3GPP TS 32.225 V5.11.0 (2006-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS) (Release 5)

Keywords
UMTS, multimedia, IP, charging, management

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 Specification 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 covers both online and offline charging for the IMS. For clarity, the terms Offline Charging and Online charging as applied to the IMS are defined here in clause 3. These definitions are the same as listed in TS 32.200 [2].

The IMS charging architecture details, requirements, definitions and principles are listed in TS 32.200 [2] and therefore are not repeated here.

In the present document the charging data triggers, message content and format are specified along with the transport of these messages using the Diameter protocol. Details about charging message flows and the definitions of the Diameter AVPs are also included in the present document. This information is divided into two main clauses: Online Charging and Offline Charging.

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 32.200: "Telecommunication management; Charging management; Charging principles".

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

[4] 3GPP TS 33.210: "Network domain security".

[5] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[6] IETF RFC 2486: "The Network Access Identifier".

[7] 3GPP TS 23.207: "End to end quality of service concept and architecture".

[8] 3GPP TS 29.207: "Policy control over Go interface".

[9] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[10] ITU-T Recommendation X.691: "Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".

[11] ITU-T Recommendation X.693: "Information Technology - ASN.1 encoding rules: XML encoding Rules (XER)".

[12] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[13] IETF RFC 4006, "Diameter Credit Control Application".

[14] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3."

[15] IETF Internet-Draft, "Private Extensions to the Session Initiation Protocol (SIP) for the 3rd Generation Partnership Projects (3GPP)". http://www.ietf.org/internet-drafts/draft-garcia-sipping-3gpp-p-headers-02.txt or ftp://ftp.rfc-editor.org/in-notes/rfc3455.txt

NOTE: The above reference will need to be updated to reference the assigned RFC number, once the draft achieves RFC status within the IETF.

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] IETF Internet-Draft, "SDP: Session Description Protocol". http://www.ietf.org/internet-drafts/draft-ietf-mmusic-sdp-new-13.txt

NOTE: The above reference will need to be updated to reference the assigned RFC number, once the draft achieves RFC status within the IETF.

[18] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[19] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol; Protocol Details".

[20] IETF RFC 2806: "URLs for Telephone Calls".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

offline charging: charging mechanism where charging information **does not** affect, in real-time, the service rendered

online charging: charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with session/service control is required

3.2 Symbols

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

Bi	The Interface between the IMS charging function and the BS
Rb	Online Charging Reference Point between Session Charging Function and Correlation Function
Rc	Online Charging Reference Point between ECF and Correlation Function
Re	Online Charging Reference Point towards a Rating Server
Rf	Offline Charging Reference Point between an IMS Network Entity or an AS and CCF
Ro	Online Charging Reference Point between an AS or MRFC and the ECF

3.3 Abbreviations

For the purposes of the present document, the abbreviations defined in TR 21.905 [1], TS 32.200 [2] and the following apply:

ABNF	Augmented Backus-Naur Form
ACA	Accounting Answer
ACR	Accounting Request
AS	Application Server
AVP	Attribute Value Pair
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
BS	Billing System
CCA	Credit Control Answer
CCF	Charging Collection Function
CCR	Credit Control Request
CDR	Charging Data Record
CPCF	Content Provider Charging Function

ECF	Event Charging Function
ECUR	Event Charging with Unit Reservation
CSCF	Call Session Control Function (I-Interrogating; P-Proxy; and S-Serving)
IANA	Internet Assigned Numbers Authority
IEC	Immediate Event Charging
IMS	IP Multimedia Subsystem
ISC	IMS Service Control
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
MRFP	Multimedia Resource Function Processor
OCS	Online Charging System
SCCF	Subscriber Content Charging Function
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent
UE	User Equipment

4 Offline and Online Charging

4.1 Implementation of Offline and Online Charging

The IMS charging architecture, described in TS 32.200 [2], specifies that for offline charging all communications between the IMS network entities and the CCF are carried out on the Rf interface. On the other hand, for online charging the Ro interface is used by the AS and MRFC towards the Event Charging Function and the ISC interface is used between the S-CSCF and the Session Charging Function. The rules governing the selection of the proper interfaces are described in the subclauses below.

4.1.1 Usage of Rf and Ro Interfaces

The AS and MRFC are able to distinguish whether to apply offline or online charging, i.e. whether to send charging information on the Rf interface to the CCF or on the Ro interface to the ECF (or to use both). The decision of which interface to use is based on the information (CCF and/or ECF address) the AS/MRFC receive in the SIP signalling and the system configuration as provisioned by the operator. If the AS/MRFC only receive the CCF address and do not receive an ECF address then they use only the Rf interface. If only the ECF address was provided then they use only the Ro interface. In cases where both CCF and ECF addresses are provided it is possible to use both interfaces simultaneously.

However, operators may overrule the addresses received via the SIP signalling and use their own configured rules instead. Operators may configure locally on the AS/MRFC an ECF and/or CCF address. The CCF address may be locally configured on all other IMS nodes. The choice of whether the IMS nodes use the locally configured addresses or the addresses received by SIP signalling, and the decision on which interface(s) to use, is left for operator configuration.

4.1.2 Usage of Rf and ISC Interfaces

All other IMS nodes (S-CSCF, P-CSCF, I-CSCF, BGCF and MGCF) apply offline charging via the Rf interface using the CCF address as received via SIP signalling or the locally configured CCF address. The S-CSCF supports online charging using the ISC interface, i.e. if the application server addressed over ISC is the Session Charging Function of the OCS.

4.1.3 Support of Local File Storage

The present document does not mandate the support of persistent storage on the IMS nodes nor does it require any protocol except Diameter to be used for either online or offline charging. However, if an IMS node supports a local persistent storage media, the IMS application may copy the accounting information sent to the Diameter client to this local filestore. Operator's post-processing systems may then pull the contents of the filestore via FTP applying the same file transfer procedures as those specified for the 'Bi' interface. Further details are implementation specific and are out of the scope of standardisation.

4.2 Diameter Protocol Basic Principles and Use

The present document defines a 3GPP IMS charging Diameter application, which utilizes the Diameter Base Protocol IETF RFC 3588 [3]. This application is used for both online and offline charging. The generic description of the protocol is provided in the subclauses below while the portions of the protocol application associated with offline and online charging are described in clauses 5 and 6, respectively.

4.2.1 Basic Principles

The IMS charging Diameter application is based on the following general principles:

- The basic functionality of Diameter, as defined by the Diameter Base Protocol IETF RFC 3588 [3] is re-used in IMS.
- For offline charging IMS network elements report accounting information to the Charging Collection Function (CCF). The CCF uses this information to construct and format CDRs.
- For online charging, the AS and MRFC in the IMS network report accounting information to the Event Charging Function (ECF). The ECF uses this information to support the event based charging (content charging) function of the OCS.

4.2.2 Application Requirement for the Base Protocol

4.2.2.1 Offline Specific Base Protocol Requirements

A configurable timer is supported in the CCF to supervise the reception of the ACR [Interim] and/or ACR [Stop]. An instance of the 'Timer' is started at the beginning of the accounting session, reset on the receipt of an ACR [Interim] and stopped at the reception of the ACR [Stop]. Upon expiration of the timer, the CCF stops the accounting session with the appropriate error indication.

For offline charging, the client implements the state machine described in IETF RFC 3588 [3]. The server (CCF) implements the STATELESS ACCOUNTING state machine as specified in IETF RFC 3588 [3], i.e. there is no order in which the server expects to receive the accounting information.

4.2.2.2 Online Specific Base Protocol Requirements

The usage and values of *Acct-Interim-Interval* AVP and the timer 'Tx' are under the sole control of the credit control server (OCS) and determined by operator configuration of the OCS. There are no specific requirements on the client concerning the *Acct-Interim-Interval* AVP population in the CCR.

The online client (e.g. AS, MRFC) implements the state machine described in IETF RFC 4006 [13] for "CLIENT, EVENT BASED" or "CLIENT, SESSION BASED", i.e. when the client applies Immediate Event Charging (IEC) it uses the "CLIENT, EVENT BASED" state machine, or when the client applies Event Charging with Unit Reservation (ECUR) it uses the "CLIENT, SESSION BASED" state machine.

The online charging server that is part of the OCS implements the state machine described in IETF RFC 4006 [13] for the "SERVER, SESSION AND EVENT BASED" in order to support Immediate Event Charging and Event Charging with Unit Reservation.

4.2.2.3 Security Considerations

Diameter security is addressed in the base protocol IETF RFC 3588 [3]. Network security is specified in TS 33.210 [4].

5 Offline Charging

5.1 Diameter Description on the Rf Interfaces

5.1.1 Basic Principles

The offline charging functionality is based on the IMS network nodes reporting accounting information upon reception of various SIP methods or ISUP messages, as most of the accounting relevant information is contained in these

messages. This reporting is achieved by sending Diameter *Accounting Requests* (ACR) [Start, Interim, Stop and Event] from the IMS nodes to the CCF and/or ECF.

The Diameter client uses ACR Start, Interim and Stop in procedures related to successful SIP sessions. It uses ACR Events for unsuccessful SIP sessions and for session unrelated procedures. Further details are specified in the tables below and in subclause 5.1.2.

It is operator configurable in the nodes for which SIP method or ISUP messages an *Accounting Request* is sent, with the exception that if accounting information is collected for sessions the ACR [Start] and ACR [Stop] messages are mandatory according to the tables below. Table 5.1 describes all possible ACRs that might be sent from a P-CSCF, I-CSCF, S-CSCF, MGCF or BGCF. A list of node specific ACRs, along with the AVPs to be included are detailed in section 5.1.3.3.

The ACRs to be sent from a MRFC are described in table 5.2.

In the tables below, the terms "configurable" implies that operators may enable or disable the generation of an ACR message by the IMS node in response to a particular "Triggering SIP Method /ISUP Message". However, for those table entries marked with *, the operator can enable or disable the ACR message based on whether or not the SIP (Re) Invite message that is replied to by the "Triggering SIP Method /ISUP Message" carried piggybacked user data.

Table 5.1: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for all IMS nodes except for MRFC and AS

Diameter Message	Triggering SIP Method /ISUP Message	Mandatory/ Configurable
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE	Mandatory
	ISUP:ANM (applicable for the MGCF)	Mandatory
ACR [Interim]	SIP 200 OK acknowledging a SIP RE-INVITE or SIP UPDATE [e.g. change in media components]	Configurable
	Expiration of AVP [Acct-Interim-Interval]	Configurable
ACR [Stop]	SIP BYE message (both normal and abnormal session termination cases)	Mandatory
	ISUP:REL (applicable for the MGCF)	Mandatory
ACR [Event]	SIP 200 OK acknowledging non-session related SIP messages, which are:	
	SIP NOTIFY	Configurable
	SIP MESSAGE	Configurable
	SIP REGISTER	Configurable
	SIP SUBSCRIBE	Configurable
	SIP 3xx Redirection Response	Configurable
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up	Configurable *
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure	Configurable *
	SIP CANCEL, indicating abortion of a SIP session set-up	Configurable *
	I-CSCF completing a Cx Query that was issued in response to a SIP INVITE	Configurable
NOTE: SIP SUBSCRIBE with the field "Expires" set to 0 means unsubscribe. SIP REGISTER with its "Expires" header field or "Expires" parameter equal to 0 means Deregistration [14].		

Table 5.2: Accounting Request Messages Triggered by SIP Methods for the MRFC

Diameter Message	Trigger	Mandatory/ Configurable
ACR [Start]	SIP 200 OK acknowledging an SIP INVITE for initiating a multimedia ad hoc conferencing session	Mandatory
ACR [Interim]	SIP ACK acknowledging a SIP INVITE to connect an UE to the conferencing session	Configurable
	Expiration of AVP [Acct-Interim-Interval]	Configurable
ACR [Stop]	SIP BYE message	Mandatory
	SIP Final Response with error codes 4xx, 5xx or 6xx indicating termination of an ongoing session	Mandatory

ASs support all four ACR types (Start/Interim/Stop/Event). The use of ACR Start, Interim and Stop (Session Charging) versus ACR Event (Event Charging) depends on the services provided by the application server. Example flows for an AS employing Event Charging and an AS using Session Charging are shown in subclause 5.1.2.1.3.

The ability of SIP methods not listed in tables 5.1 and 5.2 to trigger ACRs is for further study.

5.1.2 Message Flows and Types

The flows described in the present document specify the charging communications between IMS entities and the charging functions for different charging scenarios. The SIP messages associated with these charging scenarios are shown primarily for general information and to illustrate the charging triggers. They are not intended to be exhaustive of all the SIP message flows discussed in TS 24.228 [12].

5.1.2.1 Message Flows - Successful Cases and Scenarios

5.1.2.1.1 Session Related Procedures

5.1.2.1.1.1 Session Establishment - Mobile Origination

Figure 5.1 shows the Diameter transactions that are required between CSCF and CCF during session establishment originated by a UE.

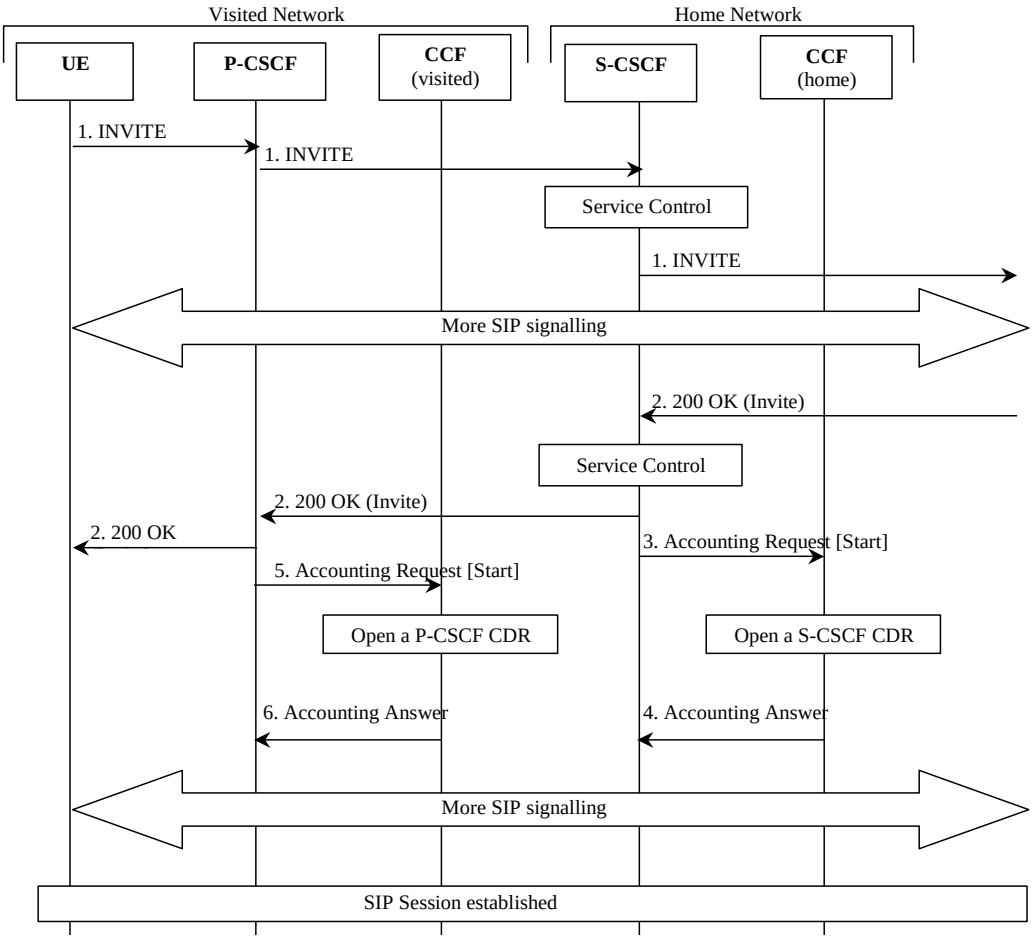

Figure 5.1: Message Sequence Chart for Session Establishment (Mobile Origination)

1. The session is initiated.
2. The destination party answers and a final response is received.
3. Upon reception of the final response, the S-CSCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a user session and start of a media component in the S-CSCF CDR.
4. The CCF acknowledges the reception of the data and opens a S-CSCF CDR.
5. Same as 3, but for P-CSCF.
6. Same as 4, but creating a P-CSCF CDR.

5.1.2.1.1.2 Session Establishment - Mobile Termination

Figure 5.2 shows the Diameter transactions that are required between CSCF and CCF during a session establishment that is terminated to a mobile. The I-CSCF is only involved in the INVITE transaction.

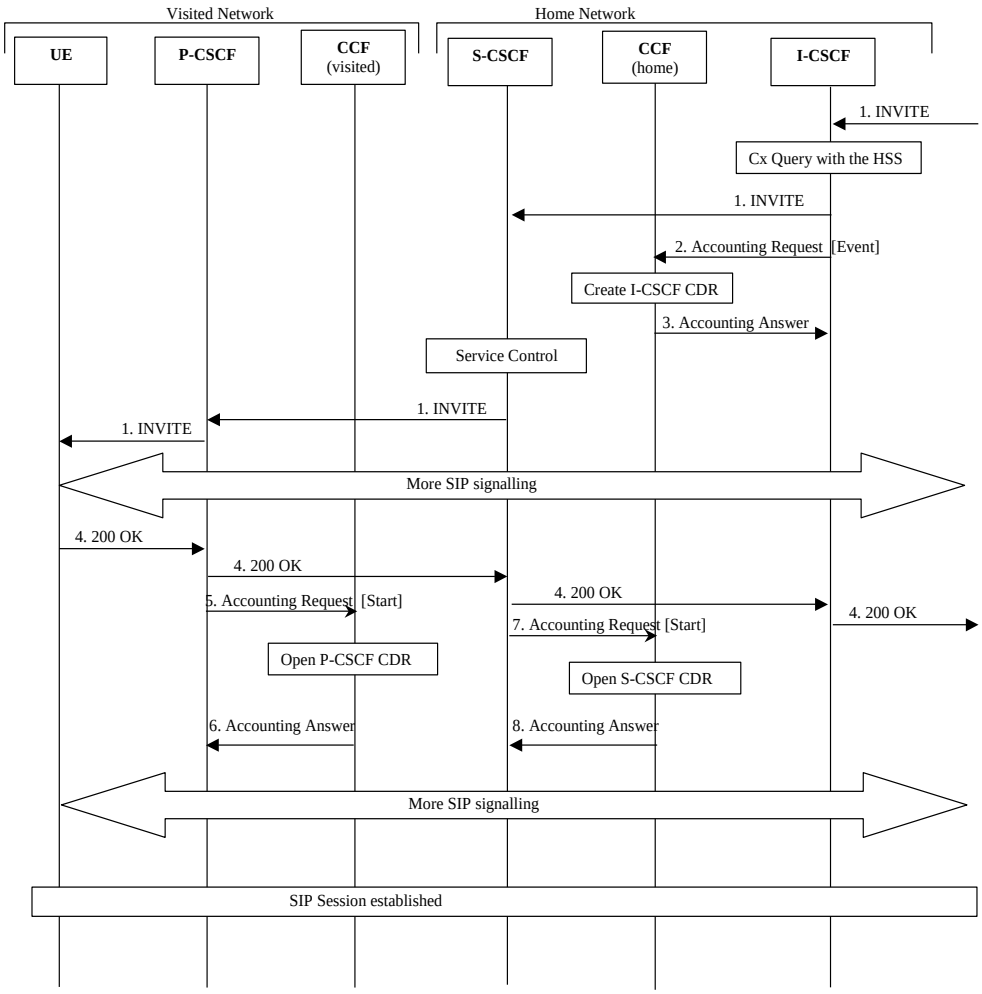

Figure 5.2: Message Sequence Chart for Session Establishment (Mobile Termination)

1. The session is initiated.
2. Upon completing a Cx query the I-CSCF sends an *Accounting Request* with the *Accounting-Record-Type* set to EVENT.
3. The CCF acknowledges the data received and creates an I-CSCF CDR.
4. The destination party answers and a final response is sent.
5. - 8. These steps are identical to the corresponding steps described in subclause 5.1.2.1.1.1.

5.1.2.1.1.3 Mid-Session Procedures

Figure 5.3 shows the Diameter transactions that are required between CSCF and CCF when a UE generates a SIP (Re-)INVITE or SIP UPDATE in mid-session, e.g. in order to modify media component(s), or when the hold and resume procedure is executed.

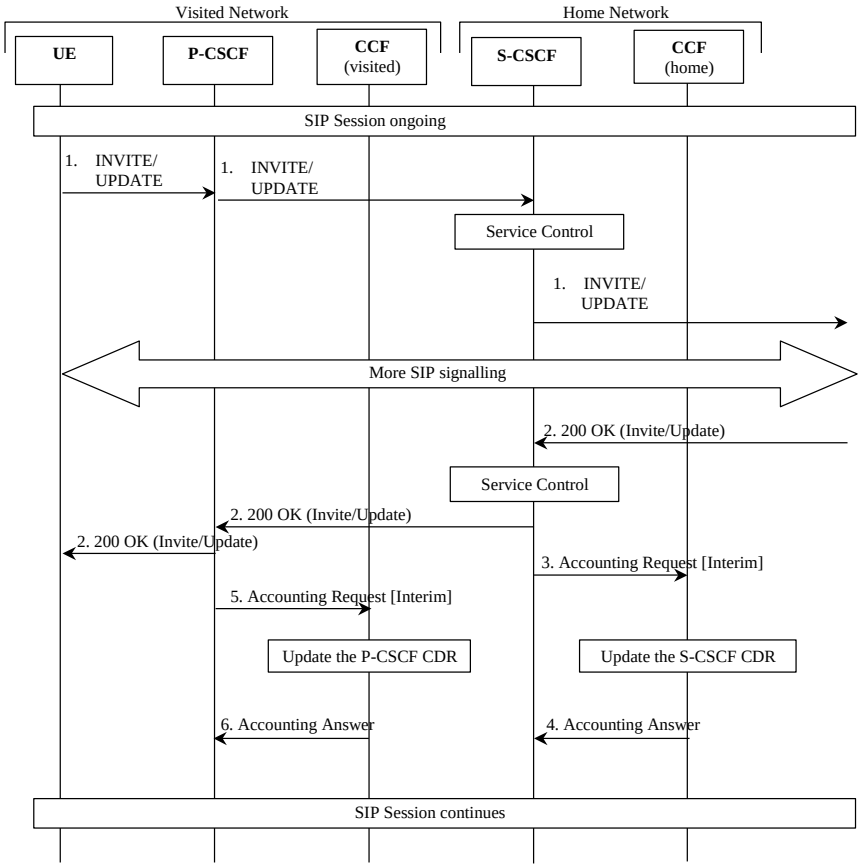

Figure 5.3: Message Sequence Chart for Media Modification

1. Modified media information is received from the subscriber.
2. The destination party acknowledges the media modification.
3. At modification of a media, the S-CSCF sends *Accounting-Request* with *Accounting-Record-Type* indicating INTERIM_RECORD to record modification of a media component in the S-CSCF CDR.
4. The CCF acknowledges the reception of the data and updates the S-CSCF CDR.
5. Same as 3, but for P-CSCF.
6. Same as 4, updating the P-CSCF CDR.

5.1.2.1.1.4 Session Release - Mobile Initiated

Figure 5.4 shows the Diameter transactions that are required between CSCF and CCF for a session release that is initiated by the UE.

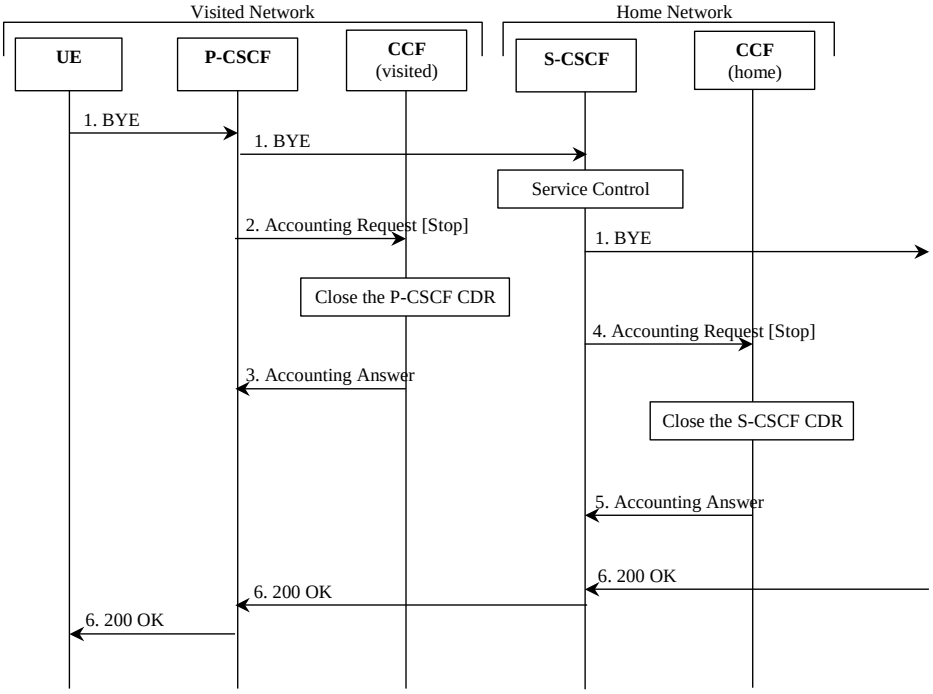

Figure 5.4: Message Sequence Chart for Session Release

1. The session is released.
2. At session termination the P-CSCF sends *Accounting-Request* with *Accounting-Record-Type* indicating STOP_RECORD to record stop of a session and stop of a media component in the P-CSCF CDR.
3. The CCF acknowledges the reception of the data and closes the P-CSCF CDR.
4. Same as 2, but for S-CSCF.
5. Same as 3, closing the S-CSCF CDR.
6. The release is acknowledged.

5.1.2.1.1.5 Session Release - Network Initiated

In the case of network initiated session release the IMS node sends a SIP BYE message which is replied to by the UE with a SIP 200 OK message. The charging message flow for this case is identical to the mobile initiated session release described in subclause 5.1.2.1.1.4.

5.1.2.1.1.6 Session Release - CCF initiated

The IMS operator may request the release of SIP session(s) upon certain trigger conditions being met, for example as soon as a fraud is detected.

Figure 5.5 shows the Diameter transactions that are required in order to release an ongoing SIP session.

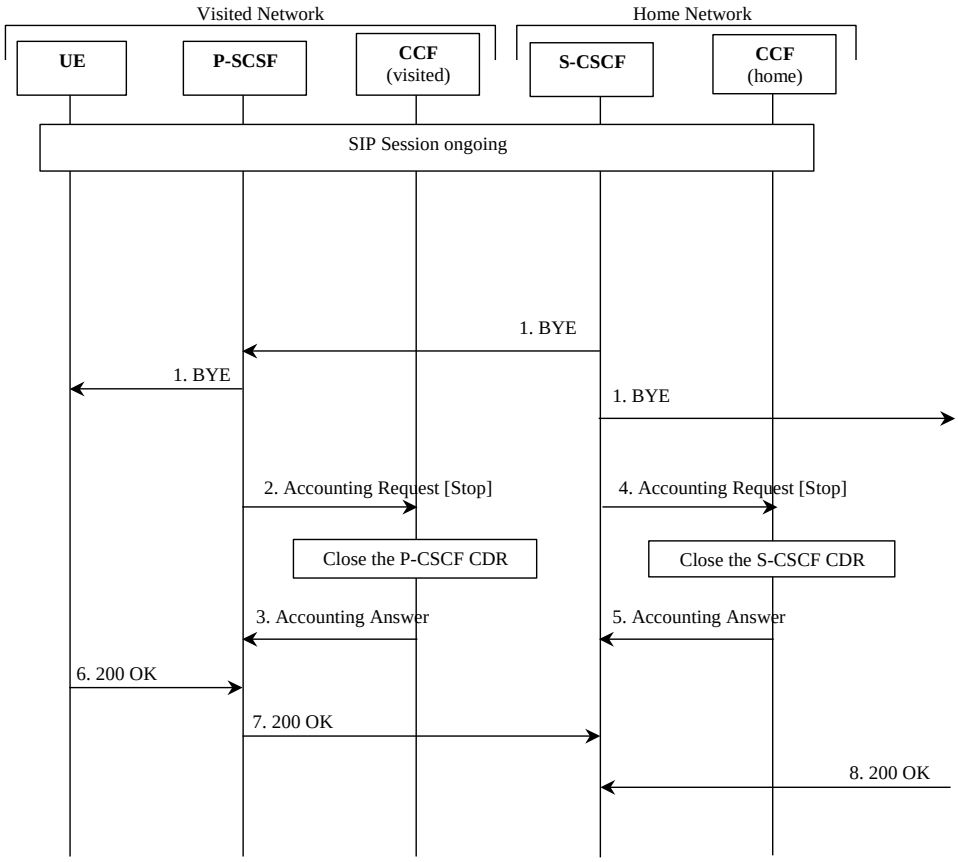

Figure 5.5: Message Sequence Chart for Network Initiated Session Release

1. The S-CSCF initiates the SIP session release by sending SIP BYE request to both the originating and the terminating parties, as specified in TS 23.218 [5].
2. At session termination the P-CSCF sends *Accounting-Request* with *Accounting-Record-Type* indicating STOP_RECORD to record stop of a session and stop of a media component in the P-CSCF CDR.
3. The CCF acknowledges the reception of the data and closes the P-CSCF CDR.
4. Same as 2, but for S-CSCF.
5. Same as 3, but for S-CSCF CDR.
6. - 8. The S-CSCF receives the 200 OK responses from originating and terminating parties.

5.1.2.1.2 Session-Unrelated Procedures

Figure 5.6 shows the Diameter transactions that are required between CSCF and CCF for session-unrelated IMS procedures, i.e. those that relate to the Diameter ACR [Event], as listed in table 5.1.

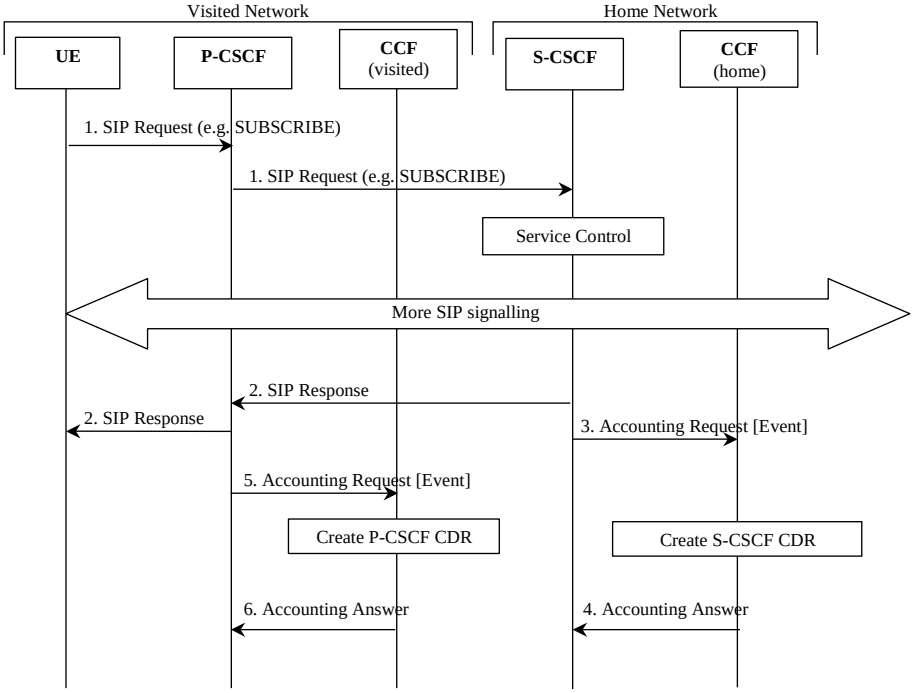

Figure 5.6: Message Sequence Chart for Session-Unrelated Procedure

1. The P-CSCF receives a "SIP Request" (e.g. SUBSCRIBE) from the subscriber.
2. The "SIP Request" is acknowledged by the "SIP Response" as follows:
   - in the successful case, a 200 OK message is returned;
   - in case of failure an appropriate SIP error message is returned.

Depending on the used SIP method, there might be additional signalling between steps 1 and 2.

3. After the completion of the procedure, the S-CSCF sends *Accounting-Request* with *Accounting-Record-Type* indicating EVENT_RECORD to record transaction specific information in the S-CSCF CDR.
4. The CCF acknowledges the reception of the data and produces an S-CSCF CDR.
5. Same as 3, but for P-CSCF.
6. Same as 4, creating a P-CSCF CDR.

5.1.2.1.3 PSTN Related Procedures

5.1.2.1.3.1 Session Establishment - PSTN Initiated

Figure 5.7 shows the Diameter transactions that are required between MGCF and CCF during session establishment initiated from the PSTN side.

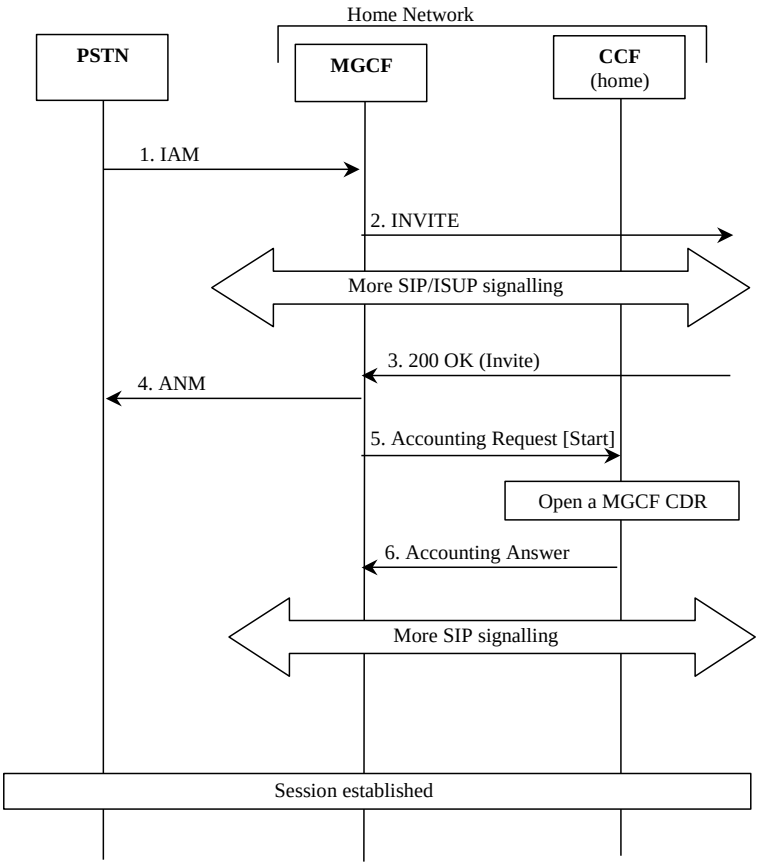

Figure 5.7: Message Sequence Chart for Session Establishment (PSTN Initiated)

1. The session is originated from the PSTN.

2. The session setup is triggered in the IMS.

3. The destination party answers and a final response is received.

4. MGCF forwards an answer message to the PSTN.

5. Upon reception of the final response, the MGCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a user session and start of a media component in the MGCF CDR.

6. The CCF acknowledges the reception of the data and opens a MGCF CDR.

5.1.2.1.3.2 Session Establishment - IMS Initiated

Figure 5.8 shows the Diameter transactions that are required between BGCF, MGCF and CCF during session establishment initiated from the IMS side.

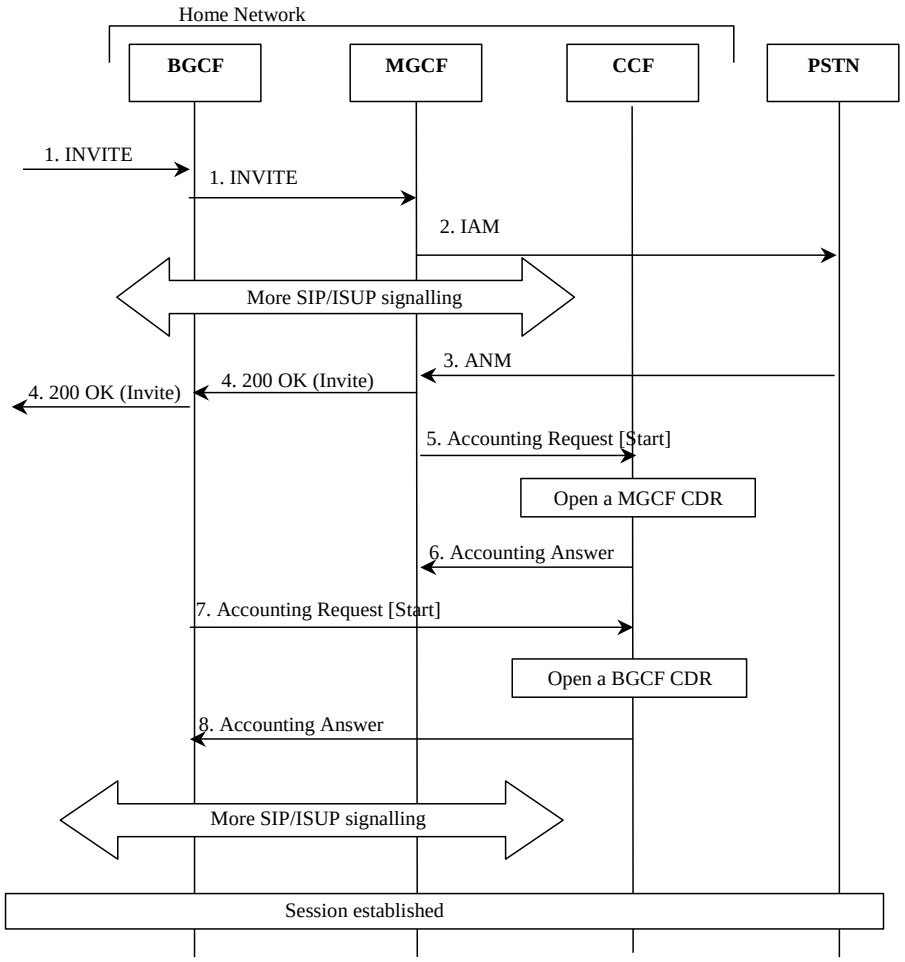

Figure 5.8: Message Sequence Chart for Session Establishment (IMS Initiated)

1. The session is originated from the IMS.
2. A session towards PSTN is established.
3. The destination party answers and an answer message is received.
4. A final response message is sent to the session originator.
5. Upon reception of the answer message, the MGCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a user session and start of a media component in the MGCF CDR.
6. The CCF acknowledges the reception of the data and opens a MGCF CDR.
7. Upon reception of the 200 OK message, the BGCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a user session and start of a media component in the BGCF CDR.
8. The CCF acknowledges the reception of the data and opens a BGCF CDR.

5.1.2.1.3.3 Session Release - PSTN Initiated

Figure 5.9 shows the Diameter transactions that are required between BGCF, MGCF and CCF during a PSTN initiated session release. The BGCF is only involved if the session had been initiated from the IMS side.

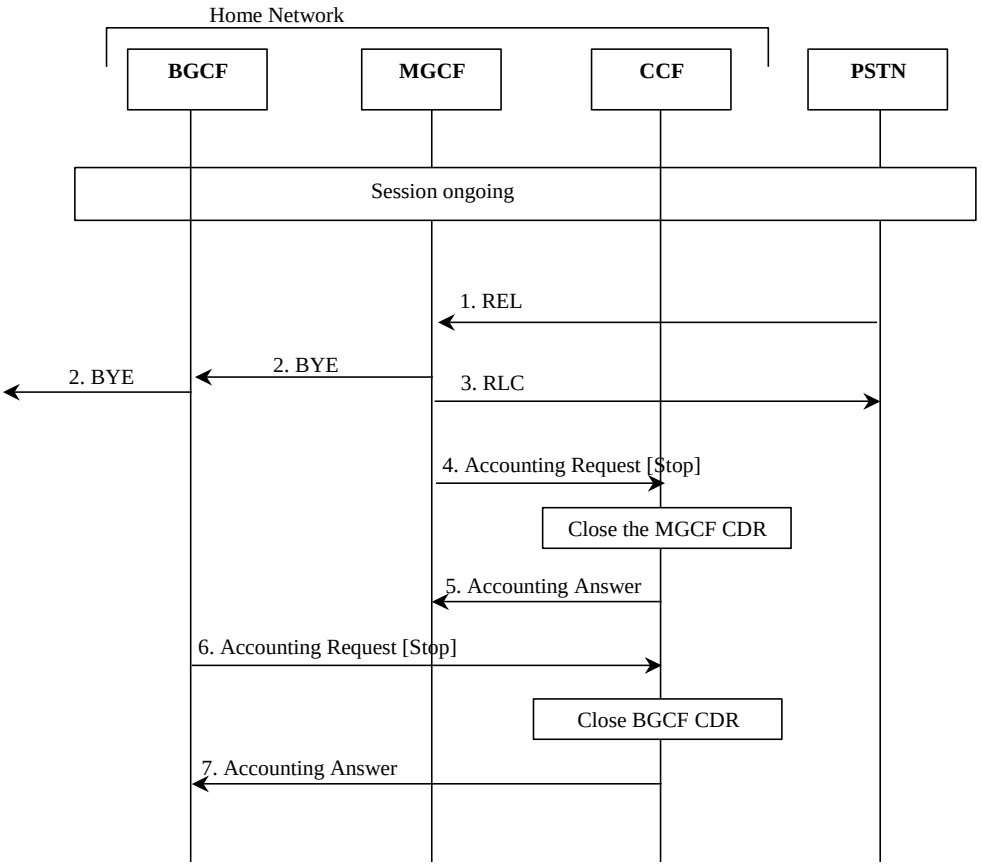

Figure 5.9: Message Sequence Chart for Session Release (PSTN initiated)

1. The session release is initiated from PSTN.
2. Session release continues within IMS.
3. The reception of the release message is acknowledged.
4. Upon reception of the release message, the MGCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating STOP_RECORD to record stop of a session in the MGCF CDR.
5. The CCF acknowledges the reception of the data and closes the MGCF CDR.
6. Same as 4, but for BGCF.
7. Same as 5, but for BGCF.

5.1.2.1.3.4 Session Release - IMS Initiated

Figure 5.10 shows the Diameter transactions that are required between BGCF, MGCF and CCF during a IMS initiated session release.

The BGCF is only involved if the session had been initiated from the IMS side.

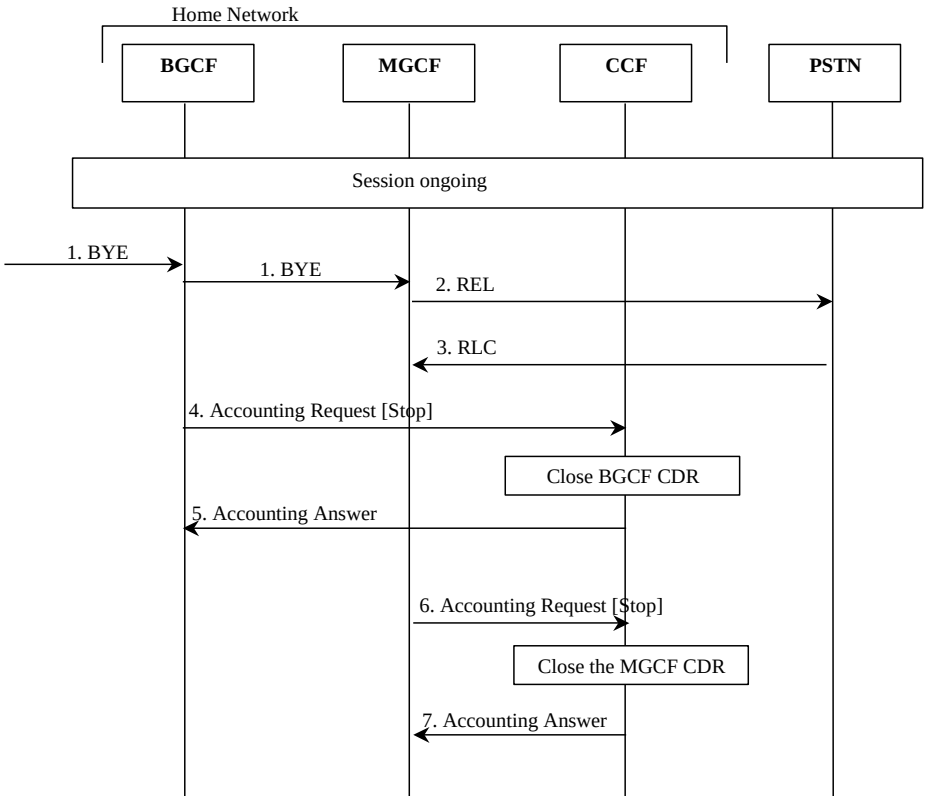

Figure 5.10: Message Sequence Chart for Session Release (IMS initiated)

1. The session release is initiated from the IMS side.
2. A release message is sent towards PSTN.
3. The acknowledgement of the release message is received from PSTN.
4. Upon reception of the BYE message, the BGCF sends an *Accounting-Request* with *Accounting-Record-Type* indicating STOP_RECORD to record stop of a session in the BGCF CDR.
5. The CCF acknowledges the reception of the data and closes the BGCF CDR.
6. Same as 4, but for MGCF.
7. Same as 5, but for MGCF.

5.1.2.1.4 MRFC Related Procedures

5.1.2.1.4.1 Multi-Party Call

Figure 5.11 shows the establishment of an ad hoc conference (multiparty call). An AS (acting as B2BUA) performs third party call control with the MRFC, where the S-CSCF is in the signalling path. The Application Server that is in control of the ad hoc conference is aware of the MRFC capabilities.

NOTE: Only accounting information sent from the MRFC is shown in detail in the figure. The SIP messages are for illustrative purpose only.

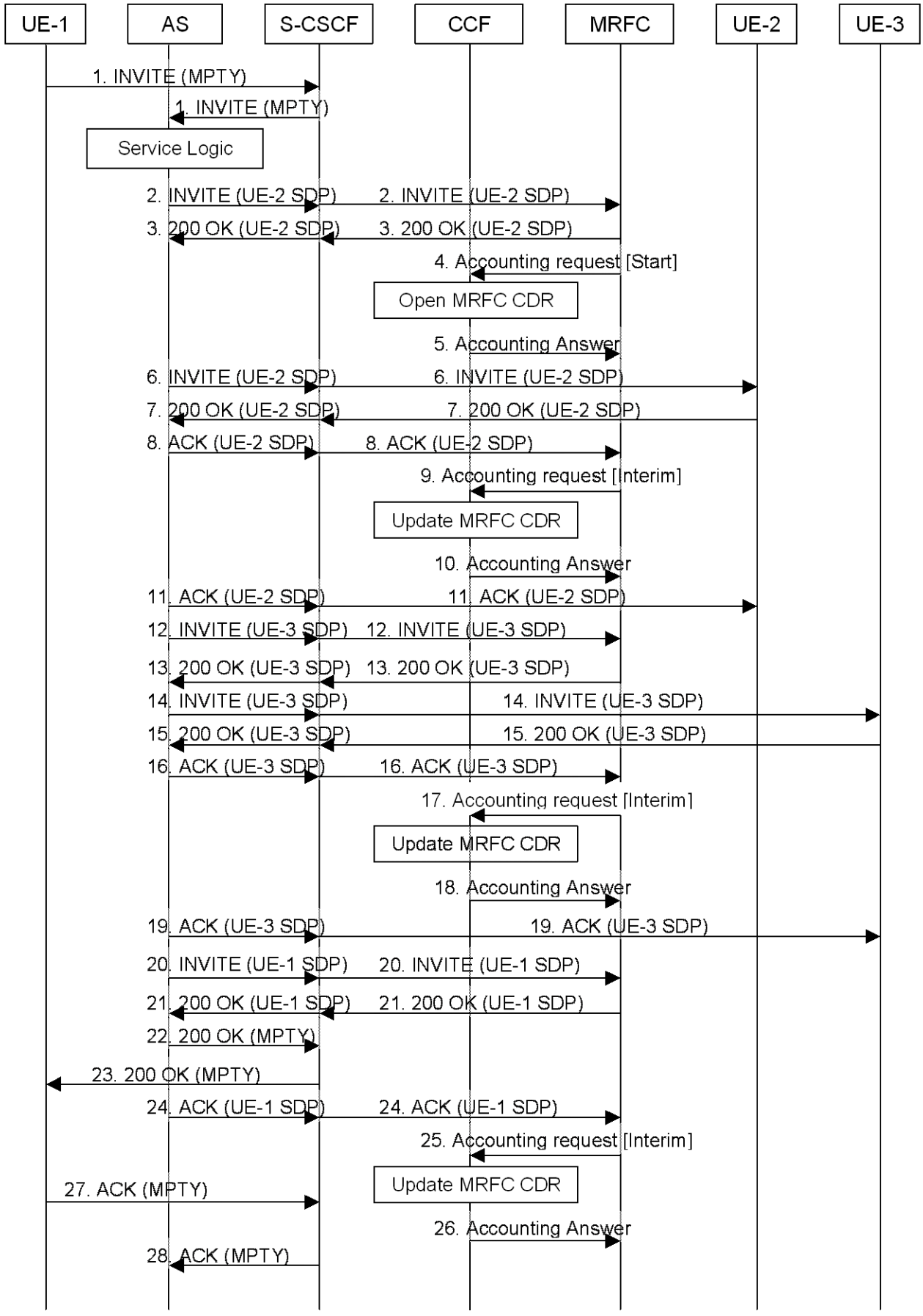

Figure 5.11: Message Sequence Chart for Multi-Party Call Establishment in MRFC

1. Sessions exist between UE-1 and UE-2, and between UE-1 and UE-3. A request is received from UE-1for putting all parties together to a multi-party call.
2 - 3. Request and acknowledgement to initiate a multi-party call. MRFC assigns a conference-ID that is used by the AS in subsequent interactions with the MRFC in INVITE messages connecting other endpoints (see TS 23.228 [18]). Path establishment between AS and MRFC for UE-2.
4. At start of session establishment the MRFC sends an *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a multi-party call in the MRFC CDR.
5. The CCF acknowledges the reception of the data and creates the MRFC CDR. 'Calling Party Address', 'Service Request Time Stamp', 'Service ID' (holding the conference-ID) etc. are included in the MRFC CDR
6 - 7. Path establishment between UE-2 and AS. Same ICID is used as for the path between AS and MRFC for UE-2 (step 2. - 3.).
8. Acknowledgement of path between AS and MRFC for UE-2.
9. The MRFC may send an *Accounting-Request* with *Accounting-Record-Type* indicating INTERIM_RECORD to report that UE-2 has been connected to the multi-party call.
10. The CCF acknowledges the reception of the data and includes UE-2 in the field 'Application Provided Called Parties' of the MRFC CDR.
11. Acknowledgement of path between AS and UE-2.
Now a path between UE-2 and MRFP via AS is established
12 - 13. Request and acknowledgement to establish path between AS and MRFC for UE-3.
14 - 15. Path establishment between UE-3 and AS. Same ICID is used as for the path between AS and MRFC for UE-3 (step 12. - 13.).
16. Acknowledgement of path between AS and MRFC for UE-3.
17. The MRFC may send an *Accounting-Request* with *Accounting-Record-Type* indicating INTERIM_RECORD to report that UE-3 has been connected to the multi-party call.
18. The CCF acknowledges the reception of the data and includes UE-3 in a new field 'Application Provided Called Parties' of the MRFC CDR.
19. Acknowledgement of path between AS and UE-3.
Now a path between UE-3 and MRFP via AS is established.
20 - 21. Request and acknowledgement to establish path between AS and MRFC for UE-1. Same ICID is used as for the path between UE-1 and AS (step 1.).
22 - 23. Request for multi-party conference with UE-2 and UE-3 is acknowledged to UE-1.
Implicit acknowledgement of path UE-1 to AS.
24. Acknowledgement of path between AS and MRFC for UE-1.
Now a path between UE-1 and MRFP via AS is established
25. The MRFC may send an *Accounting-Request* with *Accounting-Record-Type* indicating INTERIM_RECORD to report that UE-1 has been connected to the multi-party call.
26. The CCF acknowledges the reception of the data and includes the field 'Service Delivery Start Time Stamp' into the MRFC CDR.
27 - 28. UE-1 acknowledges the multi-party call session establishment.

NOTE: It is in the responsibility of the AS to terminate the sessions existing at the beginning of the multi-party call establishment between UE-1 and UE-2 and between UE-1 and UE-3 (see step 1.) in case of successful multi-party call establishment. This is not shown in figure 5.11.

5.1.2.1.5 AS Related Procedures

Application servers may support a multitude of services which are not specified in 3GPP standards. Therefore it is not possible to standardise charging flows and procedures for those services. However, for all such services, the AS may apply either Event Charging, where ACR [Event] messages are generated, or Session Charging, using ACR [Start, Stop and Interim]. The following subclauses depict one example for each of the two scenarios. The first procedure, AS acting as a Redirect Server, depicts the "event" case, while the second procedure, AS acting as a Voice Mail Server, depicts the "session" case.

5.1.2.1.5.1 AS Acting as a Redirect Server

Figure 5.12 shows the case where an Application Server acts as a Redirect Server. In the figure below, UE-1 sets up a session towards UE-2 but due to Call Forwarding functionality located in the AS, a new number (to UE-3) is returned to UE-1. Finally UE-1 sets up the session towards UE-3.

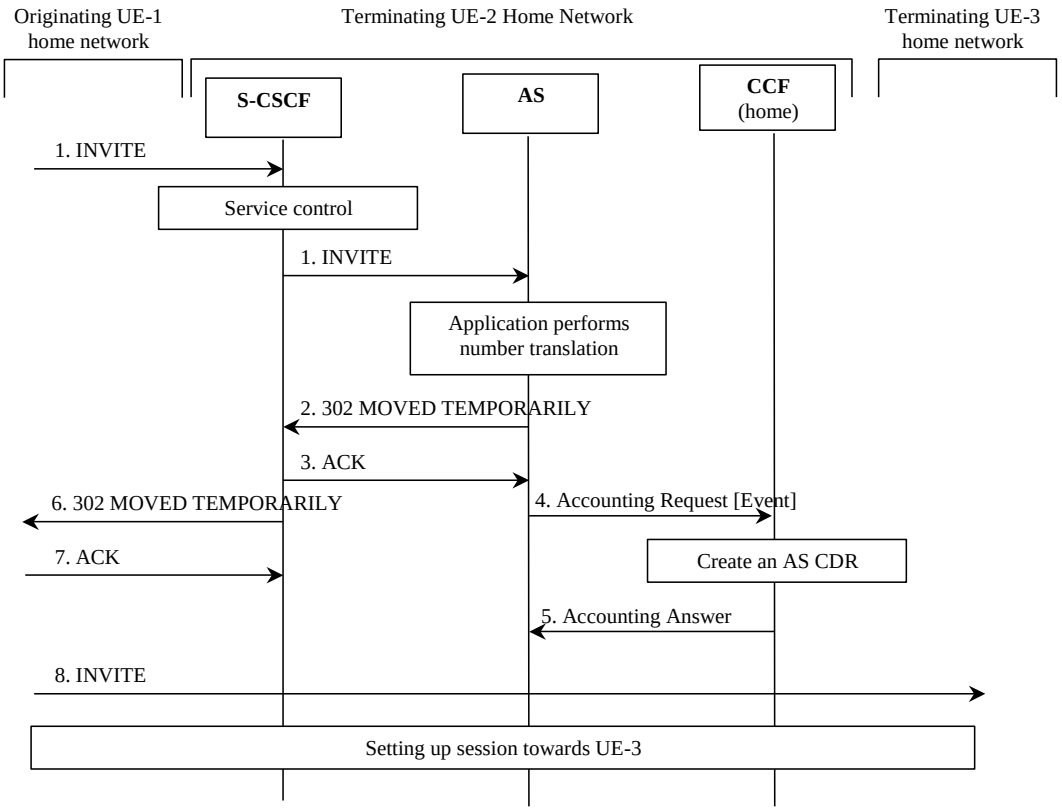

Figure 5.12: Message Sequence Chart for AS Acting as a Redirect Server

1. Sessions initiated by UE-1 towards UE-2.
2. - 3. Response indicating that session should be redirected towards another number (UE-3).
4. After successful service execution, the AS sends *Accounting-Request* with *Accounting-Record-Type* indicating EVENT_RECORD to record service specific information in the AS CDR.
5. The CCF acknowledges the reception of the data and creates the AS CDR.
6-7. Response indicating that session should be redirected towards another number (UE-3).
8. Session is initiated by UE-1 towards UE-3.

5.1.2.1.5.2 AS Acting as a Voice Mail Server

Figure 5.13 shows the case where an Application Server acts as a Voice Mail Server. S-CSCF invokes the AS acting as Voice Mail Server according to procedure as defined in TS 23.218 [5].

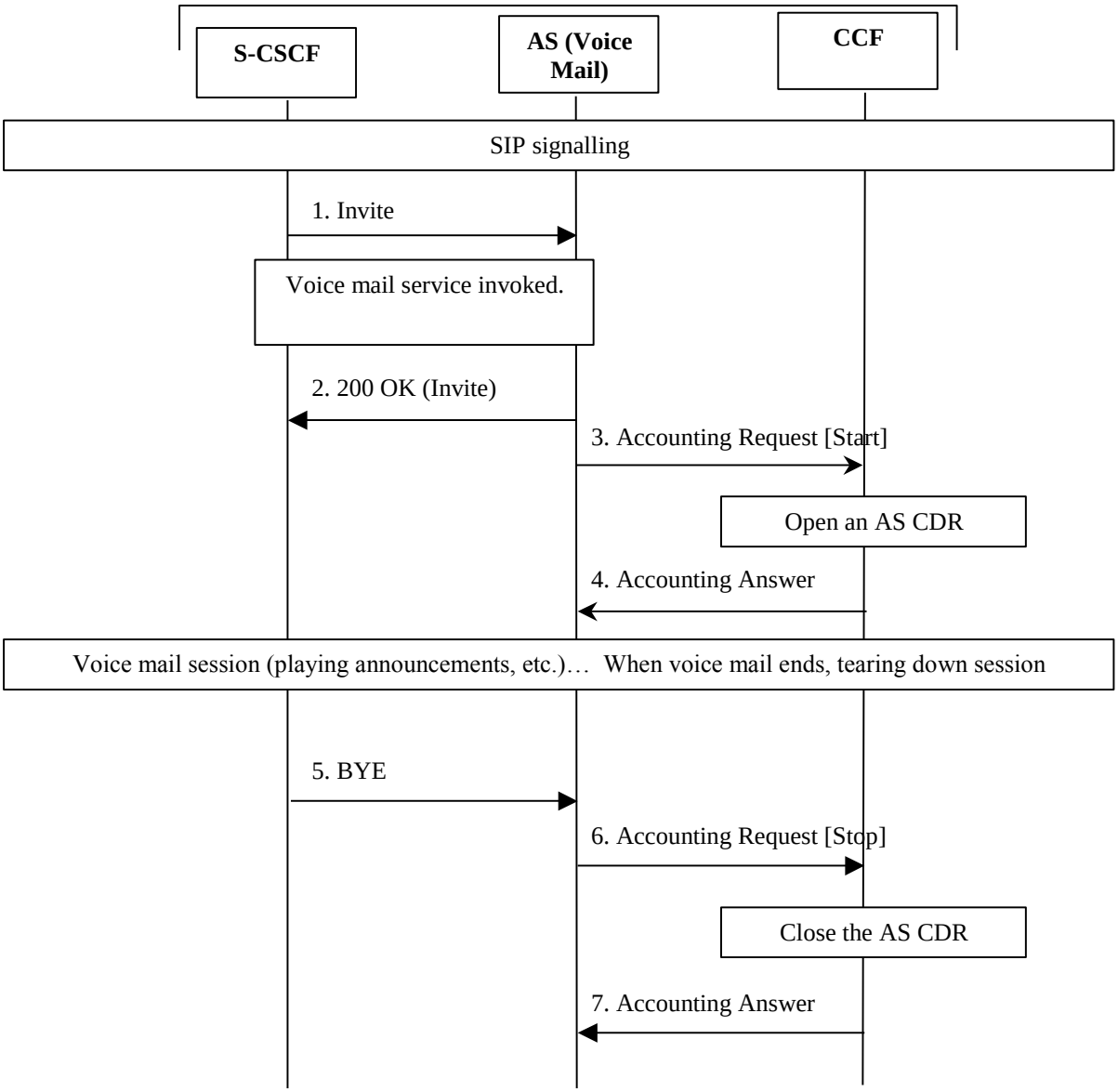

Figure 5.13: Message Sequence Chart for AS Acting as a Mail Server

1. AS receives the INVITE from the S-CSCF.
2. AS acknowledges the initiated Voice Mail session by issuing a 200 OK in response to the INVITE.
3. AS sends *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD to record start of a voice mail session.
4. The CCF acknowledges the reception of the *Accounting-Request* with *Accounting-Record-Type* indicating START_RECORD and opens a AS CDR.
5. Voice mail session release is initiated.
6. Upon reception of release message AS sends an *Accounting-Request* with *Accounting-Record-Type* indicating STOP_RECORD to record stop of a session in the AS CDR.
7. The CCF acknowledges the reception of the data and closes the AS CDR.

5.1.2.2 Message Flows - Error Cases and Scenarios

This subclause describes various error cases and how these should be handled. The error cases are grouped into the following categories:

- Failure in SIP Related Procedures:
  - Session Related Error Scenarios;
  - Session Unrelated Error Scenarios.
- Errors in Diameter (Accounting) Related Procedures.

5.1.2.2.1 Error Cases - Session Related SIP Procedures

5.1.2.2.1.1 Reception of SIP error messages

A SIP session is closed abnormally by the reception of a BYE message indicating the reason for such termination.

In this case, an ACR [Stop] message that includes an appropriate error indication is sent.

5.1.2.2.1.2 SIP session failure

All nodes involved in the SIP session are expected to exercise some kind of session supervision. In case a node detects an error in the SIP session, such as a timeout or the occurrence of an invalid SIP message that results in the inability to maintain the session, this IMS node will generate a BYE message towards both ends of the connection.

The node that sent the BYE to trigger session termination identifies the cause of the failure in the ACR [Stop] towards the CCF. All other nodes, i.e. those that receive the BYE, are not aware of an error, and therefore they treat this situation as any normal SIP session termination.

5.1.2.2.2 Error Cases - Session Unrelated SIP procedures

As described in subclause 5.1.2.1.2, a session unrelated SIP procedure may either be completed with the reception of a 200OK, or a SIP error message. If the latter occurs, i.e. there is a failure in the procedure, the ACR [Event] sent towards the CCF includes an appropriate error indication.

5.1.2.2.3 Error Cases - Diameter procedures

5.1.2.2.3.1 CCF Connection Failure

When the connection towards the primary CCF is broken, the process of sending accounting information should continue towards a secondary CCF (if such a CCF is configured). For further CCF connection failure functionality, see subclause "*Transport Failure Detection*" in IETF RFC 3588 [3].

If no CCF is reachable the network element may buffer the generated accounting data in non-volatile memory. Once the CCF connection is working again, all accounting messages stored in the buffer is sent to the CCF, in the order they were stored in the buffer.

5.1.2.2.3.2 No Reply from CCF

In case an IMS node does not receive an ACA in reply to an ACR, it may repeat the ACR message. The waiting time until a repetition is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of repetitions is reached and still no ACA reply has been received, the IMS node executes the CCF connection failure procedure as specified above.

If retransmitted ACRs are sent, they are marked with the T-flag as described in IETF RFC 3588 [3] , in order to allow duplicate detection in the CCF, as specified in the next subclause.

5.1.2.2.3.3 Duplicate Detection

A Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in IETF RFC 3588 [3].

If the CCF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information

in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

5.1.2.2.3.4 CCF Detected Failure

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular SIP session have not been received for a period of time. The exact behaviour of the CCF is operator configurable.

5.1.3 Message Formats

5.1.3.1 Summary of Offline Charging Message Formats

The IMS nodes generate accounting information that can be transferred from the nodes to the CCF. For this purpose, the IMS Charging application employs the *Accounting-Request* and *Accounting-Answer* messages from the base Diameter protocol.

Table 5.3 describes the use of these messages for offline charging.

Table 5.3: Offline Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
Accounting-Request	S-CSCF, I-CSCF, P-CSCF, MRFC, MGCF, BGCF, AS	CCF	ACR
Accounting-Answer	CCF	S-CSCF, I-CSCF, P-CSCF, MRFC, MGCF, BGCF, AS	ACA

5.1.3.2 Structure for the Accounting Message Formats

The following is the basic structure shared by all offline charging messages. This is based directly on the format of the *Accounting-Request* and *Accounting-Answer* messages defined in the base Diameter protocol specification IETF RFC 3588 [3]. Detailed description of the AVPs and their use for offline and online charging are provided in clause 7.

Those Diameter AVPs that are used for offline charging are marked "Yes" in tables 5.4 to 5.7. Those Diameter AVPs that are not used for offline charging are marked "No" in tables 5.4 to 5.7. This implies that their content can (Yes) or can not (No) be used by the CCF to construct CDRs.

The following symbols (adopted from IETF RFC 3588 [3]) are used in the tables:

- <AVP> indicates a mandatory AVP with a fixed position in the message.
- {AVP} indicates a mandatory AVP in the message.
- [AVP] indicates an optional AVP in the message.
- *AVP indicates that multiple occurrences of an AVP are possible.

5.1.3.2.1 Accounting-Request Message

Table 5.4 illustrates the basic structure of a Diameter *Accounting-Request* message as used for offline charging. The use of the AVPs is specified in subclause 5.1.3.3 per IMS node and ACR type.

Table 5.4: Accounting-Request (ACR) Message Contents for Offline Charging

Diameter base protocol AVPs	
AVP	**Used in offline ACR**
<Diameter-Header:271,REQ,PXY>	Yes
<Session-Id> -- Diameter Session Id	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Destination-Realm}	Yes
{Accounting-Record-Type}	Yes
{Accounting-Record-Number}	Yes
[Acct-Application-Id]	No
[Vendor-Specific-Application-Id]	Yes
[User-Name]	Yes
[Accounting-Sub-Session-Id]	No
[Accounting-RADIUS-Session-Id]	No
[Acct-Multi-Session-Id]	No
[Acct-Interim-Interval]	Yes
[Accounting-Realtime-Required]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Proxy-Info]	No
*[Route-Record]	No
*[AVP]	No
3GPP Diameter accounting AVPs	
[Event-Type]	Yes
[Role-of-node]	Yes
[User-Session-ID]	Yes
[Calling-Party-Address]	Yes
[Called-Party-Address]	Yes
[Time-stamps]	Yes
*[Application-Server-Information]	Only for S-CSCF/MRFC
*[Inter-Operator-Identifier]	Yes
[IMS-Charging-Identifier]	Yes
*[SDP-Session-Description]	Yes
*[SDP-Media-Component]	Yes
[GGSN-Address]	Yes
[Served-Party-IP-Address]	Only for P-CSCF
[Authorised-QoS]	Only for P-CSCF
[Server-Capabilities]	Only for I-CSCF
[Trunk-Group-ID]	Only for MGCF
[Bearer-Service]	Only for MGCF
[Service-ID]	Only for MRFC
[Service-Specific-Data]	Only for AS
[Cause]	Yes

NOTE: For AVP of type "Grouped" only the group AVP is listed in table 5.4. Detailed descriptions of the AVPs is provided in clause 7.

5.1.3.2.2 Accounting-Answer Message

Table 5.5 illustrates the basic structure of a Diameter *Accounting-Answer* message as used for IMS charging. This message is always used by the CCF as specified below, regardless of the IMS node it is received from and the ACR record type that is being replied to.

Table 5.5: Accounting-Answer (ACA) Message Contents for Offline Charging

Diameter base protocol AVPs	
AVP	**Used in Offline ACA**
<Diameter-Header:271,PXY>	Yes
<Session-Id>	Yes
{Result-Code}	Yes
{Origin-Host}	Yes
{Origin-Realm}	Yes
{Accounting-Record-Type}	Yes
{Accounting-Record-Number}	Yes
[Acct-Application-Id]	No
[Vendor-Specific-Application-Id]	Yes
[User-Name]	Yes
[Accounting-Sub-Session-Id]	No
[Accounting-RADIUS-Session-Id]	No
[Acct-Multi-Session-Id]	No
[Error-Reporting-Host]	No
[Acct-Interim-Interval]	Yes
[Accounting-Realtime-Required]	No
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Proxy-Info]	No
*[AVP]	No

5.1.3.3 Detailed Message Formats

Following the base protocol specification, the following "types" of accounting data may be sent:

- Start session accounting data.
- Interim session accounting data.
- Stop session accounting data.
- Event accounting data.

ACR types Start, Interim and Stop are used for accounting data related to successful SIP sessions. In contrast, Event accounting data is unrelated accounting data, such as a simple registration or interrogation and successful service event triggered by an AS. In addition, Event accounting data are also used for unsuccessful SIP session establishment attempts.

The following table specifies per ACR type the accounting data that are sent by each of the IMS network elements:

- S-CSCF
- P-CSCF
- I-CSCF
- MRFC
- MGCF
- BGCF
- AS

The ACR types in the table are listed in the following order: S (start)/I (interim)/S (stop)/E (event). Therefore, when all ACR types are possible it is marked as SISE. If only some ACR types are allowed for a node, only the appropriate letters are used (i.e. SIS or E) as indicated in the table heading. The omission of an ACR type for a particular AVP is marked with "-" (i.e. SI-E). Also, when an entire AVP is not allowed in a node the entire cell is marked as "-".

Note that not for all Grouped AVPs the individual AVP members are listed in the table. See clause 7 for a detailed list of the AVP group members and for the description of the AVPs.

For the ACA the same details listed in table 5.8 applies with the addition that *Error-Reporting-Host* AVP is supported in all ACAs in a similar manner as most other base protocol AVPs (e.g. in the same manner as *Origin-State-Id* AVP).

Table 5.8: Detailed Diameter ACR Message Contents for Offline Charging

AVP name	Node Type	S-CSCF	P-CSCF	I-CSCF	MRFC	MGCF	BGCF	AS
	Supported ACRs	S/I/S/E	S/I/S/E	E	S/I/S	S/I/S/E	S/I/S/E	S/I/S/E
AVPs from the Diameter base protocol								
<Session-Id>		SISE	SISE	E	SIS	SISE	SISE	SISE
{Origin-Host}		SISE	SISE	E	SIS	SISE	SISE	SISE
{Origin-Realm}		SISE	SISE	E	SIS	SISE	SISE	SISE
{Destination-Realm}		SISE	SISE	E	SIS	SISE	SISE	SISE
{Accounting-Record-Type}		SISE	SISE	E	SIS	SISE	SISE	SISE
{Accounting-Record-Number}		SISE	SISE	E	SIS	SISE	SISE	SISE
[Vendor-Specific-Application-Id]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Acct-Application-Id]		-	-	-	-	-	-	-
[User-Name] (see note)		SISE	SISE	E	SIS	SISE	SISE	SISE
[Accounting-Sub-Session-Id]		-	-	-	-	-	-	-
[Accounting-RADIUS-Session-Id]		-	-	-	-	-	-	-
[Acct-Multi-Session-Id]		-	-	-	-	-	-	-
[Acct-Interim-Interval]		SIS-	SIS-	-	SIS-	SIS-	SIS-	SIS-
[Accounting-Realtime-Required]		-	-	-	-	-	-	-
[Origin-State-Id]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Event-Timestamp]		SISE	SISE	E	SIS	SISE	SISE	SISE
*[Proxy-Info]		-	-	-	-	-	-	-
*[Route-Record]		-	-	-	-	-	-	-
*[AVP]		-	-	-	-	-	-	-
Diameter Credit Control AVP								
[Subscription-Id]		-	-	-	-	-	-	-
[Requested-Action]		-	-	-	-	-	-	-
*[Requested-Service-Unit]		-	-	-	-	-	-	-
*[Used-Service-Unit]		-	-	-	-	-	-	-
*[Service-Parameter-Info]		-	-	-	-	-	-	-
[Abnormal-Termination-Reason]		-	-	-	-	-	-	-
*[Accounting-Correlation-Id]		-	-	-	-	-	-	-
[Credit-Control-Failure-Handling]		-	-	-	-	-	-	-
[Direct-Debiting-Failure-Handling]		-	-	-	-	-	-	-
3GPP Diameter accounting AVPs								
[Event-Type]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Role-of-Node]		SISE	SISE	E	SIS	SISE	SISE	SISE
[User-Session-Id]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Calling-Party-Address]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Called-Party-Address]		SISE	SISE	E	SIS	SISE	SISE	SISE
[Time-stamps]		SISE	SISE	E	SIS	SISE	SISE	SISE
*[Application-server-Information] (see note)		SISE	-	-	SIS-	-	-	-
*[Inter-Operator-Identifiers] (see note)		SISE	SISE	E	SIS	SISE	SISE	SISE
[IMS-Charging-Identifier]		SISE	SISE	E	SIS	SISE	SISE	SISE
*[SDP-Session-Description]		SI-E	SI-E	-	SI-	SI-E	SI-E	SI-E
*[SDP-Media-component]		SI-E	SI-E		SI-	SI-E	SI-E	SI-E
[GGSN-Address]		SI-E	SI-E		SI-	SI-E	SI-E	SI-E
[Served-Party-IP-Address] (see note)		-	SISE	-	-	-	-	-
[Authorized-QoS] (see note)		-	SISE	-	-	-	-	-
[Server-Capabilities]		-	-	E	-	-	-	-
[Trunk-Group-ID]		-	-	-	-	SISE	-	-
[Bearer-Service]		-	-	-	-	SISE	-	-
[Service-Id]		-	-	-	SIS	-	-	-
[Service-Specific-Data]		-	-	-	-	-	-	SISE
[Cause]		--SE	--SE	E	--S	--SE	--SE	--SE
NOTE: Only present if available in the IMS node.								

5.2 CDR Description on the Bi Interface

5.2.1 CDR Field Types

The following Standard CDR content and format are considered:

- S-CSCF-CDR generated based on information from the S-CSCF.
- I-CSCF-CDR generated based on information from the I-CSCF.
- P-CSCF-CDR generated based on information from the P-CSCF.
- BGCF-CDR generated based on information from the BGCF.
- MGCF-CDR generated based on information from the MGCF.
- MRFC-CDR generated based on information from the MRFC.
- AS-CDR generated based on information from the AS.

The content of each CDR type is defined in Table 5.9 . For each CDR type the field definition includes the field name and category. The field descriptions are provided in clause 5.2.4.

Equipment vendors shall be able to provide all of the fields listed in the CDR content table in order to claim compliance with the present document. However, since CDR processing and transport consume network resources, operators may opt to eliminate some of the fields that are not essential for their operation. This operator provisionable reduction is specified by the field category.

A field category can have one of two primary values:

M This field is **M**andatory and shall always be present in the CDR.

C This field shall be present in the CDR only when certain **C**onditions are met. These Conditions are specified as part of the field definition.

Some of these fields are designated as Operator provisionable. Using TMN management functions or specific tools provided by an equipment vendor, operators may choose if they wish to include or omit the field from the CDR. Once omitted, this field is not generated in a CDR. To avoid any potential ambiguity, a CDR generating element MUST be able to provide all these fields. Only an operator can choose whether or not these fields should be generated in their system.

Those fields that the operator may configure to be present or absent are further qualified with the "Operator provisionable" subscript as follows:

M_o This is a field that, if provisioned by the operator to be present, shall always be included in the CDRs. In other words, an M_o parameter that is provisioned to be present is a mandatory parameter.

C_o This is a field that, if provisioned by the operator to be present, shall be included in the CDRs when the required conditions are met. In other words, a C_o parameter that is configured to be present is a conditional parameter.

The CCF provides the CDRs at the Bi interface in the format and encoding described in the present document. Additional CDR formats and contents may be available at the interface to the billing system to meet the requirements of the billing system, these are outside of the scope of 3GPP standardisation.

5.2.2 CDR Triggers

5.2.2.1 Session Related CDRs

Reflecting the usage of multimedia sessions IMS CDRs are generated by the CCF on a per session level. In the scope of the present document the term "session" refers always to a SIP session. The coherent media components are reflected inside the session CDRs with a media component container comprising of all the information necessary for the description of a media component.

Accounting information for SIP sessions is transferred from the IMS nodes involved in the session to the CCF using Diameter ACR Start, Interim and Stop messages. A session CDR is opened in the CCF upon reception of a Diameter ACR [Start] message. Partial CDRs may be generated upon reception of a Diameter ACR [Interim] message which is sent by the network entity towards the CCF due to a session modification procedure (i.e. change in media). Session CDRs are updated, or partial CDRs are generated upon reception of a diameter ACR [Interim] message which is sent by the network entity due to expiration of the Accounting-Interim-Interval AVP. The CCF closes the final session CDR upon reception of a Diameter ACR [Stop] message, which indicates that the SIP session is terminated. Further details on triggers for the generation of IMS CDRs are specified in [2].

Accounting information for unsuccessful session set-up attempts may be sent by the IMS node to the CCF employing the Diameter ACR [Event] message. The behaviour of the CCF upon receiving ACR [Event] messages is specified in subclause 5.2.2.2.

5.2.2.2 Session Unrelated CDRs

To reflect chargeable events not directly related to a session the CCF may generate CDRs upon the occurrence of session unrelated SIP procedures, such as registration respectively de-registration events. Accounting information for SIP session-unrelated procedures is transferred from the IMS nodes involved in the procedure to the CCF using Diameter ACR [Event] messages. Session unrelated CDRs are created in the CCF in a "one-off" action based on the information contained in the Diameter ACR [Event] message. One session unrelated CDR is created in the CCF for each Diameter ACR [Event] message received, whereas the creation of partial CDRs is not applicable for session unrelated CDRs. The cases for which the IMS nodes send ACR [Event] messages are listed per SIP procedure in tables 5.1 and 5.2.

Further details on triggers for the generation of IMS CDRs are specified in [2].

5.2.3 CDR Content

Table 5.9 specifies the content of each CDR type. For each column describing the CDR type, the field name and its category are specified. The detailed description of the field is provided in section 5.2.1. Diagonal shading of a cell indicates, that the particular CDR field is not included in the particular CDR type.

Table 5.9: Charging Data of IMS CDR Types

Field	CDR Type						
	S-CSCF-CDR	P-CSCF-CDR	I-CSCF-CDR	MRFC-CDR	MGCF-CDR	BGCF-CDR	AS-CDR
Record Type	M	M	M	M	M	M	M
Retransmission	Co	Co	Co	Co	Co	Co	Co
SIP Method	Co	Co	Co	Co	Co	Co	Co
Role of Node	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Node Address	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Session ID	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Service ID				Mo			
Calling Party Address	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Called Party Address	Mo	Mo	Mo	Co	Mo	Mo	Mo
Private User ID	Mo						
Served Party IP Address		Mo					
Service Request Time Stamp	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Service Delivery Start Time Stamp	Mo	Mo		Mo	Mo	Mo	Mo
Service Delivery End Time Stamp	Co	Co		Co	Co	Co	Co
Record Opening Time	Co	Co		Co	Co	Co	Co
Record Closure Time	Mo	Mo		Mo	Mo	Mo	Mo
Application Servers Information	Co			Co			
Application Servers Involved	Co			Co			
Application Provided Called Parties	Co			Co			
Inter Operator Identifiers	Co	Co	Co	Co	Co	Co	Co
originating IOI	Co	Co	Co	Co	Co	Co	Co
terminating IOI	Co	Co	Co	Co	Co	Co	Co
Local Record Sequence Number	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Record Sequence Number	Co	Co		Co	Co	Co	Co
Cause For Record Closing	Mo	Mo	Mo	Mo	Mo	Mo	Mo
Incomplete CDR Indication	Co	Co	Co	Co	Co	Co	Co
S-CSCF Information			Co				
IMS Charging Identifier	Mo	Mo	Mo	Mo	Mo	Mo	Mo
SDP Session Description	Co	Co		Co	Co	Co	Co
List of SDP Media Components	Co	Co		Co	Co	Co	Co
SIP Request Timestamp	Mo	Mo		Mo	Mo	Mo	Mo
SIP Response Timestamp	Mo	Mo		Mo	Mo	Mo	Mo
SDP Media Components	Mo	Mo		Mo	Mo	Mo	Mo
SDP Media Name	Mo	Mo		Mo	Mo	Mo	Mo
SDP Media Description	Mo	Mo		Mo	Mo	Mo	Mo
GPRS Charging ID	Co	Co		Co	Co	Co	Co
Media Initiator Flag	Co	Co		Co	Co	Co	Co
Authorised QoS		Co					
GGSN Address	Co	Co		Co	Co	Co	Co
Service Delivery Failure Reason	Co	Co	Co	Co	Co	Co	Co
Service Specific Data							Co
List of Message Bodies	Co	Co					Co
Content-Type	Co	Co					Co
Content-Disposition	Co	Co					Co
Content-Length	Co	Co					Co
Originator	Co	Co					Co
Trunk Group ID Incoming/Outgoing					Mo		
Bearer Service					Mo		
Record Extensions	Co	Co	Co	Co	Co	Co	Co

5.2.4 CDR Parameter Description

This clause contains a brief description of each field of the CDRs described in Table 5.9. The fields are listed in alphabetical order according to the field name as specified in the table above.

5.2.4.1 Application Provided Called Parties

Holds a list of the Called Party Address(es), if the address(es) are determined by an AS (SIP URL, E.164…).

5.2.4.2 Application Servers Information

This a grouped CDR field containing the fields: "Application Server Involved" and "Application Provided Called Parties".

5.2.4.3 Application Servers Involved

Holds the ASs (if any) identified by the SIP URLs.

5.2.4.4 Authorised QoS

Authorised QoS as defined in TS 23.207 [7] / TS 29.207 [8] and applied via the Go interface.

5.2.4.5 Bearer Service

Holds the used bearer service for the PSTN leg.

5.2.4.6 Called Party Address

In the context of an end-to-end SIP transaction this field holds the address of the party (Public User ID) to whom the SIP transaction is posted.

For a subscription/registration procedure this field holds the party to be registered/subscribed.

This field contains either a SIP URL (according to IETF RFC3261 [16]) or a TEL URL (according to RFC2806 [20]).

5.2.4.7 Calling Party Address

The address (Public User ID) of the party requesting a service or initiating a session. This field holds either the SIP URL (according to IETF RFC 3261 [16]) or the TEL URL (according to RFC 2806 [20]) of the calling party.

5.2.4.8 Cause for Record Closing

This field contains a reason for the release of the CDR including the following:

- normal release: end of session;
- partial record generation: time (duration) limit, maximum number of changes in charging conditions (e.g. maximum number in 'List of Message Bodies' exceeded) or service change (e.g. change in media components);
- abnormal termination;
- management intervention (request due to O&M reasons).
- CCF initiated record closure;

A more detailed reason may be found in the Service Delivery Failure Reason field.

5.2.4.9 Content Disposition

This sub-field of Message Bodies holds the content disposition of the message body inside the SIP signalling, Content-disposition header field equal to “render”, indicates that “the body part should be displayed or otherwise rendered to the user”. Content disposition values are: session, render, inline, icon, alert, attachment, etc.

5.2.4.10 Content Length

This sub-field of Message Bodies holds the size of the data of a message body in bytes.

5.2.4.11 Content Type

This sub-field of Message Bodies holds the MIME type of the message body, Examples are: application/zip, image/gif, audio/mpeg, etc.

5.2.4.12 GGSN Address

This parameter holds the control plane IP address of the GGSN that handles one or more media component(s) of a IMS session. If GPRS is used to access the IMS, the GGSN address is used together with the GPRS charging ID as the access part of the charging correlation vector. The charging correlation vector is comprised of an access part and an IMS part, which is the IMS Charging Identifier. For further information regarding the composition of the charging correlation vector refer to the appropriate clause in TS 32.200 [2].

5.2.4.13 GPRS Charging ID

This parameter holds the GPRS charging ID (GCID) which is generated by the GGSN for a GPRS PDP context. There is a 1:1 relationship between the GCID and the PDP context. If GPRS is used to access the IMS, the GCID is used together with the GGSN address if received over the Go interface as the access part of the charging correlation vector that is comprised of an access part and an IMS part, which is the IMS Charging Identifier.

For further information regarding the composition of the charging correlation vector refer to the appropriate clause in TS 32.200 [2].

5.2.4.14 IMS Charging Identifier

This parameter holds the IMS charging identifier (ICID) as generated by the IMS node for the SIP session. The value of the ICID parameter is identical with the 'icid-value' parameter defined in [15]. The 'icid-value' is a mandatory part of the P-Charging-Vector and coded as a text-based UTF-8 charset (as are all SIP messages). For further information regarding the composition and usage of the P-Charging-Vector refer to TS 32.200 [2], TS 24.229 [14] and [15].

The ICID value is globally unique across all 3GPP IMS networks for a time period of at least one month, implying that neither the node that generated this ICID nor any other IMS node reuse this value before the uniqueness period expires. The one month minimum uniqueness period counts from the time of release of the ICID, i.e. the ICID value no longer being used. This can be achieved by using node specific information, e.g. high-granularity time information and / or topology / location information. The exact method how to achieve the uniqueness requirement is an implementation issue.

An ICID is generated by the P-CSCF during the initial IMS registration procedure for a Private User ID. At each SIP session unrelated method (e.g., REGISTER, NOTIFY, MESSAGE etc.), a new, session unrelated specific ICID is generated at the first IMS network element that processes the method.

At each SIP session establishment a new, session specific ICID is generated at the first IMS network element that processes the session-initiating SIP INVITE message. This ICID is then used in all subsequent SIP messages for that session (e.g., 200 OK, (re-)INVITE, BYE etc.) until the session is terminated.

5.2.4.15 Incomplete CDR Indication

This field provides additional diagnostics when the CCF detects missing ACRs.

5.2.4.16 Inter Operator Identifiers

Holds the identification of the home network (originating and terminating) if exchanged via SIP signalling, as recorded in the *Inter-Operator-Identifier* AVP. For further information on the IOI please refer to TS 24.229 [14].

5.2.4.17 List of Message Bodies

This grouped field comprising several sub-fields describing the data that may be conveyed end-to-end in the body of a SIP message. Since several message bodies may be exchanged via SIP-signalling, this grouped field may occur several times.

The List of Message Bodies contains the following elements:

- Content Type
- Content Disposition
- Content Length
- Originator

They are described in the appropriate subclause. Message bodies with the "Content-Type" field set to *application/sdp* and the "Content-Disposition" field set to *session* are not included in the "Message Bodies" field.

5.2.4.18 List of SDP Media Components

This is a grouped field comprising several sub-fields associated with one media component. It may occur several times in one CDR. The field is present only in a SIP session related case.

The List of SDP Media Components contains following elements:

- SIP Request Timestamp
- SIP Response Timestamp
- SDP Media Components
- Media Initiator flag

These field elements are described in the appropriate subclause.

5.2.4.19 Local Record Sequence Number

This field includes a unique record number created by this node. The number is allocated sequentially for each partial CDR (or whole CDR) including all CDR types. The number is unique within the CCF.

The field can be used e.g. to identify missing records in post processing system.

5.2.4.20 Media Initiator Flag

This field indicates if the called party has requested the session modification and it is present only if the initiator was the called party.

5.2.4.21 Node Address

This item holds the address of the node providing the information for the CDR. This may either be the IP address or the FQDN of the IMS node generating the accounting data. This parameter corresponds to the O*rigin-Host* AVP.

5.2.4.22 Originator

This sub-field of the "List of Message Bodies" indicates the originating party of the message body.

5.2.4.23 Private User ID

Holds the used Network Access Identifier of the served party according to RFC2486 [6]. This parameter corresponds to the *User-Name* AVP.

5.2.4.24 Record Closure Time

A Time stamp reflecting the time the CCF closed the record.

5.2.4.25 Record Extensions

A set of operator/manufacturer specific extensions to the record, conditioned upon existence of an extension.

5.2.4.26 Record Opening Time

A time stamp reflecting the time the CCF opened this record. Present only in SIP session related case.

5.2.4.27 Record Sequence Number

This field contains a running sequence number employed to link the partial records generated by the CCF for a particular session (characterised with the same Charging ID and GGSN address pair). The Record Sequence Number is not present if the record is the only one produced in the CCF for a session. The Record Sequence Number starts from one (1).

5.2.4.28 Record Type

Identifies the type of record. The parameter is derived from the *Origin-Host* AVP.

5.2.4.29 Retransmission

This parameter, when present, indicates that information from retransmitted Diameter ACRs has been used in this CDR.

5.2.4.30 Role of Node

This fields indicates the role of the AS/CSCF. As specified in TS 23.218 [5] the role can be:

- originating (CSCF serving the calling subscriber or AS initiated session)
- terminating (CSCF serving the called subscriber or AS terminated session)
- proxy (only applicable for an AS, when a request is proxied)
- B2BUA (only applicable for an AS, when the AS performs third party control/acts in B2BUA mode.

5.2.4.31 SDP Media Components

This is a grouped field comprising several sub-fields associated with one media component. Since several media components may exist for a session in parallel these sub-fields may occur several times (as much times as media are involved in the session).

The x-CSCF, BGCF, MGCF shall retrieve the value for this parameter from the SDP payload of SIP INVITE messages, if present. The x-CSCF, BGCF, MGCF shall then include this information in the ACR that is triggered when receiving the 200 OK responding to the SIP INVITE. This includes both the case of initial session set-up and SDP changes during the session.

The SDP media component contains the following elements:

- SDP media name.
- SDP media description.
- GPRS Charging ID.

These field elements are described in the appropriate subclause.

5.2.4.32 SDP Media Description:

This field holds the attributes of the media as available in the SDP data tagged with “i=”, “c=”,“b=”,“k=”, “a=”. Only the attribute lines relevant for charging are recorded. To be recorded “SDP lines” shall be recorded in separate “SDP Media Description” fields, thus multiple occurrence of this field is possible. Always complete “SDP lines” are recorded per field.

This field corresponds to the *SDP-Media-Description* AVP as defined in Table 5.8.

Example: “c=IN IP4 134.134.157.81”

For further information on SDP please refer to IETF draft 'SDP.Session Description Protocol' [17].

Note: session unrelated procedures typically do not contain SDP data.

5.2.4.33 SDP Media Name

This field holds the name of the media as available in the SDP data tagged with "m=". Always the complete "SDP line" is recorded.

This field corresponds to the *SDP-Media-Name* AVP as defined in Table 5.8.

Example: "m=video 51372 RTP/AVP 31".

For further information on SDP please refer to IETF draft 'SDP: Session Description Protocol' [17].

5.2.4.34 SDP Session Description

Holds the Session portion of the SDP data exchanged between the User Agents in the SIP transaction.

The x-CSCF, BGCF, MGCF shall retrieve the value for this parameter from the SDP payload of SIP INVITE messages, if present. The x-CSCF, BGCF, MGCF shall then include this information in the ACR that is triggered when receiving the 200 OK responding to the SIP INVITE. This includes both the case of initial session set-up and SDP changes during the session.

This field holds the attributes of the media as available in the session related part of the SDP data tagged with "c=" and "a=" (multiple occurrence possible). Only attribute lines relevant for charging are recorded.

The content of this field corresponds to the SDP-Session-Description AVP of the ACR message.

NOTE: Session unrelated procedures typically do not contain SDP data.

5.2.4.35 Service Delivery End Time Stamp

This field records the time at which the service delivery was terminated. It is Present only in SIP session related case.

The content of this field corresponds to the *SIP-Request-Timestamp* AVP of a received ACR[Stop] message indicating a session termination.

5.2.4.36 Service Delivery Failure Reason

Holds the reason for why a requested service could not be successfully provided (i.e. SIP error codes taken from *SIP-Method* AVP). This field is not present in case of a successful service delivery.

5.2.4.37 Service Delivery Start Time Stamp

This field holds the time stamp reflecting either:

- a successful session set-up: this field holds the start time of a service delivery (session related service)
- a delivery of a session unrelated service: the service delivery time stamp
- an unsuccessful session set-up and an unsuccessful session unrelated request: this field holds the time the network entity forwards the unsuccessful indication (SIP "RESPONSE" with error codes 3xx, 4xx, 5xx) towards the requesting User direction.

The content of this field corresponds to the *SIP-Response-Timestamp* AVP as defined in Table 5.8.

For partial CDRs this field remains unchanged.

5.2.4.38 Service ID

This field identifies the service the MRFC is hosting. For conferences the conference ID is used here.

5.2.4.39 Service Request Timestamp

This field contains the time stamp which indicates the time at which the service was requested ("SIP request" message) and is present for session related and session unrelated procedures. The content of this item is derived from the *SIP-Request-Timestamp* AVP as defined in Table 5.8. If the *SIP-Request-Timestamp* AVP is not supplied by the network entity this field is not present.

For partial CDRs this field remains unchanged.

This field is present for unsuccessful service requests if the ACR message includes the *SIP-Request-Timestamp* AVP.

5.2.4.40 Service Specific Data

This field contains service specific data.

5.2.4.41 Session ID

The Session identification. For a SIP session the Session-ID contains the SIP Call ID as defined in the Session Initiation Protocol RFC [16].

5.2.4.42 Served Party IP Address

This field contains the IP address of either the calling or called party, depending on whether the P-CSCF is in touch with the calling or called network.

5.2.4.43 SIP Method

Specifies the SIP-method for which the CDR is generated. Only available in session unrelated cases.

5.2.4.44 SIP Request Timestamp

This parameter contains the time of the SIP Request (usually a (Re)Invite).

5.2.4.45 SIP Response Timestamp

This parameter contains the time of the response to the SIP Request (usually a 200 OK).

5.2.4.46 S-CSCF Information

This field contains Information related to the serving CSCF, e.g. the S-CSCF capabilities upon registration event or the S-CSCF address upon the session establishment event. This field is derived from the *Server-Capabilities* AVP if present in the ACR received from the I-CSCF.

5.2.4.47 Trunk Group ID Incoming/Outgoing

Contains the outgoing trunk group ID for an outgoing session/call or the incoming trunk group ID for an incoming session/call.

5.2.5 Bi interface Conventions

The present document gives several recommendations for the main protocol layers for the Bi interface protocol stack. These recommendations are not strictly specified features, since there are a lot of variations among the existing Billing Systems.

As a minimum, all implementations shall support a file based bulk interface for the transfer of CDRs from the CCF to the BS. The recommendation is FTP over TCP/IP.

5.2.6 Abstract Syntax Description

```
TS32225-DataTypes {42} -- to be allocated, value "42" is used to allow compilation of the code
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Exports everything
IMPORTS
TimeStamp, ManagementExtensions
FROM TS32205-DataTypes {itu-t (0) identified-organization (4) etsi(0) mobileDomain (0)
umts-Operation-Maintenance (3) ts-32-205 (205) informationModel (0) asn1Module (2) version1 (1)}
IMSRecord ::= SET
{
    -- Fields used by several multimedia Record types ("Common fields"):
    -- (which field is used in which record type is defined in section 5.2.3)
    recordType                      [0] CallEventRecordType,
    retransmission                  [1] NULL OPTIONAL,
    sIP-Method                      [2] SIP-Method OPTIONAL,
```

```
    role-of-Node                    [3] Role-of-Node OPTIONAL,
    nodeAddress                     [4] NodeAddress OPTIONAL,
    session-Id                      [5] Session-Id OPTIONAL,
    calling-Party-Address           [6] InvolvedParty OPTIONAL,
    called-Party-Address            [7] InvolvedParty OPTIONAL,
    privateUserID                   [8] GraphicString OPTIONAL,
    serviceRequestTimeStamp         [9] TimeStamp OPTIONAL,
    serviceDeliveryStartTimeStamp   [10] TimeStamp OPTIONAL,
    serviceDeliveryEndTimeStamp     [11] TimeStamp OPTIONAL,
    recordOpeningTime               [12] TimeStamp OPTIONAL,
    recordClosureTime               [13] TimeStamp OPTIONAL,
    interOperatorIdentifiers        [14] InterOperatorIdentifiers OPTIONAL,
    localRecordSequenceNumber       [15] LocalRecordSequenceNumber OPTIONAL,
    recordSequenceNumber            [16] INTEGER OPTIONAL,
    causeForRecordClosing           [17] CauseForRecordClosing OPTIONAL,
    incomplete-CDR-Indication       [18] Incomplete-CDR-Indication OPTIONAL
    iMS-Charging-Identifier         [19] IMS-Charging-Identifier OPTIONAL,
    sDP-Session-Description         [20] SEQUENCE OF Graphic STRING OPTIONAL,
    list-Of-SDP-Media-Components    [21] SEQUENCE OF Media-Components-List OPTIONAL,
    gGSNaddress                     [22] NodeAddress OPTIONAL,
    serviceDeliveryFailureReason    [23] ServiceDeliveryFailureReason OPTIONAL,
    list-Of-Message-Bodies          [24] SEQUENCE OF MessageBody OPTIONAL,
    recordExtensions                [25] ManagementExtensions OPTIONAL,
    -- Space left for further "common fields"
    -- Fields particular used in the S-CSCF-recordType:
applicationServersInformation    [40] SEQUENCE OF ApplicationServersInformation OPTIONAL,
    -- Fields particular used in the P-CSCF-recordType:
    servedPartyIPAress              [50] ServedPartyIPAddress OPTIONAL,
    -- < ServedPartyIPAddress to be defined >
    -- Fields particular used in the I-CSCF-recordType:
    transactionTimestamp            [60] TimeStamp OPTIONAL,
    s-CSCF-Information              [61] S-CSCF-Information OPTIONAL,
    -- Fields particular used in the MRFC-recordType:
    service-Id                      [70] Service-Id OPTIONAL,
    -- <Service-Id to be defined>
    -- Fields particular used in the MGCF-recordType:
    trunkGroupID                    [80] TrunkGroupID OPTIONAL,
    bearerService                   [81] TransmissionMedium OPTIONAL,
    -- Fields particular used in the BGCF-RecordType (start with tag 90):
    -- <empty so far>
    -- Fields particular used in the AS-RecordType:
    serviceSpecificData             [100] OCTET STRING OPTIONAL
}
ACRInterimLost ::= ENUMERATED
{
    no (0),
    yes (1),
    unknown (2)
}
ApplicationServersInformation ::= SEQUENCE
{
    applicationServersInvolved       [0] GraphicString OPTIONAL, -- SIP URL refer to rfc3261
    applicationProvidedCalledParties [1] SEQUENCE OF InvolvedParty OPTIONAL
}
CauseForRecordClosing ::= ENUMERATED
{
    serviceDeliveryEndSuccessfully (0),
    unSuccessfulServiceDelivery    (1),
    timeLimit                      (3),
    serviceChange                  (4), -- e.g. change in media due to Re-Invite
    managementIntervention         (5),
    maxChangeCond                  (6)  -- e.g. number in 'List of Message Bodies' exceeeded
-- partial record generation reasons to be added
--  Additional codes are for further study
}
IMS-Charging-Identifier ::= OCTET STRING
Incomplete-CDR-Indication ::= SET
{
    aCRStartLost [0] BOOLEAN, -- TRUE if ACR[Start] was lost, FALSE otherwise
    aCRInterimLost [1] ACRInterimLost,
    aCRStopLost [2] BOOLEAN -- TRUE if ACR[Stop] was lost, FALSE otherwise
}
InterOperatorIdentifiers ::= SEQUENCE
{
    originatingIOI [0] GraphicString OPTIONAL,
    terminatingIOI [1] GraphicString OPTIONAL
}
InvolvedParty ::= CHOICE
```

```
{
    sIP-URI [0] GraphicString, -- refer to rfc3261
    tEL-URL [1] GraphicString  -- refer to rfc3261
}
IPAddress ::= CHOICE
{
    ipV4Addr [0] GraphicString, -- "dot" notation is used
    ipV6Addr [1] GraphicString  -- "dot" notation is used
}
LocalRecordSequenceNumber ::= INTEGER (0..+2147483647)
-- A unique number assigned by the CCF and supplied to all CDRs. The value range
-- limits the field to a maximum 4 octet INTEGER.
Media-Components-List ::= SEQUENCE
{
    sIP-Request-Timestamp  [0] TimeStamp OPTIONAL,
    sIP-Response-Timestamp [1] TimeStamp OPTIONAL,
    sDP-Media-Components   [2] SDP-Media-Components OPTIONAL,
    mediaInitiatorFlag     [3] NULL OPTIONAL,
    authorized-QoS         [4] GraphicString OPTIONAL
}
MessageBody ::= SEQUENCE
{
    Content-Type          [0] GraphicString OPTIONAL,
    Content-Disposition   [1] GraphicString OPTIONAL,
    Content-Length        [2] INTEGER OPTIONAL,
    Originator            [3] InvolvedParty OPTIONAL
}
NodeAddress ::= CHOICE
{
    iPAddress  [0] IPAddress,
    domainName [1] GraphicString
}
Role-of-Node ::= ENUMERATED
{
    originating (0),
    terminating (1),
    proxy       (2),
    b2bua       (3)
}
S-CSCF-Information ::=  SEQUENCE
{
mandatoryCapabilities  [0] SEQUENCE OF GraphicString OPTIONAL,
optionalCapabilities      [1] SEQUENCE OF GraphicString OPTIONAL,
serverName                [2] Graphic String OPTIONAL
}
SDP-Media-Components ::= SEQUENCE
{
    sDP-Media-Name         [0] GraphicString OPTIONAL,
    sDP-Media-Descriptions [1] SEQUENCE OF GraphicString OPTIONAL,
    gPRS-Charging-Id       [2] INTEGER OPTIONAL
}
ServiceDeliveryFailureReason ::= GraphicString
-- holds the SIP error code as received via a SIP Final response (4xx, 5xx or 6xx)
Session-Id ::= GraphicString
-- rfc3261: example for SIP Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@foo.bar.com
Sip-Method ::= GraphicString
TransmissionMedium ::= SEQUENCE {
    -- Transmission Medium Required, refer to ITU-T Q.763:
    tMR [0] OCTET STRING (SIZE (1)) OPTIONAL,
    -- Transmission Medium USED, refer to ITU-T Q.763:
    tMU [1] OCTET STRING (SIZE (1)) OPTIONAL
}
TrunkGroupID ::= CHOICE {
    incoming [0] GraphicString,
    outgoing [1] GraphicString
}
END
```

5.2.7 Data Encoding Rules

Data encoding rules are descried in [9] for BER, in [10] for PER, or in [11] for XER.

6 Online Charging

6.1 Diameter Description on the Ro Interface

6.1.1 Basic Principles

IMS online charging essentially uses the same protocol that is used for offline charging. However, for online charging the protocol may include additional Attribute-Value Pairs (AVPs) within the existing messages.

Two cases for online event charging are distinguished:

- Immediate Event Charging (IEC); and
- Event Charging with Unit Reservation (ECUR).

In the case of Immediate Event Charging (IEC), granting units to the AS is performed in a single operation that also includes the deduction of the corresponding monetary units from the subscriber's account. The charging process is controlled by the corresponding *CC-Request-Type* EVENT_REQUEST which is sent with an CCR for a given accounting event.

In contrast, Event Charging with Unit Reservation (ECUR) also includes the process of requesting, reserving, releasing and returning unused units. The deduction of the corresponding monetary units then occurs upon conclusion of the ECUR transaction. In this case, the *CC-Request-Type* INITIAL/ UPDATE/ TERMINATE-REQUEST are used to control the accounting session. During a SIP session there can be repeated execution of unit reservation and debit operations as specified in TS 32.200 [2].

The AS/MRFC may apply either IEC, where CCR Event messages are generated, or ECUR, using CCR INITIAL, TERMINATE and UPDATE. The decision whether to apply IEC or ECUR is based on the service and/or operator's policy.

NOTE: To the extent possible alignment with IETF RFC 4006 [13] is planned.

6.1.2 Message Flows and Types

This subclause describes the message flows for the event charging procedures on the Ro interface.

6.1.2.1 Immediate Event Charging (IEC)

This subclause provides the details of the "Debit Units" operation specified in TS 32.200 [2].

6.1.2.1.1 Message Flows - Successful Cases and Scenarios

6.1.2.1.1.1 IEC - Debit Units Operation

Figure 6.1 shows the transactions that are required on the Ro interface in order to perform IEC with Debit Units operations. The Debit Units operation may alternatively be carried out prior to, concurrently with or after service/content delivery. The AS/MRFC must ensure that the requested service execution is successful, when this scenario is used.

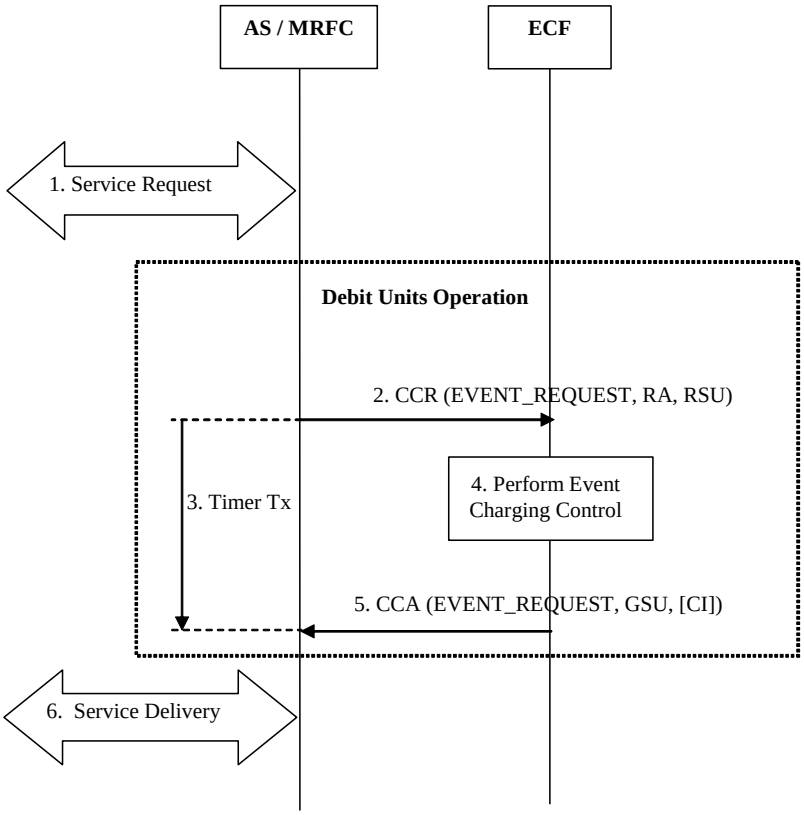

Figure 6.1: IEC - Debit Units Operation

1. The AS/MRFC receives a SIP related service request from S-CSCF.

   The Debit Units Operation is performed as described in TS 32.200 [2].
2. The AS/MRFC performs IEC prior to service execution. AS/MRFC sends *Credit-Control-Request* (CCR) with *CC-Request-Type* AVPset to EVENT_REQUEST to indicate service specific information to the ECF. The *Requested-Action* AVP (RA) is set to DIRECT_DEBITING. If known, the AS/MRFC may include *Requested-Service-Unit* AVP (RSU) (monetary or non monetary units) in the request message.
3. Having transmitted the *CC_request*message the AS/MRFC starts the communication supervision timer Tx IETF RFC 4006 [13]. Upon receipt of the *Credit-Control-Answer* (CCA) message the AS/MRFC shall stop timer Tx.
4. The ECF determines the relevant service charging parameters in conjunction with the other internal charging functions of the OCS.
5. The ECF returns *CC_answer* message with *CC-Request-Type* AVP set to EVENT_REQUESTto the AS/MRFC in order to authorize the service execution (*Granted-Service-Unit* AVP (GSU) and possibly *Cost-Information* AVP (CI) indicating the cost of the service are included in the *CC_answer* message). The *CC_answer* message has to be checked by the AS/MRFC accordingly and the requested service is controlled concurrently with service delivery.
6. Service is being delivered.

6.1.2.1.2 Message Flows - Error Cases and Scenarios

This subclause describes various error cases and how these should be handled.

The failure handling behaviour is locally configurable in the AS/MRFC. If the *Direct-Debiting-Failure-Handling* AVP is not used, the locally configured values are used instead.

6.1.2.1.2.1 Reception of SIP Error Messages

If SIP errors occur during service delivery, as defined in [5] and [12], it is up to the AS/MRFC to determine to what extent the service was delivered before the error occurred and act appropriately with respect to charging. This may imply that no units at all (or no more units) are debited.

6.1.2.1.2.2 Debit Units Operation Failure

This case comprises situations where either no, or an erroneous response, is received from the ECF. The “no response” case is detected by the AS/MRFC when the connection supervision timer Tx expires IETF RFC 4006 [13] before a response *Credit-Control-Answer* (CCA) is received. The case of receiving an erroneous response implies that the AS/MRFC receives an *Credit-Control-Answer* (CCA), which it is unable to process, while Tx is running. The failure handling complies with the failure procedures for "Direct Debiting" scenario described in IETF RFC 4006 [13].

6.1.2.1.2.3 Duplicate Detection

The detection of duplicate request is needed and must be enabled. To speed up and simplify as much as possible the duplicate detection, the all-against-all record checking should be avoided and just those records marked as potential duplicates need to be checked against other received requests (within a reasonable time window) by the receiver entity.

The AS/MRFC mark the request messages that are retransmitted after a link failover as possible duplicates with the T-flag as described in IETF RFC 3588 [3]. For optimized performance, uniqueness checking against other received requests is only necessary for those records marked with the T-flag received within a reasonable time window. This focused check is based on the inspection of the *Session-Id* and *CC-Request-Number* AVP pairs.

Note that for IEC the duplicate detection is performed in the Correlation Function that is part of the OCS. The ECF that receives the possible duplicate request should mark as possible duplicate the corresponding request that is sent over the Rc interface.

6.1.2.2 Event Charging with Unit Reservation (ECUR)

This subclause provides the details of the "Reserve Units" and "Debit Units" operations specified in TS 32.200 [2].

6.1.2.2.1 Message Flows - Successful Cases and Scenarios

6.1.2.2.1.1 ECUR - Reserve Units and Debit Units Operations

Figure 6.2 shows the transactions that are required on the Ro interface in order to perform ECUR with Reserve Units and Debit Units operations. Multiple replications of both of these operations are possible.

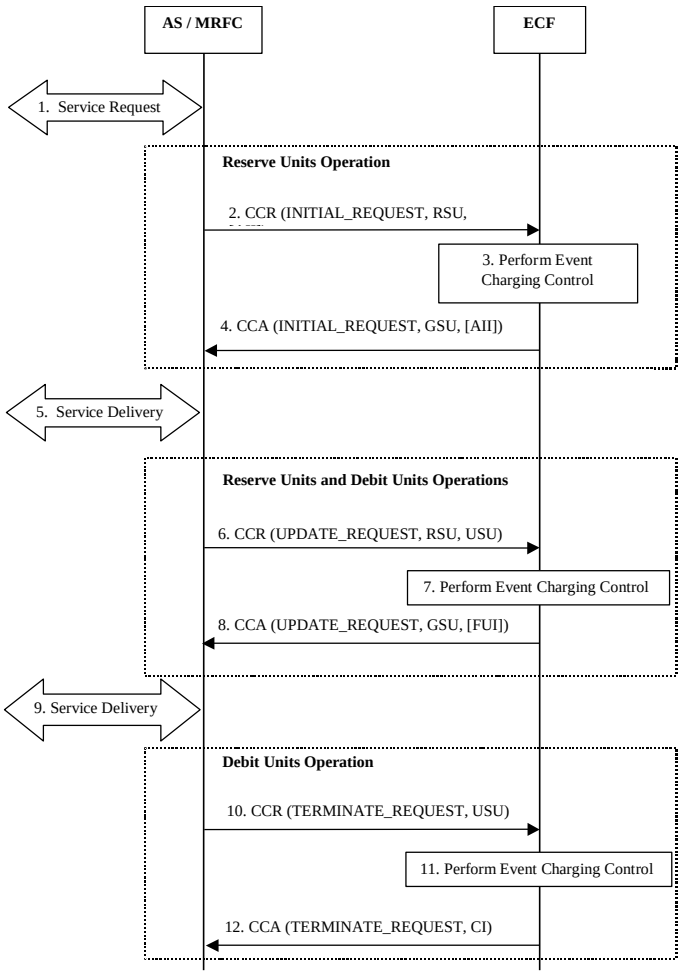

Figure 6.2: ECUR - Reserve Units and Debit Units Operations

1. The AS/MRFC receives a SIP related service request from S-CSCF. The service request may be initiated by either the user or an AS/MRFC.

The Reserve Units Operation is performed as described in TS 32.200 [2].

2. In order to perform Reserve Units operation for a number of units (monetary or non-monetary units), the AS/MRFC sends an CCR with *CC-Request-Type* AVP set to INITIAL-REQUEST to the ECF. If known, the AS/MRFC may include *Requested-Service-Unit* (RSU) AVP (monetary or non monetary units) and *Acc-Interim-Interval* (AII) AVP in the request message.
3. If the service cost information is not received by the ECF, the ECF determines the price of the desired service according to the service specific information received by issuing a rating request to the Rating Function. If the cost of the service is included in the request, the ECF directly reserves the specified monetary amount. If the credit balance is sufficient, the ECF reserves the corresponding amount from the users account.
4. Once the reservation has been made, the ECF returns *CC_answer* message with *CC-Request-Type* set to INITIAL-REQUEST to the AS/MRFC in order to authorize the service execution (*Granted-Service-Unit* and possibly *Cost-Information* indicating the cost of the service are included in the *CC_answer* message). If requested, the ECF returns the *Acc-Interim-Interval* (AII) AVP with value field set to a non-zero value.
5. Content/service delivery starts and the reserved units are concurrently controlled.

The Reserve Units and Debit Units Operations are performed as described in TS 32.200 [2].

6. During content/service delivery, in order to perform Debit Units and subsequent Reserve Units operations, the AS/MRFC sends an CCR with *CC-Request-Type* AVP set toUPDATE-REQUEST, to report the units used and request additional units, respectively. The CCR message with *CC-Request-Type* AVP set to UPDATE-REQUEST must be sent by the AS/MRFC between the INITIAL-REQUEST and TERMINATE-REQUEST either on request of the credit control application within the interim interval or if the interim interval is elapsed. If known, the AS/MRFC may include *Requested-Service-Unit* AVP (monetary or non monetary units) in the request message. The *Used-Service-Unit* (USU) AVP is complemented in the CCR message to deduct units from both the user's account and the reserved units, respectively.
7. The ECF deducts the amount used from the account. If the service cost information is not received by the ECF, the ECF determines the price of the desired service according to the service specific information received by issuing a rating request to the Rating Function. If the cost of the service is included in the request, the ECF directly reserves the specified monetary amount. If the credit balance is sufficient, the ECF reserves the corresponding amount from the users account.
8. Once the deduction and reservation have been made, the ECF returns *CC_answer* message with *CC-Request-Type* set to UPDATE-REQUEST to the AS/MRFC, in order to allow the content/service delivery to continue (new *Granted-Service-Unit (GSU) AVP* and possibly *Cost-Information (CI) AVP* indicating the cumulative cost of the service are included in the *CC_answer* message). The ECF may include in the CCA message the *Final-Unit-Indication* (FUI) AVP to indicate the final granted units.
9. Content/service delivery continues and the reserved units are concurrently controlled.

The Debit Units Operation is performed as described in TS 32.200 [2].

10. When content/service delivery is completed or the final granted units have been consumed, the AS/MRFC sends *CCR* with *CC-Request-Type* AVP set to TERMINATE-REQUEST to terminate the active accounting session and report the used units.
11. The ECF deducts the amount used from the account. Unused reserved units are released, if applicable.
12. The ECF acknowledges the reception of the CCR message by sending *CCA* message with *CC-Request-Type* AVP indicating TERMINATE-REQUEST (possibly *Cost-Information* AVP indicating the cumulative cost of the service is included in the *CC_answer* message).

NOTE: The ECUR scenario is supervised by corresponding timers (e.g. accounting interval timer) that are not shown in the figure 6.2.

6.1.2.2.1.2 Support of Tariff Switch

Changes to the tariffs pertaining to the service may be handled in the following ways.

- Tariff Changes handled using Acct-Interim-Interval AVP; or
- Tariff changes handled using the Tariff Switch Time AVP.

6.1.2.2.1.2.1 Tariff Changes handled using Acct-Interim-Interval AVP

The tariff change for online charging can be achieved by setting the value of the *Acct-Interim-Interval* AVP (ECF controlled) in a manner that it matches the desired tariff switch time.

6.1.2.2.1.2.2 Tariff changes handled using the Tariff Switch Time AVP

To indicate a change of tariff to the AS/MRFC, the ECF can include the Tariff Switch Time (*Tariff-Switch-Definition* AVP), i.e. a timer value referring to the change of tariff, in the *CC_answer*. The Tariff Switch Time is evaluated by the AS/MRFC relative to the time stamp of the *CC_request* (*Accounting-Request-Type* INITIAL-REQUEST orUPDATE-REQUEST). By that it is possible to eliminate any delays of the signalling between AS/MRFC and ECF.

Together with the Tariff Switch Time the ECF also provides the granted service units. These units can be provided in one portion or in two, referring to the granted service units before and after the tariff switch.

If a Tariff Switch Time is received, the AS/MRFC starts the tariff switch timer and use the granted service units for usage metering. If both, granted service units before and after the tariff switch have been provided, the AS/MRFC uses the units granted before the tariff switch (pre-switch quota).

If the pre-switch quota is exhausted, the AS/MRFC sends an *CC_request* to the ECF. The *CC_request* contains the amount of service units used from the beginning of the connection only. The value of the tariff switch timer is discarded in the AS/MRFC and it is the responsibility of the ECF to provide a new Tariff Switch Time in the *CC_answer*.

If the tariff switch timer expired, the AS/MRFC further continues usage metering using the post-switch quota, if provided, but no *CC_request* is sent. If no specific units were granted to after tariff switch time, the AS/MRFC continues usage metering with the remaining units granted.

If the post switch quota is exhausted, the AS/MRFC sends an *CC_request* to the ECF, containing the service units used before the last tariff switch, the service units used after the last tariff switch and the tariff switch time.

If the granted units - provided in one portion - are exhausted, an *CC_request* is sent. If a tariff switch has occurred in this time, the *CC_request* contains the service units used before the tariff switch, the service units used after the tariff switch and the time of the tariff switch. Otherwise, if no tariff switch has occurred, the *CC_request* contains the overall amount of used service units.

There may be some AS/MRFCs that do no support tariff switching. In this case, the AS/MRFC ignores the AVPs associated with this feature (i.e. *Tariff-Switch-Definition* and *Unit-Value-After-Tariff-Switch* AVPs). The *Granted-Service-Unit*, *Unit-Value* and *Used-Service-Unit* AVPs are treated as if the Tariff Switch feature does not exist.

Figure 6.3 shows the messages exchanged on the Ro interface for ECUR for a tariff change. This scenario covers a tariff switch where the granted service units are provided in two portions, before and after the tariff switch. No additional CC_request takes place, as the granted service units were not exhausted.

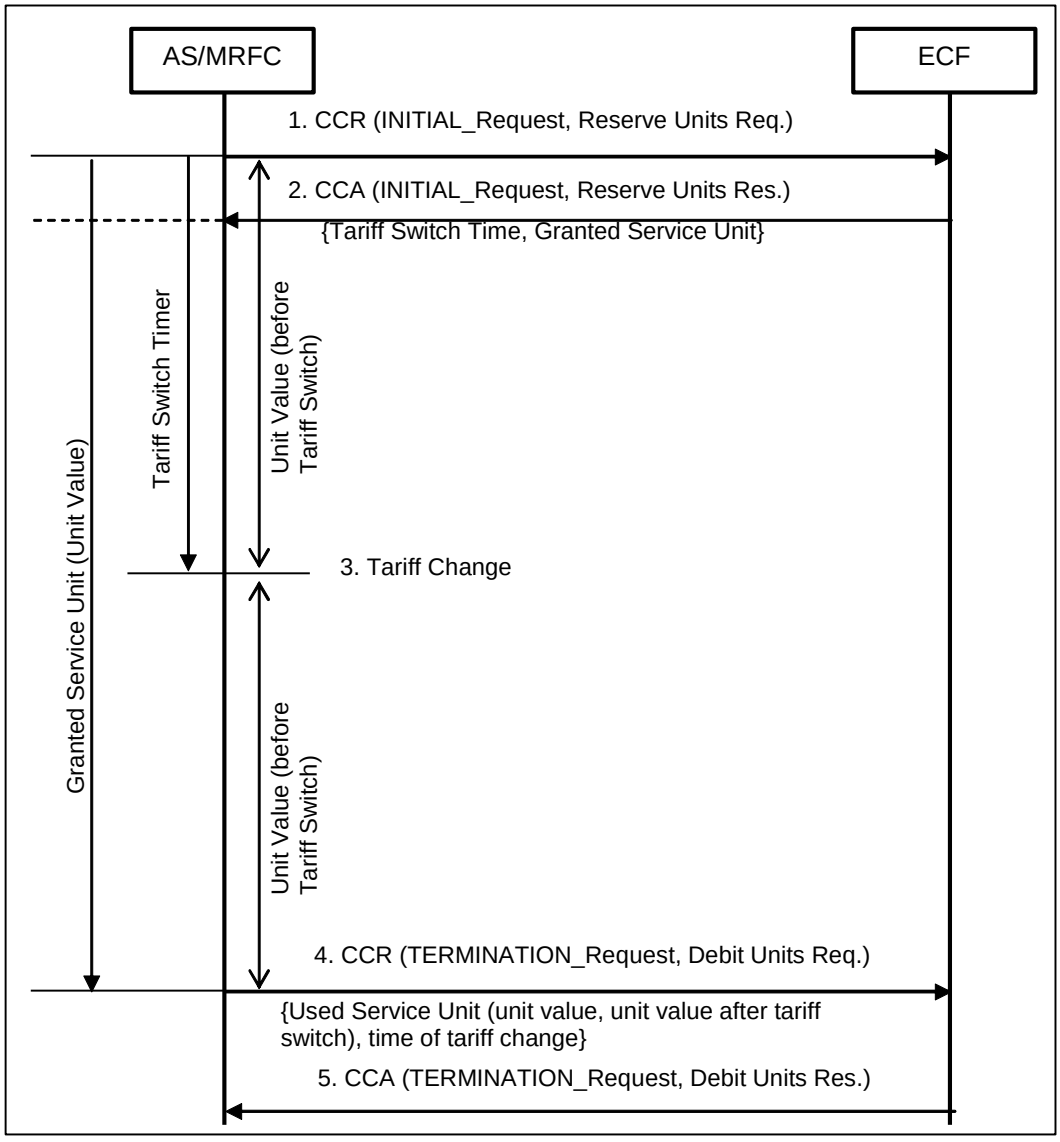

Figure 6.3: Tariff Change in the AS/MRFC

1. In order to perform credit control with reservation of an amount of units (monetary or non-monetary units) the AS/MRFC sends an CCR with *CC-Request-Type* set to INITIAL-REQUEST to ECF. The *Requested-Action* is set to RESERVE_UNITS.
2. Once the reservation has been made, ECF returns an CCA with *CC-Request-Type* set to INITIAL-REQUEST to the AS/MRFC in order to authorize the content/service delivery. The CCA includes the Tariff Switch Time, the service units granted before the tariff switch and the service units granted after the tariff switch.
   Upon receipt of the CCA, the AS/MRFC evaluates the tariff switch time relative to the timestamp of the CCR, starts the tariff switch timer and monitors service usage based on the service units granted before the tariff switch.
3. The Tariff Switch Timer expires. The AS/MRFC now monitors service usage based on the service units granted after the tariff switch.
4. The AS/MRFC sends CCR with *CC-Request-Type* set to TERMINATE-REQUEST to terminate the active accounting session. The message includes the amount of service units used before the tariff switch, the amount of service units used after the tariff switch and the time of the tariff change.
5. An *CC_answer* is sent from the ECF back to the AS/MRFC as an acknowledgment of the successful debit process and to finalize the transaction.

6.1.2.2.1.3 Expiration of Reservation Validity

This subclause defines how reserved units are returned, if not used, within a reasonable time. It should be possible that both the reservation and SIP sessions are cancelled or only the reservation is cancelled without removing the SIP session.

NOTE: Alignment with IETF RFC 4006 [13] is planned.

6.1.2.2.2 Message Flows - Error Cases and Scenarios

This subclause describes various error cases and how these should be handled.

The failure handling behaviour is locally configurable in the AS/MRFC. If *Credit-Control-Failure-Handling* AVP is not used, the locally configured values are used instead.

6.1.2.2.2.1 Reception of SIP Error Messages

If SIP errors occur during service delivery, as defined in [5] and [12], it is up to the AS/MRFC to determine to what extent the service was delivered before the error occurred and act appropriately with respect to charging. This may imply that no units at all (or no more units) are reserved or debited.

6.1.2.2.2.2 Reserve Units and Debit Units Operation Failure

This case comprises of ECF connection failure, and/or receiving error responses from the ECF.

The AS/MRFC detects an ECF connection failure when the timer Tx expires IETF RFC 4006 [13] or a transport failure is detected as defined in IETF RFC 3588 [3]. The ECF also has the capability to detect failures when the timer Ts IETF RFC 3588 [3] expires. The ECF should indicate the cause of failure by setting the appropriate result code as defined in IETF RFC 3588 [3] and IETF RFC 4006 [13]. In any case, the failure handling of AS/MRFC and ECF complies with the failure procedures for "Session Based Credit Control" scenario described in IETF RFC 4006 [13].

6.1.2.2.2.3 Duplicate Detection

For credit control duplicate detection is performed only for possible duplicate event requests related to IEC as mentioned in subclause 6.1.2.1.2.3,as retransmission of ECUR related accounting requests is not allowed.

6.1.3 Message Formats

6.1.3.1 Summary of Online Charging Message Formats

IETF RFC 4006 [13] proposes an approach based on a series of "interrogations":

- Initial interrogation (extending the initial credit control report message).
- Zero, one or more interim interrogations (extending the update credit control report message).
- Final interrogation (extending the terminate credit control report message).

In addition to a series of interrogations, also a one time event (interrogation) can be used e.g. in the case when service execution is always successful.

All of these interrogations make use of the same *CC_request* and *CC_answer* messages in the base Diameter protocol as for the offline charging. Additional AVPs are specified for the purposes of online charging. These additional AVPs include all the AVPs listed in IETF RFC 4006 [13] and the *Tariff-Switch-Definition* AVP as specified in clause 7.

The *CC_request* for the "interim interrogation" and "final interrogation" reports the actual number of "units" that were used, from what was previously reserved. This determines the actual amount debited from the subscriber's account.

Such an approach has the benefit of a common basic message structure, and accounting data reporting mechanism for both offline and online charging.

Table 6.1 describes the use of these messages for online charging.

Table 6.1: Online Charging Messages Reference Table

Command-Name	Source	Destination	Abbreviation
CC-Request	MRFC, AS	ECF	CCR
CC-Answer	ECF	MRFC, AS	CCA

6.1.3.2 Structure for the Credit Control Message Formats

The following is the basic structure shared by all online charging messages. This is based directly on the format of the *CC_Request* and *CC_Answer* messages defined in the base Diameter protocol specification IETF RFC 3588 [3] with the extensions defined in IETF RFC 4006 [13].

Those Diameter AVPs that are used for online charging are marked "Yes" in tables 6.2 to 6.3. Those Diameter AVPs that are not used for online charging are marked "No" in tables 6.2 to 6.3. This implies that their content can (Yes) or can not (No) be used by the ECF for charging purposes.

The following symbols are used in the tables:

- <AVP> indicates a mandatory AVP with a fixed position in the message.
- {AVP} indicates a mandatory AVP in the message.
- [AVP] indicates an optional AVP in the message.
- *AVP indicates that multiple occurrences of an AVP is possible.

6.1.3.2.1 Credit-Control-Request Message

Table 6.2 illustrates the basic structure of a Diameter *CC-Request* message as used for IMS online charging.

Table 6.2: CC-Request (CCR) Message Contents for Online Charging

Diameter Base Protocol AVPs	
AVP	**Used in Online CCR**
<Diameter Header: 271, REQ, PXY>	Yes
<Session-Id>	Yes
{ Origin-Host }	Yes
{ Origin-Realm }	Yes
{ Destination-Realm }	Yes
{ Auth-Application-Id }	Yes
{ Service-Context-Id }	Yes
{ CC-Request-Type}	Yes
{ CC-Request-Number}	Yes
[Destination-Host]	Yes
[User-Name]	Yes
[CC-Sub-Session-Id]	Yes
[Acct-Multi-Session-Id]	Yes
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Subscription-Id]	Yes
[Service-Identifier]	Yes
[Termination-Cause]	Yes
[Requested-Service-Unit]	Yes
[Requested-Action]	Yes
*[Used-Service-Unit]	Yes
[Multiple-Service-Indicator]	Yes
*[Multiple-Service-Credit-Control]	Yes
*[Service-Parameter-Info]	Yes
[CC-Correlation-Id]	Yes
[User-Equiqment-Info]	Yes
*[Proxy-Info]	Yes
*[Route-Record]	Yes
*[AVP]	Yes

The detailed use of the AVPs for MRFC/AS and for each CCR record type (initial/update/terminate/event) is specified in subclause 6.1.3.3.

6.1.3.2.2 Credit-Control-Answer Message

Table 6.3 illustrates the basic structure of a Diameter *CC-Answer* message as used for IMS charging. This message is always used by the ECF as specified below, independent of the receiving IMS node and the CCR record type that is being replied to.

Table 6.3: Credit-Control-Answer (CCA) Message Contents for Online Charging

Diameter Credit Control AVPs	
AVP	**Used in online CCA**
<Diameter Header: 272, PXY>	Yes
<Session-Id>	Yes
{ Result-Code }	Yes
{ Origin-Host }	Yes
{ Origin-Realm }	Yes
{ Auth-Application-Id }	Yes
{ CC-Request-Type}	Yes
{ CC-Request-Number}	Yes
[User-Name]	Yes
[CC-Session-Failover]	Yes
[CC-Sub-Session-Id]	Yes
[Acct-Multi-Session-Id]	Yes
[Origin-State-Id]	Yes
[Event-Timestamp]	Yes
*[Subscription-Id]	Yes
[Granted-Service-Unit]	Yes
*[Multiple-Service-Credit-Control]	Yes
[Cost-Information]	Yes
[Final-Unit-Indication]	Yes
[Check-Balance-Result]	Yes
[Credit-Control-Failure-Handling]	Yes
[Debit-Debiting-Failure-Handling]	Yes
[Validity-Time]	Yes
*[Redirect-Host AVP]	Yes
[Redirect-Host-Usage]	Yes
[Redirect-Max-Cache-Time]	Yes
*[Proxy-Info]	Yes
*[Route-Record]	Yes
*[AVP]	Yes

6.1.3.3 Detailed Message Formats

Following the protocol specifications, the following "types" of accounting data may be sent:

- Initial request credit control data.
- Update request credit contol data.
- Terminate request credit control data.
- Event accounting data.

CCR types initial, update and terminate are used for accounting data related to successful SIP sessions. In contrast, event accounting data is used for session-unrelated accounting data, such as a simple registration or interrogation, and for accounting data related to unsuccessful SIP session establishment attempts.

The following table specifies per CCR type the chargingaccounting data for IMS online charging that are sent by MRFC and AS.

Tables 6.4 and 6.5 are the basic structure for online charging messages via Ro Interface. This is based directly on the *CC-Request* and *CC-Answer* messages defined in the Diameter protocol specifications.

Table 6.4: Detailed Diameter CCR Message Contents for online Charging

AVP name	Node Type	MRFC	AS
	Supported CCRs	I/U/T/E	I/U/T/E
Diameter Credit-Control AVP			
<Session-Id>		IUTE	IUTE
{ Origin-Host }		IUTE	IUTE
{ Origin-Realm }		IUTE	IUTE
{ Destination-Realm }		IUTE	IUTE
{ Auth-Application-Id }		IUTE	IUTE
{ Service-Context-Id }		IUTE	IUTE
{ CC-Request-Type }		IUTE	IUTE
{ CC-Request-Number }		IUTE	IUTE
[Destination-Host]		IUTE	IUTE
[User-Name]		IUTE	IUTE
[CC-Sub-Session-Id]		IUTE	IUTE
[Acct-Multi-Session-Id]		IUTE	IUTE
[Origin-State-Id]		IUTE	IUTE
[Event-Timestamp]		IUTE	IUTE
*[Subscription-Id]		IUTE	IUTE
[Service-Identifier]		IUTE	IUTE
[Termination-Cause]		IUTE	IUTE
[Requested-Service-Unit]		IUTE	IUTE
[Requested-Action]		IUTE	IUTE
*[Used-Service-Unit]		IUTE	IUTE
[Multiple-Service-Indicator]		IUTE	IUTE
*[Multiple-Service-Credit-Control]		IUTE	IUTE
*[Service-Parameter-Info]		IUTE	IUTE
[CC-Correlation-Id]		IUTE	IUTE
[User-Equipment-Info]		IUTE	IUTE
* [Proxy-Info]		-	-
* [Route-Record]		-	-
* [AVP]		-	-

Table 6.5: Detailed Diameter CCA Message Contents for Online Charging

AVP name	Node Type	ECF
	Supported CCAs	I/U/T/E
AVPs from Diameter Credit Control		
<Session-Id>		IUTE
{ Result-Code }		IUTE
{ Origin-Host }		IUTE
{ Origin-Realm }		IUTE
{ Auth-Application-Id }		IUTE
{CC-Request-Type}		IUTE
{CC-Request-Number}		IUTE
[User-Name]		-
[CC-Session-Failover]		IUTE
[CC-Sub-Session-Id]		IUTE
[Acct-Multi-Session-Id]		IUTE
[Origin-State-Id]		IUTE
[Event-Timestamp]		IUTE
*[Subscription-Id]		IUTE
[Granted-Service-Unit]		IUTE
*[Multiple-Service-Credit-Control]		IUTE
[Cost-Information]		IUTE
[Final-Unit-Indication]		IUTE
[Check-Balance-Result]		IUTE
[Credit-Control-Failure-Handling]		IUTE
[Debit-Debiting-Failure-Handling]		IUTE
[Validity-Time]		IUTE
*[Redirect-Host AVP]		IUTE
[Redirect-Host-Usage]		IUTE
[Redirect-Max-Cache-Time]		IUTE
* [Proxy-Info]		-
* [Route-Record]		-
* [AVP]		-

7 AVPs Used for Offline and Online Charging

7.1 Diameter Base Protocol AVPs

The use of the Attribute Value Pairs (AVPs) that are defined in IETF RFC 3588 [3] is specified in subclause 5.1.3 for offline charging and in subclause 6.1.3 for online charging. The information is summarized in table 7.1 with the base protocol AVPs listed in alphabetical order. Detailed specification of these AVPs is available in the base protocol specifications.

The 3GPP IMS Charging Application uses the value 10415 (3GPP) as *Vendor-Id*.

Those Diameter AVPs that are used for IMS charging are marked "Yes" in table 7.1. Those Diameter AVPs that are not used for IMS charging are marked "No" in table 7.1. This implies that their content can (Yes) or can not (No) be used by the CCF for charging purposes.

The following symbols (adopted from IETF RFC 3588 [3]) are used in the tables:

- <AVP> indicates a mandatory AVP with a fixed position in the message.
- {AVP} indicates a mandatory AVP in the message.
- [AVP] indicates an optional AVP in the message.
- *AVP indicates that multiple occurrences of an AVP are possible.

Table 7.1: Use Of Diameter Base Protocol AVPs in IMS

AVP name	Mechanism	Offline	
	Type	ACR	ACA
	Table #	5.4	5.5
[Accounting-Multi-Session-Id]		No	No
[Accounting-RADIUS-Session-Id]		No	No
[Accounting-Realtime-Required]		No	No
{Accounting-Record-Number}		Yes	Yes
{Accounting-Record-Type}		Yes	Yes
[Accounting-Sub-Session-Id]		No	No
[Acct-Application-Id]		No	No
[Acct-Interim-Interval]		Yes	Yes
{Auth-Application-Id}		-	-
<Diameter-Header:271,REQ,PXY>		Yes	Yes
{Destination-Host}		-	-
{Destination-Realm}		Yes	-
[Error-Message]		-	-
[Error-Reporting-Host]		-	No
[Event-Timestamp]		Yes	Yes
*[Failed-AVP]		-	-
*[Proxy-Info]		No	No
{Origin-Host}		Yes	Yes
{Origin-Realm}		Yes	Yes
[Origin-State-Id]		Yes	Yes
*[Redirected-Host]		-	-
[Redirected-Host-Usage]		-	-
[Redirected-Max-Cache-Time]		-	-
{Result-Code}		-	Yes
*[Route-Record]		No	-
<Session-Id>		Yes	Yes
[User-Name]		Yes	Yes
[Vendor-Specific-Application-Id]		Yes	Yes

NOTE: *Result-Code* AVP is defined in IETF RFC 3588 [3]. However, new values are used in IMS charging applications. These additional values are defined below.

7.1.1 Acct-Application-Id AVP

The *Acct-Application-Id* AVP (AVP code 259) shall contain the value of 3.

7.1.2 Result-Code AVP

This subclause defines new *Result-Code* AVP (AVP code 298) values that must be supported by all Diameter implementations that conform to the present document.

The *Accounting-Answer* message includes the *Result-Code* AVP, which may indicate that an error was present in the *Accounting-Request* message. A rejected *Accounting-Request* message should cause the user's session to be terminated.

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but MAY be able to satisfy the request in the future.

DIAMETER_END_USER_SERVICE_DENIED 4100

The ECF denies the service request due to service restrictions or limitations related to the end-user, for example the end-user's account could not cover the requested service.

DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE 4102

The credit control server determines that the service can be granted to the end user but no further credit control needed for the service (e.g. service is free of charge).

Errors that fall within permanent failure category are used to inform the peer that the request failed, and should not be attempted again.

DIAMETER_END_USER_NOT_FOUND 5100

The specified end user could not be found in the CCF or ECF.

7.1.3 User-Name AVP

The *User-Name* AVP (AVP code 1) contains the Private User Identity [18], if available in the node.

7.1.4 Vendor-Id AVP

The *Vendor-Id* AVP (AVP code 266), as part of the *Vendor-Specific-Application-Id* grouped AVP, shall contain the value of 10415, which is the IANA registered value for '3GPP'.

7.2 Additional AVPs

For the purpose of IMS charging additional AVPs are used in ACR and ACA for offline charging. The use of these AVPs are described in subclause 5.1.3 for offline charging and in subclause 6.1.3 for online charging. The information is summarized in table 7.2 along with the AVP flag rules.

Detailed descriptions of AVPs that are used specifically for IMS charging are provided in the subclauses below the table. However, for AVPs that are just borrowed from other applications only the reference (e.g. IETF RFC 4006 [13]), is provided in table 7.2 and the detailed description is not repeated.

Table 7.2: Use Of Diameter Credit Control and 3GPP accounting AVPs for IMS

AVP Name	AVP Code	Clause Defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
CC-Correlation-Id	411	[13]	OctetString					
CC-Input-Octets	412	[13]	Unsigned64					
CC-Money	413	[13]	Grouped					
CC-Output-Octets	414	[13]	Unsigned64					
CC-Request-Number	415	[13]	Unsigned32					
CC-Request-Type	416	[13]	Enumerated					
CC-Service-Specific-Units	417	[13]	Unsigned64					
CC-Session -Failover	418	[13]	Enumerated					
CC-Sub-Session-Id	419	[13]	Unsigned64					
CC-Time	420	[13]	Unsigned32					
CC-Total-Octets	421	[13]	Unsigned64					
CC-Unit-Type	454	[13]	Enumerated					
Check-Balance-Result	422	[13]	Enumerated					
Cost-Information	423	[13]	Grouped					
Cost-Unit	424	[13]	UTF8String					
Credit-Control	426	[13]	Enumerated					
Credit-Control-Failure-Handling	427	[13]	Enumerated					
Currency-Code	425	[13]	Unsigned32					
Direct-Debiting-Failure-Handling	428	[13]	Enumerated					
Exponent	429	[13]	Integer32					
Final-Unit-Action	449	[13]	Enumerated					
Final-Unit-Indication	430	[13]	Grouped					
Granted-Service-Unit	431	[13]	Grouped					
Granted-Service-Unit -Pool-Identifier	453	[13]	Unsigned32					
Granted-Service-Unit -Pool-Reference	457	[13]	Grouped					
Multiple-Services-Credit-Control	456	[13]	Grouped					
Multiple-Services-Indicator	455	[13]	Enumerated					
Rating-Group	432	[13]	Unsigned32					
Redirect-Address-Type	433	[13]	Enumerated					
Redirect-Server	434	[13]	Grouped					
Redirect-Server-Address	435	[13]	UTF8String					
Requested-Action	436	[13]	Enumerated					
Requested-Service-Unit	437	[13]	Grouped					
Restriction -Filter-Rule	438	[13]	IPFiltrRule					
Service-Context-Id	461	[13]	UTF8String					
Service-Identifier	439	[13]	UTF8String					
Service-Parameter-Info	440	[13]	Grouped					
Service-Parameter-Type	441	[13]	Unsigned32					
Service- Parameter-Value	442	[13]	OctetString					
Subscription-Id	443	[13]	Grouped					
Subscription-Id-Data	444	[13]	UTF8String					
Subscription-Id-Type	450	[13]	Enumerated					
Tariff-Change-Usage	452	[13]	Enumerated					
Tariff-Time-Change	451	[13]	Time					
Unit-Value	445	[13]	Grouped					
Used-Service-Unit	446	[13]	Grouped					
User-Equipment-Info	458	[13]	Grouped					
User-Equipment-Info-Type	459	[13]	Unsigned32					
User-Equipment-Info-Value	460	[13]	UTF8String					
Value-Digits	447	[13]	Integer64					
Validity-Time	448	[13]	Unsigned32					
3GPP Diameter Accounting AVPs								
[Event-Type]	823	7.2.16	Grouped	V				
[SIP-Method]	824	7.2.34	UTF8String	V				
[Event]	825	7.2.15	UTF8String	V				
[Content-Type]	826	7.2.12	UTF8String	V				
[Content-Length]	827	7.2.11	UTF8String	V				
[Content-Disposition]	828	7.2.10	UTF8String	V				
[Role-of-Node]	829	7.2.27	Enumerated	V				
[User Session Id]	830	7.2.45	UTF8String	V				
[Calling-Party-Address]	831	7.2.7	UTF8String	V				
[Called-Party-Address]	832	7.2.6	UTF8String	V				
[Time-stamps]	833	7.2.39	Grouped	V				
[SIP-Request-Timestamp]	834	7.2.35	UTF8String	V				
[SIP-Response-Timestamp]	835	7.2.36	UTF8String	V				
*[Application-server-Information]	850	7.2.2a	Grouped	V				
[Application-server]	836	7.2.3	UTF8String	V				
*[Application-provided-called-party-address]	837	7.2.2	UTF8String	V				

AVP Name	AVP Code	Clause Defined	Value Type	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
*[Inter-Operator-Identifier]	838	7.2.22	Grouped	V				
[Originating-IOI]	839	7.2.25	UTF8String	V				
[Terminating-IOI]	840	7.2.38	UTF8String	V				
[IMS-Charging-Identifier]	841	7.2.20	UTF8String	V				
*[SDP-Session-Description]	842	7.2.31	UTF8String	V				
*[SDP-Media-component]	843	7.2.28	Grouped	V				
[SDP-Media-Name]	844	7.2.30	UTF8String	V				
*[SDP-Media-Description]	845	7.2.29	UTF8String	V				
[GPRS-Charging-Id]	846	7.2.18	UTF8String	V				
[GGSN-Address]	847	7.2.17	IPAddress	V				
[Served-Party-IP-Address]	848	7.2.32	IPAddress	V				
[Authorized-QoS]	849	7.2.4	UTF8String	V				
[Server-Capabilities]	603	[19]	Grouped	V				
*[Mandatory-Capability]	604	[19]	Unsigned32	V				
*[Optional-Capability]	605	[19]	Unsigned32	V				
*[User-Data]	606	[19]	OctetString	V				
[Trunk-Group-Id]	851	7.2.40	Grouped	V				
[Incoming-Trunk-Group-Id]	852	7.2.21	UTF8String	V				
[Outgoing-Trunk-Group-Id]	853	7.2.26	UTF8String	V				
[Bearer-Service]	854	7.2.5	OctetString	V				
[Service-Id]	855	7.2. 33	UTF8String	V				
[Cause]	860	7.2.8	Grouped	V				
{Cause-Code}	861	7.2.9	Enumerated	V				
{Node-Functionality}	862	7.2.24	Enumerated	V				
[Service-Specific-Data]	863	7.2.31a	UTF8String	V				

7.2.1 Amount-of-UUS-Data AVP

Void.

7.2.2 Application-Provided-Called-Party-Address AVP

The *Application-Provided-Called-Party-Address* AVP (AVP code 837) is of type UTF8String and holds the called party number (SIP URL, E.164), if it is determined by an application server.

7.2.3 Application-Server-Information AVP

The *Application-Server-Information* AVP (AVP code 850) is of type Grouped and holds the Application-Server and multiple Application-Provided-Called-Party-Address.

It has the following ABNF grammar:

< Application-Server-Information >::=<AVP Header: 850 >

[Application-Server]

*[Application-Provided-Called-Party-Address]

7.2.4 Application-Server AVP

The *Application-Server* AVP (AVP code 836) is of type UTF8String and holds the SIP URL(s) of the AS(s) addressed during the session.

7.2.5 Authorised-QoS AVP

The *Authorised-QoS* AVP (AVP code 849) is of type UTF8String and holds the Authorised QoS as defined in TS 23.207 [7] / TS 29.207 [8] and applied via the Go interface.

7.2.6 Bearer-Service AVP

The *Bearer-Service* AVP (AVP code 854) is of type OctetString and holds the used bearer service for the PSTN leg.

7.2.7 Called-Party-Address AVP

The *Called-Party-Address* AVP (AVP code 832) is of type UTF8String and holds the address (Public User ID: SIP URL, E.164, etc.) of the party to whom a session is established.

7.2.8 Calling-Party-Address AVP

The *Calling-Party-Address* AVP (AVP code 831) is of type UTF8String and holds the address (Public User ID: SIP URL, E.164, etc.) of the party initiating a session.

7.2.9 Cause AVP

The *Cause* AVP (AVP code 860) is of type Grouped. The Cause AVP includes the *Cause-Code* AVP that contains the cause value and the *Node-Functionality* AVP that contains the function of the node where the cause code was generated.

Cause has the following ABNF grammar:

<Cause>::=<AVP Header: 860>

{Cause-Code}

{Node-Functionality}

7.2.10 Cause-Code AVP

The *Cause-Code* AVP (AVP code 861) is of type Enumerated and includes the cause code value from IMS node. It is used in Accounting-request[stop] and/or Accounting-request[event] messages.

Within the cause codes, values ≤ 0 are reserved for successful causes while values ≥ 1 are used for failure causes. In case of errors where the session has been terminated as a result of a specific known SIP error code, then the SIP error code is also used as the cause code.

Successful cause code values.

"Normal end of session" 0

The cause "Normal end of session" is used in Accounting-request[stop] message to indicate that an ongoing SIP session has been normally released either by the user or by the network (SIP BYE message initiated by the user or initiated by the network has been received by the IMS node after the reception of the SIP ACK message).

"Successful transaction" -1

The cause "Successful transaction" is used in Accounting-request[event] message to indicate a successful SIP transaction (e.g. REGISTER, MESSAGE, NOTIFY, SUBSCRIBE). It may also be used by an Application Server to indicate successful service event execution.

"End of SUBSCRIBE dialog" -2

The cause "End of SUBSCRIBE dialog" is used to indicate the closure of a SIP SUBSCRIBE dialog . For instance a successful SIP SUBSCRIBE transaction terminating the dialog has been detected by the IMS node (i.e. SUBSCRIBE with expire time set to 0).

"3xx Redirection" -3xx

The cause "3xx Redirection" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 3xx response [16].

Failure cause code values.

"Unspecified error" 1

The cause "Unspecified error" is used when the SIP transaction is terminated due to an unknown error.

" 4xx Request failure" 4xx

The cause "4xx Request failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 4xx error response [16].

"5xx Server failure" 5xx

The cause "5xx Server failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 5xx error response [16].

"6xx Global failure" 6xx

The cause "6xx Global failure" is used when the SIP transaction is terminated due to an IMS node receiving/initiating a 6xx error response [16].

"Unsuccessful session setup" 2

The cause "Unsuccessful session setup" is used in the Accounting-request[stop] when the SIP session has not been successfully established (i.e. Timer H expires and SIP ACK is not received or SIP BYE is received after reception of the 200OK final response and SIP ACK is not received) [14] [16].

"Internal error" 3

The cause "Internal error" is used when the SIP transaction is terminated due to an IMS node internal error (e.g. error in processing a request/response).

7.2.11 Content-Disposition AVP

The *Content-Disposition* AVP (AVP code 828) is of type UTF8String and indicates how the message body or a message body part is to be interpreted (e.g. session, render), as described in [17].

7.2.12 Content-Length AVP

The *Content-Length* AVP (AVP code 827) is of type UTF8String and holds the size of the of the message-body, as described in [17].

7.2.13 Content-Type AVP

The *Content-Type* AVP (AVP code 826) is of type UTF8String and holds the media type (e.g. application/sdp, text/html) of the message-body, as described in [17].

7.2.14 Direction AVP

Void.

7.2.15 Event AVP

The *Event* AVP (AVP code 825) is of type UTF8String and holds the content of the "Event" header used in SUBSCRIBE and NOTIFY messages.

7.2.16 Event-Type AVP

The *Event-Type* AVP (AVP code 823) is of type Grouped and contains information about the type of chargeable telecommunication service/event for which the accounting-request message is generated.

It has the following ABNF grammar:

<Event-Type>::=<AVP Header: 823 >

[SIP-Method]

[Event]

[Content-Type]

[Content-Length]

[Content-Disposition]

7.2.17 GGSN-Address AVP

The *GGSN-Address* AVP (AVP code 847) is of type IPAddress and holds the IP-address of the GGSN that generated the GPRS Charging ID, as described in [2].

7.2.18 GPRS-Charging-ID AVP

The *GPRS-Charging-ID* AVP (AVP code 846) is of type UTF8String and holds a sequence number generated by the GGSN at PDP context activation, as described in [2].

7.2.19 IMS-Charging-Identifier (ICID) AVP

The *IMS-Charging-Identifier* AVP (AVP code 841) is of type UTF8String and holds the IMS Charging Identifier (ICID) as generated by a IMS node for a SIP session and described in subclause 5.2.4.14.

7.2.20 Incoming-Trunk-Group-ID AVP

The *Incoming-Trunk-Group-ID* AVP (AVP code 852) is of type UTF8String and identifies the incoming PSTN leg.

7.2.21 Inter-Operator-Identifier AVP

The *Inter-Operator-Identifier* AVP (AVP code 838) is of type Grouped and holds the identification of the network neighbours (originating and terminating) as exchanged via SIP signalling and described in [15].

It has the following ABNF grammar:

<Inter-Operator-Identifier>::=< AVP Header: 838 >

[Originating-IOI]

[Terminating-IOI]

7.2.22 Mime-Type AVP

Void.

7.2.23 Node-Functionality AVP

The *Node-Functionality* AVP (AVP code 862) is of type Enumerated and includes the *functionality* identifier of the *node* where the cause code was generated.

The functionality identifier can be one of the following:

S-CSCF 0

P-CSCF 1

I-CSCF 2

MRFC 3

MGCF 4

BGCF 5

AS 6

UE 7

7.2.24 Originating-IOI AVP

The *Originating-IOI* AVP (AVP code 839) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier for the originating network as generated by the S-CSCF in the home network of the originating end user [15].

7.2.25 Outgoing-Trunk-Group-ID AVP

The *Outgoing-Trunk-Group-ID* AVP (AVP code 853) is of type UTF8String and identifies the outgoing PSTN leg.

7.2.26 Role-of-Node AVP

The *Role-Of-Node* AVP (AVP code 829) is of type Enumerated and specifies the role of the AS/CSCF.

The identifier can be one of the following:

ORIGINATING_ROLE 0
The AS/CSCF is applying a originating role, serving the calling subscriber.

TERMINATING_ROLE 1
The AS/CSCF is applying a terminating role, serving the called subscriber.

PROXY ROLE 2
The AS is applying a proxy role.

B2BUA_ROLE 3
The AS is applying a B2BUA role.

7.2.27 SDP-Media-Component AVP

The *SDP- Media-Component* AVP (AVP code 843) is of type Grouped and contains information about media used for a IMS session.

It has the following ABNF grammar:

<SDP-Media-Component>::=<AVP Header: 843 >

[SDP-Media-Name]

*[SDP-Media-Description]

[GPRS-Charging-Id]

7.2.28 SDP-Media-Description AVP

The *SDP-Media-Description* AVP (AVP code 845) is of type UTF8String and holds the content of an "attribute-line" (i=, c=, b=, k=, a=, etc.) related to a media component, as described in [17]. The attributes are specifying the media described in the SDP-Media-Name AVP.

7.2.29 SDP-Media-Name AVP

The *SDP-Media-Name* AVP (AVP code 844) is of type UTF8String and holds the content of a "m=" line in the SDP data.

7.2.30 SDP-Session-Description AVP

The *SDP-Session-Description* AVP (AVP code 842) is of type UTF8String and holds the content of an "attribute-line" (i=, c=, b=, k=, a=, etc.) related to a session, as described in [17].

7.2.31 Served-Party-IP-Address AVP

The *Served-Party-IP-Address* AVP (AVP code 848) is of type IPAddress and holds the IP address of either the calling or called party, depending on whether the P-CSCF is in touch with the calling or the called party. This AVP is only provided by the P-CSCF.

7.2.32 Service-ID AVP

The *Service-ID* AVP (AVP code 855) is of type UTF8String and identifies the service the MRFC is hosting. For conferences the conference ID is used as the value of this parameter.

7.2.33 Service-Specific-Data AVP

The *Service-Specific-Data* AVP (AVP Code 863) is of type UTF8String and holds service specific data if and as provided by an Application Server.

7.2.34 SIP-Method AVP

The *SIP-Method* AVP (AVP code 824) is of type UTF8String and holds the name of the SIP Method (INVITE, UPDATE etc.) causing an accounting request to be sent to the CCF.

7.2.35 SIP-Request-Timestamp AVP

The *SIP-Request-Timestamp* AVP (AVP code 834) is of type UTF8String and holds the time in UTC format of the initial SIP request (e.g. Invite).

7.2.36 SIP-Response-Timestamp AVP

The *SIP-Response-Timestamp AVP* (AVP code 835) is of type UTF8String and holds the time in UTC format of the response to the initial SIP request (e.g. 200 OK).

7.2.37 Terminating-IOI AVP

The *Terminating-IOI* AVP (AVP code 840) is of type UTF8String (alphanumeric string) and holds the Inter Operator Identifier for the originating network as generated by the S-CSCF in the home network of the terminating end user [15].

7.2.38 Time-Stamps AVP

The *Time-Stamp* AVP (AVP code 833) is of type Grouped and holds the time of the initial SIP request and the time of the response to the initial SIP Request.

It has the following ABNF grammar:

<Time-Stamps>::=< AVP Header: 833 >

[SIP-Request-Timestamp]

[SIP-Response-Timestamp]

7.2.39 Trunk-Group-ID AVP

The *Trunk-Group-ID* AVP (AVP code 851) is of type Grouped and identifies the incoming and outgoing PSTN legs.

It has the following ABNF grammar:

<Trunk-Group-ID>::=<AVP Header: 851>

[Incoming-Trunk-Group-ID]

[Outgoing-Trunk-Group-ID]

7.2.40 User-Session-ID AVP

The *User-Session-Id* AVP (AVP code 830) is of type UTF8String and holds the session identifier. For a SIP session the *Session-ID* contains the SIP Call ID, as defined in [16].

7.2.41 UUS-Data AVP

Void.

Annex A (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	R	Subject/Comment	Cat	Old	New
Mar 2002	SA_15	SP-020033	--	--	Submitted to TSG SA #15 for Information	--	1.0.0	--
Jun 2002	SA_16	SP-020327	--	--	Submitted to TSG SA #16 for the 2nd time for Information	--	1.5.0	--
Sep 2002	SA_17	SP-020453	--	--	Submitted to TSG SA #17 for Approval	--	2.0.0	5.0.0
Dec 2002	SA_18	SP-020739	0001	--	Remove ambiguity of the CCF Session State	F	5.0.0	5.1.0
Dec 2002	SA_18	SP-020739	0002	--	Addition of Application Server (AS) acting as a Voice Mail Server	B	5.0.0	5.1.0
Dec 2002	SA_18	SP-020739	0003	--	Corrections of definitions and ambiguity	F	5.0.0	5.1.0
Mar 2003	SA_19	SP-030057	0004	--	Alignment of Immediate Event Charging (IEC) description with the latest draft IEFT Credit-Control specification	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0005	--	Correction of the IMS Charging Identifier (ICID) definition	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0006	--	Correction of IMS-CDR definitions	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0007	--	Inclusion of IETF draft 'Hakala-diameter-credit-control' specification version 05	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0008	--	Removal of Re-Transmission Attribute Value Pair (AVP) in order to align duplicate detection procedure with the Diameter Base protocol	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0009	--	Correction of the accounting session supervision (Offline) - alignment with the Diameter Base protocol	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0010	--	Correction of the accounting session supervision (Online) - alignment with the Diameter Base protocol	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0011	--	Correction of the support of local file storage and use of FTP for transfer of Accounting Information	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0012	--	Correction of abnormal session termination procedure	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0013	--	Correction of network initiated session release procedure - alignment with SIP (IETF RFC 3261)	F	5.1.0	5.2.0
Mar 2003	SA_19	SP-030057	0014	--	Correction of media modification procedures - add the UPDATE SIP method	F	5.1.0	5.2.0
Jun 2003	SA_20	SP-030271	0015	--	Corrections to align “Event Charging with Unit Reservation” (ECUR) with IETF Credit Control Application	F	5.2.0	5.3.0
Jun 2003	SA_20	SP-030271	0016	--	Correction of usage of Application-Provided-Called-Party-Address AVP	F	5.2.0	5.3.0
Jun 2003	SA_20	SP-030271	0017	--	Correction of “Cause” and “Service-ID”AVP	F	5.2.0	5.3.0
Jun 2003	SA_20	SP-030271	0018	--	Correction to some AVP definitions	F	5.2.0	5.3.0
Jun 2003	SA_20	SP-030271	0019	--	Correction on ICID definition	F	5.2.0	5.3.0
Dec 2003	SA_22	SP-030622	0020	--	Correction of MRFC-CDR content definition for multi-party-call establishment	F	5.3.0	5.4.0
Dec 2003	SA_22	SP-030622	0021	--	Correction on ICID definition	F	5.3.0	5.4.0
Dec 2003	SA_22	SP-030622	0022	--	Removal of ASR and ASA	F	5.3.0	5.4.0
Mar 2004	SA_23	SP-040143	0023	--	Correction of AVP Codes and Diameter protocol specific details	F	5.4.0	5.5.0
Mar 2004	SA_23	SP-040143	0024	--	Corrections on the Session Description Protocol (SDP) parameters	F	5.4.0	5.5.0
Mar 2004	SA_23	SP-040143	0025	--	Correction of reference to diameter base protocol	F	5.4.0	5.5.0
Jun 2004	SA_24	SP-040278	0026	--	Correction of reference to security specification	F	5.5.0	5.6.0
Jun 2004	SA_24	SP-040278	0027	--	Correction on CauseForRecordClosing	F	5.5.0	5.6.0
Jun 2004	SA_24	SP-040278	0028	--	Correction of Diameter credit control protocol reference - Align with RFC 3588	F	5.5.0	5.6.0
Dec 2004	SA_26	SP-040776	0029	--	Align SDP-Media-Components in ACR with CDR	F	5.6.0	5.7.0
Dec 2004	SA_26	SP-040776	0030	--	Reassign Vendor specific AVP codes - Align with CN4’s 29.230	F	5.6.0	5.7.0
Dec 2004	SA_26	SP-040776	0031	--	Correct multiple occurrence of Inter-Operator-Identifier, ApplicationServer, Application-provided-Called-Party-Address	F	5.6.0	5.7.0
Mar 2005	SA_27	SP-050030	0032	--	Correction of missing Service Specific Data AVP (Attribute Value Pair)	F	5.7.0	5.8.0
Mar 2005	SA_27	SP-050030	0033	--	Correction of criteria for the presence of the GPRS charging ID in the IMS CDRs – Align with SA2’s TS 23.228	F	5.7.0	5.8.0
Sep 2005	SA_29	SP-050620	0034	1	S-CSCF-Information is undefined	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0035	--	Correction in handling of 3xx response	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0036	--	Removal of GGSN Address from the I-CSCF CDR	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0037	--	Correct AVP descriptions	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0038	1	Correct names and assigned values in CDR	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0039	--	Correct Media-Components-List	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0040	--	Correct Diameter credit control AVP code definitions	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0041	--	Correct Service-Context-Id AVP definition - Align with IETF DCCA	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0042	--	Correct UUS-Data AVPs	F	5.8.0	5.9.0
Sep 2005	SA_29	SP-050620	0043	--	Correct Application-provided-called-party-address AVP	F	5.8.0	5.9.0
Dec 2005	SA_30	SP-050693	0044	--	Correct RecordExtensions ASN.1 definitons - Align with 32.205	F	5.9.0	5.10.0
Jan 2006	--	--	--	--	Updated Cover on TS version (5.9.0 to 5.10.1)	--	5.10.0	5.10.1
Mar 2006	SA_31	SP-060074	0045	--	Correction of Acct-Application-Id AVP value - Align with IETF RFC 3588	F	5.10.0	5.11.0