4.1.2.2 are the baseline (again according to 3GPP TS 23.203 [2]). The coloured functional entities and the interfaces indicated with thick line are in scope of this study.

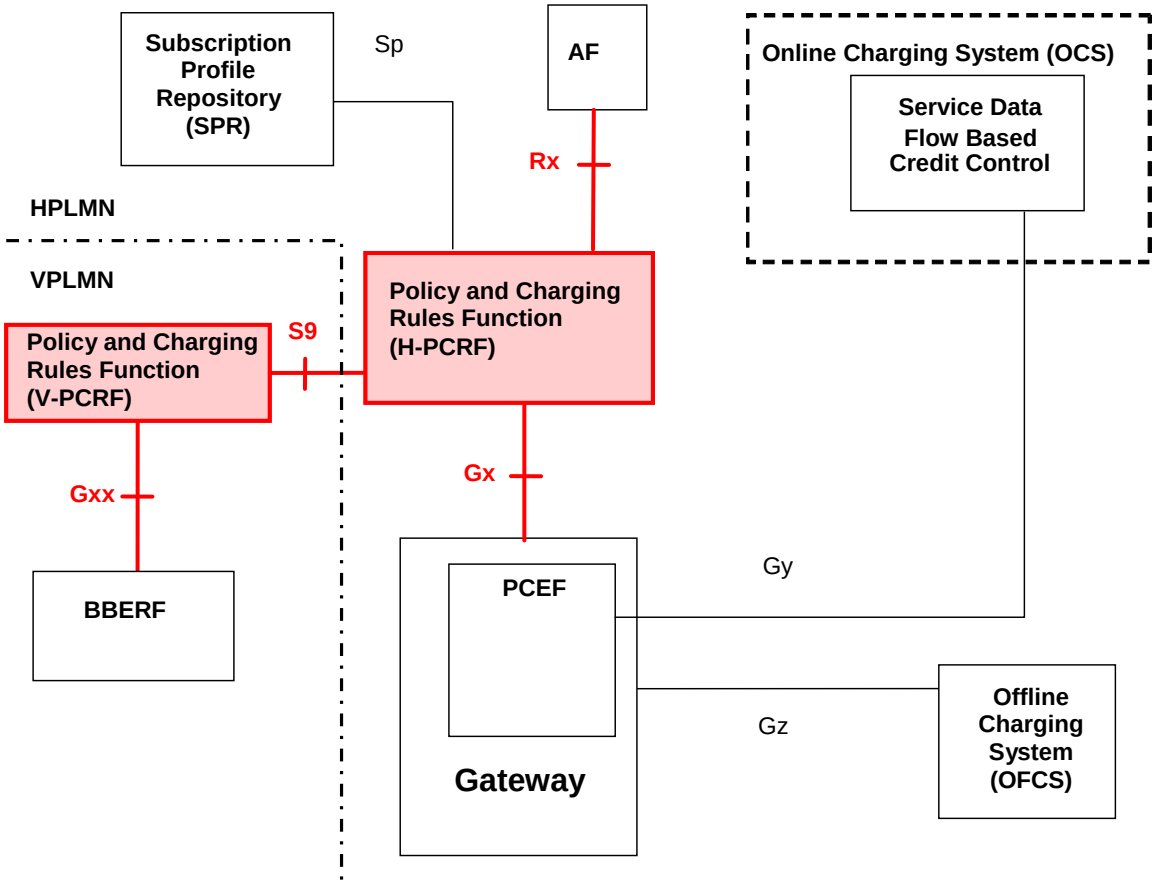

Figure 4.1.2.1: Baseline architecture for study on PCRF failure and restoration (roaming, with home routed traffic)

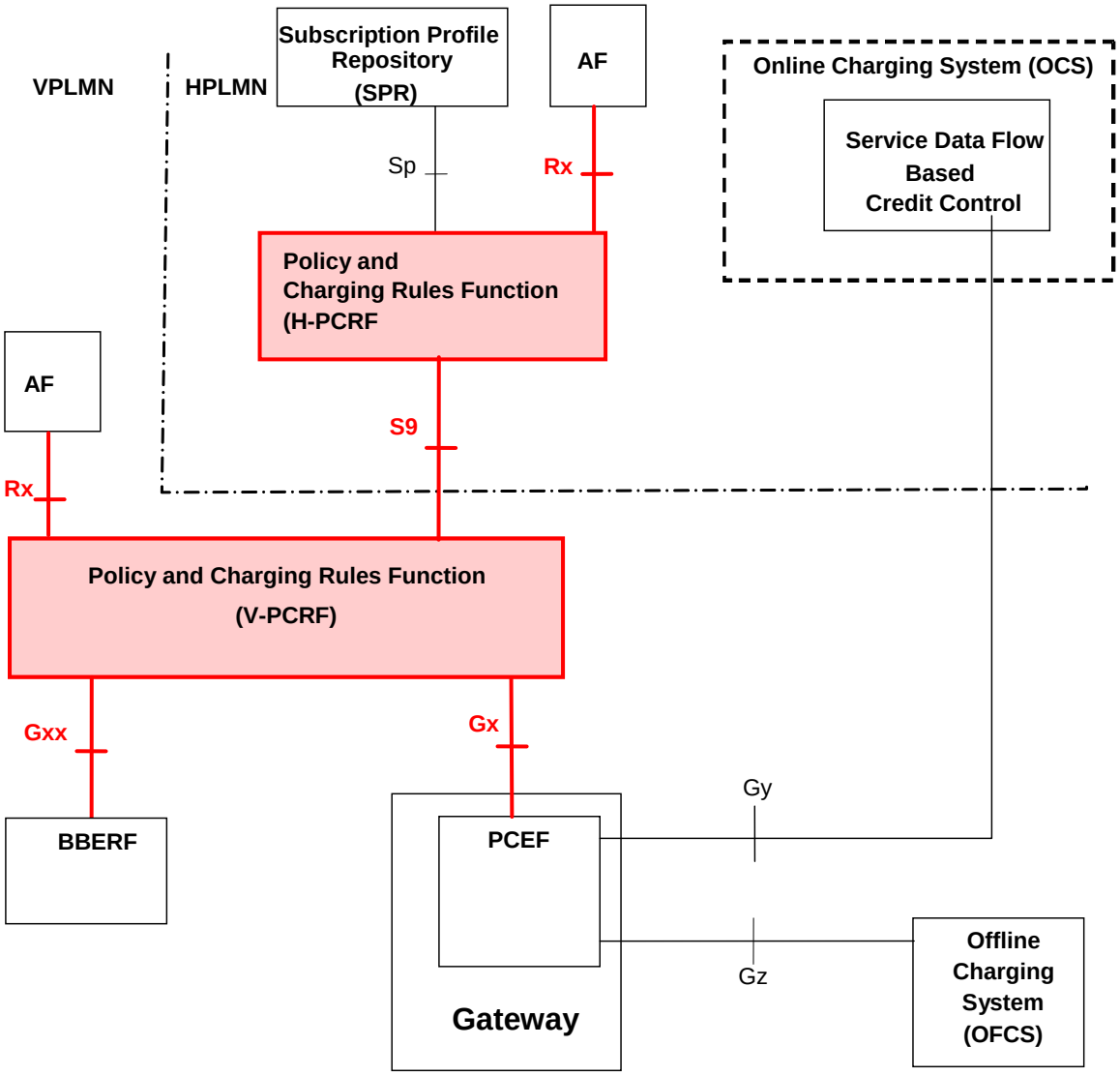

Figure 4.1.2.2: Baseline architecture for study on PCRF failure and restoration (roaming, with local breakout)

4.1.3 DRA deployment case

From figure 4.1.1.1 the deployment aspects are not visible; the two important ones to be considered in this study are:

- deployment of multiple PCRFs by one operator, and
- deployment of DIAMETER Routing Agent(s) (DRA, i.e. proxy agent and redirect agent according to subclause 7.6.2 of 3GPP TS 23.203 [2] and IETF RFC 3588 [4].).

Figure 4.1.3.1 illustrates the non-roaming case of a multiple PCRF deployment with a single DRA and serves as the reference within this study (SPR, OCS and OFCS are left out for simplicity).

NOTE: deployment of DRA combines with both the non-roaming and roaming case; for brevity only the first one is shown here.

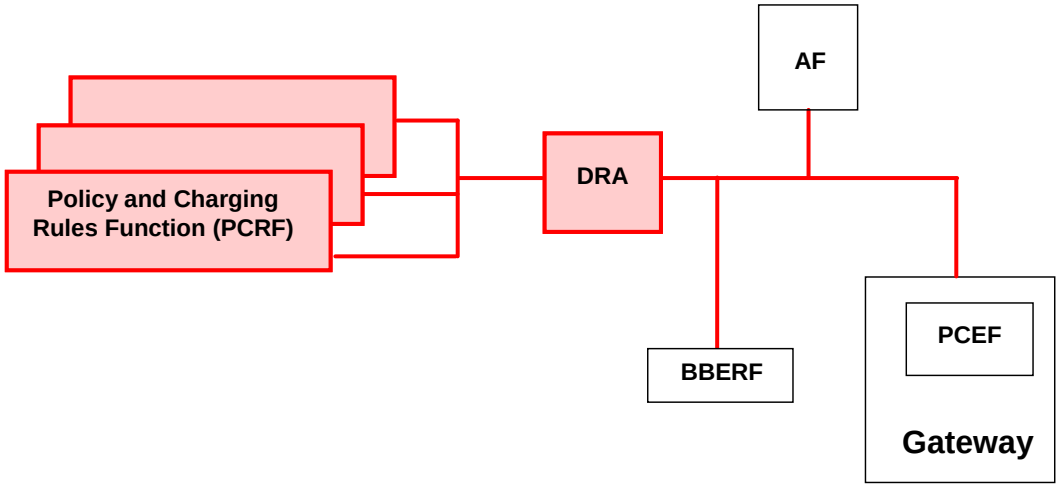

Figure 4.1.3.1: Deployment of multiple PCRFs with (single) DRA

4.2 Failure and recovery detection

4.2.1 General

Figure 4.2.1.1 gives a schematic view of the protocol structure for PCRF interfaces.

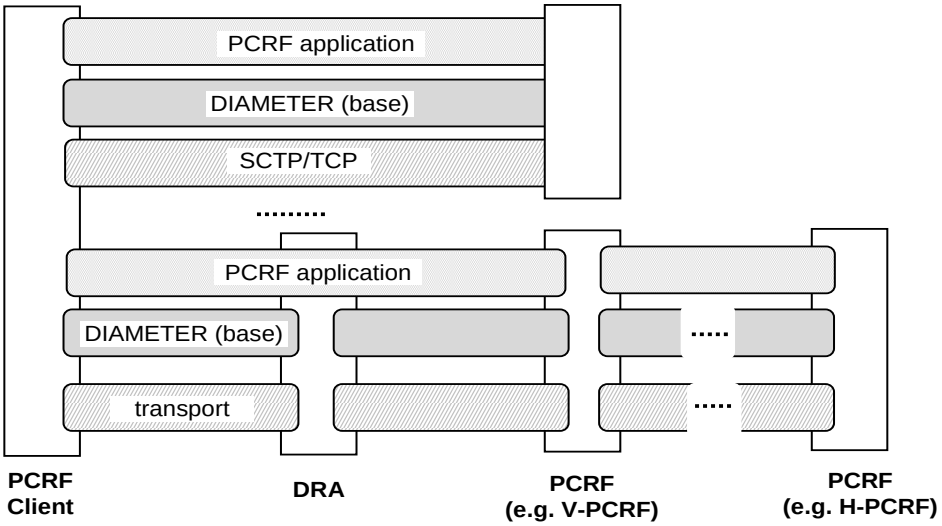

Figure 4.2.1.1: Protocol structure for PCRF interfaces

A client may detect a PCRF node failure or unavailability in several ways, e.g.:

- on protocol layers below the PCRF application: periodic signaling (by e.g. SCTP heartbeat or DIAMETER device-watchdog) will lead to detection of a PCRF node's (un)reachability. This signaling is independent of PCRF session handling. Unreachability on layers below PCRF application implicitly means unavailability of the PCRF functionality (on a specific target PCRF node), but the opposite does not hold.
- on PCRF application protocol layer: it will lead to detection of a total PCRF node failure by a PCRF client, also within the timespan of lower layer periodic signaling, but only if PCRF session requests are to be handled (by timeout of requests). Immediate detection of PCRF node recovery would require enhancements in signaling and node behaviour.

- independent from signaling, e.g. by TMN interaction. This method could be suitable for pro-active failure and recovery detection (e.g. based on permanent auditing on a PCRF node) and also for a controled withrawal of service of a PCRF node (e.g. for maintenance, reconfiguration etc.).

Editor's note: the details of TMN involvement for failure detection are FFS (e.g. standardized interfaces). The work of SA5 needs to be considered.

In case of single PCRF/multiple PCRF deployment without DRA, the PCRF clients must detect the failure; in case of multiple PCRF deployment with DRA, the failure must be detected by the DRA, and – depending on the required recovery handling – additionally PCRF clients may need to be informed.

There is a characteristic difference between PCRF failure and PCRF recovery detection, depending on the deployment scenario: a PCRF failure must be detected as fast as possible in any case, as there is a potential risk associated with the latency of failure detection; the same applies for PCRF recovery detection for single PCRF deployment. For multiple PCRF deplyoment the requirements for recovery detection are less stringent (because the effect of a delayed recovery detection would only be that PCRF sessions are unnecessarily still handled at alternative PCRF nodes; it does not increase the operator's risk, under the assumption that the overall load can still be handled).

Detection of recovery is commonly done by a restart indication sent by a restarted node to relevant clients immediately after a restart.

4.2.2 Failure detection on transport level

Transport of DIAMETER sigaling utilizes reliable (mostly SCTP) transport.

For SCTP, the heartbeat mechanism according to IETF RFC 4960 [3] can be used to detect unreachability of a peer; the recommended heartbeat interval is 30 sec.

4.2.3 Failure and recovery detection on DIAMETER level

According to IETF RFC 3539 [9], transport failures are detectable on DIAMETER level by the device watchdog mechanism. It has the following characteristics:

- operation is between DIAMETER peers (i.e. hop by hop, so that a failure of a PCRF node behind a DIAMETER agent cannot be detected by a PCRF client directly);

- the latency for failure detection is determined by the device watchdog timer setting (the default setting is 30 sec and minimum time is 6 sec); the maximum latency time results approximately in two time spans of this setting's length (first one for timing out pending DIAMETER responses, the second one due to waiting for the subsequent device watchdog response).

- the type of failure is unspecific; the only information derivable by the DIAMETER client is that the DIAMETER peer is not able to respond in time. Still, this criterion is the one defined for a failover procedure.

- smaller values of the timer do not cause traffic problems, as any response from the DIAMETER peer (e.g. normal traffic conditions) leads to a reset of the timer and does not lead to sending of the device watchdog request, and in low traffic conditions watchdog requests anyway do not compete with normal traffic. However, smaller values of the timer may increase the probability of a premature failure detection.

A further means to report problems of a peer on DIAMETER level is to send an explicit disconnect request, as defined in section 5.4 of IETF RFC 3588 [4]. A reason is included in the request, and may indicate e.g. a reboot or a busy situation.

Recovery of a DIAMETER peer is detected by a successful periodic attempt to connect to a failed peer (as per IETF RFC 3588 with a default and recommended value of 30 sec).

The loss of previous state may be indicated by the Origin-State-Id AVP in DIAMETER messages (which is monotonically increased with every state reset).

NOTE: in a simplified implementation, total PCRF failures may be linked firmly to loss of DIAMETER session state and thus Origin-State-Id AVP may be used for indication of PCRF restart.

4.2.4 Failure and recovery detection on PCRF application level

Currently no failure detection mechanism is defined on PCRF application level (i.e. in 3GPP TS 29.212 [10], 3GPP TS 29.213 [11], 3GPP TS 29.214 [12] and 3GPP TS 29.215 [13]). A distinctive feature of such dedicated signaling would be:

- it can be tailored to the specific needs for PCRF related signaling and the required information;
- it works directly between PCRF and its clients, e.g. without a need to enhance intermediate DIAMETER nodes; and
- only by signaling on the same level (i.e. application level) the failure or recovery of the corresponding functionality can be determined.

A restarting/restarted PCRF can handle the previou total failure and the related restart explicitly by an indication to relevant clients; in more detail:

- The PCRF maintains a restart counter in a non-volatile memory, increments the counter immediately after every restart and sends the new counter value to relevant clients within an existing PCRF application message (i.e. in a response message to a previous request from a client) or with a dedicated restart indication message (i.e. as a new request message to a client). The restart counter is not modified in case of a partial PCRF failure. (For current use of a restart counter mechanism, refer e.g. to 3GPP TS 23.007 [15] and 3GPP TS 29.274 [16].)

The restart counter mechanism can be utilized within several solutions described in clause 6.

A possible coding for Gx messages CCA/RAR and Rx messages AAA/RAR is given in annex A.2.

4.3 PCRF node failure scenarios

Figures 4.3.1 and 4.3.2 show the related scenarios for a (total) failure. Failure detection via signaling is assumed and indicated.

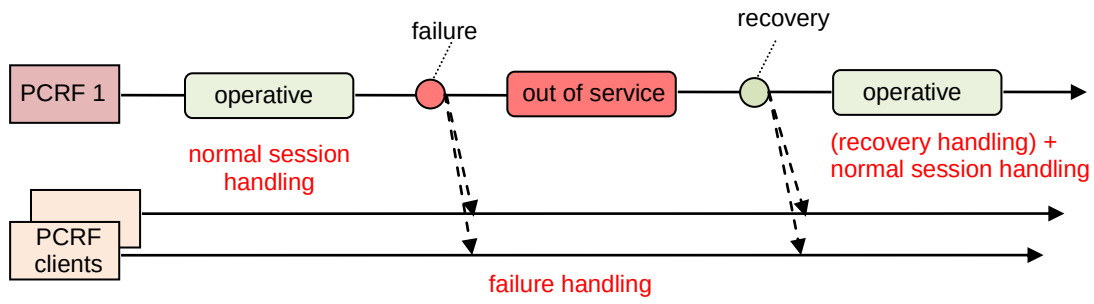

Figure 4.3.1: Total PCRF failure scenario for single PCRF deployment (or equivalently multiple PCRF deployment without DRA)

In the case of a single PCRF deployed recovery handling can only take place if/after the PCRF has come back into operation. (Note: the case that the outage becomes permanent can not be handled; instead, it must be assumed that in such a deployment the PCRF implementation itself guarantees that only temporary failures occur.)

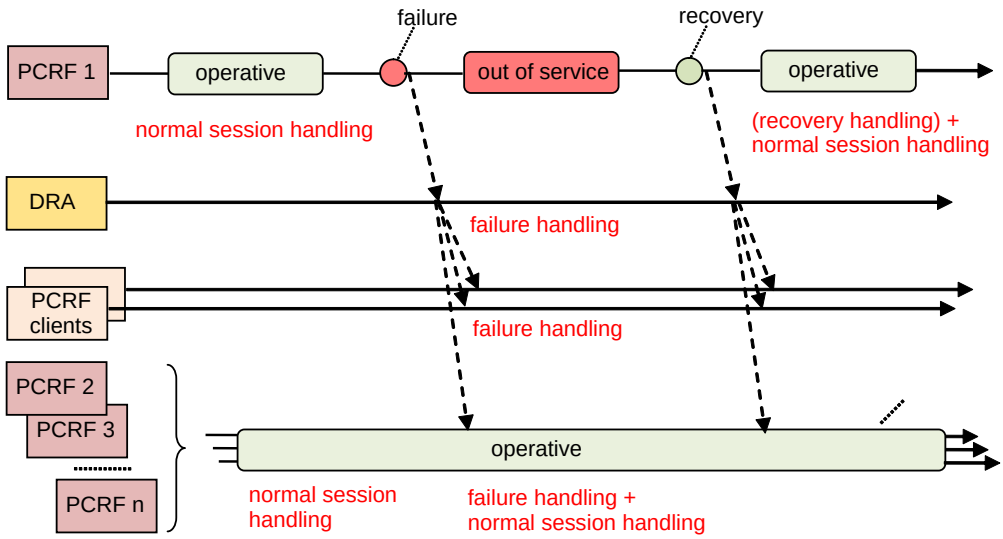

Figure 4.3.2: Total PCRF failure scenario for multiple PCRF deployment with DRA

In the case of multiple PCRFs, recovery handling can set in immediately after detection of the failure, on the remaining, operative PCRFs. Recovery handling on the failed PCRF can be done only after it has become operative again. In this deployment also a permanent PCRF failure is admissible; however, because there seems to be no easy criterion how to distinguish between permanent and temporary failure, we refrain from doing so from now on. Both the description of the failure scenario and solutions shall consider the permanent failure case as the border case when the outage time of the failed PCRF becomes infinite.

PCRF nodes may exhibit also partial failures, e.g. (list is non-exhaustive):

- the PCRF node is still functioning (i.e. message handling on the application interfaces Rx, Gx, etc. is working), but the context data for some target UEs/sessions has been lost.

- the PCRF node is still functioning but processing capability has degraded.

The corresponding scenarios are illustrated generically in figures 4.3.3a and 4.3.3b.

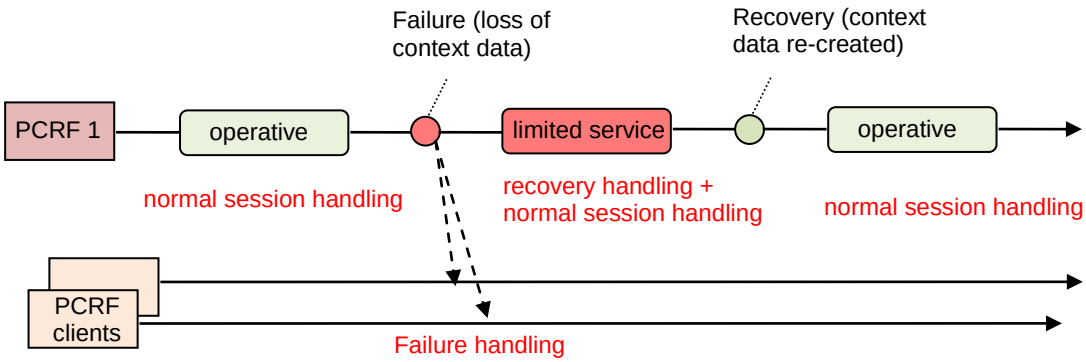

Figure 4.3.3a: Partial PCRF failure scenario for single PCRF deployment (or equivalently multiple PCRF deployment without DRA)

In a single PCRF deployment, during the time of the partial node failure, the PCRF may be able to provide limited service and also perform to some extent recovery handling for the sessions affected by the partial failure. However, it can be expected that for performance reasons some deviation from the normal PCRF functionality is necessary (e.g. provision of simplified rules, reduced event reporting).

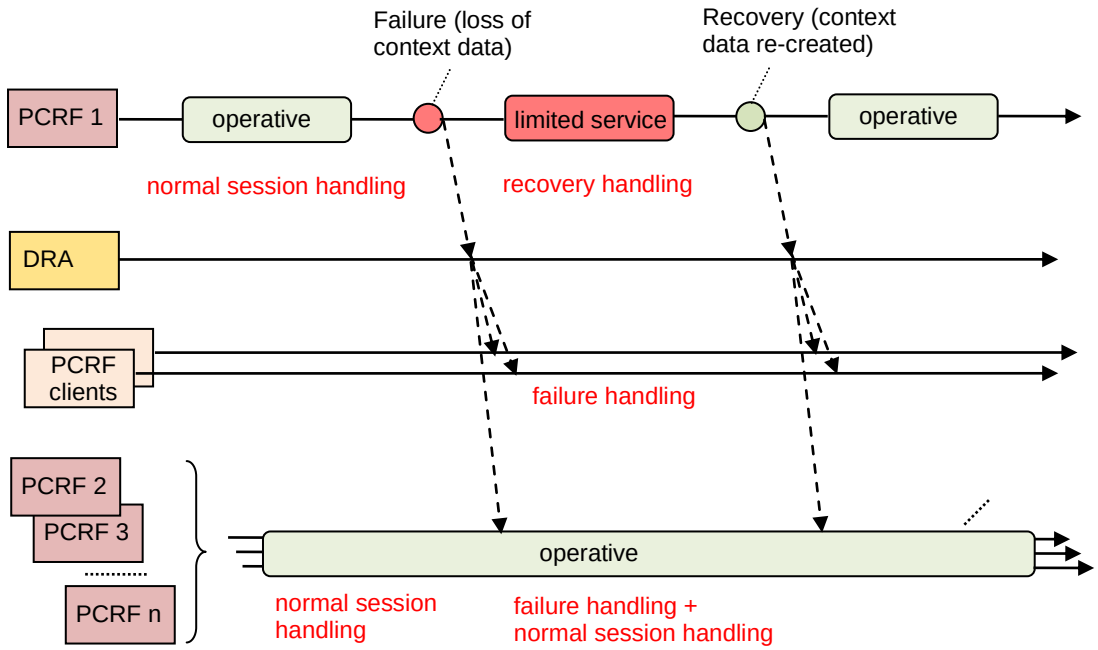

Figure 4.3.3b: Partial PCRF failure scenario for multiple PCRF deployment with DRA

In a multiple PCRF deployment with DRA, during the time of the partial node failure the DRA would preferably route new session requests to alternative PCRF nodes. Recovery handling for the sessions affected by the partial failure could be done on the (partially) failed node, or on the alternative nodes. The decision may depend on factors like amount of context loss, number of alternative PCRF nodes and their capacity, general operator's policy concerning PCRF failure handling, etc.

Table 4.3.1 lists the target failure scenarios.

Table 4.3.1: Categorization of failure scenarios

Nr.	Description	Consequences	Examples of failure handling	
			in parallel	subsequent
Single PCRF deployment / multiple PCRF deployment without DRA				
1	(total) PCRF node failure → complete PCRF functionality is not available	no new session requests can be handled	Potentially: drop of sessions (graceful or strict)	Potentially: restoration of state (on the same PCRF node)
2	partial PCRF node failure → part of session context not usable	new session requests unavoidable for this PCRF node	Potentially: restoration of state (on the same PCRF node); drop of sessions (graceful or strict); reduce PCRF funtionality	
Multiple PCRF deployment with DRA				
3	(total) PCRF node failure	route new session requests to alternative PCRF nodes	Potentially: (1) restoration of state on other PCRF nodes, or (2) drop of sessions (graceful or strict)	Potentially: restoration of state (on the same PCRF node)
4	partial PCRF node failure	route new session requests preferably to alternative PCRF node	restoration of state (on alternative PCRF node); drop of sessions (graceful or strict);	
5	DRA failure →all PCRF nodes not reachable	no new session requests can be handled	Potentially: drop of sessions (graceful or strict)	Potentially: restoration of state (per PCRF node)

The columns "Consequences" and "Examples of failure handling" are given for illustration only; the detailed handling depends on requirements imposed by the operator (these will be collected in clause 5 of this TR).

4.4 Selection of restoration scheme

Clients and PCRFs may possibly support one or more restoration schemes or no restoration scheme at all. The supported features mechanism, already in use in the current PCC technical specifications, may be used for indicating the support of a restoration scheme or restoration schemes between the clients and PCRF in cases where a restoration scheme is applicable.

NOTE: To avoid defining later restoration feature negotiation rounds after the initial supported features indication, it is assumed that all network elements, if there are more than one, related to the operations of the restoration mechanism agreed between a client and PCRF are able to support (and indicate to the PCRF the support of) the same mechanism.

5 Functional requirements for solutions

5.1 General

This clause collects diverse requirements regarding handling of PCRF failures, as they were either explicitly formulated by operators or can be generally anticipated.

It is not expected that one particular solution described in clause 6 fulfills all these requirements; rather, this list serves as the reference and maximum scope. Every solution shall describe which requirements it fulfills, and how.

An operator is also not bound to one (set of) requirement(s) for all PCRF sessions, but may e.g. follow distinct strategies for different subsets of PCRF sessions at one point in time, or for the same subset of PCRF sessions at different times.

5.2 Functional requirements for all deployments

Functional requirement #1: *It shall be possible for PCRF clients in the bearer plane (PCEF and BBERF) to continue bearer services without PCRF control, if a related PCRF session is required but cannot be handled due to PCRF failure.*

Functional requirement #2: *It shall be possible for PCRF clients in the bearer plane (PCEF and BBERF) to fall back to static policies specifically configured for this case, if a related PCRF session is required but cannot be handled due to PCRF failure.The fallback may occur at initial or subsequent PCRF requests.*

Functional requirement #3: *It shall be possible to terminate bearer services immediately, if a related PCRF session is required but cannot be handled due to PCRF failure or unreachability.*

Functional requirement #4: *It shall be possible to terminate bearer services 'gracefully', if a related PCRF session is required but cannot be handled due to PCRF failure . 'Graceful' means that active bearer services are kept, up to an operator configurable maximum time; as soon as they become idle, bearer services are terminated.*

NOTE: the definition of "idle" and "active" status of bearers is different from corresponding UE states on NAS signaling or RRC levels.

Functional requirement #5: *It shall be possible to restore PCRF session state after detection of a PCRF failure; depending on the deployment scenario and type of failure, this may happen already during the ongoing failure situation (e.g. in case of partial failures or with multiple PCRFs) or only after recovery of the failed node (in case of total failure of the PCRF node).The impacts of PCRF session state restoration on load, performance and stability of the PCRF infrastructure (PCRF nodes and clients) shall be minimized.*

Functional requirement #6: *The operator shall be able to configure the applicable handling in case of PCRF failure per APN.*

Functional requirement #7: *Independent of an operator configuration fulfilling any combination of the preceding requirements, emergency service sessions and Government Emergency Telecommunication Services/Multimedia Priority Services according to 3GPP TS 22.153 [14] shall not be terminated in case of PCRF failure.*

5.3 Functional requirements for the multiple PCRF deployment with DRA

When the redirect DRA is used, if the client (e.g. PCEF, AF) can not establish the connection with the PCRF:

- It's possible for the client to report the selected PCRF is not reachable;
- It's possible for the redirect DRA to select a PCRF basing on the status of the PCRF;

6 Solutions

6.0 General

Several solutions are presented in this clause. They described the PCRF failure and restoration from on different levels and from various perspectives all-around.

Solution1 and 2 analyse the failure detection from the deployment point of view. Solution 1 is for deployment of multiple PCRF with DRA, and the solution 2 deals with the failure detected for the single PCRF. In addition, solution 1 describe the PCRF reselection, but the rebuilding of existing sessions in the failure PCRF has no detailed presentation. Solution 2 elaborates also on the failure detection, but not on restoration. The PCRF may rebuild sessions in various ways, and the applicable ways can be reused as the description e.g. for description in subclause 6.5 / PCRF session state restoration and in subclause 6.6 / Soft recovery after a PCRF restart in the solutions5 and 6.

Solution 3 and 4 describes the termination of services as soon as the PCRF failure condition is detected. Solution 4 performs the appropriate tear-down procedure on the PCRF clients for all bearer and application sessions. And the solution 3 features the grace time for the termination of services, and re-uses of mechanisms described under solution 4.

The restoration of PCRF session state is considered is detailed in solution 5 and 6. Solution 5 is employed to re-synchronize PCC rules between PCRF nodes and PCRF clients on bearer and AF sessions whenever, due to failure of a PCRF node, the PCRF has lost the session state. The partial failure is included in solution 5, and the soft recoveries of solution 6 just act after the PCRF restart.

In addition, solution 5 is combinable with solution 1 and solution 3, but should not be combined with solution 4.

Solution 7 proposes means for bulk signalling; to be used in other solutions (e.g. solutions 4 and 5).

Solution 8 provides PCRF resilience by duplicating PCRF session state information to PCRF clients in opaque containers.

6.1 Solution 1: Solution for the PCRF failure reselection for the DRA

6.1.1 Redirect DRA

This solution is applied for the PCRF failure reselection when the redirect DRA is used.

A DRA implemented as a Diameter redirect agent shall redirect the received Diameter request message by carrying out the procedures defined in section 6.1.7 of IETF RFC 3588 [4]. The client shall use the value within the Redirect-Host AVP of the redirect response in order to obtain the PCRF identity; the redirect DRA shall only include one PCRF identity in the Redirect-Host AVP. If the client (e.g. PCEF, AF) can not establish the connection with the PCRF, it shall resend the Diameter request message (i.e. Diameter CCR) with the PCRF failure indication to the redirect DRA to indicate it can not contact with the PCRF.

After receiving this indication, based on the PCC session information, the redirect DRA shall reselect a new PCRF, and include the PCRF identity in the Redirect-Host AVP in the Diameter reply sent to the Diameter client. If the redirect DRA has selected a PCRF for the other client (e.g. BBERF) for the same UE or for the same IP-CAN session of the same UE, the redirect DRA shall select the same PCRF for the client or reject the request.The following description is just one option way to specify how the redirect DRA (re)selects the PCRF and judge the status of the PCRF, other ways may also be used (e.g. configuration), this may depend on the implementation: the redirect DRA may (re)select the PCRF based on the priority of the PCRF. The priority of the PCRF may be determined by the status of the PCRF (e.g. normal or failure). If the DRA receives the failure indication of the PCRF, the DRA may set the status of the PCRF to failure and allocate a lower priority to it; if the DRA has to (re)select a lower priority PCRF (failure PCRF) for the client in some condition (e.g. there is no other PCRF or the redirect DRA has selected a PCRF for the other client for the same IP-CAN session of the same UE) and does not receive the failure indication in a configurable time, the DRA may think the PCRF has recovered and set the status of this PCRF to normal and allocate a higher priority to the PCRF.

The following message flow demonstrates that how the client requests a new PCRF identity if it can not establish the connection with the PCRF.

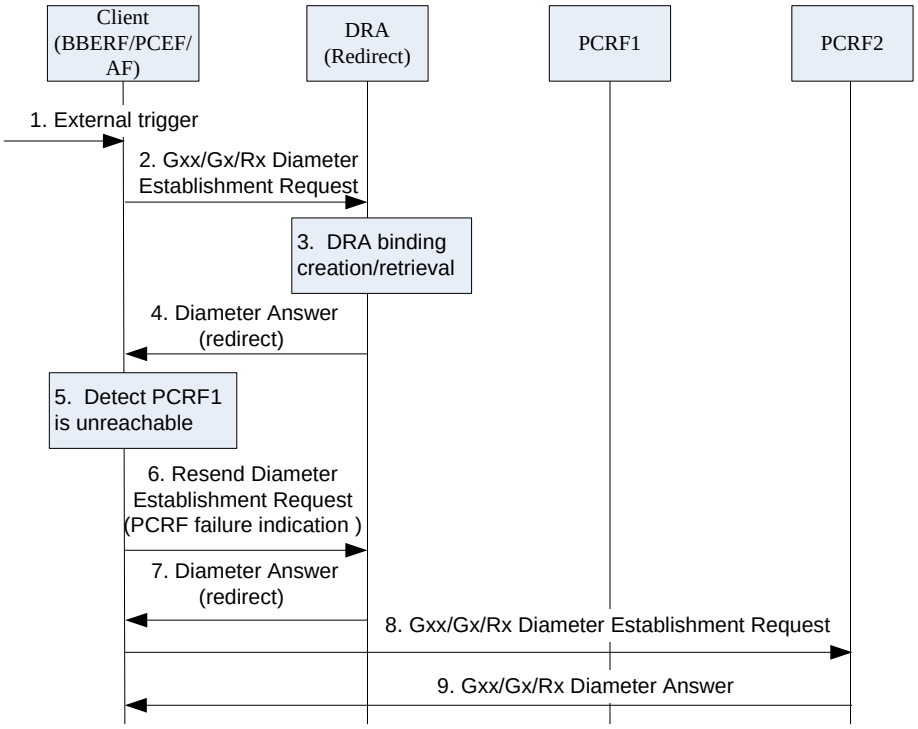

Figure 6.1.1.1: Message flow of PCRF failure reselection for the redirect DRA

1 - 2. Same as steps 1- 2 in figure 7.4.2.1.1.1 of 3GPP TS 29.213 [11].

3. The same as step 3 in the figure 7.4.2.1.1.1 of 3GPP TS 29.213 [11]. Additionally, the DRA (redirect) may select the PCRF based on the status of the PCRF (e.g. determined by the watchdog or the priority of the PCRF).

4. Same as steps 4 in figure 7.4.2.1.1.1 of 3GPP TS 29.213 [11].

5. The client detects that it can not establish the connection with the PCRF1.

6. The client resends the Diameter request message with the PCRF failure indication to the redirect DRA to indicate it can not contact with the PCRF1.

7. The DRA (redirect) reselects a new PCRF2 within the Redirect-Host AVP and sends the redirect response to the client.

8 - 9. Same as steps 5 - 6 in figure 7.4.2.1.1.1 of 3GPP TS 29.213 [11].

6.1.2 Proxy DRA

This solution is applied for the PCRF failure reselection when the proxy DRA is used.

The DRA shall support the functionality of a Diameter proxy agent as defined in IETF RFC 3588 [14].

When the DRA receives a request from a client, it shall select the PCRF and proxy the request to the selected PCRF as described in clause 7.3.5 3GPP TS 29.213 [11]. If the DRA detected the PCRF Failure (e.g. received the failure indication from the PCRF), the DRA will reject the request.

If the DRA received the PCRF failure indication and the new PCRF identity is included, the following request may be proxied to the new PCRF. If the Proxy DRA has selected the new PCRF for the other client (e.g. BBERF) for the same UE or for the same IP-CAN session of the same UE, the Prxoy DRA shall select the same PCRF for the client or reject the request. DRA can (re)select the PCRF and judge the status of the PCRF according to the clause 6.1.2.

The following message flow demonstrates one option to specify how the proxy DRA performs the client request when a PCRF failure occurs.

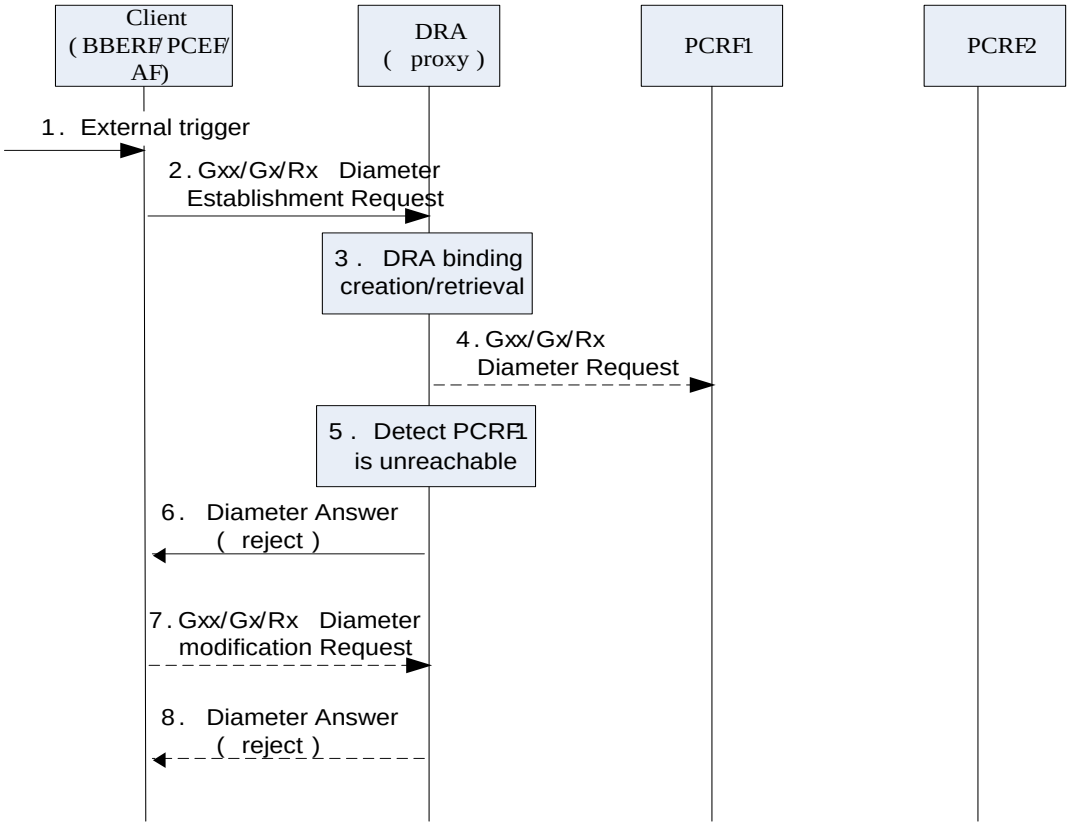

Figure 6.1.2.1: Message flow of PCRF failure reselection for the proxy DRA

1 - 2. Same as steps 1- 2 in figure 7.4.1.1.1.1 of 3GPP TS 29.213 [11].

3. The same as step 3 in the figure 7.4.1.1.1.1 of 3GPP TS 29.213 [11]. Additionally, if the proxy DRA detects that PCRF1 sha failured, it will mark it with the failure (the latter messages which should be proxied to the PCRF1 will be rejected according to the mark), and steps 4 and 5 wil not be carried out.

4. If the proxy DRA doesn't know that PCRF1 has failured, same as steps 4 in figure 7.4.1.1.1.1 of 3GPP TS 29.213 [11].

5. After the DRA knowing the PCRF failure, it will mark it with the failure (the following messages which should be proxied to the PCRF1 will be rejected according to the mark).

6. The DRA (proxy) returns a Diameter Answer to the client to reject the establishment request.

7-8. If there are Gx/Gxx session modification request, which is the same UE with the request in step 2, is send to the DRA during the PCRF failure, it will be rejected by the DRA.

NOTE 1: How the DRA knows about the PCRF failure is FFS; one possible procedure is that PCRF informes the DRA about the failure)

NOTE 2: If the DRA knows the target PCRF of the rebuilding exist Session and the following request from the clients may be proxy to the same one. The procedures are according to clause 7.4.1.1.1 of 3GPP TS 29.213[11].

6.2 Solution 2: use of DIAMETER base protocol in Single PCRF deployment (with Direct Client-Server Connection)

6.2.1 PCRF Failure Detection

The diameter client at the BBERF, PCEF and AF shall probe the liveliness of the PCRF by sending the diameter Device-Watchdog-Request message per IETF RFC 3588 [4] and IETF RFC 3539 [9].

The PCRF shall be prepared to receive a Device-Watchdog-Request message and respond with Device-Watchdog-Answer message per IETF RFC 3588 [4] and IETF RFC 3539 [9].

6. 2.1.1 Response of the Diameter Client (AF/PCEF/BBERF)

Handling of existing sessions when PCRF failure is detected is implementation specific. The client at the AF/BBERF/PCEF may terminate a session when it receives a session modification request with the exception of Emergency Services and Government Emergency Telecommunication Services/ Multimedia Priority Service (3GPP TS 22.153 [14]).

6. 2. 2 PCRF Restart

After a PCRF restart the status of the sessions is unknown. The PCRF may rebuild sessions in various ways, using information requested from the related clients (PCEF, BBERF, AF/P-CSCF). Applicable ways are described e.g. in subclause 6.5 / PCRF session state restoration and in subclause 6.6 / Soft recovery after a PCRF restart.

6.3 Solution 3: Graceful termination of services

6.3.1 General

This solution is constituted by:

1. supervision of bearer sessions in the GW(s) (where PCEFs and BBERFs are located) and application sessions in AFs,
2. running corresponding timers, and
3. re-use of mechanisms described under solution 4 “Strict termination of services” in subclause 6.4.

NOTE: users will be unaffected by graceful termination in some cases:

- in multiple PCRF deployments: if, within the grace time, the bearer or application session associated with the failed PCRF node becomes inactive and is subsequently torn down and re-established with PCRF session(s) on a different PCRF node (this may be triggered either by the UE or the network).
- with some probability in all deployments, including single PCRF deployment: if restoration of PCRF session was successful during the grace time.

6.3.2 Graceful termination in PCEF

If the node implementing PCEF itself performs the graceful termination, it monitors those bearer sessions which are subject to this type of handling in case of PCRF failure. If within a configurable time (grace time) no teardown of service occurs, the procedure as for strict termination of services according to subclause 6.4, bullet 1, is executed; if within the grace time teardown of service was initiated by other entities, e.g. by BBERF, the condition for graceful termination is reset and no further action is taken.

The node implementing PCEF may propagate a request for graceful termination of service to neighbouring nodes in the bearer plane (e.g. Serving GW in EPC, SGSN in GPRS).

Editor’s note: the details of propagation and the necessary signaling is out of scope of the present study and should be coordinated with CT4.

6.3.3 Graceful termination in BBERF (Serving GW)

The Serving GW performs similar actions as described in the first paragraph of subclause 6.3.2 (substituting bullet 1 by bullet 2 and BBERF by PCEF).

The Serving GW may propagate the request for graceful termination of service to MME.

Editor's note: the details of propagation and the necessary signaling is out of scope of the present study and should be coordinated with CT4 and CT1.

NOTE: BBERF and PCEF are not synchronized with respect to the timing of graceful termination.

6.3.4 Graceful termination in AF

The AF/P-CSCF monitors those application sessions which are subject to this type of handling in case of PCRF failure. If within a configurable time (grace time) no teardown of service occurs, the procedure as for strict termination of services according to subclause 6.4, bullet 3, is executed; if within the grace time teardown of service was initiated by other entities, the condition for graceful termination is reset and no further action is taken.

6.4 Solution 4: Strict termination of bearer services

The solution consists in performing the appropriate tear-down procedure on the PCRF clients for all bearer and application sessions, for which PCRF control would be required, but cannot take effect, due to PCRF failure or unreachability, as soon as this failure condition is detected. More concretely, depending on the deployed network architecture, the following procedures are invoked (with the obvious modification that the normally foreseen PCRF interactions in these procedures, if any, are left out):

1) on network nodes implementing PCEF:

   - at PDN GW: once PDN GW detects the PCRF failure, PDN GW initiates the PDN GW initiated bearer deactivation procedure as described in subclause 5.4.4.1 of 3GPP TS 23.401 [5] ;

   - at the trusted non-3GPP access: once the trusted non-3GPP access detects the PCRF failure, the trusted non-3GPP access initiates the network initiated detach procedures as described in subclauses 6.4.1 and 6.4.4 of 3GPP TS 23.402 [6];

   - at GGSN: once GGSN detects the PCRF failure, GGSN initiates the GGSN initiated PDP Context deactivation procedure according to subclause 9.2.4.3 of 3GPP TS 23.060 [7];

2) on network nodes implementing BBERF:

   - at Serving GW:

     a. in non-roaming: once Serving GW detects the PCRF failure, Serving GW behaves according to the PCC initiated bearer deactivation procedure described in subclause 5.4.5.1 of 3GPP TS 23.402 [6], with the triggering message from PCRF substituted by the failure detection.

     b. in roaming: once V-PCRF detects the H-PCRF failure, V-PCRF initiates the PCC initiated bearer deactivation procedure as described in subclause 5.4.5.1 of 3GPP TS 23.402 [6]; once the Serving GW detects the failure of the V-PCRF, Serving GW behaves as in bullet 1.

3) on network nodes implementing AF:

   - at P-CSCF: once the P-CSCF detects the PCRF failure, the P-CSCF initiates the appropriate teardown action as specified in the corresponding specification (e.g. according to subclause 5.10.3.2 in 3GPP TS 23.228 [8]).

   - at any other type of AFs the behaviour is application specific;

In roaming, if H-PCRF detects the failure of the V-PCRF, the possible actions depend on the traffic routing scenario:

- for roaming with local breakout no specific action need to be taken in the control plane. It can be expected that the behaviour in the VPLMN is sufficiently detailed in roaming agreements;

- for roaming with home routed traffic, the H-PCRF can initiate the PCRF initiated IP-CAN session termination.

Editor's note: for roaming scenarios, further details how failures to either the H-PCRF or V-PCRF are handled are FFS.

In order to deal with the masses of sessions potentially involved in PCRF failure and restoration procedures, possible methods are:

1) in case of multiple PCRF deployment: equi-distribution (or at least non-concentration) of sessions on PCRFs; the number of affected sessions can be reduced roughly by a factor of N, where N is the number of deployed PCRFs.

2) rate limiting of signaling: although the termination should ideally happen immediately, the number of signaling messages per time slot should be limited (e.g. by delaying and queueing).

3) bulk signaling: it could (additionally) be used on interfaces Gx, Gxx and Rx. This concept is already in use for signaling between other network nodes (based on CSI - Connection Set Identifier, used between Serving GW, PDN GW and MME; see 3GPP TS 23.007 [15]) and can be carried over to PCRF application signaling. Details are found in subclause 6.7.

6.5 Solution 5: PCRF session state restoration

This solution can be employed to re-synchronize PCC rules between PCRF nodes and PCRF clients on bearer and AF sessions whenever, due to failure of a PCRF node, the PCRF has lost the session state. The PCRF needs to store information on all clients with which it has sessions in non-volatile memory.

The principle scheme is shown in figure 6.5.1 in the most general form. PCRF session state can be restored either on the failed PCRF node (e.g. for the single PCRF deployment, during partial failures or after its recovery from failure), or on alternative PCRF nodes (e.g. for the case of partial PCRF node failure in a deployement with multiple PCRFs).

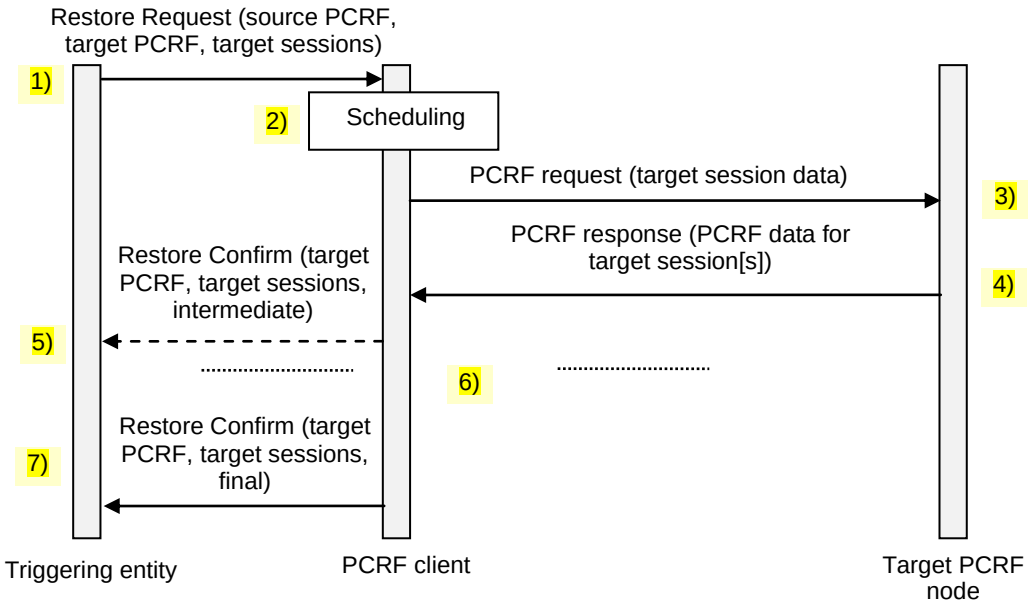

Figure 6.5.1: PCRF session state restoration (general view)

The following steps are performed:

1) the restoration process starts by a "Restore" request to a PCRF client, containing information on the source PCRF, target PCRF node and target sessions. The information on target sessions may also be null, meaning that all sessions on the PCRF client stemming from the source PCRF are requested to be restored on the target PCRF. The entity triggering the restoration may be typically the failing/failed PCRF node, but potentially also manual intervention or a TMN interface. The source PCRF is used to filter out the relevant bearer or AF sessions, together with more specific information on target sessions; this data may also be of bulk nature e.g. according to

a time stamp (all bearer or AF sessions started after a certain time), list of UEs, etc. The detailed role of "target PCRF" is FFS (e.g. whether it indicates/excludes one or more specific PCRF nodes).

2) the addressed PCRF client performs scheduling of the necessary signaling for restoration. For this purpose it should take into account its own current and excpectable load; e.g. if the received request for restoration was for a large amount of sessions, it may break the subsequent signaling into portions, and wait for successful restoration of one portion before requesting restoration of the next portion. Depending on the detailed role of "target PCRF" it may also employ load balancing between available PCRF nodes.

3) The PCRF client sends the appropriate PCRF request(s) with all bearer or AF session data to the target PCRF node(s). Although repeated single signaling requests, as for a normal establishment of PCRF sessions, could be used, the assumption here is that bulk signaling is required for reasons of performance.

4) The PCRF node establishes the requested PCRF sessions and provides their data to the PCRF client (as before, bulk signaling is assumed).

5) The PCRF client may send an intermediate confirmation of restored session data back to the triggering entity.

6) Steps 3) to 5) are repeated, depending on the scheduling of restoration requests by the PCRF client.

7) The PCRF client sends a final confirmation of restored session data back to the triggering entity.

A possible coding for messages 1) (RAR) and 7) (RAA) is given in annex A.3 for the Gx application protocol.

NOTE 1: for the single PCRF case, the source and target PCRF are the same.

NOTE 2: usage of RAA for message 7) assumes that message 5) is different from RAA.

For the sake of easier analysis and evaluation, illustrations of three specialized cases are given:

(a) figure 6.5.2 for restoration after recovery of, and onto, the previously failed PCRF node (i.e. source and target PCRF are the same);

(b) figure 6.5.3 for restoration triggered by and onto an alternative PCRF node, during the failure of one particular PCRF node; and

(c) figure 6.5.4 for the case that partially failed PCRF node triggers a PCRF client to restore PCRF session data onto an alternative PCRF.

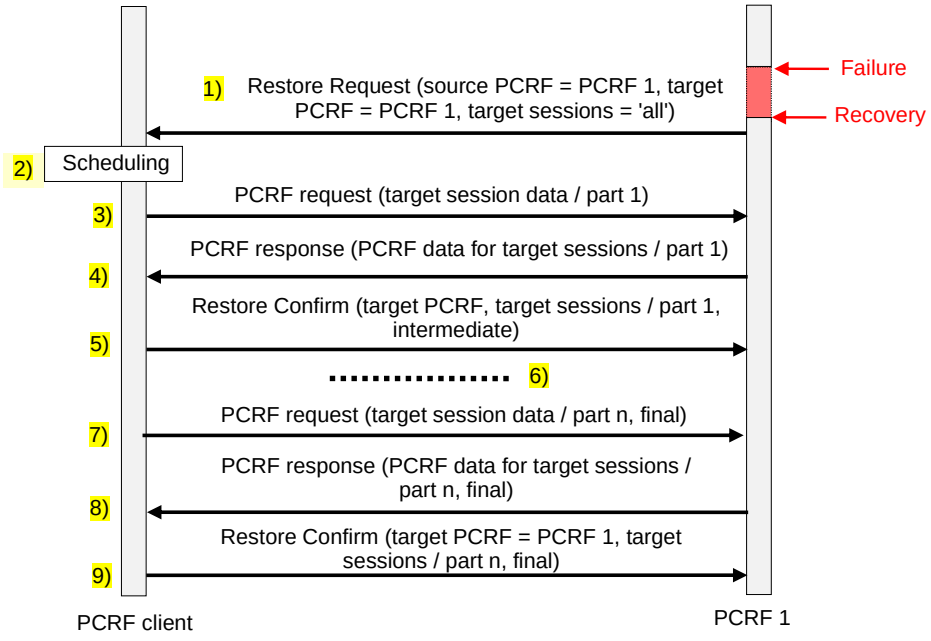

Figure 6.5.2: PCRF session state restoration (after recovery of, and onto, the previously failed PCRF node)

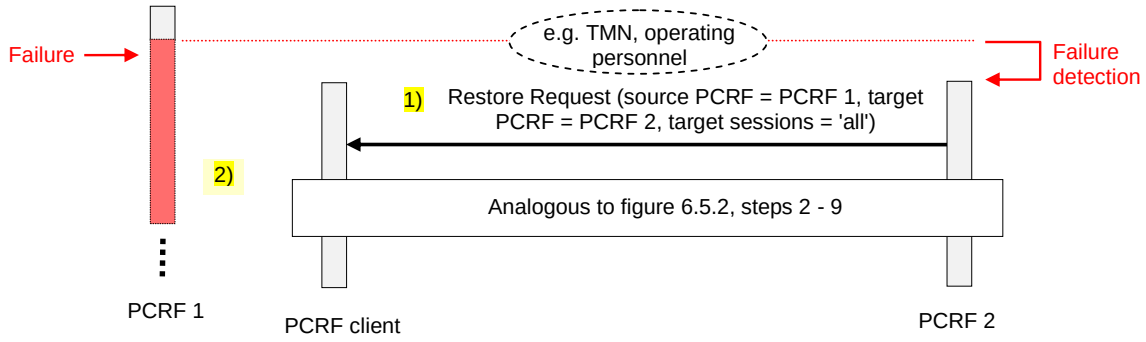

Figure 6.5.3: PCRF session state restoration (triggered by and onto an alternative PCRF node)

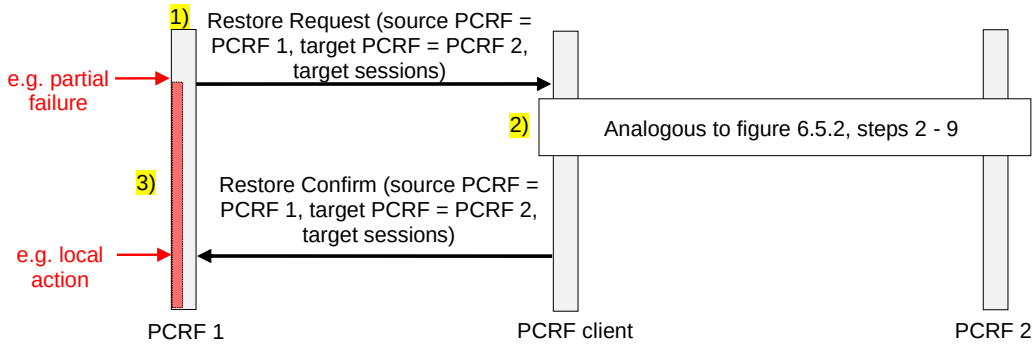

Figure 6.5.4: PCRF session state restoration (triggered by a partially failed PCRF onto an alternative PCRF node)

Two modes are possible for the restoration related signaling:

- single PCRF session mode: the restoration handling applies only for the PCRF session indicated by the given DIAMETER session id.
- multiple PCRF session mode: the restoration handling applies for a set of PCRF sessions. The same concept as for bulk signaling applies; i.e. a special session id, generated with the initial signaling between each PCRF node and PCRF client, and not bound to a UE and bearer session, is used (see subclause 6.7).

This solution is combinable with “PCRF failure reselection for the redirect DRA” described in subclause 6.1. For the deployment of multiple PCRFs with DRA, after successful restoration the target PCRF should become the new PCRF selected by the DRA in solution 1 to ensure correct DRA binding. Thus, the "Restore Request" and the "Restore Confirm" messages have to be sent via the DRA. Additionally it is required that the DRA becomes aware of "Restore Request"/"Restore Confirm" messages and of the PCRF sessions included therein.

This solution is combinable with “Graceful termination of services” described in subclause 6.3 in the time span before the grace time has expired: as soon as successful restoration of state has been achieved (i.e. after step 4), graceful termination can be revoked. If graceful termination was delegated, revocation has also to be delegated; some signaling extension is required for that purpose.

This solution should not be combined with “strict termination of services” described in subclause 6.4; even though the process of strict termination most likely will be spread out over a finite time, and within this time in theory some PCRF session state could be restored, the balance between gain and effort is estimated to be unfavourable, especially as the two methods would compete strongly for resources.

This solution does not alter the behaviour with DRA in case of single PCRF session mode; in case of multiple PCRF session mode the routing principles apply as for bulk signaling, i.e. based on FQ-PSSID (see subclause 6.7).

The extension of the procedure for linked sessions is shown in figure 6.5.5; it consists in repetition of steps as for one PCRF client and a matching function in the target PCRF node.

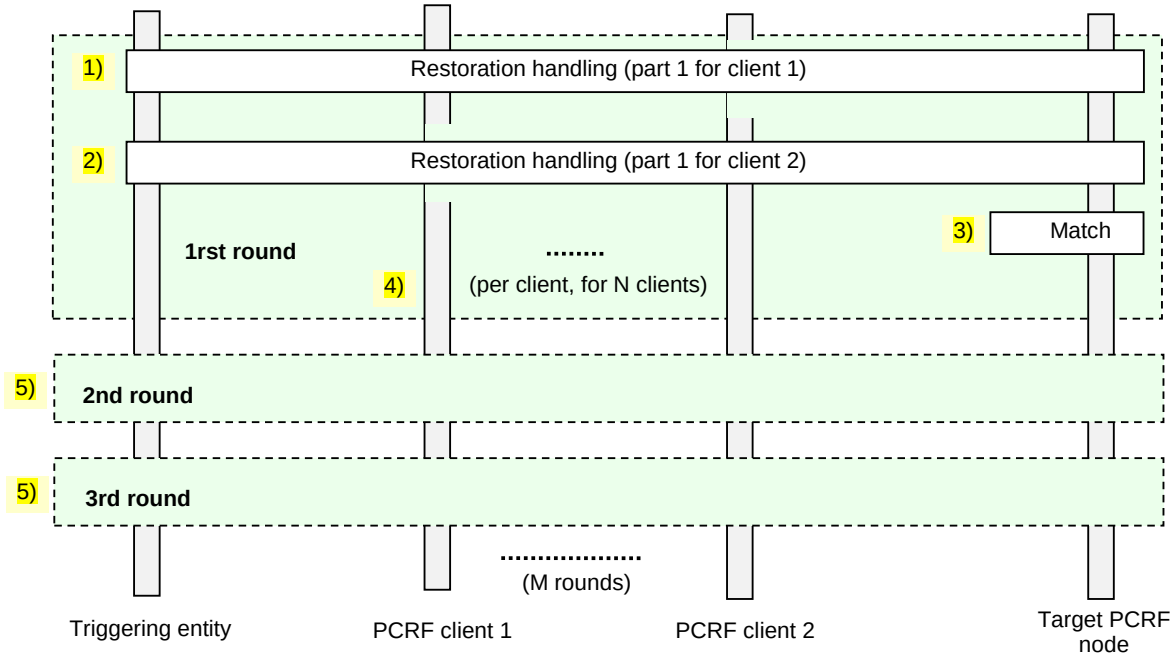

Figure 6.5.5: PCRF session state restoration for linked sessions

These are the steps:

1. steps 1 to 5 of figure 6.5.1 are executed for restoration state for part of the sessions with one of the PCRF clients .
2. the above step is repeated for another PCRF client.
3. The target PCRF tries to match (individually) restored sessions and correlates them in case of a match (e.g. as for session binding described in TS 29.213 [11]).
4. Steps 2 and 3 are repeated for other PCRF clients. Steps 1 to 4 build the first round of the overall procedure.
5. further rounds with successive parts of the sessions are executed; in the match procedure in all rounds the full set of restored session state is considered.

NOTE: After all rounds the session state is fully restored, and PCRF client sessions are linked as before the PCRF failure.

6.6 Solution 6: Soft recovery after a PCRF restart

6.6.1 Role of PCRF

PCRF receives session information and authorizes requests when a user session is set up. PCRF may also re-authorize ongoing sessions, if a session modification is requested, e.g. resources added/removed or due to a user plane event. When a user session is terminated, PCRF receives termination messages. When no session modification requests are sent by the clients to the PCRF, the PCRF is not visible to ongoing user sessions. A user session may need message exchange between the PCRF and the related clients (e.g. AF/P-CSCF and PCEF/BBERF) only when the session is started and when the session is terminated.

Consequently, a failure and the following restart of a PCRF may have no impact at all on ongoing sessions. The sessions may continue and end normally and naturally.

There is an impact only if a client handling an ongoing user session tries to contact the failed and restarted PCRF. The PCRF is not able to respond properly, because it has lost the status and information of the related Diameter sessions.

6.6.2 Actions required for a soft recovery

6.6.2.1 Procedure

The minimum actions required for a soft recovery from a PCRF restart:

- The restarted PCRF and connected/related clients know to act according to the same recovery and restoration rules (e.g. by rules/behaviour agreed through a feature negotiation).
- The restarted PCRF informs the related clients about the restart. The clients may respond by sending basic information, like user IDs of Diameter sessions that were active with the PCRF at the failure and restart, to help the PCRF with later restoration actions, e.g. to bind users to Diameter clients.
- The restarted PCRF and connected/related clients let the ongoing user sessions go on with no immediate recovery/restoration action towards the restarted element.
- The clients informed about the PCRF restart rebuild sessions at and with the restarted PCRF, when there is a need for a re-authorization request (e.g. due to an IP-CAN session modification or a user plane event). The client puts the Diameter session related information (e.g. user ID, IP address, PCC/QoS rules or related information), needed by the PCRF to rebuild the lost session status and information, in the re-authorization request message.
- The restarted PCRF sends recovery/restoration request message(s) with parameters identifying the user (e.g. user ID, IP address) to related other client(s) to request information for rebuilding the related lost Diameter session(s) with the client(s).
- A client receiving a recovery/restoration request message after a PCRF restart uses the user identity information to identify ongoing Diameter session(s) with the PCRF and responds to the PCRF by sending the Diameter session status and information (e.g. session ID, parameters received from the PCRF before the restart) lost by the PCRF at the failure and restart.
- The restarted PCRF rebuilds the Diameter session(s) towards the client(s), based on the session related parameters and information received from the client(s).

Figure 6.6.2.1.1 describes the soft recovery actions, when a PCEF requests a re-authorization (CC-Request) after a PCRF restart. In addition to AF/P-CSCF, there could be also other clients that should be involved in the session rebuilding towards the PCRF, e.g. BBERF and SPR. Similar session rebuilding actions could be caused also by a BBERF sending a CC-Request or an AF/P-CSCF sending an AA-Request to the PCRF after a PCRF restart.

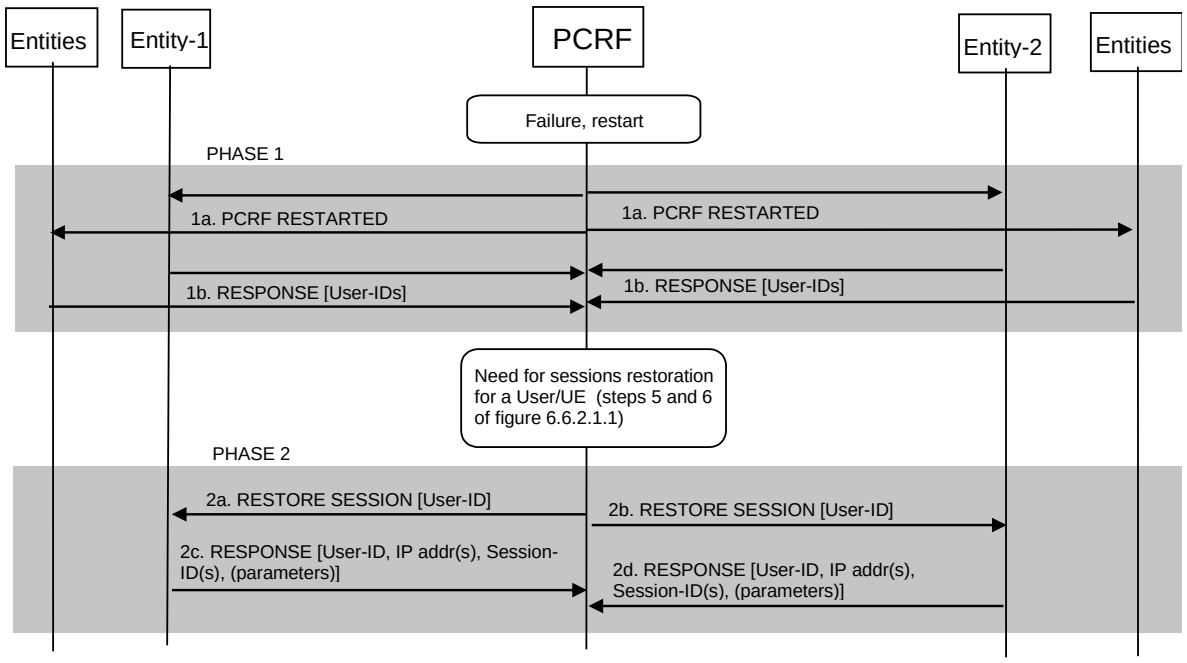

Figure 6.6.2.1.1: Soft recovery actions when PCEF requests re-authorization after a PCRF restart.

1. Connections between the PCRF and clients are established. The entities may agree/negotiate on the usage of restoration methods to be used in case of a failure.
2. Diameter sessions are established and ongoing as per established IP-CAN and AF sessions.
3. The PCRF fails and restarts.
4. The PCRF indicates the restart to its clients. The clients may send the PCRF some basic information, like user IDs of Diameter sessions that were active with the PCRF at the failure and restart, to help the PCRF with later restoration actions, e.g. to bind users to Diameter clients. (Different alternatives to perform the user-to-clients binding are described in subclause 6.2.2.2).
5. A PCEF identifies a need to send a CC-Request to the PCRF, e.g. due to an IP-CAN session modification or a user plane event.
6. The PCEF send a CC-Request to the PCRF. The PCEF may include Diameter session related information (e.g. user ID, IP address, PCC/QoS rules or related information), needed by the PCRF to rebuild the lost Gx session status and information.
7. The PCRF rebuilds the lost Gx Diameter session based on the information received from the PCEF.
8. The PCRF sends restoration request message with parameters identifying the user (e.g. user ID, IP address) to the AF/P-CSCF to request information for rebuilding the related lost Rx Diameter session with the AF/P-CSCF.
9. The AF/P-CSCF acknowledges request and may include Diameter Rx session related information (e.g. user ID, IP address, session information or other related information), needed by the PCRF to rebuild the lost Rx session status and information.
10. The PCRF rebuilds the lost Rx Diameter session based on the information received from the AF/P-CSCF.
11. The PCRF authorizes / responds to the CC-Request from the PCEF with a CC-Answer and relevant parameters, e.g. PCC rules.

6.6.2.2 Binding

6.6.2.2.1 Status after restart

After a restart the PCRF does not anymore have any binding information and it does not even know the network entities the to-be-rebuilt Diameter sessions are related to (e.g. which AF of the many in the network, which PCEF/GW of the many in the network, etc.).

Initially, when the PCEF and AF (and BBERF and visited PCRF) contact a PCRF, the PCRF selection is based on the user/UE idendity. The selected PCRF uses the identity also for binding the relevant Diameter sessions (Rx, Gx, etc.), i.e. deduces from the user/UE identity that the Diameter sessions are related to the same user/UE, as described in 3GPP TS 29.213 [11]. But this does not work in the reverse direction, i.e. when the restarted PCRF should find the relevant network entities for each user/UE session and perform the related session binding.

Alternative ways for the restarted PCRF to find the network entities related to the to-be-rebuilt Diameter sessions and to get the information required for the Diameter session binding:

6.6.2.2.2 OPTION 1: Identities exchange with recovery/rebuild messages

In phase 1, the entity (e.g. PCEF/GW or AF or H/V-PCRF) receiving the "PCRF RESTARTED" message (messages 1a in figure 6.6.2.2.2.1) sends (in the response to the "PCRF RESTARTED" message, messages 1b in figure 6.6.2.2.2.1) the user/UE ID of each UE related to a Diameter session (or Diameter sessions) between the entity and the PCRF. This way the restarted PCRF knows/identifies the network element (e.g. PCEF/GW or AF) per user/UE, and is able to contact the correct network elements later, if/when sending “RESTORE SESSION” messages for re-building the Diameter sessions.

In phase 2, if/when the PCRF requests user/UE related Diameter session information from an entity (messages 2a and 2b 8 in figure 6.6.2.2.2.1) including the user/UE identity as a parameter, the reply message includes the UE IP address/addresses and the Diameter session ID/IDs and APN and PDN connection IDs where applicable. The reply may also include a parameter / parameters indicating the role of the Diameter entity, e.g. “AF/Rx-over-S9” or “H-PCRF/S9”

to give the restarted PCRF a hint of its own role related to the UE's sessions. (The PCRF may possibly be able to deduce its role even without extra parameters, using e.g. the IP address, ID, APN and/or related realm information.)

NOTE: Several addresses and/or Diameter session IDs are possible, when the PCRF has several Diameter sessions with the element, e.g. with an AF having several AF sessions and/or possibly a Diameter Rx session for the signalling path status, or e.g. the UE has several IP-CAN sessions, or e.g. the AF is in a visited network meaning there is an Rx Diameter session and an S9 Diameter session between the H-PCRF and V-PCRF.

The PCRF deduces from user/UE IDs and IP addresses (and possibly from APNs and PDN connection IDs where applicable) that the Diameter sessions are related to the same UE and IP-CAN session, i.e. linked together, as per 3GPP TS 29.212 [10]. Especially, the PCRF performs session binding and associates the described service IP flows within the AF session information (and therefore the applicable PCC rules) to an existing IP-CAN session as per 3GPP TS 29.213 [11], i.e. by comparing the user IP address/addresses received via the Rx interface with the IP address/addresses received via the Gx interface and possibly using also the UE Identity.

Editor's Note: It is FFS how the binding is supposed to work, if the AF does not know the user identity used on the user plane. (Operations when the AF does not know the user identity are FFS also in the current Technical Specifications, see Editor's Notes in 3GPP TS 29.213 [11] and 3GPP TS 29.215 [13]).

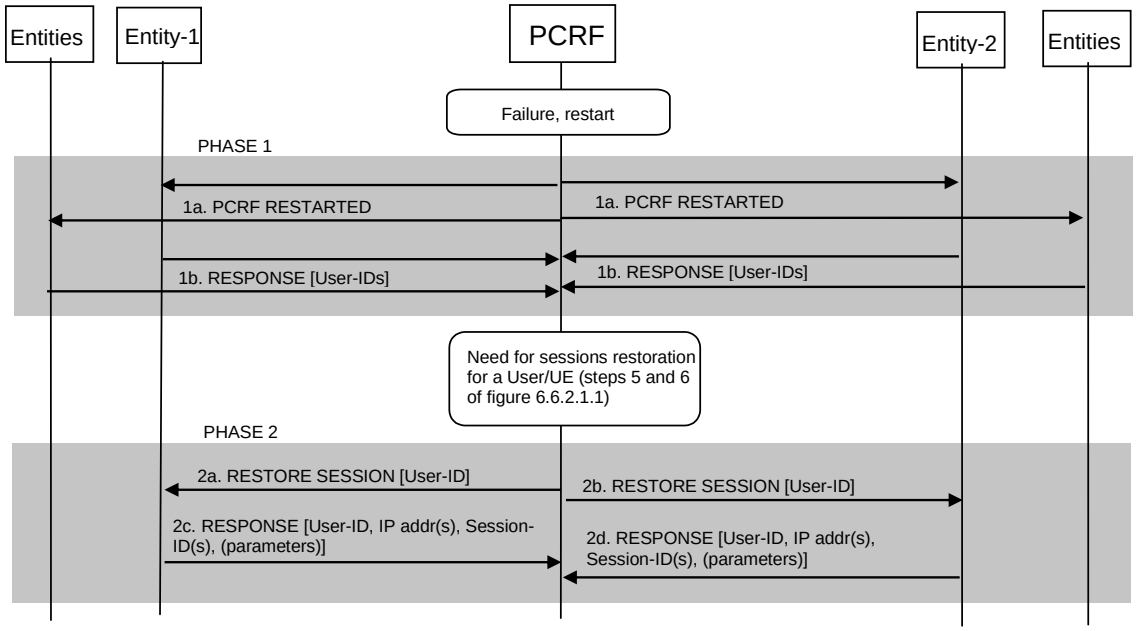

Figure 6.6.2.2.2.1: PCRF gets User-IDs in restart-response messages (phase 1 / messages 1x), PCRF requests session ID(s), IP address(es), etc. of active sessions of a given user (phase 2 / messages 2x) when needed.

6.6.2.2.3 OPTION 2: Restore/rebuild request sent to all candidates

If/when the restarted PCRF requests user/UE related Diameter session information from an entity (e.g. AF), the PCRF sends the request / "RESTORE SESSION" message (messages 1 in figure 6.6.2.2.3.1) to all entities that may possibly handle sessions for the UE, e.g. to all AFs in the network, including the user/UE identity as a parameter. The acknowledgement message, with Diameter session identity/identities and IP address/addresses and APN and PDN connection IDs where applicable, is received from the entity that recognizes the UE/user identity and/or IP address as being related to a Diameter session or Diameter sessions handled by the entity (messages 2 in figure 6.6.2.2.3.1), whereas the other entities reject the request message.

The PCRF performs session binding as above in option 1.

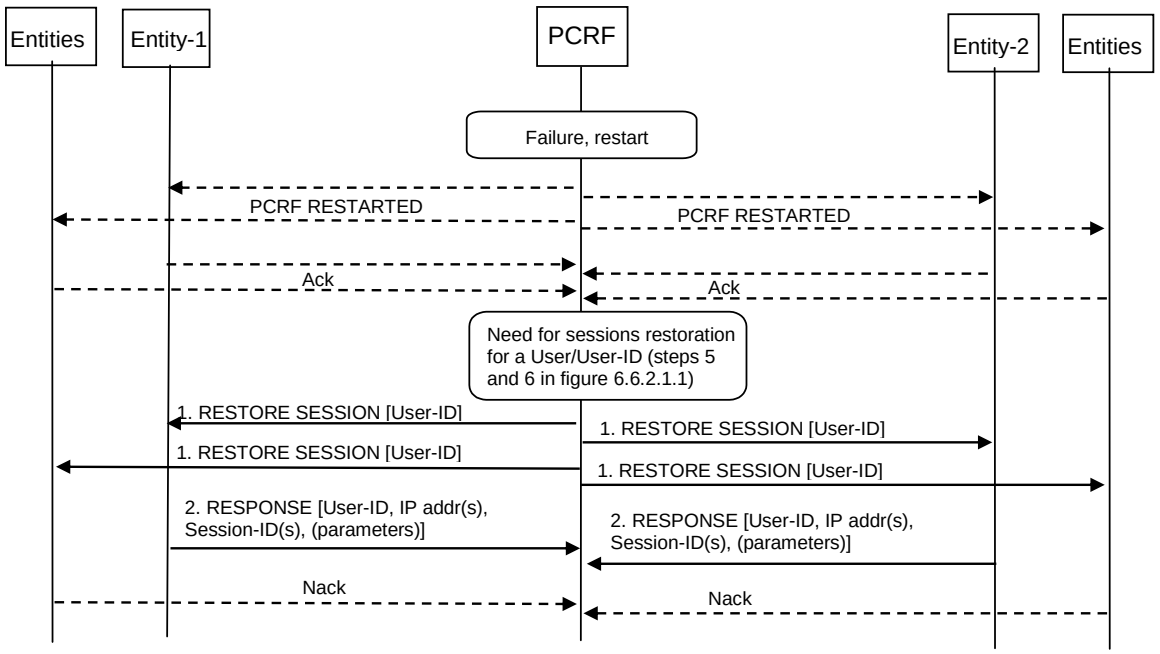

Figure 6.6.2.2.3.1: PCRF sends a restore session request (for a given user) to all candidate entities (step 1). PCRF receives reponse with parameters from entities having session(s) with the user/User-ID (step 2).

6.6.2.2.4 OPTION 3: Related Diameter identities saved and retrieved

As described in figure 6.6.2.2.4.1, essential parameters ("Params" in the figure) like the Diameter session identities of the Diameter sessions releated to a given UE and the IP addresses of the entities running the Diameter sessions (A, B and X in the figure) are saved in a PCRF-external entity (Client-X in the figure) e.g. upon each IP-CAN session or AF session establishment or upon each Diameter session establishment. Further information to be saved may be a parameter / parameters indicating the role of the Diameter entity, e.g. "AF/Rx-over-S9" or "H-PCRF/S9" to give the restarted PCRF a hint of its own role related to the UE's sessions. (The PCRF may possibly be able to deduce its role even without extra parameters, using e.g. the IP address, ID, APN and/or related realm information.) The entity saving the information may be one or several or all of the involved entities (e.g. an SPR and/or PCEF/GW and /or AF).

The information to be saved may be included in the UE sessions related Diameter commands/responses from the PCRF to the related entities. The identities and the addresses of the related entities need to be retrieved to the PCRF after a PCRF restart only if/when required by the PCRF. For example, when a PCEF sends a CC Request to the PCRF to modify an IP-CAN session after a restart has taken place, the PCRF may retrieve the related Diameter session identity and IP address information from the SPR. As another example, if the PCEF has saved the information, it may send the information to the PCRF in the CC Request.

If/when the PCRF needs to request user/UE related Diameter session information from an entity (e.g. AF after receiving a CC Request from a PCEF), the PCRF uses the retrieved IP address of the entity (to send the request to the correct network element) and the retrieved Diameter session identity/identities (to identify the Diameter session/sessions).

The PCRF performs session binding as above in option 1.

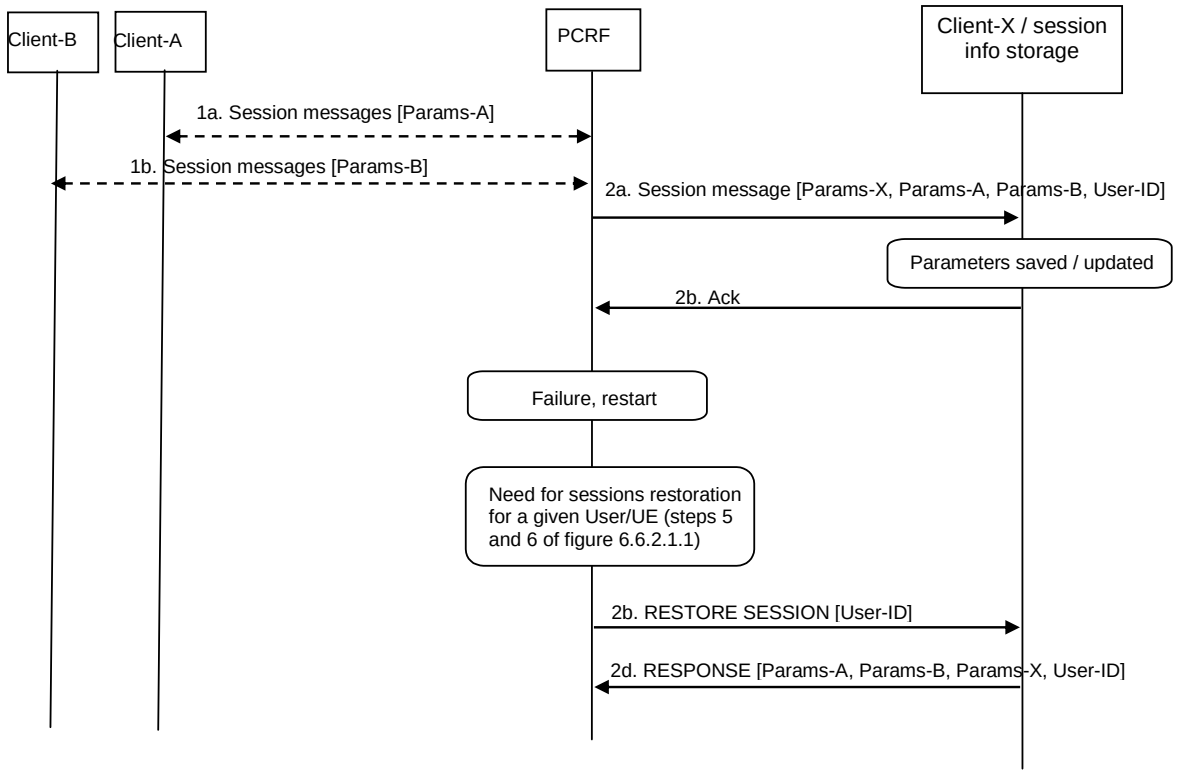

Figure 6.6.2.2.4.1: Session identities and IP addresses saved in PCRF external entity, PCRF retrieves the parameters of a given user when needed.

6.6.2.3 Information exchange between PCRF and clients

6.6.2.3.1 Status after restart

A restarted PCRF has most probably lost all ongoing Diameter session information like the AF session information received from the AF, bearer level related information received from PCEF/BBERF and/or from the V-PCRF in the visited case, PCC/QoS rules received from the H-PCRF in a visited case, subscription related information received from the SPR.

Related network entities may have been informed about the restart of the PCRF, as described elsewhere in this TR.

The restarted PCRF may be triggered to request the missing Diameter session information (e.g. per Diameter session or per UE identity) or related Diameter counterpart entity / client may be triggered to modify the session and perform the after-the-restart refresh for the Diameter session(s) of the user/UE at the same time, as described elsewhere in this TR.

6.6.2.3.2 Information from AF

Retrieved information from an AF to a restarted PCRF contains, for each Diameter session existing at the AF for an AF session, the latest full session information sent by the AF to the PCRF before the PCRF restart and the requests for notifications of bearer events as per 3GPP TS 29.214 [12].

NOTE: The negotiated session information is assumed to be saved by the AF/P-CSCF for the duration of an ongoing AF session, because it is possible for the AF/P-CSCF to modify the session information at any time e.g. due to an AF internal trigger (refer to 3GPP TS 29.214 [12]).

6.6.2.3.3 Information from PCEF

The PCRF should be able to retrieve the UE and IP-CAN session related information (i.e. PCC rules, authorized QoS, event triggers, charging related information, thresholds for usage monitoring control) sent to the PCEF or received from the PCEF before the PCRF restart but possibly lost at the restart.

6.6.2.3.3.1 OPTION 1: PCRF retrieves input parameters and recreates the lost information

The PCRF recreates the information itself as it did originally when the UE's IP-CAN session(s) and AF session(s) were established.

If the rebuilding of the UE related Diameter sessions is triggered by an IP-CAN session modification request (CC Requst) from the PCEF and if the PCEF is aware of the restart of the PCRF (as described elsewhere in this TR), the PCEF may send the CC Request with a complete set of parameters (as per 3GPP TS 29.212 [10], subclause 4.5.1) related to the existing IP-CAN session (possibly with a new CC-Request-Type AVP value "REBUILD_REQUEST"). The PCEF may also send the accumulated usage / data volume reported to the PCRF before the PCRF restart. The PCRF requests the related AF session information from the AF, the related subscription profile from the SPR and possibly further related information from the V/H-PCRF and BBERF. The PCRF recreates the information assumed to be sent earlier to the PCEF (i.e. the PCC rules, authorized QoS, event triggers, charging related information, thresholds for usage monitoring control).

If the rebuilding of the UE related Diameter sessions is triggered by an AF session modification request (AA Request from the AF/P-CSCF), the PCRF requests the IP-CAN session related information from the PCEF (using a proper request type value). The PCEF responds by sending a complete set of parameters (as per 3GPP TS 29.212, subclause 4.5.1) related to the existing IP-CAN session. The PCEF may also send the accumulated usage / data volume reported to the PCRF before the PCRF restart. The PCRF requests similarly the related subscription profile from the SPR and possibly further related information from the V/H-PCRF and BBERF. The PCRF recreates the information assumed to be sent earlier to the PCEF (i.e. the PCC rules, authorized QoS, event triggers, charging related information, thresholds for usage monitoring control). To verify that the PCEF is synchronized with the rebuilt information (PCC rules, authorized QoS, etc.), the PCRF may push the information to the PCEF with an RA Request.

NOTE: This option obviously poses a requirement for the PCEF to be able to return to the PCRF the accumulated usage / data volume reported to the PCRF before the PCRF restart.

6.6.2.3.3.2 OPTION 2: PCRF retrieves information sent to PCEF before restart

The restarted PCRF receives the lost information (assumed to be sent earlier to the PCEF, i.e. the PCC rules, authorized QoS, event triggers, charging related information, thresholds for usage monitoring control) from the PCEF as such, i.e. in the format the PCRF has earlier sent the information to the PCEF. The PCEF sends also the up-to-date user plane event status to the PCRF. The PCEF may also send the accumulated usage / data volume reported to the PCRF before the PCRF restart.

If the rebuilding of the UE related Diameter sessions is triggered by an IP-CAN session modification request (CC Requst) from the PCEF and if the PCEF is aware of the restart of the PCRF (as described elsewhere in this TR), the PCEF may send the lost information within the CC Request.

If the rebuilding of the UE related Diameter sessions is triggered by some other entity (e.g. by an AF/P-CSCF requesting AF session modification), the PCRF requests the lost information from the PCEF.

NOTE 1: This option poses a requirement for the PCEF to be able to return the information (PCC rules, authorized QoS, etc) to the PCRF as such, i.e. in the format the PCRF has earlier sent the information to the PCEF.

NOTE 2: This option obviously poses a requirement for the PCEF to be able to return to the PCRF the accumulated usage / data volume reported to the PCRF before the PCRF restart.

6.6.2.3.4 Information from BBERF

The same principle and options can be applied to BBERF as to PCEF above, but the information is limited to what is defined for Gxx in 3GPP TS 29.212 [10], subclause 4a.5 (i.e. excluding e.g. charging and usage monitoring related information and using QoS rules rather than PCC rules).

6.6.2.3.5 Information from PCRF

Retrieved information from an PCRF to a restarted PCRF depends on whether the restarted PCRF is an H-PCRF or a V-PCRF for the to-be-rebuilt Diameter session, whether the case is a home routed access or a visited access and whether the AF is in the visited network or in the home network, as per 3GPP TS 29.215 [13], and recapped in the subclauses below.

6.6.2.3.5.1 Restarted V-PCRF, home routed access

The restarted V-PCRF in home routed access receives from the H-PCRF the up-to-date QoS rules and event triggers (per gateway control session) assumed to be received from the H-PCRF before the V-PCRF restart.

6.6.2.3.5.2 Restarted V-PCRF, visited access

The restarted V-PCRF in visited access receives from the H-PCRF the up-to-date PCC rules and event triggers (per IP-CAN and gateway control session) assumed to be received from the H-PCRF before the V-PCRF restart.

6.6.2.3.5.3 Restarted H-PCRF, home routed access

The restarted H-PCRF in home routed access receives from the V-PCRF the up-to-date QoS rules and event triggers (per gateway control session) assumed to be sent by the H-PCRF to the V-PCRF before the H-PCRF restart.

6.6.2.3.5.4 Restarted H-PCRF, visited access, AF in HPLMN

The restarted H-PCRF in visited access case receives from the V-PCRF the up-to-date PCC rules and event triggers (per IP-CAN and gateway control session) assumed to be sent by the H-PCRF to the V-PCRF before the H-PCRF restart.

6.6.2.3.5.5 Restarted H-PCRF, visited access, AF in VPLMN

The restarted H-PCRF in visited access case receives from the V-PCRF the up-to-date PCC rules and event triggers (per IP-CAN and gateway control session) assumed to be sent by the H-PCRF to the V-PCRF before the H-PCRF restart.

The restarted H-PCRF in visited access case and with the AF in the VPLMN receives from the V-PCRF also the up-to-date AF session information (per AF session) assumed to be received from the V-PCRF before the H-PCRF restart.

6.6.2.3.6 Information from SPR

Retrieved information from an SPR to a restarted PCRF contains the latest subscription data profile as provided to the PCRF before the PCRF restart.

NOTE: The subscription data profile and the interface between the PCRF and SPR have not been defined in the present release.

6.6.2.3.7 Messages for information transfer

If the rebuilding of the UE related Diameter sessions is triggered by some entity/client, a regular application specific message is used, but the message may contain extra information (described above for each possible interface and entity), if/when the requesting entity/client is aware of the restart of the PCRF.

The PCRF requests the related information from other related entities/clients in order to be able to recreate or retrieve the information lost at the restart. The requested entities may send the session information within separate application specific Diameter request/answer messages per Diameter session, meaning that no new messages are required. Alternatively, the reply/acknowledge message to the request by PCRF may contain the per Diameter session information.

6.6.3 Impact of the solution on specifications

6.6.3.1 Minimum impact

Apart from the general issues of failure detection and selection of restoration scheme (refer to clause 4), the minimum impact described in this subclause applies, no matter which alternatives of the soft recovery solution are used.

NOTE: The following list of impacts complies with the current specification structure. The final specification structure may be different, if for example new technical specifications are established during the course of the work.

TS 29.212:

- Details of the request from the PCRF to the PCEF/BBERF to send parameters for restoration shall be defined. For example the usage of a RAR message with a new AVP / new AVPs on Gx/Gxx.
- It shall be defined which parameters the PCEF/BBERF shall send to the PCRF in response to the restoration request.
- The usage reporting AVPs shall be complemented with the possibility for the PCEF to be able to return to the PCRF the accumulated usage / data volume reported to the PCRF before the PCRF restart

TS 29.214:

- Details of the request from the PCRF to the AF to send parameters for restoration shall be defined. For example the usage of a RAR message with a new AVP / new AVPs on Rx.
- It shall be defined which parameters the AF shall send to the PCRF in response to the restoration request.

TS 29.215:

- Details of the request from the H-PCRF to the V-PCRF, and vice versa, to send parameters for restoration shall be defined. For example the usage of a RAR message with a new AVP / new AVPs from the H-PCRF to the V-PCRF and the usage of a CCR message with a new AVP / new AVPs from the V-PCRF to the H-PCRF.
- It shall be defined which parameters the H-PCRF shall send to the V-PCRF, and vice versa, in response to the restoration request.

6.6.3.2 Possible further impact

The further impact described in this subclause may apply, depending on the chosen alternatives.

TS 29.212:

- Parameters (e.g. Diameter session IDs) sent from the PCEF/BBERF to the PCRF on restart detection. This is required, if it is specified that the PCRF uses option 1 in subclause 6.6.2.2.2 to find related network entities.
- Definition of sending parameters in the opposite direction over Gx/Gxx, if it is specified that the PCRF uses option 2 in subclause 6.6.2.3.3.2 to restore information to the PCRF.
- If it is specified that the PCRF uses option 3 with the PCEF/BBERF in subclause 6.6.2.2.4 for identifying lost Diameter sessions and finding related network elements, an AVP / AVPs is/are required for transferring the Diameter session ID and network entity address information between the PCRF and PCEF/BBERF.

TS 29.214:

- Parameters (e.g. Diameter session IDs) sent from the AF to the PCRF on restart detection. This is required, if it is specified that the PCRF uses option 1 in subclause 6.6.2.2.2 to find related network entities.
- If it is specified that the PCRF uses option 3 with the AF in subclause 6.6.2.2.4 for identifying lost Diameter sessions and finding related network elements, an AVP / AVPs is/are required for transferring the Diameter session ID and network entity address information between the PCRF and AF.

TS 29.215:

- Parameters (e.g. Diameter session IDs) sent from the H-PCRF to the V-PCRF, and vice versa, on restart detection. This is required, if it is specified that the PCRF uses option 1 in subclause 6.6.2.2.2 to find related network entities.
- If it is specified that the H-PCRF uses option 3 with the V-PCRF, or vice versa, in subclause 6.6.2.2.4 for identifying lost Diameter sessions and finding related network elements, an AVP / AVPs is/are required for transferring the Diameter session ID and network entity address information between the PCRFs.

6.7 Solution 7: Bulk Signaling

6.7.1 General bulk signaling

If signaling for a larger number of PCRF sessions has to occur at the same time, but the information to be signaled is not shared between sessions but rather is individual, the more optimized PSSID concept (see subclause 6.7.2) cannot be used. There is still the benefit of bulk signaling in terms of reduced total amount of transmitted data and less parsing; in this case the PCRF application signaling message can be built like shown in figure 6.7.1.1.

NOTE: This usage is e.g. useful in case of partial PCRF failures.

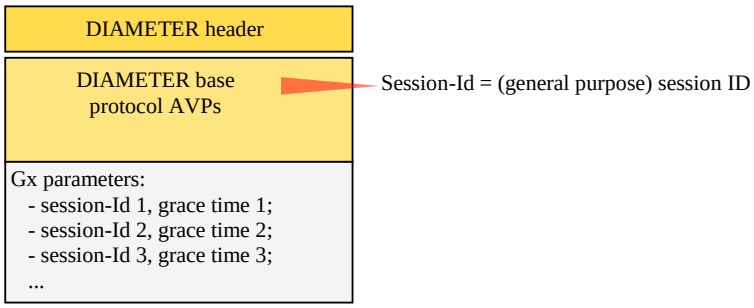

Figure 6.7.1.1: General bulk signaling (example: teardown of Gx sessions using RAR command)

For that purpose, per application command the admissible structures of bulk signaling need to be defined.

6.7.2 Bulk signalling based on PCRF Session Set ID (PSSID)

6.7.2.1 Concept

This kind of signaling allows to handle large amounts of PCRF sessions efficiently and is based on session sets. A prerequisite is that the information to be signaled in addition to session identification (it may also be null) is shared by all the sessions of a set (e.g. a grace time).

A PCRF Session Set Identifier (PSSID) identifies a set of PCRF sessions within a PCRF node and its PCRF clients. PCRF Session Sets may be created and maintained by the PCRF nodes. Each node (PCRF and clients) maintains a local mapping of PSSID to its internal resources. PSSIDs can be used in bulk signaling in case of total or partial failures, e.g. to tear down PCRF sessions or to restore PCRF session data efficiently. However, the PSSID concept may not be supported by a PCRF if the PCRF performs the bulk signaling always per nodal basis.

The fully qualified PSSID (FQ-PSSID) is the combination of the node identity and one or more PSSIDs assigned locally by the node, and identifies a set of PCRF sessions.The node identifier shall be globally unique across all 3GPP networks.

Editor's note: the format of FQ-PSSID needs to be defined in 3GPP TS 29.21x series.

Further characteristics of the PSSID concept are:

- PSSIDs may relate to diverse input criteria in the allocating node e.g. a HW components (blades), a SW components (DB slices), a service or a user;
- the PSSID which is linked to a PCRF session is allocated by the PCRF node and is signaled to PCRF client(s);
- in comparison with bulk signaling using a flat list of PCRF/DIAMETER session ids, PSSIDs allow for compacting the amount of session identification information in the signaling;
- the size of the set represented by a PSSID (i.e. the granularity of bulk signaling) depends on the implementation, but the trade-off between the effort of encoding/decoding FQ-PSSIDs and the amount of signaled information should be considered.

Figure 6.7.2.1.1 visualizes the concept at the example of two PCRF nodes and two PCRF clients.

The support of PSSIDs is an optional feature for PCRF and PCRF clients.

In order to terminate in the bearer plane all sessions that correspond to the PSSID, a PCRF client should link a PSSID to a CSI that is used for the S5/S8/S11 interfaces. In this way, a bulk session termination over the S5/S8/S11 interfaces can be achieved.

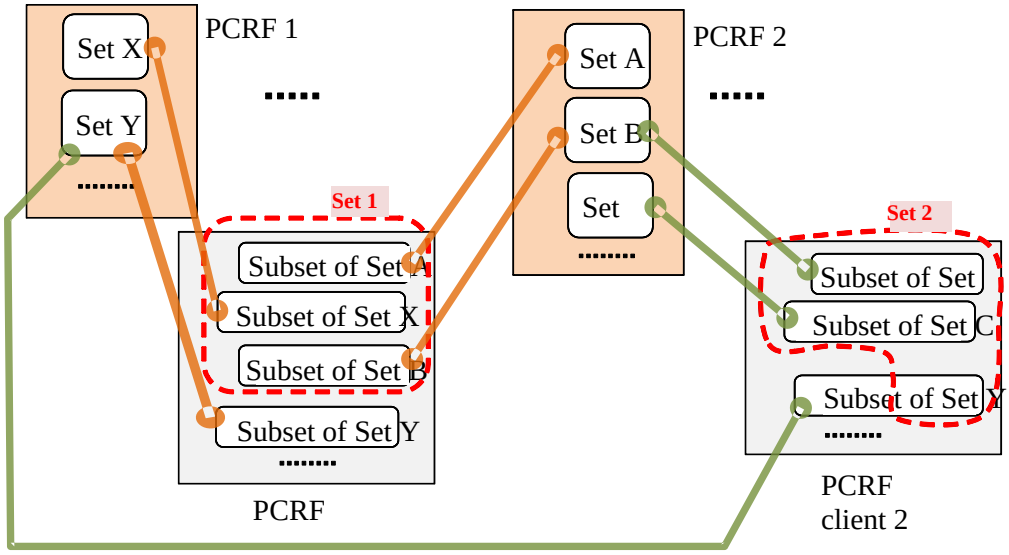

Figure 6.7.2.1.1: Concept of PSSIDs

6.7.2.2 Use in signaling

During PCRF session establishment, depending on the support of the feature, both the PCRF node and the PCRF client may provide a FQ-PSSID containing exactly one PSSID for that particular PCRF session in the appropriate request and response message(s) (CCR, CCA). The receiving node shall store the Node-ID and PSSID values from the FQ-PSSID in its PCRF session data.

If there is a need for bulk signaling, PSSIDs can be used instead of individual session identification (e.g. the "target sessions" in step 1 of the procedure described in figure 6.5.1). A possible coding is illustrated in Annex A.1.

NOTE: when using FQ-PSSIDs, their size should be considered in conjunction with rest of signaled DIAMETER AVPs with respect to IP fragmentation.

An example for the use of PSSID in signaling is shown in figure 6.7.2.2.1. Here a general purpose session is used for the signaling on DIAMETER level, wheres PSSIDs are used inside the bulk signaling message to address sets of PCRF application sessions.

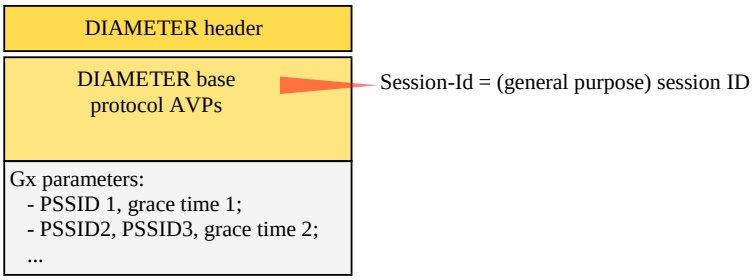

Figure 6.7.2.2.1: Use of PSSID in signaling (example: teardown of Gx sessions using RAR command)

For that purpose, per application command the admissible structures of bulk signaling need to be defined.

6.7.3 Embedding in the DIAMETER signaling concept

DIAMETER, as a AAA type of protocol, is session oriented and up to now does not foresee the concept of bulk signaling (or structuring of a multitude of sessions); PCRF applications are based on the underlying DIAMETER session model. A simple solution consists in defining a session specifically for the bulk signaling; it should be created as the first one after a PCRF client has started up, e.g. by exchanging a dummy RAR/RAA message with empty FQ-PSSIDs. All further bulk signaling messages reuse the same session-id.

Editor's note: DIME WG within IETF#78 has started a discussion on the DIAMETER General Purpose Session concept, see http://tools.ietf.org/html/draft-liebsch-dime-diameter-gps-00 and http://www.ietf.org/proceedings/78/minutes/dime.txt. Results thereof should be cross checked, if and when available.

The routing of bulk signaling requests and responses in DRA has to be done directly based on the node identity within FQ-PSSID.

6.8 Solution 8: Adding explicit resilience to PCRF sessions

6.8.1 Concept

The overall concept consists in distribution of PCRF relevant information in transparent form to other nodes, in particular to PCRF clients. This helps in later, quick restoration of PCRF session state after a PCRF failure, while avoiding the efforts/costs of e.g. full mirroring of PCRF nodes.

A PCRF session information container is defined for this purpose as shown in figure 6.8.1.1 for the example of a PCEF as PCRF client. PCRF clients, when receiving and storing it, need not understand its detailed contents and internal structure; fig. 6.8.1.1 is thus only an illustration. It is plausible to assume that the leading part of the container consists of information elements which allow to access PCRF the internal database fast and efficiently.

Since this solution consumes memories in PCRF clients and also makes the recovery process longer, limiting resilience only for higher prioritized sessions could be beneficial. This priority handling can be performed in the PCRF based on the operator policy, for example only for IMS related sessions or based on a subscription; the PCRF does not distribute a PCRF session information container to PCRF clients for sessions which are not subject to explicit resilience handling.

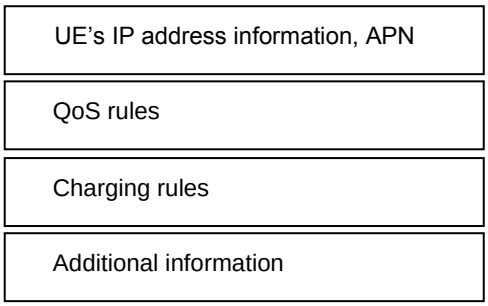

Figure 6.8.1.1: Contents of PCRF session information container (example of PCEF as PCRF client)

As this is an optional feature for both PCRF clients and servers, it is necessary to indicate the capability in initial signaling between the two.

Because the largest part of PCRF session information container is transparent to clients, it is up to the PCRF implementation how to apply this scheme to linked sessions, e.g.:

1. per leg, including only leg specific information in a corresponding, specific PCRF session information container; or
2. common for all legs, including all necessary information from linked sessions in one common PCRF session information container.

Consequently it is also a PCRF implementation issue when to update the PCRF session information container; the tradeoff between criticality/significance of state change and amount of signaling should be considered. The minimum

requirement for the restoration to work to the maximum extent possible is that the PCRF updates the PCRFsession information container whenever the PCRF session state changes, e.g. also due to updates from any leg in case of a linked sessions or an internal PCRF internal update. This may require additional signalling procedures, apart from adding the information in update signaling which is in any case exchanged with PCRF clients (i.e. independent of this resilience scheme).

6.8.2 Signaling procedures

Figure 6.8.2.1 displays the information flow for an initial PCRF session setup in course of an initial attachment in EUTRAN, followed by PCRF failure and PCRF session restoration based on the explicit resilience scheme. This example holds for EPS with GTP as the mobility protocol.

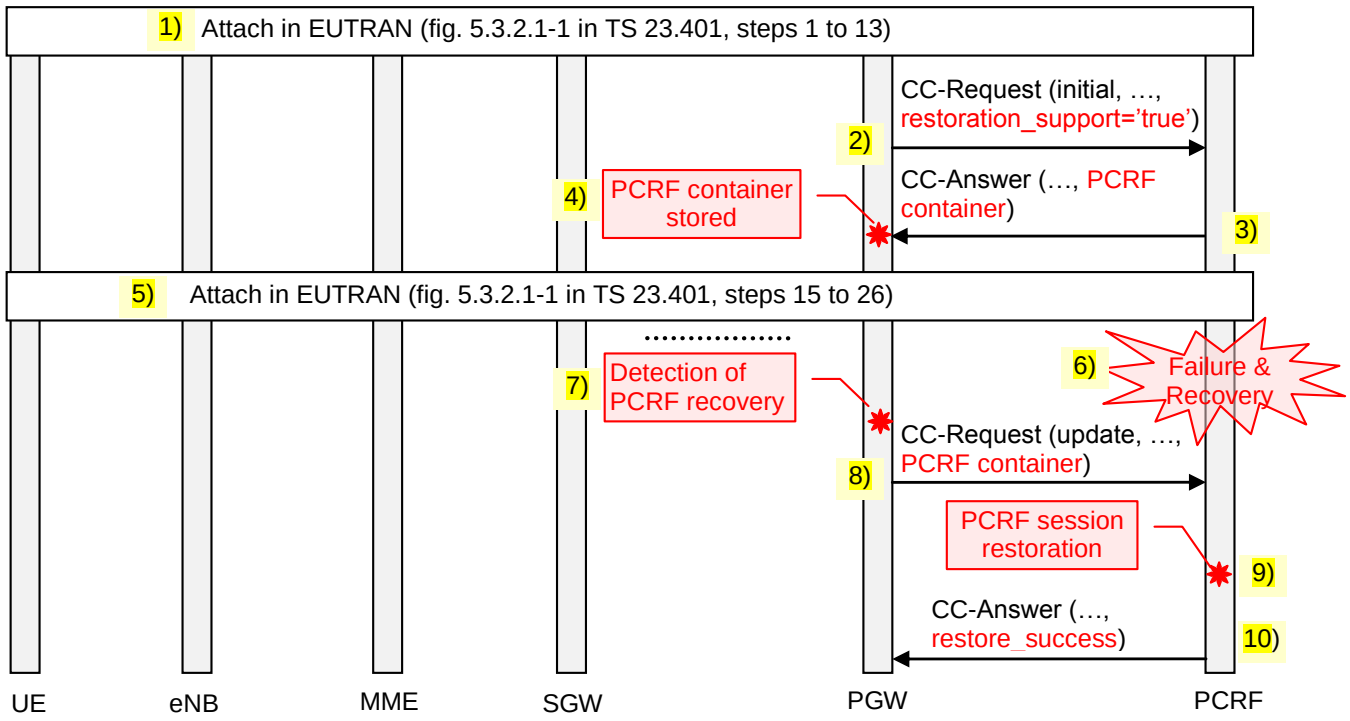

Figure 6.8.2.1: Information flow for PCRF session setup, PCRF failure and PCRF session state restoration based on the explicit resilience scheme

These steps are performed:

1) The first part of initial attachment is executed (up to the request for establishment of bearer sessions).

2) At the point where IPCAN session establishment takes place from PGW, the DIAMETER message CC-Request is enhanced by an indication for support of the scheme described here.

3) If the PCRF supports the explicit resilience scheme and the requested session is subject to explicit resilience, handling, it includes in the CC-Answer signaling message additionally a PCRF session information container as described in subclause 6.6.1.

4) The PCRF client (PGW) stores the PCRF session information container but does not interpret it.

5) All the rest of steps of initial attachment are executed.

6) After some time a failure and subsequently recovery occurs at the PCRF.

7) PGW detects the recovery of the PCRF node by means according to subclause 4.2.

8) PGW retrieves the stored PCRF session information container and sends an CC-Request message with update indication, transferring the PCRF session information container back to the PCRF. According to the operator policy, the PGW may initiate this procedure at any time (e.g. immediately or when user interaction takes place).

9) PCRF node restores the PCRF session data.

10) PCRF confirms its successful restoration of PCRF session data to PGW with an CC-Answer message including a success indication.

For steps 8 to 10 the variant with bulk signaling is easily possible, reducing largely the signaling load; in this case one CC-Request message carries a whole set of PCRF session information containers.

Note that for additional PDN connections a similar message flow can be used (involving potentially another PGW and another or the same PCRF). In a similar way the PCRF session information container is transferred also when re-authorization of resources by PCRF occurs, with equivalent enhancements for RA-Request and RA-Answer messages.

For the PMIP based EPC case, the same enhancements for the CC-Request and CC-Answer procedure as described in this section shall apply to the signaling on the Gxx interface between PCRF and SGW.

The explicit resilience concept can be applied also to an AF as a PCRF client, this is visible from figure 6.8.2.2 for the example of PCRF-AF interaction in course of the initial attachment in EUTRAN (i.e. based on figure 6.8.2.1).

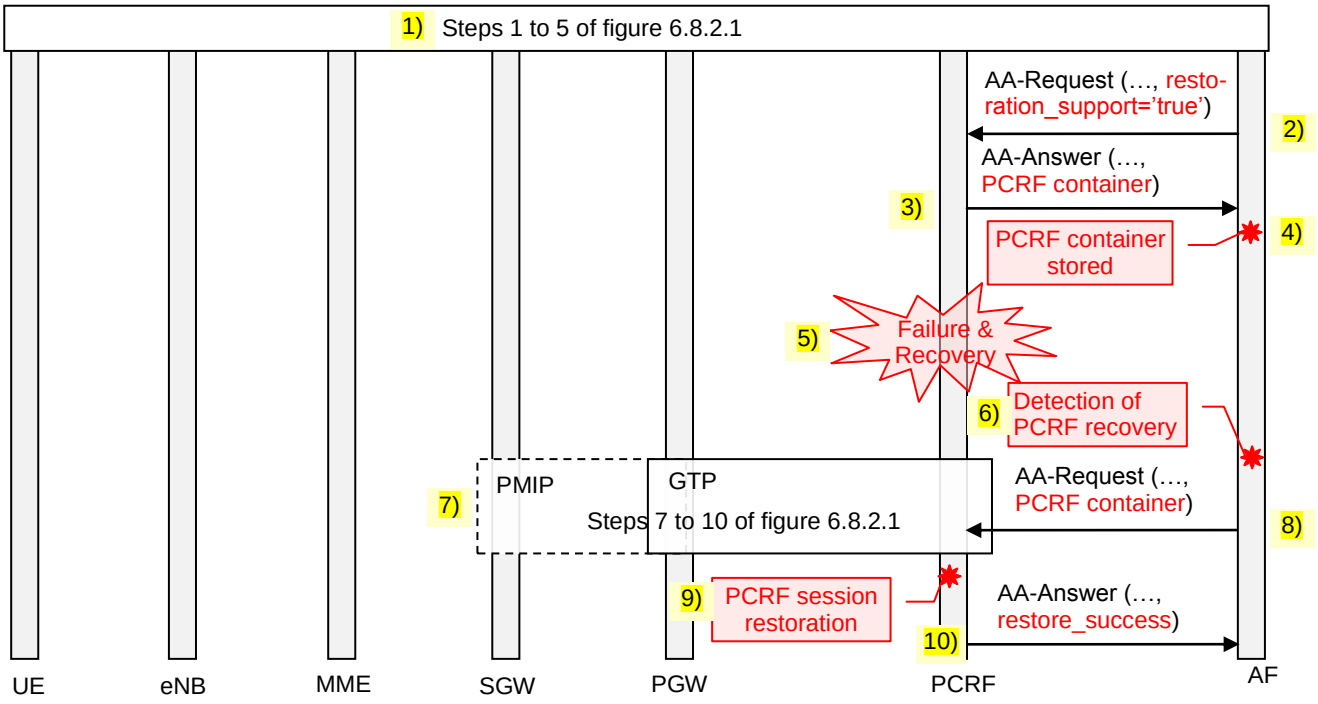

Figure 6.8.2.2: Explicit resilience scheme applied to AF session

The signaling procedure consists of the following steps:

1) An attachment in EUTRAN has been performed, including PCRF control (as detailed in the first part of the previous flow graph).

2) An application function requires PCRF support and directs an AA-request message to the PCRF node in charge of the bearer session; in this message an indication for support of explicit resilience mechanism is included.

3) If the PCRF supports the explicit resilience scheme and the requested session is subject to explicit resilience handling, it includes in the AA-Answer signaling message additionally a PCRF session information container as described in subclause 6.8.1.

4) The PCRF client (AF) stores the PCRF session information container but does not interpret it.

5) After some time a failure and subsequently recovery occurs at the PCRF.

6) AF detects the recovery of the PCRF node by means according to subclause 4.2.

7) The signaling for restoration of the bearer plane is performed. (For generality also the difference between GTP and PMIP case is visualized here.)

8) AF retrieves the stored PCRF session information container and sends an AA-Request message with update indication, transferring the PCRF session information container back to the PCRF. According to the operator policy, the AF may initiate this procedure at any time (e.g. immediately or when user interaction takes place).

9) PCRF node restores the PCRF session data.

10) PCRF confirms its successful restoration of PCRF session data to the AF with an AA-Answer message including a success indication.

The usage of this concept with DRA is shown in figure 6.8.2.3 for some bearer plane related PCRF session; here it is assumed that failure and recovery of PCRF 1 is detected by PGW indirectly via the DRA (but other means are not excluded). PCRF session information container and other, above described enhanced information elements of DIAMETER signaling messages are passed transparently through the DRA.

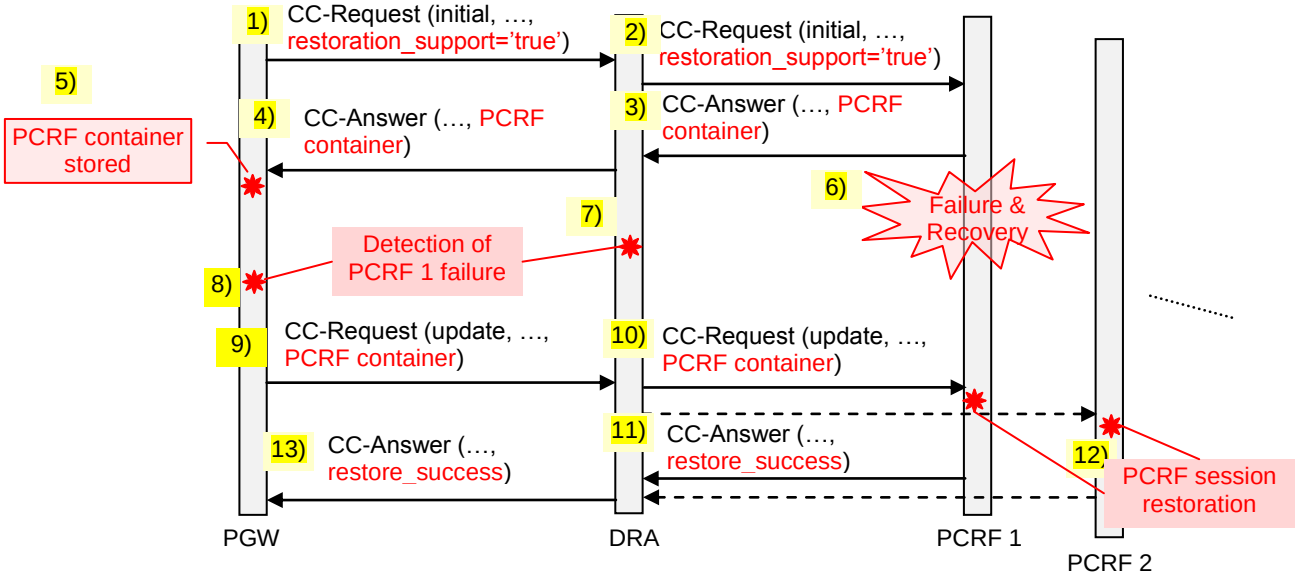

Figure 6.8.2.3: explicit resilience scheme applied with DRA

The signaling procedure consists of the following steps:

1) A PGW requires PCRF support and directs a CC-request message to the DRA; in this message an indication for support of explicit resilience mechanism is included.

2) DRA forwards a CC-request message to a PCRF node in charge of the bearer session.

3) If the PCRF supports the explicit resilience scheme and the requested session is subject to explicit resilience handling, it includes in the CC-Answer signaling message additionally a PCRF session information container as described in subclause 6.8.1.

4) The DRA forwards a CC-Answer message to the PGW.

5) The PCRF client (PGW) stores the PCRF session information container but does not interpret it.

6) After some time a failure and subsequently recovery occurs at the PCRF 1.

7) The DRA detects the recovery of the PCRF node by means according to subclause 4.2.

8) The PGW is informed about the recovery of the PCRF 1 by the DRA. (A particular way of doing this is not shown here.)

9) PGW retrieves the stored PCRF session information container and sends a CC-Request message with update indication, transferring the PCRF session information container back to the DRA.

10) The DRA forwards the CC-Request message to the PCRF 1 if it is known by DRA that it has recovered. If the PCRF 1 has not yet been recovered, the DRA alternatively chooses the PCRF 2 to continue the PCC management for the session. This procedure is shown with the dotted lines.

11) The chosen PCRF node (PCRF1 or PCRF 2, depending on step 10) restores the PCRF session data.

12) The chosen PCRF confirms its successful restoration of PCRF session data to the DRA with a CC-Answer message including a success indication.

13) The DRA forwards a CC-Answer message to the PGW.

This solution can preferably be combined with "bulk signaling" for the restoration part as described in subclause 6; in this manner the efficiency of the restoration process can be greatly enhanced and the time span reduced. This solution should not be combined with "strict termination of services" as described in subclause 6.4, as these two try to achieve opposing goals. A possible coding of signaling messages and their parameters in TS 29.212, for the example of including PCRF session information transparent container in the CC Request and CC Answer messages, is given in annex A.4.6.9.

6.9 Solution 9: Unified solution for termination of bearer services

The three distinct cases regarding termination of bearer services (solution 3, solution 4 and "loose handling", which is not documented separately) can be unified by defining a an overall grace time and varying it from zero to (practically) infinity. A grace time of zero corresponds to immediate teardown of bearer resources, a very large grace time to loose handling.

The constituent parts of this unified solution are:

- PCRF failure detection,
- timer setting,
- (optional): indicating a grace time handling to neighbouring node(s),
- supervision of bearer(s)/application sessions regarding timer expiry and tear down of bearer(s)(or tear down of application sessions leading to tear down of bearer resources) by other nodes, and
- if timer expired: local tear down.

This is visualized in figure 6.9.1 for a PCRF client in the bearer plane and in figure 6.9.2 for a PCRF client in the application plane (i.e. an AF).

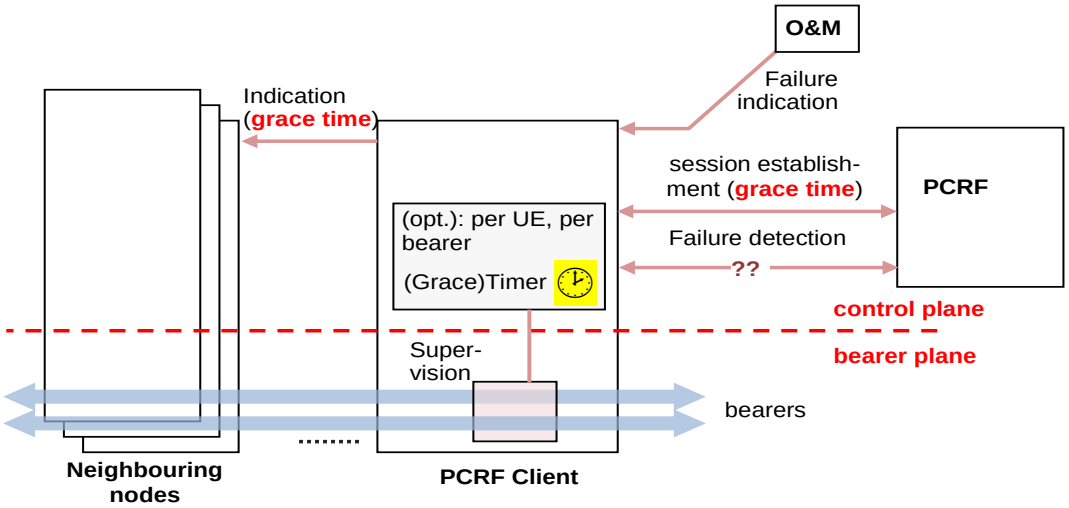

Figure 6.9.1: Overall view of unified solution for strict, graceful and loose handling of PCRF failure (non-roaming case for PCRF client in the bearer plane)

NOTE: the delegation of grace time to neighboring nodes may lead to earlier tear down of resources and thus earlier resynchronization of state, without impact on user experience. E.g. an MME may detect that a UE falls into idle mode and can be re-attached.

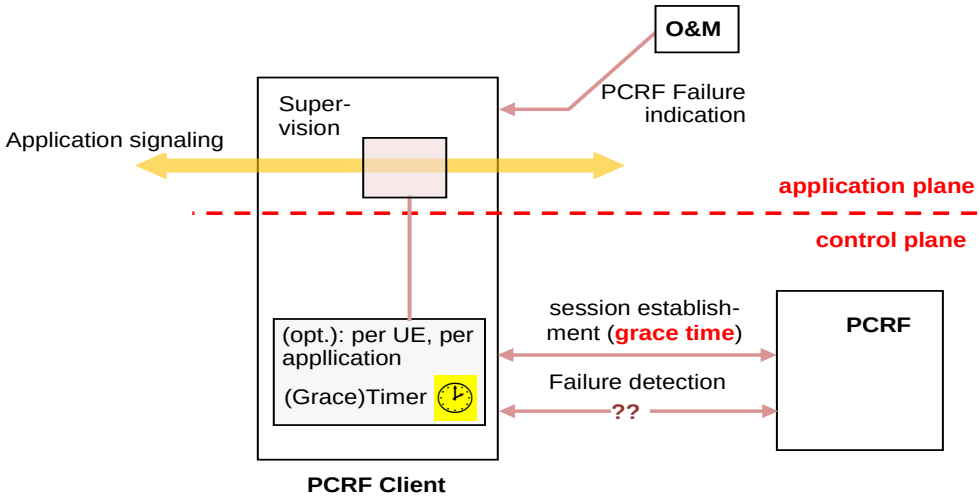

Figure 6.9.2: Overall view of unified solution for strict, graceful and loose handling of PCRF failure (non-roaming case, for PCRF client in the application plane)

PCRF failure detection by PCRF clients is necessary in any case and the same for all three methods.

For the grace time handling the following is proposed:

a) PCRF may send the grace time (including zero) in PCRF session establishment or in any update signaling to the PCRF client; the grace time may be specific for a UE or IP-CAN Session. If it is omitted, it means that a loose handling of bearer(s) regarding subsequent PCRF failure is allowed (by PCRF); however, there may be an additional grace time configured in the PCRF client. The grace timer is used to avoid the EPS service disruption due to the PCRF failure. The value of the grace timer should be decided by the PCRF based on bearer information. E.g. for bearers related to a voice call (consisting of a bearer with QCI=5 for SIP signaling and a bearer with QCI=1 for voice data) the grace timer should be longer than the typical voice call durations, in order to minimize impacts to active calls (with reasonably high probability).

b) Optionally a PCRF client may propagate a grace time indication to neighbouring nodes, using existing signaling messages but with enhanced information. This depends also on the actual signaling capability and configuration in the PCRF client.

c) The PCRF client supervises the grace time(s) by running corresponding timers. If a grace time is reached, the PCRF client tears down the bearer(s) or application session(s); if a bearer/application session is torn down due to other reasons (e.g. by the UE or other NW nodes, especially neighbouring nodes), the corresponding timer is stopped.

NOTE: if grace timers are communicated in parallel to PCRF clients (e.g. AF and PCEF) they should obey a useful relationship (e.g. AF related grace timer shorter than the PCEF related one).

In order to realize this functionality, the enhancements listed in an overview manner in table 6.9.1 are required.

Table 6.9.1: Required enhancements in signaling

Signaling between …	Interface	Enhancement	NOTE
PCRF - PCEF	Gx	Delivery of grace time parameter in 'Provisioning and Policy Enforcement of Authorized QoS' and 'Provisioning of PCC	Small enhancements in TS 29.212 and TS 29.213 required.

		rules' procedures	
PCRF - BBERF	Gxx	Delivery of grace time parameter in 'Gateway control and QoS Rules Provision' and 'Provisioning and Policy Enforcement of Authorized QoS' procedures	Small enhancements in TS 29.212 and TS 29.213 required.
PCRF - AF	Rx	Delivery of grace time parameter in 'Initial Provisioning of Session Information' and 'Modification of Session Information' procedures	Small enhancements in TS 29.213 and TS 29.214 required.
PCRF- PCRF	S9	Delivery of grace time parameter in above mentioned procedures	Small enhancements in TS 29.215 required.
PCEF (P-GW) – S-GW	S5/S8	Delivery of grace time parameter in bearer related signaling ('Delete PDN Connection Set Request' or 'Update Bearer Request')	**Not in scope of CT WG3, but CT WG4.** Bulk signaling is preferred.
BBERF (S-GW) - MME	S11	Delivery of grace time parameter in bearer related signaling ('Delete PDN Connection Set Request')	**Not in scope of CT WG3, but CT WG4.** Bulk signaling is preferred.

The support of this "grace" feature is optional; if grace time is received in signaling message but not supported, the local configuration of grace time is relevant. If a node does also not support such local handling, the behaviour remains as it is now, namely implementation specific.

7 Evaluation

7.1 General

Table 7.1.1 compiles an evaluation for all 9 solutions on a first level.

Table 7.1.1: Level 1 evaluation of solutions

Solution	Main characteristics	Impact on specification	Relationship to other solutions
1 (Solution for the PCRF failure reselection for the DRA)	This solution describes how Redirection-DRA and Proxy-DRA can handle PCRF failures for session establishment and modification.	Uses only DIAMETER base functionality for signaling with both Red-and Proxy-DRA. Describes additional, but optional behaviour for the DRA which could be imported into specifications (TS 29.212 – 215).	If it is known to DRA that PCRF state has been restored (solutions 5, 6, 8), this can be utilized in modification requests.
2 (use of DIAMETER base protocol in Single PCRF deployment (with Direct Client-Server Connection)	Gives small clarifications.	Refers to DIAMETER base functionality. Text on particular handling in failure case is quite unspecific.	Refers to other solutions. Text on emergency services needs to be considered for all other solutions.
3 (Graceful termination of services)	Timer based handling with potential improvement of user experience. Enables further handling in other nodes.	Details yet to be described.	Refers to solution 4 for teardown handling. Can be used with bulk signaling (solution 7).
4 (Strict termination of bearer services)	Describes usage of existing mechanisms for immediate teardown of bearer sessions.	No impact if bulk signaling is not used; requires DIAMETER extensions if bulk signaling is used (preferred).	Refers to bulk signaling (solution 7) as preferred mechanism.
5 (PCRF session state restoration)	Describes how PCRF sessions can be restored on the same or on a different PCRF, in a quite general and flexible approach.	Impact on Gx/Rx interfaces, as documented in coding example in annex A.3.	May be combined with solution 3, may not be combined with solution 4. May be be combined with solution 7 (for maximum benefit).
6 (Soft recovery after a PCRF restart)	Describes that in some cases user sessions may not be impacted by PCRF failure and restoration is not required. Handles the state restoration on the same PCRF after restart. No notion of bulk signaling. Has several options for binding procedure and information from PCEF.	Proposes restoration method as a feature to be known/agreed on by both sides. Impacts on PCRF application signaling, but amount not yet described in detail.	Is explicitly not suitable for combination with solution 7.
7 (Bulk Signaling based on PCRF Session Set ID (PSSID))	Proposes extension of the similar concept (CSID) in the bearer plane.	Impacts on PCRF signaling as documented by coding example in annex A.1, and potentially in DIAMETER. Corresponding enhancements in node behaviour (3GPP TS 23.007) .	Can be used by solutions 3, 4, 5 and 8.
8 (Adding explicit	Distributes PCRF's session	Requires enhancements in	Potentially usable in

resilience to PCRF sessions)	information in transparent container towards clients.	Gx/Rx interfaces and node behaviour. Details yet to be described.	conjunction with solution 5.
9 (Unified solution for termination of bearer services)	Allows to handle termination of bearer services flexibly in the range from a strict (immediate termination) to loose (no termination).	Extension in signaling interfaces Gx, Gxx, Rx, S9 for delivery of grace time parameter.	Combines solutions 3, 4 and the "loose handling", (i.e. "do nothing" solution, which is not specifically described).

In a second step the solutions are analysed further in conjunction with the functional requirements stated in subclause 5.2 and propose a way forward for several solutions.

Solution 1: there is some benefit for documenting the DRA behaviour with PCRF failure, as it was not clear enough from the current specifications. It is proposed to specify some reasonable amount of details, with consideration of PCRF session state restoration.

Solution 2: it is assumed that the small clarifications given, beyond already specified bahviour, may be considered when specifying other solutions and with general brush up of specifications. Consequently there is no extra effort and no extra place needed for documenting solution 2. Functional requirement #7 will then be fulfilled.

Solution 3, Solution 4: it is possible to unify these, together with the “loose handling” (which is not described as a separate solution). The benefit would be that functional requirements #1, #3 and #4 can be fulfilled with one mechanism. As this is an important portion of operator requirements this should be considered for specification.

Solution 5: this one fulfills functional requirement #5 to a great extent. When combined with solution 7 (bulk signaling) it reduces impacts on load and performance of the PCRF infrastructure and achieves most timely PCRF restoration . Yet, in its generality it seems to go quite far, taking into account that PCRF failure and restoration handling is a new topic in 3GPP’s specification work.

Solution 6: it fulfills functional requirement #5 in part. The solution lets user sessions continue untouched, when the PCRF fails. Diameter sessions between the PCRF and clients are restored after the restart of the PCRF only if/when required, e.g. when a client requests a session modification. The solution describes several options for finding the clients and the sessions to be restored.

Solution 7: this solution can serve as a base mechanism, for both PCRF session state restoration (solutions 5 and 8) and termination (solutions 3 and 4).

Solution 8: this one fulfills functional requirement #5 to a great extent. When combined with solution 7 (bulk signaling), it additionally minimizes impacts on load and performance of the PCRF infrastructure. It can be combined with solutions 7 and potentially 5.

Solution 9: it contains solutions 3 and 4 and fulfills requirements #1, #3 and #4.

7.2 Comparison of restoration solutions

7.2.1 Restoration behaviour over time

Figure 7.2.1.1 visualizes solution 5 in a compact form, for a total failure of (source) PCRF 1 and restoration on (target) PCRF 2 (this can easily be extrapolated to several target PCRFs). Looking at the behaviour over the time axis, it is seen that the restoration process sets in soon after the detection of failure of PCRF 1 and potentially (but depending on the duration of the PCRF outage) leads to full restoration before recovery of the failed PCRF. Bulk signaling is foreseen and intended to improve the efficiency and speed up the process. This solution can be characterized as “pro-active” (meaning that state is restored even before it is absolutely required). The slope of the curve representing the percentage of sync’ed (after failure these are the restored) sessions depends on whether bulk signaling is used (steeper) or not (less steep).

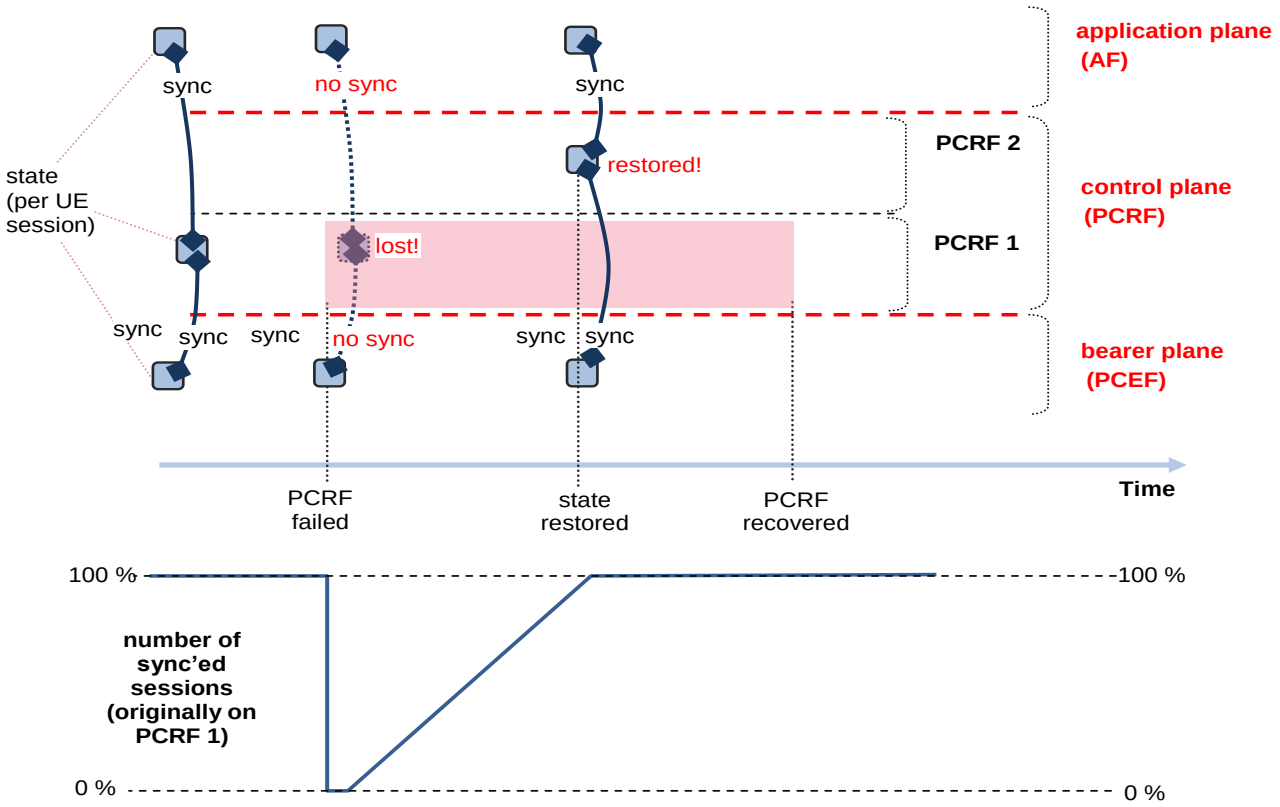

Figure 7.2.1.1: behaviour of solution 5 ("PCRF session state restoration")

The overall behaviour of solution 6 is presented in figure 7.2.1.2. This solution describes restoration ("re-building") of PCRF session state on the same PCRF, so it can set in only after PCRF recovery. This solution is characterized as "soft", which can also be interpreted as re-active; not more than necessary is restored beforehand. For that reason also no bulk handling is described here. As a result, the slope of the line showing the percentage of already restored sessions is smaller than in fig. 7.2.1.1.

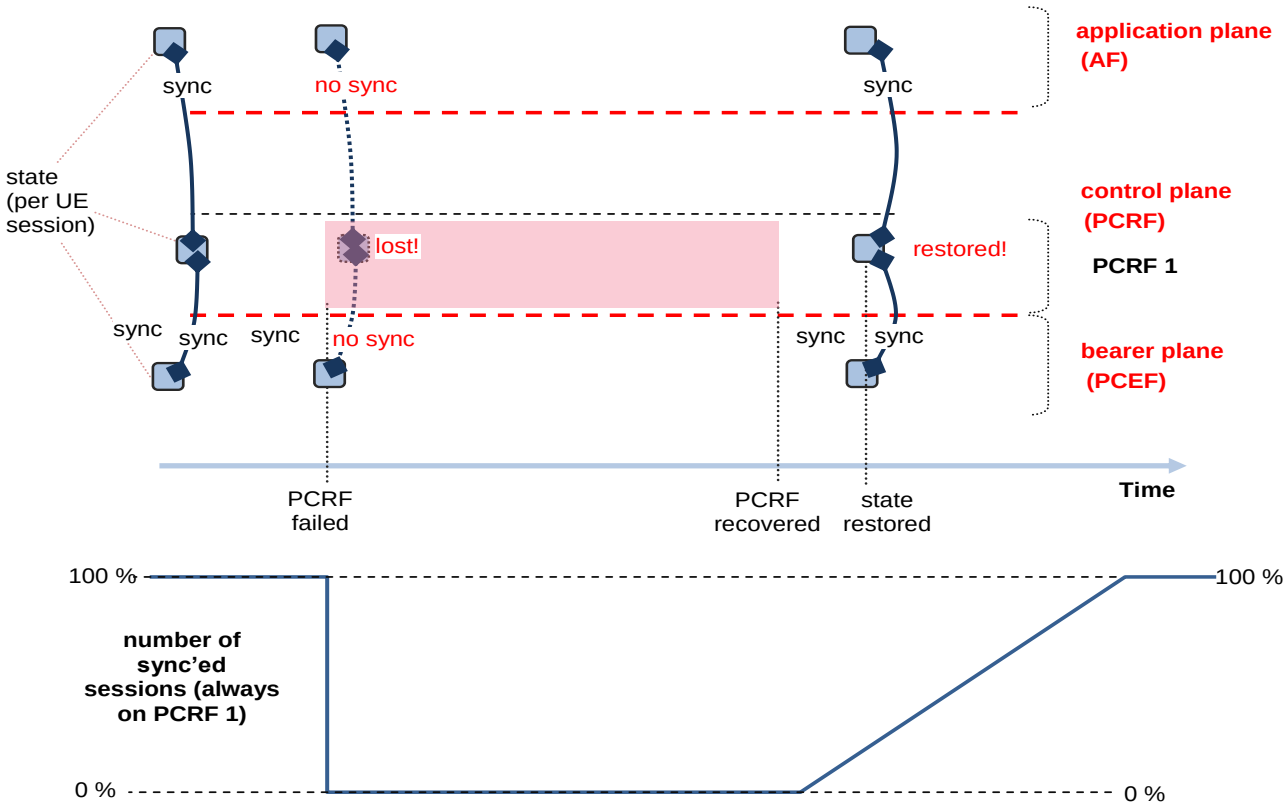

Figure 7.2.1.2: behaviour of solution 6 ("Soft recovery after a PCRF restart")

Solution 8 ("Adding explicit resilience to PCRF sessions") seems to be a variant of of solution 5; it is described only for PCRF session state restoration on the same PCRF after recovery. Its main characteristics is to allow simplified restoration on the PCRF by distributing a copy of its own session data (valid before the failure) to its client(s); this is done also pro-actively. Bulk signaling is foreseen and allows to improve efficiency further. The behaviour can be deduced from fig. 7.2.1.1 and 7.2.1.2, and is shown in figure 7.2.1.3: the curve representing the percentage of restored sessions starts only after recovery (like in fig. 7.2.1.2), but has even a steeper slope than in fig. 7.2.1.1.

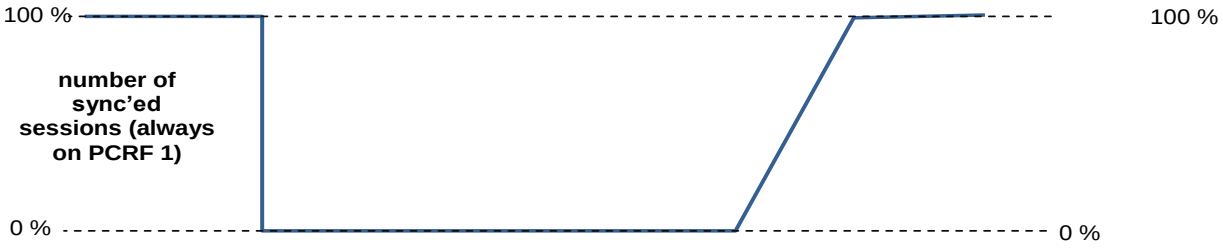

Figure 7.2.1.3: behaviour of solution 8 ("Adding explicit resilience to PCRF sessions")

7.3 Evaluation of failure and recovery detection mechanisms

In a stacked protocol environment it is not necessary to utilize failure and recovery detection mechanisms on every layer. E.g., as described in subclause 4.2, the heartbeat and watchdog mechanisms on SCTP transport and DIAMETER levels, respectively, are very similar, and the recommended timer value for both is 30 sec; in this case the mechanism on the higher protocol level provides more benefit. Also, detecting failures and recovery on transport layer may not be sufficient for the detection necessary for PCRF node failure and recovery.

For limited deployments (e.g. without multiple DIAMETER hops) and with a simplified implementation (i.e total PCRF failures seen equivalent to loss of DIAMETER state), the DIAMETER failover mechanisms as defined in IETF RFC 3588 [4] can be used. However, it seems advantageous, for the sake of a general, complete and consistent specification of PCRF node behaviour after failure, to define an application restoration mechanism based on a restart counter

mechanism in full analogy with other EPC nodes, including signaling on PCRF at application level. A signaling variant independent of individual user session related signaling is preferred.

NOTE: For the sake of functional symmetry, when specifying the restart counter mechanism between PCRF servers and clients both directions should be taken into account.

8 Conclusion

This Technical Report has studied the PCRF node failure categories and identified that the characteristic of total and partial failures need to be taken into account.

Regarding PCRF failure and recovery detection it can be concluded that, although basic mechanisms on lower protocol levels are readily available, a mechanisms on application level provides more flexibility and is more general.

The set of functional requirements for solutions to PCRF failure handling, collected in course of the study, illustrates that no unique procedure can be mandated; rather, operators want to have a choice of either more strict or more loose failure handling.

The deployment aspect of single and multiple PCRFs (with and without DRA) has been considered in solutions in this TR on the level of elaboration targetted by the study; any subsequent specification needs to take these different deployment schemes into account in detail.

Three categories of solutions to PCRF failure handling have been identified and described:

1. solutions of general use (behaviour of DRA with PCRF failure, bulk signaling): these can be seen as building blocks for more resilience and efficiency with signaling. Partially they can be used also in conjunction with restoration solutions. Overall, they require only modest enhancements in PCRF application signaling and 3GPP specifications.

2. solution for termination of services: in a unified manner it can include graceful handling and also range from immediate termination to (practically) infinite grace time with the ongoing service. The termination may be applied selectively, per service and/or user. The required protocol enhancements are quite limited.

3. PCRF restoration solutions: these can be designed with different degrees of support for pro-activeness and feature support. Generally they require more extensive enhancements in node behaviour and signaling (thus also 3GPP specifications); for none of the solutions a blocking point has been identified. This TR does not decide and give recommendations for a particular restoration solution, but clause 7 contains evaluations of and comparisons between restoration solutions. Some (incomplete) examples of coding in PCRF application protocols for solutions are given in annex A and demonstrate their feasibility.

None of the solutions to PCRF failure handling produces UE impact.

Annex A: coding examples

Editor's note: this annex captures examples of DIAMETER coding for functionalities proposed in the solutions clauses. The changes with respect to current specifications are not marked by change marks but in yellow.

A.1 Bulk signaling

According to the concept described in subclause 6.7, bulk signaling is foreseen for optimizing teardown and restoration procedures.

For teardown of bearer services according to subclause 6.4, bulk signaling may be used on Gx, Gxx and Rx interfaces in RAR and ASR messages.

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.212:

Table 5.3.1: Gx specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Acc. Type	Applicability (note 3)
				Must	May	Should not	Must not			
…										
FQ-PSSID	tbd	5.3.x	OctetString	?	?	?	?	?	All	Both
…										

…

5.3.x FQ-PSSID AVP (All access types)

The FQ-PSSID AVP (AVP code tbd) is of type OctetString and is coded according to figure A.x:

Octets	Bits 8	7	6	5	4	3	2	1
1 to 2	Length = n							
3	Node-ID Type				Number of PSSIDs= m			
4 to p	Node-ID							
(p+1) to (p+2)	First PCRF Session Set Identifier (PSSID)							
(p+3) to (p+4)	Second PCRF Session Set Identifier (PSSID)							
...	...							
q to q+1	m"th PCRF Session Set Identifier (PSSID)							
(q+2) to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure A.x: FQ-PSSID

Where Node-ID Type values are:

0 indicates that Node-ID is a global unicast IPv4 address and p = 7.

1 indicates that Node-ID is a global unicast IPv6 address and p = 19.

2 indicates that Node-ID is a 4 octets long field with a 32 bit value stored in network order, and p= 9. The coding of the field is specified below:

- Most significant 20 bits are the binary encoded value of (MCC * 1000 + MNC).

- Least significant 12 bits is a 12 bit integer assigned by an operator to a PCRF node or PCRF client. Other values of Node-ID Type are reserved.

The node that creates the FQ-PSSID is responsible for making sure the Node-ID is globally unique and the PSSID value is unique within that node.

…

5.6.4 Re-Auth-Request (RAR) Command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the BBERF/PCEF in order to provision QoS/PCC rules using the PUSH procedure initiate the provision of unsolicited QoS/PCC rules. It is used to provision QoS/PCC rules, event triggers and event report indications for the session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                *[ Supported-Features ]
                 [ Session-Release-Cause ]
                 [ Origin-State-Id ]
                *[ Event-Trigger ]
                 [ Event-Report-Indication ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Default-EPS-Bearer-QoS ]
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                *[ Usage-Monitoring-Information ]
                *[ FQ-PSSID ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP]
```

…

Table 5a.4.1: Gxx re-used Diameter AVPs

Attribute Name	Reference	Description	Acc. type
…			
…			
FQ-PSSID	5.3.x	Defines a set of PCRF sessions for bulk signaling purposes.	All
…			

…

Table 5.4.1: Rx re-used Diameter AVPs

Attribute Name	Reference	Comments
…		
FQ-PSSID	3GPP TS 29.212 [8]	Defines a set of PCRF sessions for bulk signaling purposes.
…		

…

5a.6.4 Re-Auth-Request (RAR) Command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the BBERF in order to provision QoS rules using the PUSH procedure initiate the provision of unsolicited QoS rules. It is used to provision QoS rules, event triggers and event report indications for the session.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
```

```
                { Destination-Realm }
                { Destination-Host }
                { Re-Auth-Request-Type }
               *[ Supported-Features ]
                [ Session-Release-Cause ]
                [ Origin-State-Id ]
               *[ Event-Trigger ]
               *[ QoS-Rule-Remove ]
               *[ QoS-Rule-Install ]
                [ QoS-Information ]
                [ Default-EPS-Bearer-QoS ]
               *[ FQ-PSSID ]
               *[ Proxy-Info ]
               *[ Route-Record ]
               *[ AVP]
```

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.214:

…

5.6.7 Abort-Session-Request (ASR) command

The ASR command, indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field, is sent by the PCRF to inform the AF that bearer for the established session is no longer available.

Message Format:

```
<AS-Request>  ::= < Diameter Header: 274, REQ, PXY >
                   < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
                  { Auth-Application-Id }
                  { Abort-Cause }
                 *[ FQ-PSSID ]
                  [ Origin-State-Id ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                 *[ AVP ]
```

A.2 Restart indication

According to the description in subclause 4.2.4, the restart of a PCRF node can be indicated either in any existing or a dedicated new PCRF message. A possible coding for both cases is given below by showing the required modifications in specifications.

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.212:

2 References

…

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

…

4.5.x PCRF restart indication

At any time the PCRF may indicate to the PCEF that it has restarted and recovered from a failure by including its restart counter in any session-related signaling message (CCA, RAR) towards the PCEF. Alternatively, the PCRF may indicate its restart in a session-unrelated signaling RAR message (as used for bulk signaling, see annex A.x).

The required behaviour of PCEF upon PCRF restart indication is defined in 3GPP TS 23.007.

Editor's note: changes to 3GPP TS 23.007 are to be coordinated with CT4.

….

4a.5.x PCRF restart indication

See subclause 4.5.x, with BBERF substituted for PCEF.

…

5.3.x Restart-counter AVP

The restart-counter (AVP code tbd) is of type Unsigned32; it is sent from the PCRF to the PCEF to indicate the restart of PCRF node e.g. after a failure (for the detailed behaviour see 3GPP TS 23.007 [xx]).

…

Table 5a.4.1: Gxx re-used Diameter AVPs

…			
Restart-counter	5.3.x	Indicates that the PCRF node has restarted e.g. after a failure. The Restart-counter values are monotonously increasing.	All
…			

…

5.6.3 CC-Answer (CCA) Command

The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the PCEF in response to the CCR command. It is used to provision PCC rules and event triggers for the bearer/session and to provide the selected bearer control mode for the IP-CAN session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level. The primary and secondary CCF and/or primary and secondary OCS addresses may be included in the initial provisioning.

Message Format:

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 { CC-Request-Type }
                 { CC-Request-Number }
                *[ Supported-Features ]
                 [ Bearer-Control-Mode ]
                *[ Event-Trigger ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Charging-Information ]
                 [ Online ]
                 [ Offline ]
```

```
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                 [ Default-EPS-Bearer-QoS ]
                 [ Bearer-Usage ]
                *[ Usage-Monitoring-Information ]
                *[ CSG-Information-Reporting ]
                 [ Restart-counter ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

…

5.6.4 Re-Auth-Request (RAR) Command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the BBERF/PCEF in order to provision QoS/PCC rules using the PUSH procedure initiate the provision of unsolicited QoS/PCC rules. It is used to provision QoS/PCC rules, event triggers and event report indications for the session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                *[ Supported-Features ]
                 [ Session-Release-Cause ]
                 [ Origin-State-Id ]
                *[ Event-Trigger ]
                 [ Event-Report-Indication ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Default-EPS-Bearer-QoS ]
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                *[ Usage-Monitoring-Information ]
                 [ Restart-counter ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP]
```

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.214:

4.4.x PCRF restart indication

At any time the PCRF may indicate to the AF that it has restarted and recovered from a failure by including its restart counter in any session-related signaling message (AAA, RAR) towards the AF. Alternatively, the PCRF may indicate its restart in a session-unrelated signaling RAR message (as used for bulk signaling, see annex A.x).

The required behaviour of AF upon PCRF restart indication is defined in 3GPP TS 23.007 [xx].

Editor's note: changes to TS 23.007 are to be coordinated with CT4.

…

Table 5.4.1: Rx re-used Diameter AVPs

Attribute Name	Reference	Comments
…		
Restart-counter	TS 29.212 [8]	Indicates that the PCRF node has restarted e.g. after a failure. The Restart-counter values are monotonously increasing.
…		

…

5.6.2 AA-Answer (AAA) command

The AAA command, indicated by the Command-Code field set to 265 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the AF in response to the AAR command.

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [ Acceptable-Service-Info ]
                 [ IP-CAN-Type ]
                 [RAT-Type ]
                *[ Supported-Features ]
                *[ Class ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                 [ Origin-State-Id ]
                 [ Restart-counter ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                *[ AVP ]
```

…

5.6.3 Re-Auth-Request (RAR) command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the AF in order to indicate an Rx specific action.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Specific-Action }
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                *[ Flows ]
                *[ Subscription-ID ]
                 [ Abort-Cause ]
                 [ IP-CAN-Type ]
                 [ RAT-Type ]
                 [ Restart-counter ]
                 [ Origin-State-Id ]
                *[ Class ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

A.3 PCRF session state restoration

A possible coding for the scheme presented in subclause 6.5 is given below by showing the required modifications in the specification.

Editor's note: messages are not yet covered exhaustively.

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.212:

4.5.x Triggering PCRF session state restoration

The PCRF may trigger, via the Gx reference point, the restoration of PCRF session state from the PCEF onto itself or onto another PCRF node by sending to the PCEF a RAR message, containing the Restoration-Target-Sessions AVP and setting the Restoration-PCRF-Target appropriately. The PCEF shall respond, after completion of the restoration procedure towards the target PCRF node, with a RAA message indicating the success or failure.

…

Table 5.3.1: Gx specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Acc. type	Applicability (note 3)
				Must	May	Should not	Must not			
…										
Restoration-PCRF-Source	tbd	5.3.x	Node-id	V	P			Y	All	Both
Restoration-PCRF-Target	tbd	5.3.y	Node-id	V	P			Y	All	Both
Restoration-Status	tbd	5.3.z	Enumerated	V	P			Y	All	Both
Restoration-Target-Sessions	tbd	5.3.xx	Grouped	V	P			Y	All	Both
…										

..

5.3.x Restoration-PCRF-Source (All access types)

The Restoration-PCRF-Source AVP (AVP code tbd) is of type Node-id and defines the scope of restoration, only for PCRF sessions existing currently with a PCRF node identified as a source a PCRF client needs to consider PCRF restoration. The 'Node-id' is defined in subclause 8.62 in TS 29.274 [14].

Editor's note: an alternative to this definition, e.g. the re-use of a definition based on the DIAMETER protocol entities, is FFS.

5.3.y Restoration-PCRF-Target (All access types)

The Restoration-PCRF-target AVP (AVP code tbd) is of type Node-id and defines on which PCRF node the PCRF session state shall be restored. The 'Node-id' is defined in subclause 8.62 in TS 29.274 [14].

5.3.z Restoration-Status (All access types)

The Restoration-Status AVP (AVP code tbd) is of type 'Enumerated' and indicates the success/failure of PCRF session restoration. The following values are defined:

FINAL (0)

This value shall be used to indicate the success of restoration of all the requested target sessions.

INTERMEDIATE (1)

This value shall be used to indicate intermediately the success of restoration of a subset of the requested target sessions.

FAILURE (2)

This value shall be used to indicate a failure of restoration of a subset of the requested target sessions.

5.3.xx Restoration-Target-Sessions (All access types)

The Restoration-Target-Sessions AVP (AVP code tbd) is of type 'Grouped' and is used by a PCRF client to indicate to a target PCRF node, in the multiple PCRF session mode, which PCRF sessions need to be restored.This AVP is not needed in the single PCRF session mode.

…

5.6.4 Re-Auth-Request (RAR) Command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the BBERF/PCEF in order to provision QoS/PCC rules using the PUSH procedure initiate the provision of unsolicited QoS/PCC rules. It is used to provision QoS/PCC rules, event triggers and event report indications for the session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level. It is also used to trigger restoration of PCRF session data.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                *[ Supported-Features ]
                 [ Session-Release-Cause ]
                 [ Origin-State-Id ]
                *[ Event-Trigger ]
                 [ Event-Report-Indication ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Default-EPS-Bearer-QoS ]
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                *[ Usage-Monitoring-Information ]
                 [ Restoration-PCRF-Source]
                 [ Restoration-PCRF-Target]
                 [ Restoration-Target-Sessions]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP]
```

5.6.5 Re-Auth-Answer (RAA) Command

The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field, is sent by the PCEF to the PCRF in response to the RAR command, to communicate current UE and bearer specific data. It is also used to indicate the success of restoration of PCRF session data.

Message Format:

```
<RA-Answer> ::=  < Diameter Header: 258, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                 *[ Supported-Features ]
```

```
                [ Result-Code ]
                [ Experimental-Result ]
                [ Origin-State-Id ]
                [ IP-CAN-Type ]
                [ RAT-Type ]
             0*2[ AN-GW-Address ]
                [ 3GPP-SGSN-MCC-MNC ]
                [ 3GPP-SGSN-Address ]
                [ 3GPP-SGSN-IPv6-Address ]
                [ RAI ]
                [ 3GPP-User-Location-Info ]
                [ 3GPP-MS-TimeZone ]
               *[ Charging-Rule-Report]
                [ Access-Network-Charging-Address ]
               *[ Access-Network-Charging-Identifier-Gx ]
                [ Restoration-PCRF-Source]
                [ Restoration-PCRF-Target]
                [ Restoration-Target-Sessions]
                [ Restoration-Status]
                [ Error-Message ]
                [ Error-Reporting-Host ]
               *[ Failed-AVP ]
               *[ Proxy-Info ]
               *[ AVP ]
```

A.4 Adding explicit resilience to PCRF sessions

An example of additional procedures and a possible coding for the signaling of PCRF session information transparent container defined is given below for the example of PCEF as the PCRF client.

Note: this listing is not yet exhaustive, and further procedures/message enhancements are required (e.g. with RAR).

>>>>>>>>>>>>>>>>>>>>>>>> Proposed change in 3GPP TS 29.212:

…

4.5.x PCRF Restoration Support

In order to indicate support for PCRF restoration procedures the PCEF may include the corresponding feature bit in Feature-List-ID AVP (see table 5.4.1.1) in CC-Request messages.

If the PCEF has indicated support for PCRF restoration procedures, the PCRF may include a Transparent-Container AVP in any CC-Answer message. The PCEF shall not interpret the contents of this AVP but only store it for the case that a PCRF recovery is detected.

After recovery of a PCRF has been detected, the PCEF may send a CC-Request message with the Transparent-Container AVP to the PCRF. The PCRF may restore session data and answer with a CC-Answer message containing the Restore-Success AVP.

…

Table 5.3.1: Gx specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Acc. Type	Applicability (note 3)
				Must	May	Should not	Must not			
…										
Transparent-Container	tbd	5.3.x	xxx	?	?	?	?	?	All	Both
Restore-Success	tbd	5.3.y	yyy	?	?	?	?	?	All	Both
…										

Table 5.4.1.1: Features of Feature-List-ID 1 used in Gx

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits. AVPs introduced with this feature are marked with "Rel8" in table 5.3.1.
1	Rel9	M	This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits. AVPs introduced with this feature are marked with "Rel9" in table 5.3.1.
X	ProvAFsignalFlow	O	This feature indicates support for the feature of IMS Restoration as described in subclause 4.5.18. If PCEF supports this feature the PCRF may provision AF signalling IP flow information.
X			This feature indicates support for the feature of PCRF Restoration as described in subclause 4.5.x. If PCEF supports this feature the PCRF may provide, for the purpose of restoration after failure and recovery, data to PCEF in a transparent container.
Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0". Feature: A short name that can be used to refer to the bit and to the feature, e.g. "EPS". M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") in this 3GPP Release. Description: A clear textual description of the feature.			

…

5.3.x Transparent-Container AVP (All access types)

The Transparent-Container AVP (AVP code tbd) is of type OctetString. It is sent from PCRF to PCEF or from PCEF to PCRF and contains data encoded by the PCRF for restoring its session data after failure and recovery.

5.3.y Restore-Success AVP (All access types)

The Restore-Success AVP (AVP code tbd) is of type Enumerated. It is sent from PCRF to PCEF and indicates whether the restoration of session data has successfully been performed in PCRF.

The following values are defined:

RESTORE_FAILURE (0)

This value indicates that the PCRF could not successfully restore session data, without communicating any further details.

RESTORE_SUCCESS (1)

This value indicates that the PCRF has successfully decoded the transparent container and restored its session data accordingly.

Usage of further values are FFS, e.g. for indicating additonal reasons of restoration failure.

…

5.6.2 CC-Request (CCR) Command

The CCR command, indicated by the Command-Code field set to 272 and the 'R' bit set in the Command Flags field, is sent by the PCEF to the PCRF in order to request PCC rules for a bearer. The CCR command is also sent by the PCEF to the PCRF in order to indicate bearer or PCC rule related events or the termination of the IP CAN bearer and/or session.

This command is also used to provide data to be intermediately stored for the purpose of session restoration after PCRF failure and recovery.

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Destination-Host ]
                 [ Origin-State-Id ]
                *[ Subscription-Id ]
                *[ Supported-Features ]
                 [ Network-Request-Support ]
                *[ Packet-Filter-Information ]
                 [ Packet-Filter-Operation ]
                 [ Bearer-Identifier ]
                 [ Bearer-Operation ]
                 [ Framed-IP-Address ]
                 [ Framed-IPv6-Prefix ]
                 [ IP-CAN-Type ]
                 [ 3GPP-RAT-Type ]
                 [ RAT-Type ]
                 [ Termination-Cause ]
                 [ User-Equipment-Info ]
                 [ QoS-Information ]
                 [ QoS-Negotiation ]
                 [ QoS-Upgrade ]
                 [ Default-EPS-Bearer-QoS ]
               0*2[ AN-GW-Address ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ 3GPP-SGSN-Address ]
                 [ 3GPP-SGSN-IPv6-Address ]
                 [ RAI ]
                 [ 3GPP-User-Location-Info]
                    [ 3GPP-MS-TimeZone ]
                 [ Called-Station-ID ]
                 [ PDN-Connection-ID ]
                 [ Bearer-Usage ]
                 [ Online ]
                 [ Offline ]
                *[ TFT-Packet-Filter-Information ]
                *[ Charging-Rule-Report]
                *[ Event-Trigger]
                 [ Event-Report-Indication]
                 [ Access-Network-Charging-Address ]
                *[ Access-Network-Charging-Identifier-Gx ]
                *[ CoA-Information ]
                *[ Usage-Monitoring-Information ]
                *[ Transparent-Container ]
                *[ Restore-Success ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

…

5.6.3 CC-Answer (CCA) Command

The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the PCEF in response to the CCR command. It is used to provision PCC rules and event triggers for the bearer/session and to provide the selected bearer control mode for the IP-CAN session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level. The primary and secondary CCF and/or primary and secondary OCS addresses may be included in the initial provisioning.

This command is also used to provide intermediately stored PCRF with data for session restoration after failure and recovery.

Message Format:

Editor's Note: CSG-ID is needed to support CSG but the AVP has not been defined yet. It is for further study if an existing AVP may be reused or a new one needs to be created.

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 { CC-Request-Type }
                 { CC-Request-Number }
                *[ Supported-Features ]
                 [ Bearer-Control-Mode ]
                *[ Event-Trigger ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Charging-Information ]
                 [ Online ]
                 [ Offline ]
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                 [ Default-EPS-Bearer-QoS ]
                 [ Bearer-Usage ]
                 [ 3GPP-User-Location-Info]
                *[ Usage-Monitoring-Information ]
                *[ CSG-Information-Reporting ]
                *[ Transparent-Container ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
...
```

Annex B: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2009-08					Initial skeleton provided by rapporteur		0.0.0
2009-09					Contributions agreed in CT3#54: C3-091033 (clause 4 header change), C3-091035 (baseline architecture, failure detection and PCRF node failure scenarios; initial references and abbreviations), C3-091158 (scope)	0.0.0	0.1.0
2009-10					Contributions agreed in CT3#55: C3-091556, C3-091591, C3-091503, C3-091502, C3-091553, C3-091554, C3-091577, C3-091509, C3-091506, C3-091424	0.1.0	0.2.0
2009-11					Contributions agreed in CT3#56: C3-091935, C3-091936, C3-091888, C3-091889, C3-091891, C3-091924, C3-091937, C3-091925, C3-091941	0.2.0	0.3.0
2010-03					Contributions agreed in CT3#57: C3-100367, C3-100368, C3-100369, C3-100373, C3-100374, C3-100375, C3-100376, C3-100377, C3-100379, C3-100380, C3-100422	0.3.0	0.4.0
2010-03					v1.0.0 was produced by MCC	0.4.0	1.0.0
2010-05					Contributions agreed in CT3#58: C3-100716, C3-100717, C3-100718, C3-100719, C3-100686, C3-100645	1.0.0	1.1.0
2010-09					Contributions agreed in CT3#59: C3-100985, C3-100935, C3-100804, C3-101026, C3-100806, C3-101027, C3-101030, C3-101028, C3-101029	1.1.0	1.2.0
2010-09					v2.0.0 was produced by MCC	1.2.0	2.0.0
2010-09					v10.0.0 was produced by MCC	2.0.0	10.0.0