3GPP TR 23.858 V1.1.0 (2013-2)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Usage Monitoring Control PCC Enhancement;
(Release 12)

Keywords
3GPP, Architecture, monitoring, PCC

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 scope of this technical report is to capture the results of a study that investigates if enhancements to the existing policy control architecture are needed in the area of usage monitoring control. The goals of the study are to derive possible requirements and architecture enhancements for:

1. Monitoring of service (s) / application (s) in more than one usage monitoring group;
2. Disabling a service (s) / application (s) from the existing usage monitoring group of services/group of applications;
3. Excluding the usage of a particular service (s) / application (s) from the accumulated usage for the IP-CAN session/TDF session;
4. Usage control for a subscriber group, e.g. the members of a family or a company subscriber, or a group of devices belonging to subscribers that share the same usage allowance threshold.

In addition, study the different proposed solutions for effective time based usage monitoring and how associated start and end of usage is defined.

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 Control and Charging architecture".

[3] 3GPP TS 22.278: " Service requirements for the Evolved Packet System (EPS) ".

[4] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Usage Monitoring Group: A Usage Monitoring Group is a set of service data flow(s)/application(s) of a UE that share a common traffic usage allowance and need to be monitored together for usage monitoring control purposes.

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].

4 Key Issue 1: Service/Application Monitored in more than one monitoring group

Editor's Note: This clause will describe the use cases, requirements, and proposed solutions for monitoring of one service/application in more than one monitoring group.

4.1 Description

4.2 Use Cases

4.2.1 Descriptions

This use case describes a scenario where one service is monitored in more than one monitoring group.

4.2.2 Pre-conditions

Alice is a subscriber of mobile network X and she has the following subscription:

(A) 50M allowance usage per month for the streaming and P2P downloading, in which,

(B) the P2P downloading should not exceed 10M per month.

In this profile, the P2P downloading is included into 2 usage monitoring groups: group (A) according to subscription profile (A) and group (B) according to subscription profile (B).

4.2.3 Service Flows

If Alice attaches to the mobile network X and accesses only streaming service, the subscription profile (A) will apply: the network will be able to monitor the traffic usage and detect if the 50M allowance for streaming and P2P downloading is used up.

If Alice attaches to the mobile network X, and accesses both streaming services and P2P downloading, both subscription profile (A) and (B) will apply. The network will be able to monitor the traffic usage and detect if either the allowance for P2P downloading defined in profile (B) or the allowance for streaming and P2P downloading defined in profile (A) is used up.

4.2.4 Post-conditions

None.

4.2.5 Requirements

The 3GPP system shall be able to monitor the traffic usage of a service/application in more than one usage monitoring group.

4.3 Alternative Solutions

Editor's note: This clause will describe alternative solution to the key issue.

4.3.1 Alternative Solution 1: Multiple monitoring key within a PCC/ADC Rule

In this alternative solution, a service /application is monitored with more than one monitoring key at the PCEF/TDF.

For the purpose to monitor the usage for a service/application with several monitoring keys, the PCRF includes a list of monitoring key in a PCC/ADC rule when providing the PCC/ADC rule to PCEF/TDF. The usage for each service/application is accumulated in parallel for every monitoring key at the PCEF/TDF

Such a solution is applicable to the PCC Rules and to the ADC Rules in case of TDF/PCEF enhanced with ADC.

4.3.2 Alternative Solution 2: One monitoring key within a PCC/ADC Rule

4.3.2.1 General Description

In this alternative solution, the knowledge about what services/applications belong to a monitoring group remains in the PCRF.

4.3.2.2 A service/application belongs to more than one monitoring group

The PCRF retrieves the total group allowance for the monitoring group and the set of services belonging to it from the SPR.

Instead of assigning a common monitoring key for all services of the monitoring group, the PCRF generates an individual Monitoring Key for every service that belongs to more than one monitoring group. Then PCRF calculates a usage threshold for each of these Monitoring Keys taking into account the minimum of the individual service allowance and the group allowance(s) the service belongs to.

The PCRF provides both the Monitoring Key and the usage threshold with the PCC Rule/ADC Rule to the PCEF/TDF.

When the PCRF receives a usage report for a Monitoring Key from the requested node (PCEF or TDF), the PCRF shall deduct the value from the corresponding group allowances and from the individual allowance if needed.

As long as all group usage allowances are not reached, the PCRF calculates a new usage threshold for the Monitoring Key based on the corresponding group allowances the service belongs to.

If a group usage allowance is reached the PCRF may request a usage report from the PCEF or TDF to retrieve the accumulated usage since the time of the last usage report. The group usage allowance is updated accordingly and the remaining usage may be used by PCRF to assign a new usage threshold for each Monitoring Key.

4.4 Evaluation

Editor's Note: This clause will evaluate the alternative solutions.

4.5 Conclusion

Editor's Note: This clause will provide conclusions with respects to preferred solution and what further specification work is required.

5 Key Issue 2: Disabling Service/Application Usage Monitoring

Editor's Note: This clause will describe the use cases, requirements, and proposed solutions for how a service data flow/application can be disabled from the existing usage monitoring group of services/group of applications.

5.1 Description

5.2 Use Cases

5.2.1 Descriptions

This use case describes a scenario where the usage monitoring for a service/application will be disabled from an existing usage monitoring group.

5.2.2 Pre-conditions

Alice is a subscriber to operator X, and she has subscribed to a package:

- 50 M allowance per month for the traffic of streaming and FTP downloading.

According to her subscription, Alice can request for usage expansion on demand.

There are also online promotions for certain streaming services. During the promotion time, the traffic of these streaming services (e.g. movies) will be paid by sponsors.

5.2.3 Service Flows

Alice is watching an interesting movie and she realized that she has a subscription of 50M allowance per month for the traffic of streaming and FTP downloading, which is not enough for the movie watching. The size of the high-definition version of the movie is about 2G. Alice decides to extend her subscription of streaming to 2G and keep the 50M allowance per month for FTP downloading only, because she wants to watch this high-definition movie. She calls the customer service to command such subscription change. As a result, Alice's subscription will have 50M allowance for FTP downloading, and 2G allowances for streaming. During the subscription change, Alice does not want to stop watching the movie. After the 2G allowances for streaming is used up, the streaming will share with the FTP downloading the rest of the 50M allowance.

Another use case is the periodic promotion of a certain service from service provider or operator. For example, an online movie provider offers 24 hour online promotion of certain movies. During the promotion time, watching these movies from the online movie provider will be free both for content and for the bandwidth (e.g. the movie is sponsored by the online movie provider). The online movie provider informs the operator of such promotion and its time period, and the operator disables monitoring the traffic usage of the service data flow of watching these movies from the usage monitoring group. After the promotion time is finished, the operator will restore monitoring the traffic usage of these services within their original usage monitoring group.

5.2.4 Post-conditions

An application/service is removed from the existing usage monitoring group without impact the use of the application/service.

5.2.5 Requirements

The 3GPP System shall be able to disable the monitoring of the traffic usage of a specific service/application from a usage monitoring group.

The 3GPP System shall be able to re-activate the monitoring of the traffic usage of a specific service/application within the usage monitoring group.

5.3 Alternative Solutions

Editor's note: This clause will describe alternative solution to the key issue.

5.3.1 Alternative Solution 1: Indication based Activation/Deactivation

If usage monitoring for a service data flow/application needs to be disabled from a usage monitoring group, the PCRF provides an instruction to the PCEF or to the TDF containing the monitoring key of the usage monitoring group and the information to indicate the specific service data flow/application for which usage monitoring needs to be stopped. Based on PCRF's instruction, the PCEF or TDF removes the monitoring key from the existing PCC or ADC rule, which shall deactivate the usage monitoring for this specific service data flow/application.

If the service data flow/application which has been disabled from the usage monitoring group needs to be re-enabled, the PCRF provides an instruction to the PCEF/TDF containing the monitoring key of the usage monitoring group and the information to indicate the specific service data flow/application for which usage monitoring needs to be re-activated. Based on PCRF's instruction, the PCEF or TDF re-instates the monitoring key for the existing PCC or ADC rule, which will re-activate the usage monitoring for this specific service data flow/application.

NOTE: In the case that more than one service data flow/application need to be deactivated/re-activated from a usage monitoring group, the PCRF could provide information to indicate the usage monitoring group for all the service data flows/applications that need to be deactivated/re-activated in the same message.

5.3.2 Alternative Solution 2: PCC/ADC Rules Replacement

If usage monitoring to a service data flow/application needs to be disabled from a usage monitoring group, the PCRF generates a new PCC/ADC rule. The new PCC/ADC rule has the same information as the old PCC/ADC rule which is used to control the service data flow/application, but without the monitoring key.

The PCRF provides new PCC/ADC rules to the PCEF/TDF and removes the old PCC/ADC rules. Since the new PCC/ADC rule does not contain the monitoring key, usage monitoring for service data flow/application will be disabled from the usage monitoring group.

If the service data flow/application which has been disabled from the usage monitoring group needs to be re-enabled, the PCRF shall provide a new PCC/ADC rules with the Monitoring key and remove the old PCC/ADC rule, the operation of the PCEF/TDF is similar as above.

NOTE: It is assumed that the activation of the new PCC/ADC rules takes place at the same time as the removal of the old PCC/ADC rules. It has to be ensured that there are no other actions triggered (e.g. with respect to charging and bearer management) beside the ones related to the disabling of usage monitoring.

5.3.3 Alternative Solution 3: Monitoring Key Modification

If usage monitoring for a service data flow/application (belonging to a usage monitoring group) needs to be disabled, the PCRF can modify the monitoring key of the corresponding PCC/ADC rule based on existing functionality. Following the PCRF instruction, the PCEF or TDF updates the monitoring key in the modified PCC/ADC rule.

There are three possibilities for modifying a monitoring key to achieve the deactivation of the usage monitoring for this specific service data flow/application:

a) The operator can select any one monitoring key which is not in use for any other usage monitoring. The PCEF/TDF would provide a separate usage monitoring for this monitoring key according to the existing functionality. The PCRF would therefore still receive usage reports but could ignore them.

   NOTE: The operator should configure the usage threshold to an enough high value so that frequent usage reports can be avoided.

b) The operator can configure a specific monitoring key which is to be interpreted by the PCEF/TDF as instruction to not perform usage monitoring for a PCC/ADC rule.

c) 3GPP can define a specific value for the monitoring key which instructs the PCEF/TDF to not perform usage monitoring for a PCC/ADC rule.

If the usage monitoring for a service data flow/application (for which monitoring has been disabled before) needs to be re-activated, the PCRF modifies the monitoring key of the corresponding PCC/ADC rule back to its original value. Based on PCRF's instruction, the PCEF or TDF updates the monitoring key for the modified PCC/ADC rule and continues to perform usage monitoring for this specific service data flow/application.

5.4 Evaluation

Editor's Note: This clause will evaluate the alternative solutions.

5.5 Conclusion

Alternative 2 and alternative 3 (option (a)) are based on existing specifications and can be used to disable usage monitoring for a PCC/ADC rule. The detailed explanation on how to use/configure existing functionality for Alternative 2 and Alternative 3 (option (a)) will be documented in a new informative Annex in TS 23.203[2].

6 Key Issue 3: Exclude Usage of a Service/Application from IP-CAN session/TDF session Usage

Editor's Note: This clause will describe the use cases, requirements, and proposed solutions for how to exclude the usage of a particular service data flow/application from the accumulated usage for the IP-CAN session/TDF session.

6.1 Description

6.2 Use Cases

6.2.1 Descriptions

This use case describes a scenario in which the usage of a particular service data flow/application is excluded from the accumulated usage for a defined network.

6.2.2 Pre-conditions

Alice is a subscriber of Mobile Network X and she has following subscriptions:

1) Total allowance usage A: 50M allowance usage per month for all the traffic toward a defined IP network, in which:

2) Total allowance usage B: 10M allowance usage per month for the streaming service and this part of allowance usage is not accumulated into the allowance usage A.

Mobile network X has a business agreement with sponsor Y, who will pay for the traffic of movies delivered from sponsor Y. Mobile network X also delivers featured services, which is paid by a fixed feature fee, related data traffic will be free for users.

6.2.3 Service Flows

Alice attaches to the mobile network X and establishes a data connection toward a defined IP network. Then Alice begins the web browsing and music downloading, at the same time, Alice starts to watch a movie. According to her subscription, the maximum usage of movie (and other streaming services) is 10M per month, and the maximum usage of the other services (i.e. non-streaming) is 50M per month. The movie will be monitored separately in the streaming service usage monitoring group, and the usage of the movie will not be accumulated into the traffic toward the defined IP network.

Alice decides to watch a movie provided by a sponsor Y. Alice purchases the movie from sponsor Y, the traffic amount required for downloading the movie will be paid by the sponsor Y. According to mobile network X's policy, after

notification by the sponsor Y, the traffic flow which is considered as sponsored by Y for downloading the movie shall be monitored separately until the sponsored traffic amount consumed and shall not be accumulated into either the traffic usage toward the defined IP network or the traffic usage of streaming service which are not sponsored.

At the same time, Alice uses some special services offered by operator of network X. One example is Alice logs in the network hard disk afforded by operator of network X, clicks and watches a movie saved at the network hard disk. Related data traffic will be free for the bandwidth and charged as fixed feature fee. Such traffic data of self-operated services shall be monitored separately and shall not accumulated into either the traffic usage toward the defined IP network or the traffic usage of streaming service.

6.2.4 Post-conditions

Usages for streaming, sponsored service, and featured service are accumulated separately, and are excluded from the usage for the defined IP network.

6.2.5 Requirements

The 3GPP system shall be able to monitor the rest of the traffic usage toward a defined IP network which excludes the traffic usage of certain services/applications.

6.3 Alternative Solutions

Editor's note: This clause will describe alternative solution to the key issue.

6.3.1 Alternative Solution 1: PCEF/TDF based counting with usage monitoring interface enhancements

If usage monitoring of the service data flow (s) / application (s) need to be excluded from the total reported volume of IP-CAN / TDF session, then the PCRF shall indicate the PCC / ADC Rule (s) for which the corresponding sdf (s) / application (s) traffic volume is not to be counted toward overall IP-CAN / TDF session traffic. Based on PCRF's instruction, the total reported volume for IP-CAN / TDF session shall not include the accumulated volume traffic for sdf (s) / application (s) defined by the corresponding PCC / ADC Rule.

NOTE: In the case there are more than one service data flows / application to be excluded from the overall IP-CAN / TDF session report e.g. sharing the same Monitoring key, the PCRF will provide all corresponding PCC / ADC Rules or Monitoring key.

6.3.2 Alternative Solution 2: Using a new ADC/predefined PCC Rule by applying existing standardized methods

If usage monitoring of the service data flows / application need to be excluded from the total reported volume of IP-CAN/TDF session,

1. In case of required measurements on the application level, an ADC Rule can be created with the Application Identifier defining a new application as session's traffic excluding specific application (s), which should not be counted toward overall session's traffic. In such a case, a volume measured for such an ADC Rule shall be IP-CAN / TDF session's volume excluding accumulated usage of the application (s).

2. In case of required measurements on the sdf level, a predefined PCC Rule can be used to match a session's traffic excluding specific sdf (s), which should not be counted toward overall session's traffic. In such a case, a volume measured for such a predefined PCC Rule shall be IP-CAN / TDF session's volume excluding accumulated usage of the sdf (s).

6.3.3 Alternative Solution 3: PCRF based counting

In this solution, the PCRF derives the required usage consumption of the IP-CAN session / TDF session level by deducting the usage of the sdf (s) /application (s) from the total consumed usage of the IP-CAN session / TDF session

received from the PCEF / TDF. There are two ways for the PCRF to get the usage value of the sdf (s) /application (s) and the total consumed usage value of the IP-CAN session / TDF session:

1) When the PCRF receives usage report of the IP-CAN session / TDF session level in case of reached volume threshold, if usage monitoring to the sdf (s) /application (s) need to be excluded, then the PCRF requests the usage report from the PCEF / TDF for the corresponding sdf (s) / application (s) monitoring key.

2) The PCEF / TDF are mandated to report the usage consumption of all Monitoring Keys when the volume threshold of IP-CAN session / TDF session level is reached. The PCRF can determine which usage of the specific sdf (s) /application (s) needs to be excluded from the total consumed usage of the IP-CAN session / TDF session.

NOTE: Second option (2) can be further optimized by requesting PCEF / TDF to report only the usage(s) for the specific Monitoring key (s) its usage must to be excluded from the total consumed usage of the IP-CAN session / TDF session.

6.3.4 Alternative Solution 4: PCEF/TDF based counting by re-using key issue 1 solution "Multiple Monitoring key within a PCC/ADC Rule"

The solution shall re-use the principles defined in key issue 1 solution "Multiple keys for a single rule" by instructing the PCEF / TDF to not include a PCC / ADC rule in the usage monitoring of the IP-CAN / TDF session traffic by assigning a (session) monitoring key to all rules in addition to their specific monitoring key except for those rule which are to be excluded from the IP-CAN / TDF session overall accumulation.

NOTE: In case of ADC Rules, this alternative solution is achieved by additionally assigning ADC Rule with Application Id for the traffic not counted toward any other Application Id for the specified session in order to correctly count session's traffic.

6.4 Evaluation

Editor's Note: This clause will evaluate the alternative solutions.

6.5 Conclusion

Editor's Note: This clause will provide conclusions with respects to preferred solution and what further specification work is required.

7 Key Issue 4: Usage Monitoring Optimization

7.1 Description

7.2 Use Cases

7.2.1 Description

This use case describes a scenario which needs usage monitoring optimization.

7.2.2 Pre-conditions

Operators may have different usage allowances for the same service data flow/application or PDN connection in different conditions, e.g. leisure and busy hour, roaming and non-roaming, billing cycle change. For example, mobile operator X has a package A which has an allowance of 30M per month for streaming services during leisure hours and 5M per month for streaming services during busy hours. Majority of the subscribers of mobile operator X are

subscribed to package A. At the time of switching between leisure and busy hours, the traffic usage of the previous time space will be reported simultaneously for many sessions, which will cause substantial signalling load to the system. This is not desired by the operators. Hence, optimized solutions are needed for such scenario.

7.2.3 Service Flows

At the time of switching from leisure hours to busy hours, the report of the leisure hour usage of package A subscribers will not be reported immediately, instead, the leisure hour usage of package A subscribers will be reported later when a threshold is reached or when the IP-CAN session is terminated.

Similarly, at the time of switching from busy hours to leisure hours, the report of the busy hour usage of package A subscribers will not be reported immediately, instead, the busy hour usage of package A subscribers will be reported later when a threshold is reached or when the IP-CAN session is terminated.

7.2.4 Post-conditions

Simultaneous report of usage of multiple subscribers will be avoided, which will reduce signalling load to the network as well.

7.2.5 Requirements

The 3GPP system shall optimize the usage monitoring signalling.

7.3 Alternative Solutions

The solution for this use case was introduced under TEI11 Usage Monitoring Congestion handling feature.

7.3.1 Alternative Solution ...

7.4 Evaluation

7.5 Conclusion

This key issue was handled and resolved under TEI11.

8 Key Issue 5: Usage Monitoring for Subscriber Group

Editor's Note: This clause will describe the use cases, requirements, and proposed solutions for how to apply usage control for a subscriber group.

8.1 Description

8.2 Use Cases

8.2.1 Descriptions

The use case describes a scenario of usage control for a subscriber group.

8.2.2 Pre-conditions

Johnson family and Alice family has subscribed to mobile operator X.

ACME vending machine company has 5000 vending machines, and operator X provides data connectivity for vending machines from ACME vending machine company.

8.2.3 Service Flows

Family based usage monitoring

The Johnson family subscribe to a mobile data offering from their mobile operator that is specifically targeted at families. The data offering includes a combined allowance for 100M per month. Either of the family members can make use of this allowance. When in a particular month the combined usage allowance is exceeded, e.g. as per operator policy the maximum downlink data rate may be reduced to 384 kbits/s for each of the family members.

The Johnson family subscribe to a mobile data allowance offering from their mobile operator that is specifically targeted at families. This data allowance refers to 15 hours for video streams per month. Either of the family members can make use of this allowance when he/she initiate the corresponding video stream service and the maximum downlink data rate for each video stream can be given at 2Mbits/s. If there are 2 or more than 2 members using this allowance simultaneously, the consumption of time will be accumulated in parallel for every member. The total consumption of time is the sum of every member's consumptions of time. When the volume of 15 hours is run out of, mobile network operator will block streaming video service from Johnson family or reduce the maximum downlink data rate of this video streams to 384 kbits/s for each of the family members.

Usage Monitoring for Machine Type Communications

The ACME vending machine company has 5000 vending machines connected to a MTC Server. These vending machines generally only send a limited amounts of data to inform the MTC Server of their status. However, occasionally more data is exchanged, e.g. when a service engineer runs a remote diagnostics software program. The ACME vending machine company therefore has a contract with the operator that limits the 5000 vending machines to a combined data volume of 500M per month. The individual vending machines are not overly restricted to only a specific average monthly data volume. On the other hand, the operator can be ensured that the combined group of ACME vending machines will only require a limited amount of network capacity.

Usage monitoring of a subscriber in multiple subscriber groups simultaneously

Alice, her brother Mike, her father and mother are subscribers of mobile network X and they have following subscriptions:

1) Total allowance usage A of subscriber group A: Alice, her brother Mike, her father and mother are permitted for the total usage allowance of 50M per month, in which:

2) Total allowance usage B of subscriber group B: Alice and Mike are permitted for the total usage allowance of 30M per month.

3) There is no specific usage allowance for any person.

In this profile, Alice, her brother Mike, her father and mother constitute subscriber group A, and all the members of this subscriber group share the total usage allowance of 50M per month. Furthermore, this subscriber group includes a subscriber group B which only contains Alice and Mike. Subscriber group B is permitted for the total usage allowance of 30M per month. This is useful for parents in a family to limit the Internet usage of their children. The maximum traffic usage for children is limited to 30M per month. The parents can use the total traffic of 50M per month if the children do not use any. When only Alice or Mike or Alice and Mike is/are using the network, the network should monitor the traffic usage and detect whether it reaches the usage allowance of subscriber group B. When either Alice's father or mother is also using the network, the network should monitor the traffic usage of all the online family members simultaneously. In that case, on one hand, the network should monitor Alice's and Mike's traffic usage and detect whether their total traffic reaches the usage allowance of the subscriber group B. On the other hand, the network should monitor all persons' traffic usage and detect whether the total traffic reaches the total usage allowance of subscriber group A as well.

Usage monitoring of a subscriber in multiple subscriber groups by priority

Alice, her sister and her parents are subscribers of mobile network X and they have following subscriptions:

1) Alice and her parents constitute subscriber group A, which is permitted for the total usage allowance of 50M per month.

2) Alice and her friend Lucy constitute another subscriber group - subscriber group B, which is permitted for usage allowance of 30M per month

3) There is no specific usage allowance for any person.

4) The allowance usage for Alice is accumulated into subscriber group A firstly. And this allowance usage is not accumulated into subscriber group B. when the allowance usage of subscriber group A runs out, the allowance usage for Alice will be accumulated into subscriber group B.

In this profile, Alice and her parents share the total usage allowance of 50M per month. In addition, Alice and Lucy share the total usage allowance of 30M per month. When Alice and her parents are using the network, the network should monitor the traffic and detect whether the volume reaches the usage allowance of subscriber group A (50M). Here, this allowance usage for Alice is not accumulated into subscriber group B.

When Alice and Lucy are using the network and the allowance of subscriber group A hasn't run out, the volume used by Alice should not be accumulated into subscriber group B. The network should monitor the traffic used by Alice separately and detect whether the volume reaches the allowance of subscriber group A. At the same time, the network should monitor the traffic used by Lucy and detect whether the volume reaches the allowance of subscriber group B.

In this case, if the allowance of subscriber group A has run out, the network should monitor the traffic used by Alice and Lucy together and detect whether the volume used reaches the allowance of subscriber group B.

8.2.4 Post-conditions

None.

8.2.5 Requirements

The 3GPP system shall be able to monitor traffic for a group of UEs that are subscribed to share a common traffic usage allowance.

The 3GPP system shall be able to monitor the traffic usage of a UE in more than one subscriber group simultaneously or by priority.

The 3GPP system shall be able to perform time based usage monitoring to subscriber group.

8.3 Alternative Solutions

Editor's note: This clause will describe alternative solution to the key issue.

8.3.1 Alternative Solution 1 - correlation at the SPR/UDR

This solution is based on some functional enhancements to the SPR/UDR and the PCRF. The correlation of the group members is done at the SPR/UDR. The allowance for the whole subscriber group is managed by one SPR/UDR. The allowance for each group member is allocated by one SPR/UDR.

8.3.1.1 Terminologies

Group member remaining allowance: The current allowance allocated to a member of a subscriber group, which is part of the usage monitoring related information in the SPR/UDR and sent to the PCRF. This value is updated as the user consumes data, but is reinitialized to the initial value at the start of the each allowance period (e.g., monthly billing cycle). The initial value may not be the same for all members of the same group, which is configurable by the operators for each group member.

Group remaining allowance: The remaining allowance of a subscriber group after allocating group member remaining allowance to each group member.

8.3.1.2 Information flow

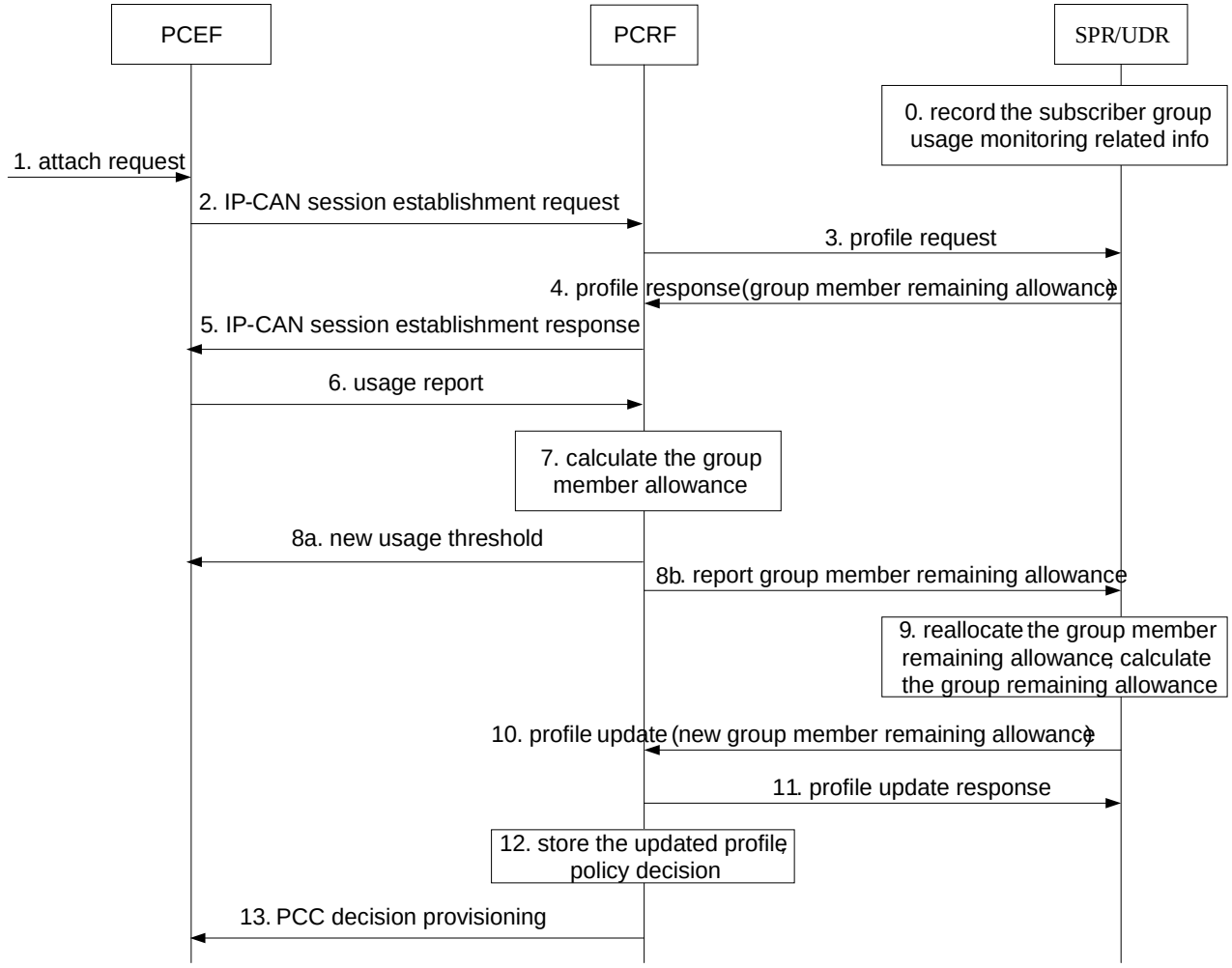

Figure 8.3.1.2-1

0. The usage monitoring related information of the subscriber group, including the subscriber group ID, the group remaining allowance, and the group member remaining allowance for each group member is stored in the SPR/UDR.

1. A group member attaches to the network and trigger the establishment of the IP-CAN session.

2. The PCEF requests to establish IP-CAN session for this subscriber.

3. The PCRF requests the subscriber profile from the SPR/UDR.

4. The SPR/UDR sends the subscriber profile to the PCRF, including the group member remaining allowance for this user.

5. The PCRF decides to enable usage monitoring for this group member, then sends a usage threshold (which is smaller than or equal to the group member remaining allowance) to the PCEF and requests the usage report trigger.

NOTE: Setting an appropriate group member remaining allowance which is larger than the usage threshold may help to reduce the interaction between the PCRF and the SPR/UDR.

6. The PCEF monitors the usage of the user and reports to the PCRF when the usage reaches the usage threshold, or the session is terminated. This is same as usage monitoring for individual subscriber.

7. The PCRF subtracts the used usage from the group member remaining allowance of the user and stores the latest group member remaining allowance in the PCRF.

8a. If the group member remaining allowance is not zero, the PCRF sends a new usage threshold (which is smaller than or equal to the group member remaining allowance) to the PCEF to continue the usage monitoring.

Step 6, 7, 8a may be repeated several times.

8b. When the group member remaining allowance in the PCRF reaches zero, or when the session is terminated, the PCRF reports this latest group member remaining allowance to the SPR/UDR.

9. When the recorded group remaining allowance in the SPR/UDR is not zero, the SPR/UDR allocates a new group remaining member allowance to this user and subtracts the allocated allowance from the remaining group allowance. When the recorded group remaining allowance in the SPR/UDR is zero, the SPR/UDR sets the user's new group member remaining allowance to zero.

10. The SPR/UDR sends the new group member remaining allowance to the PCRF for this user.

11. The PCRF responds to the SPR/UDR.

12. The PCRF stores the new group member remaining allowance.

13. If the new group member remaining allowance is not zero, the PCRF sends a new usage threshold to the PCEF to continue the usage monitoring; if the new group member remaining allowance is zero, the PCRF sends new policies to the PCEF as the subscriber group total allowance runs out.

Editor's note: This alternative solution may require further enhancements to ensure the full consumption of the total group allowance in a fair way when the group remaining allowance becomes small.

8.3.2 Alternative Solution 2 - PCRF based solution

8.3.2.1 Terminology

Subscriber Group ID (SGID): A reference that is used to identify a Subscriber Group.

Subscriber Group Member List (SGML): A vector that contains the identities of all Subscriber Group members.

Group total allowance (GTA): The allowance (volume or time based) that is assigned to a Subscriber Group by the operator. Each member of the Subscriber Group can use this allowance.

8.3.2.2 Assumptions

Assumptions 1: Subscription Group Profile (e.g. SGID, SGML, and associated GTA) is stored in SPR/UDR.

Assumptions 2: A Group-PCRF is needed to manage the associated GTA and the usage threshold.

Editor note: How to choose the Group-PCRF is described in clause 8.3.2.4.

Editor note: In this solution, we assume that the usage monitoring is disabled from the subscriber group when the user is in LBO roaming case.

8.3.2.3 Solution Description

Based on the assumption, when each member under the Subscriber Group accesses to the network, the network needs to select the Group-PCRF to serve the UE access. The Group-PCRF acquires the Subscriber Group Profile from the SPR/UDR when the IP-CAN Session/TDF Session for first UE of the Subscriber Group is established. The Group-PCRF makes decision to enable the usage monitoring to the Subscriber Group, including generating monitoring key, distributing usage threshold based on the Subscription Group Profile and provides them to the PCEF/TDF.

The PCEF/TDF performs usage monitoring based on the threshold, and reports the accumulated usage to the Group-PCRF when the threshold is reached or the report condition is met. Based on the usage reporting, the Group-PCRF makes policy decision.

If the GTA runs out, the Group-PCRF can terminate the session or terminate usage monitoring. Otherwise, the Group-PCRF can continue the usage monitoring. The Group-PCRF reports the latest remaining GTA to the SPR/UDR when the session is terminated.

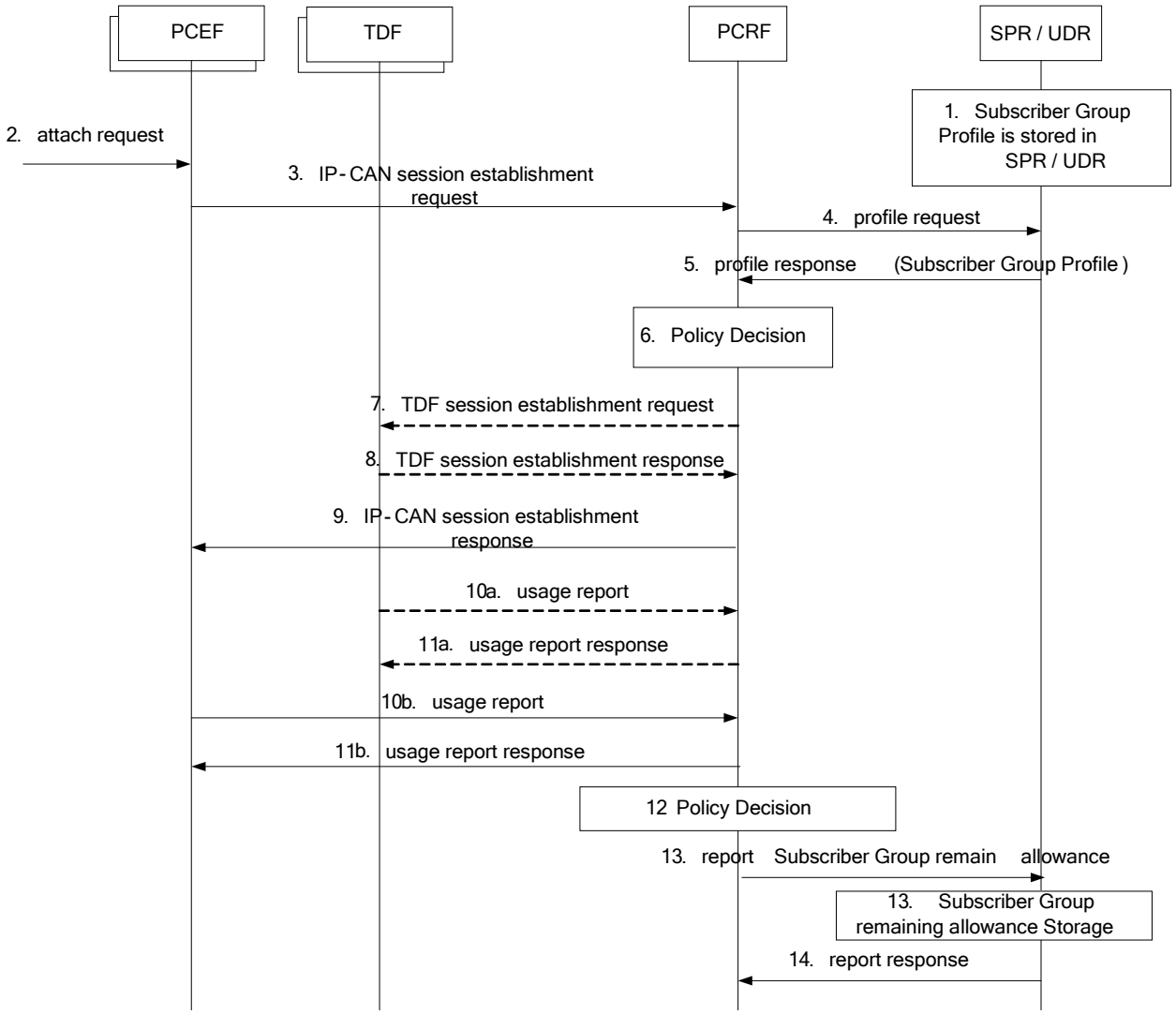

Figure 8.3.2.3-1: Usage Monitoring Control for Subscriber Group

1. The Subscriber Group Profile and the Subscriber Profile of each member of the Subscriber Group are stored in the SPR/UDR.

2. The first member of the Subscriber Group attaches to the network and trigger the establishment of the IP-CAN Session.

3. The PCEF sends IP-CAN session establishment request to the Group-PCRF.

NOTE: The Group-PCRF selection is described in clause 8.3.2.4.

4. The Group-PCRF requests the Subscriber Group Profile and the Subscriber Profile for the first member of the Subscriber Group from the SPR/UDR.

5. The SPR/UDR sends the Subscriber Group Profile and the Subscriber Profile for the first member of the Subscriber Group to the Group-PCRF.

6. The Group-PCRF decides to enable usage monitoring for the Subscriber Group member, including generating monitoring key, set a usage threshold based on the Subscription Group Profile.

7. If the TDF was deployed in the network, the Group-PCRF sends TDF session establishment request to the TDF. The usage monitoring control information is included in the request message as well.

8. The TDF returns TDF Session establishment response to the Group-PCRF.

9. Then Group-PCRF sends IP-CAN Session establishment response to the PCEF. the usage monitoring control information will be included in the message, if usage monitoring control function was enabled at the PCEF.

10a. The TDF performs usage monitoring based on the threshold, and reports the accumulated usage to the Group-PCRF when the threshold is reached or the report condition is met.

11a. The Group-PCRF returns a response to the TDF.

10b. The PCEF performs usage monitoring based on the threshold, and reports the accumulated usage to the Group-PCRF when the threshold is reached or the report condition is met.

11b. The Group-PCRF returns a response to the PCEF.

12. The Group-PCRF sets another usage threshold based on remaining GTA and send it to the PCEF/TDF, another usage monitoring cycle is started.

When the subsequent members of the Subscriber Group attach, the procedures described in step 2-12, will be performed with the exception in step 5: only the Subscriber Profile for the corresponding member of the Subscriber Group is provided to the Group-PCRF.

If the threshold for UE from the subscriber group is asked while the GTA is used out, as an optimization, the Group-PCRF can ask the other UEs to report their current usage and remaining quota slice, then PCRF can re-assign the usage threshold for all the users based on the reported remaining quota slice.

NOTE: It is assumed the same PCRF will be selected as the first member. How to select Group-PCRF is described in clause 8.3.2.4.

13. Based on the usage reporting, the Group-PCRF makes policy decision. If the GTA runs out, the Group-PCRF can terminate the IP-CAN session and TDF session or terminate usage monitoring. Otherwise, the Group-PCRF can continue the usage monitoring.

The Group-PCRF reports the latest remaining GTA to the SPR/UDR when the usage monitoring control is terminated (e.g. all the UEs belonging to the subscriber group detaches).

14. The SPR/UDR updates the remaining GTA to the Subscriber Group Profile.

15. The SPR/UDR responds to the Group-PCRF.

8.3.2.4 Group-PCRF selection

8.3.2.4.1 Option 1: SPR/UDR-method

In this option, the PCRF selected for the first UE of a Subscriber group is seen as the Group-PCRF for the corresponding Subscriber Group. The Group-PCRF locates in the HPLMN and is selected by the P-GW/PCEF (for Non-roaming case and Roaming case with Home routed) or vPCRF(for Roaming case with LBO).The IP address of the Group-PCRF is deposited in the SPR/UDR when the first UE of the Subscriber Group accesses. When the following UEs (members of the same Subscriber Group) access, the IP address of the Group-PCRF is provided from the SPR/UDR to the PCEF(s) for those UEs, the IP-CAN session establishment messages for these UEs need to be redirected to the Group-PCRF if the initially selected PCRFs are different from the Group-PCRF.

The corresponding call flow is described as below:

Taking as an example, UE-1 and UE-2 belongs to the same Subscriber Group. PCEF-1 is selected serving for UE-1, PCEF-2 is selected serving for UE-2.

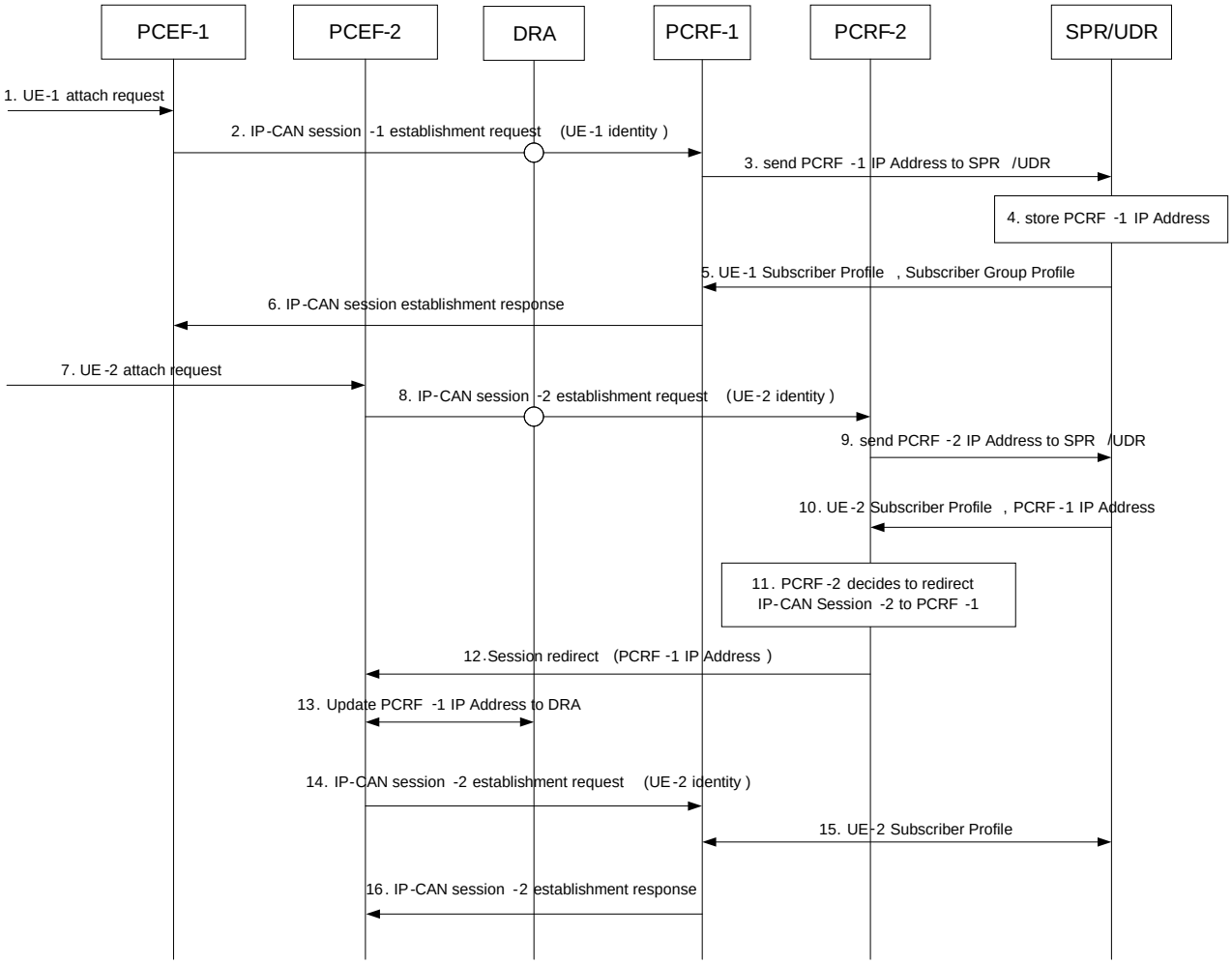

Figure 8.3.2.4.1-1: SPR/UDR based Group-PCRF Selection for Subscriber Group

Non-roaming, home routed roaming and Local Breakout cases are supported by this method. The vPCRF shall be involved in the case of Local Breakout roaming case.

1. The PCEF-1 receives a request message when UE-1(the first attached UE) attaches to the network. This triggers IP-CAN Session establishment procedure with the PCRF.

2. The PCEF-1 sends IP-CAN Session establishment request which includes UE-1 identity to the DRA. The DRA selects PCRF-1 for UE-1 based on the UE-1 identity.

3. The PCRF-1 sends a request to the SPR/UDR in order to receive UE-1 Subscriber Profile. The PCRF-1 provides the UE-1 identity to the SPR/UDR. In addition, the PCRF-1 IP Address will be included in the message as well.

4. The SPR/UDR stores the PCRF-1 IP Address. The PCRF-1 will be treated as Group-PCRF serving for the Subscriber Group member. The SPR/UDR creates a linking record between the PCRF-1 IP Address and SGID.

NOTE: If all the UEs belonging to the subscriber group detaches from the network, the PCRF-1should inform the SPR/UDR to remove the PCRF-1 IP address.

5. The SPR/UDR sends the UE-1 Subscriber Profile and the Subscriber Group Profile (SGID, SGML, GTA) to the PCRF-1.

6. The PCRF-1 stores these information and returns IP-CAN Session establishment response to the PCEF-1.

7. When UE-2 which belongs to the same Subscriber Group attaches to the network, the PCEF-2 is selected for serving UE-2 access.

8. PCEF-2 sends IP-CAN Session establishment request message to the PCRF-2 via the DRA. The PCRF-2 is selected by the DRA based on the UE-2 identity contained in the message.

9. The PCRF-2 sends a request to the SPR/UDR in order to receive UE-2 Subscriber Profile. The UE-2 identity and the PCRF-2 IP Address will be included in the request message.

10. Based on the UE-2 identity received in step 9 and the SGML stored in SPR/UDR, the SPR/UDR knows UE-2 and UE-1 belongs to the same Subscriber Group and the PCRF-1 has been selected as the Group-PCRF. The SPR/UDR returns UE-2 Subscriber Profile and the PCRF-1 IP Address to the PCRF-2.

11. After PCRF-2 receives the PCRF-1 IP Address, the PCRF-2 redirects the IP-CAN Session for the UE-2 to the PCRF-1.

12. The PCRF-2 sends the PCRF-1 IP Address to the PCEF-2.

13. The PCEF-2 provides the PCRF-1 IP Address to DRA. The DRA updates the relationship <UE-2 identity, PCRF-2 IP Address> to <UE-2 identity, PCRF-1 IP Address>.

14. The PCEF-2 sends IP-CAN Session establishment request to the PCRF-1.

15. The PCRF-1 acquires UE-2 Subscriber Profile from the SPR/UDR.

16. The PCRF-1 returns IP-CAN Session establishment response to the PCEF-2.

8.3.2.4.2 Option 2: DRA-method

In this option, when the first UE of the Subscriber Group accesses to the network, the DRA selects a PCRF for the UE based on the UE identity. This PCRF is seen as the Group-PCRF and located in the HPLMN(roaming case). During the IP-CAN Session establishment, the PCRF acquires Subscriber Group Profile (SGID, SGML, GTA) from the SPR/UDR. The PCRF retrieves SGID, SGML from the Subscriber Group Profile and provides them to the DRA. The DRA creates a relationship between SGID, SGML and the PCRF IP Address. This PCRF will be seen as the Group-PCRF serving for the other UE which under the same Subscriber Group. When the other UEs access to the network, the DRA selects the Group-PCRF for the UE based on the relationship.

There are proxy mode and redirect mode for DRA. The following solutions are based on the two mode.

The call flow described in Figure 8.3.2.4.2-1 is based on Proxy DRA.

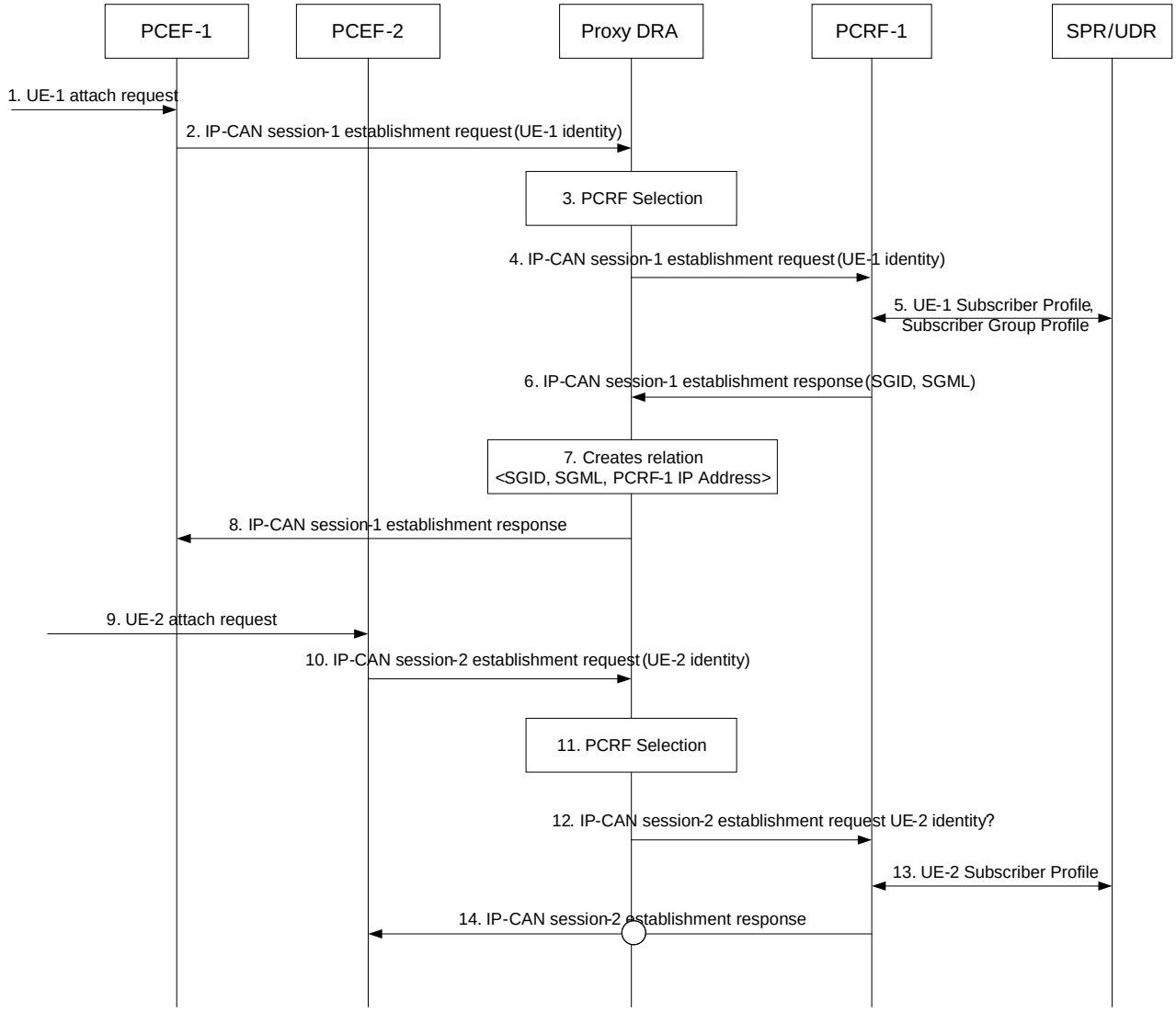

Figure 8.3.2.4.2-1: Proxy DRA based Group-PCRF Selection for Subscriber Group

Non-roaming, home routed roaming and Local Breakout cases are supported by this method. The vPCRF shall be involved in the case of Local Breakout roaming case.

1. The PCEF-1 receives a request message when UE-1 attaches to the network. This triggers IP-CAN Session establishment procedure with the PCRF.
2. The PCEF-1 sends IP-CAN Session establishment request which includes UE-1 identity to the DRA.
3. The DRA selects PCRF-1 for UE-1 based on the UE-1 identity.
4. The DRA proxy the message to the PCRF-1.
5. The PCRF-1 sends a request which includes UE-1 identity to the SPR/UDR in order to receive UE-1 Subscriber Profile. According to the UE-1 identity, the UE-1 belongs to a Subscriber Group, the related Subscriber Group Profile (SGID, SGML, GTA) along with the UE-1 Subscriber Profile is sent to the PCRF-1 by the SPR/UDR.
6. The PCRF-1 returns IP-CAN Session establishment response to the PCEF-1. Meanwhile, PCRF retrieves SGID, SGML from the Subscriber Group Profile and includes it in the message.
7. The DRA retrieves SGID, SGML from the IP-CAN Session establishment response message. A relationship between the SGID, SGML and the PCRF-1 IP Address is created at DRA.
8. The DRA returns IP-CAN Session establishment response to the PCEF-1.

9. When UE-2 which belongs to the same Subscriber Group attaches to the network, the PCEF-2 is selected for serving UE-2 access.
10. PCEF-2 sends IP-CAN Session establishment request to the DRA. The UE-2 identity is contained in the message.
11. According to the UE-2 identity and the above relationship, the DRA selects PCRF-1 for UE-2.
12. The DRA proxy the message the PCRF-1.
13. The PCRF-1 retrieves UE-2 Subscriber Profile based on the UE-2 identity from the SPR/UDR. Since the Subscriber Group Profile has been provided the PCRF-1 in step 5, this step will not include this information.
14. The PCRF-1 returns IP-CAN Session establishment response to the PCEF-2 via the DRA.

The call flow described in Figure 8.3.2.4.2-2 is based on Redirect DRA.

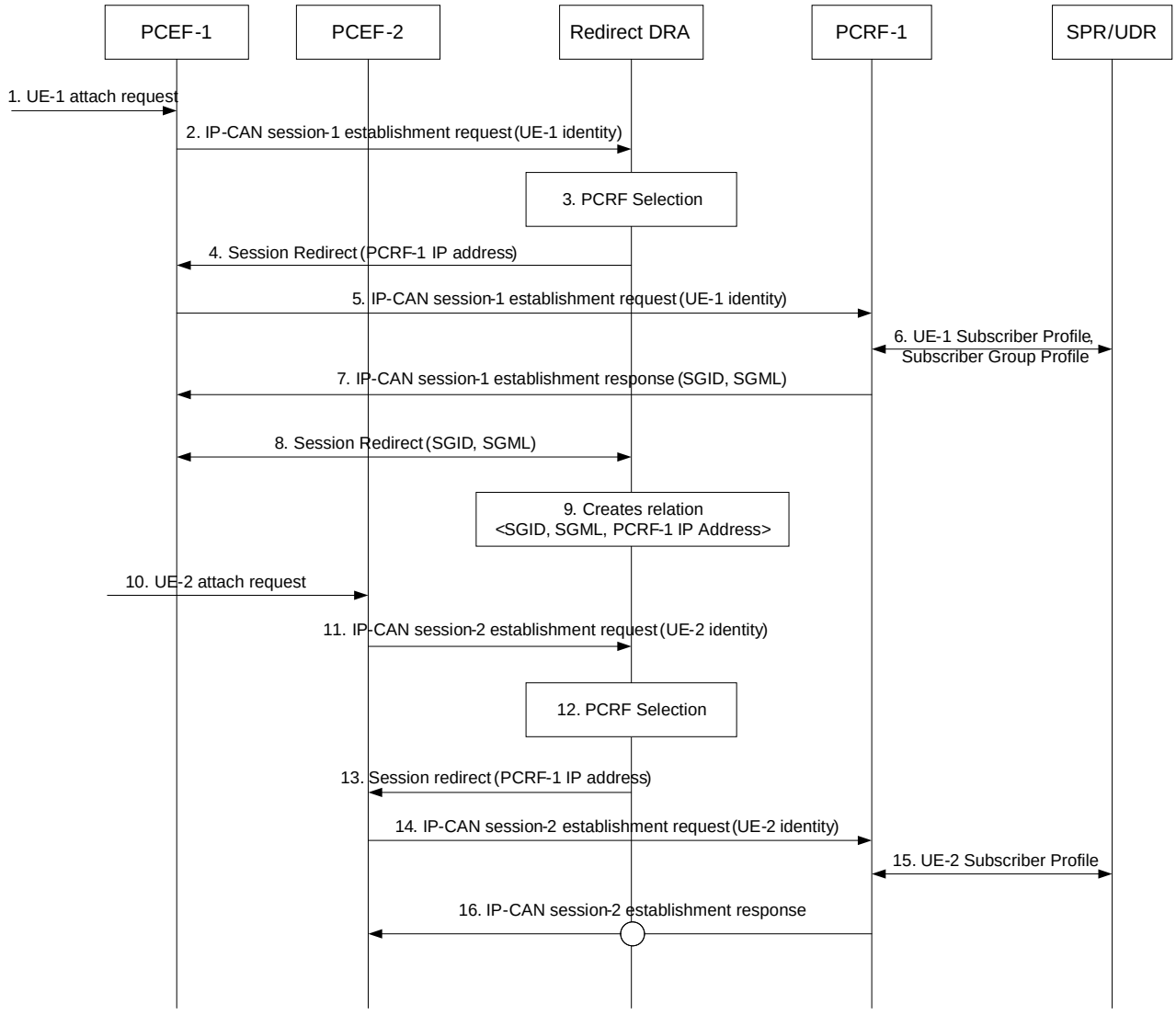

Figure 8.3.2.4.2-2: Redirect DRA based Group-PCRF Selection for Subscriber Group

Non-roaming, home routed roaming and Local Breakout cases are supported by this method. The vPCRF shall be involved in the case of Local Breakout roaming case.

1. The PCEF-1 receives a request message when UE-1 attaches to the network. This triggers IP-CAN Session establishment procedure with the PCRF.
2. The PCEF-1 sends IP-CAN Session establishment request which includes UE-1 identity to the DRA.
3. The DRA selects PCRF-1 for UE-1 based on the UE-1 identity.

4. The DRA sends a session redirect message which includes the PCRF-1 IP Address to the PCEF-1.
5. The PCEF-1 sends IP-CAN Session establishment request to the PCRF-1.
6. The PCRF-1 sends a request which includes UE-1 identity to the SPR/UDR in order to receive UE-1 Subscriber Profile. According to the UE-1 identity, the UE-1 belongs to a Subscriber Group, the related Subscriber Group Profile (SGID, SGML, GTA) along with the UE-1 Subscriber Profile is sent to the PCRF-1 by the SPR/UDR.
7. The PCRF-1 returns IP-CAN Session establishment response to the PCEF-1. Meanwhile, PCRF retrieves SGID, SGML from the Subscriber Group Profile and includes it in the message.
8. The PCEF-1 sends the SGID, SGML to the DRA.
9. The DRA creates a relationship between the SGID, SGML and the PCRF-1 IP Address.
10. When UE-2 which belongs to the same Subscriber Group attaches to the network, the PCEF-2 is selected for serving UE-2 access.
11. PCEF-2 sends IP-CAN Session establishment request to the DRA. The UE-2 identity is contained in the message.
12. According to the UE-2 identity and the above relationship, the DRA selects PCRF-1 for UE-2.
13. The DRA sends a session redirect message which includes the PCRF-1 IP Address to the PCEF-2.
14. The PCEF-2 sends IP-CAN Session establishment request to the PCRF-1.
15. The PCRF-1 retrieves UE-2 Subscriber Profile based on the UE-2 identity from the SPR/UDR. Since the Subscriber Group Profile has been provided the PCRF-1 in step 5, this step will not include this information.
16. The PCRF-1 returns IP-CAN Session establishment response to the PCEF-2.

8.3.2.5 Functionality description of the Network entity and interface

PCEF/TDF:

Same function as defined for usage monitoring in Release 11, no enhancement introduced.

PCRF:

Same function as defined for usage monitoring in Release 11, with the additions:

-for the Subscriber Group member, including generating monitoring key, set a usage threshold based on the Subscription Group Profile.

- If the GTA runs out, the PCRF shall terminate the IP-CAN session and TDF session or terminate usage monitoring. Also, the PCRF shall report the latest remaining GTA to the SPR/UDR when the usage monitoring control is terminated (e.g. all the UEs belonging to the subscriber group detaches).
- The PCRF shall redirect the IP-CAN Session establishment to another PCRF as instructed by the SPR/UDR.(only for option 1: SPR/UDR-method).

DRA:

Same as defined for usage monitoring in Release 11, with the additions:

- The DRA shall obtain the SGID, SGML from the SPR/UDR during the IP-CAN Session establishment procedure. And a relationship between the SGID, SGML and the Group-PCRF IP Address shall be created at DRA, which is used to assist to locate the Group-PCRF for other UEs in the subscriber group.(only for option 2: DRA-method).

SPR/UDR:

Same function as defined for usage monitoring in Release 11, with the additions:

- The SPR/UDR shall store the Subscription Group Profile (e.g. SGID, SGML, and associated GTA)

- The SPR/UDR shall create a linking record between the Group-PCRF IP Address and SGID, which is used to assist to locate the Group-PCRF for other UEs in the subscriber group. (only for option 1: SPR/UDR-method)

Sp Interface:

Same function as defined for usage monitoring in Release 11, with the additions:

- The Sp interface shall support to convey the Subscriber Group Profile from SPR/UDR to PCRF and convey the latest remaining GTA to the SPR/UDR when the usage monitoring control is terminated (e.g. all the UEs belonging to the subscriber group detaches).
- The Sp interface should support to convey the PCRF address between SPR/UDR and PCRF. (only for option 1: SPR/UDR-method)

8.4 Evaluation

Editor's Note: This clause will evaluate the alternative solutions.

8.5 Conclusion

Editor's Note: This clause will provide conclusions with respects to preferred solution and what further specification work is required.

9 Key Issue 6: Time based Usage Monitoring

9.1 Description

9.2 Use Cases

9.2.1 Descriptions

This use case describes a scenario for time based monitoring.

9.2.2 Pre-conditions

Alice is a subscriber of mobile network X and she has the following subscription:

(A) She is a postpaid subscriber;

(B) 3 Hour time allowance for streaming video;

(C) In addition, 2G total volume allowance for all the other traffic.

When 3 hour time allowance is reached, the streaming video will be blocked.

9.2.3 Service Flows

If Alice attaches to the mobile network X and accesses only streaming video service, the subscription profile (B) will apply: the network will be able to monitor the traffic usage and detect if the 3 hour time allowance for streaming video is used up. After the 3 hour time allowance is used up, mobile network X will block streaming video service from Alice.

If Alice attaches to the mobile network X, and accesses other services, subscription (C) will apply. The network will be able to monitor the traffic usage and detect if the volume allowance for other services is used up.

9.2.4 Post-conditions

None.

9.2.5 Requirements

The 3GPP system shall be able to perform time based usage monitoring for service data flow and/or application.

9.3 Alternative Solutions

9.3.1 Alternative Solution 1: Introduction of time based units

In this alternative solution it is proposed to use time based units for usage monitoring report requested by the PCRF from the PCEF/TDF for measuring effective time used by the sdf/applications.

The request for usage monitoring report shall be done by using the same mechanisms as currently defined for volume based usage monitoring.

The report shall be done in the same manner as for volume based usage monitoring report.

The mechanism for time based usage monitoring shall be identical to the Quota Consumption Time mechanism as defined in TS 32.299 [4] and described in the following text in details for the interactions between the PCRF and the PCEF/TDF.

In order to support time based usage monitoring, the PCRF may optionally indicate to the PCEF/TDF, along with other usage monitoring information provided, the Inactivity Detection Time. This value represents the time interval after which the time measurement shall stop for the Monitoring key, if no packets are received belonging to the corresponding Monitoring Key during that time period. Time measurement shall resume on receipt of a further packet belonging to the Monitoring key.

Time measurement for a Monitoring key shall also be stopped when time based usage monitoring is disabled, if this happens before the Inactivity Detection Time is reached.

If an Inactivity Detection Time value of zero is provided, or if no Inactivity Detection Time is present within the usage monitoring information provided by the PCRF, the time measurement shall be performed continuously from the point at which it was started until time based usage monitoring is disabled.

9.4 Evaluation

An evaluation of different alternative solutions was done in the paper S2-122743 and the decision was that other methods are not sufficient from the operator's perspective and that time based usage monitoring is required.

9.5 Conclusion

It is proposed to standardize the control of time based usage monitoring functionality over Gx/Sd as described in the Alternative Solution 1.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2011-07					Skeleton proposed by SA2		0.0.0
2011-08					TSG SA WG1 Meeting #55: Inclusion of: S1-112307, S1-112308, S1-112309, S1-112421	0.0.0	0.1.0
2011-11					TSG SA WG1 Meeting #56: Inclusion of: S1-113027, S1-113436	0.1.0	0.2.0
2012-02					TSG SA WG1 Meeting #57: Inclusion of: S1-120264	0.2.0	0.3.0
2012-2					TSG SA WG1 Meeting #58: Inclusion of: S1-121107	0.3.0	0.4.0
2012-07					TSG SA WG2 Meeting #92: Inclusion of: S2-123127, S2-122786, S2-123129, S2-123336, S2-123337, S2-123338	0.4.0	0.5.0
2012-08					TSG SA WG1 Meeting #59: Inclusion of S1-122065, S1-122120, S1-122066	0.5.0	0.6.0
2012-08					Correction to history table	0.6.0	0.6.1
2012-11					TSG SA WG2 Meeting #94: Inclusion of: S2-124654, S2-124668, S2-124871, S2-124872	0.6.1	0.7.0
2012-11	SP-56	SP-120734	-	-	MCC editorial update to version 1.0.0 for presentation to TSG SA for Information	0.7.0	1.0.0
2013-02					TSG SA WG2 Meeting #95: Inclusion of: S2-130487, S2-130689	1.0.0	1.1.0