Abstract

The development of wireless network technologies shows a strong trend towards data transport instead of regular voice communications, with UMTS and IEEE 802.11x (WLAN) as typical examples. The aim of ongoing current research is even to combine those different wireless technologies in order to create an integral platform of service to the subscribers. At the same time, Content Providers that offer Value Added Services intend to make use of the mobility of their clientele. The subscriber mobility across multiple domains with different wireless technologies induces a considerable complexity upon the accounting management. This thesis proposes the use of a Broker party to completely manage the subscribers' content and transport component sessions, as well as to manage all the accounting information of those sub-contracting content and transport providers. The focus lies on the accounting management, but the proposed architecture requires that accounting identifiers from the Broker are distributed within the session component setup requests. These identifiers are included in the accounting records and allow the Broker to combine the transport component accounting information with the content component accounting information, without taking notice of which wireless technology was used. Current accounting systems of UMTS and WLAN are investigated, as well as three accounting information exchange protocols. Additions to the UMTS and WLAN networks are described that facilitate multi-domain accounting support. The goal is to change as little as possible of the current network architectures for friendly adoption.

Preface

Enschede, 7-5-2003

This report reflects my study in Transport Accounting Management in a Multi-Access Technologies Environment. The study is the final assignment of my MSC degree and has been conducted at the APS-TMG group at the department of Electrical Engineering, Mathematics and Computer Science, University of Twente. I would like to thank my supervisors Minh van Le, Bert-Jan van Beijnum and Georgios Karagiannis for their patience, knowledge and support that enabled me to finish this work. Furthermore I would like to thank my fellow students Robert-Jan Ostermann, Tom Broens and Erwin Mijnen, and also Mr Gullstrand of the GSM Association for their input and reflections on my work.
I owe great thanks to everyone that supported me during the last year.

Volker Min

Graduation Committee:
Ir. M. van Le
Prof. ir. B.L. de Goede (†)
Dr. ir. B.J.F. van Beijnum
Dr. ir. G. Karagiannis

Table of Content

1. Introduction

The computer is arguably one of the inventions of the last century that has the biggest impact in our current lives. During the Industrial Revolution, machines were developed to relieve mankind of manual labor and now the computer is doing the same with intellectual tasks. Adding micro processing power to our lives has opened up new ways of working, communicating and recreating
Over the last decade, the interconnected network of computers, the Internet, has established itself as being one of the most important information sources, while instant communication has been made available through the development of wireless mobile technology.
Thus far these new technologies have replaced and enhanced older technologies. The Internet allows retrieval of information that in early days was only available in printed form in libraries. Wireless mobile phones have become one of the major sources of income for telecom operators, surpassing the older, fixed network. It is only a matter of time before the last bastion, mass media, will also be subject to change. Already the music industry finds itself in trouble due to the new (illegal) ways of distribution of music through MP3. Television is likely to be the next 'victim', as consumers will take full control in what they want to see and at what time, instead of the passive programming of current TV stations.
The next big step will be the integration of all these innovations. By interconnecting different types of fixed and mobile systems, a new network will emerge that allows subscribers to communicate with whoever they want, see and hear anything of their liking, and give them full mobility to do so wherever they decide to be.

One aspect has yet to be named. The aforementioned services will only be granted if the subscriber is able (and willing) to pay for them. Currently isolated ways of accounting are in force to pay for services. E.g. telephone bill, Internet fees, cable television subscription and pay-per-view are usually all billed separately. With the integration of new technologies, the integration of the accounting is also likely. Research work related to the charging of subscribers is named Accounting Management. Six stages can be identified in general Accounting Management [1] before the subscriber receives a bill, exemplified in Figure 1-1.

- Metering: this is the measuring and recording of the quantity of resources that were used.
- Collection: The metering records are gathered from different metering entities and formatted into records that resemble 'events'.
- Accumulation: The event records are gathered, stored and integrated over time. They are presented to the Charging stage.
- Pricing: Being more of a business management issue than an accounting issue, pricing fixes the rates for denotable services for a certain period of time.
- Charging: The accumulated technical information on resource usage is translated into monetary units for each subscriber according to the Pricing rules. The output is a charging record in terms of money.
- Billing: This stage is concerned with presenting the subscriber with the charging information.

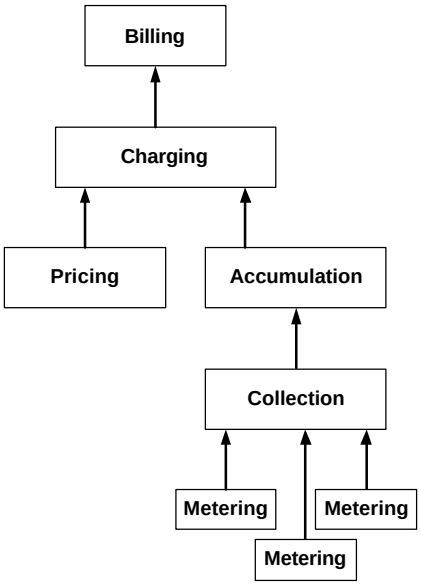

Figure 1-1: Accounting Management

Provisioning of information services can be broken down to two types. There will be a part that is concerned with the management of the information itself, the Content. The other part is the handling of the delivery of content, the Transportation. This separation is in conformance with the OSI reference model (ISO/IEC 7498-X, as described in [4]), which also distinguishes between transport-oriented ('lower layer') functions and application-oriented ('higher layer') functions.
Accounting management is necessary for both types, which will be denoted as Content Accounting and Transport Accounting. With the expected large number of Content providers (CP) and different types of Transport providers (TP), it is likely that a mediation party will emerge. Such mediation will be done by a Broker party, handling all interactions with the content and transport providers, as well as other Brokers. The subscriber will often be unaware of all these mediation interactions on its behalf. The Broker will at least take responsibility for the last step of the accounting stages, the Billing process.

This thesis regards part of the Accounting Management involved with the multi-domain Broker model, namely Transport Accounting Management. The emphasis lies on Mobility, by regarding the possibility of moving from one type of network to another without loss of connectivity (seamless roaming). Out of the different wireless access technologies, the Universal Mobile Telecommunication System (UMTS) and the Wireless Local Area Network (WLAN) will be used to exemplify such a multi-domain Transport Accounting architecture. UMTS is a large area mobile network while WLAN is a small local ('hotspot') network with higher data rate capacity. It is believed that these two types of networks will co-exist in the future and that they are functionally equal to other network types that hold similar wireless transmission properties (GPRS and CDMA2000 for UMTS, HiperLAN, Bluetooth and fixed LAN for WLAN).

Furthermore, the locations of storing and exchanging transport accounting information are investigated to come to a robust accounting mechanism.
When subscribers change their serving network system, some double registration of transport information may occur, which results in double charging. Double charging needs to be avoided.
In all, this thesis presents a robust transport accounting architecture for a multi-access technologies environment.

Various models can be constructed to come to a mobile service architecture. The chosen Broker model for this thesis is shown in Figure 1-2. It assumes that the subscriber holds a contractual relationship with only the Broker, denoted by the thick arrow. The Broker acts as the representative of the subscriber in acquiring Content and Transport facilities. After ordering Content, the information flows from the CP to the Subscriber through the TP, denoted by the dotted arrow.

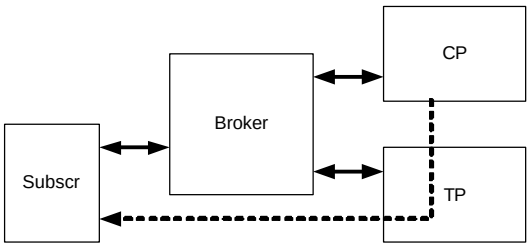

Figure 1-2: The simple Broker Model

The main research question is:

Given the chosen mobile systems and the Broker model, describe a transport accounting architecture that provisions in the transfer of transport accounting information to the Broker in such a way that the Broker is able to correlate content and transport usage for a given subscriber, even when the subscriber is roaming between different mobile systems.

This can be broken up into partial research questions:

- How do the chosen mobile networks facilitate connectivity to their subscribers?
- How do the chosen mobile networks apply Transport Accounting?
- How can the transportation resources that belong to a specific content element be registered and passed on to the Broker?
- How can several partial transportation resource records from different networks, but belonging to the same content element be correlated by the Broker?
- How does double charging occur and can it be avoided?

The remainder of this thesis is subdivided in eight chapters.
Chapter 2 describes the problem statement in three ways: The Broker model is discussed in detail, the concept of seamless roaming is described and general multi-domain accounting is regarded.
Chapter 3 presents the architecture of the UMTS network and also of WLAN implementations according to literature. Also a model is presented to describe the general functioning of Content Providers.
Chapter 4 introduces the Accounting Management structure of the UMTS and WLAN networks according to literature.
Chapter 5 describes the proposed behavior of the multi-domain Accounting Management solution for the Broker model.
Chapter 6 proposes additions to the UMTS and WLAN accounting architectures that facilitate multi-domain Transport Accounting.
Chapter 7 elaborates on the occurring and implications of double charging
Chapter 8 presents three exemplifying scenarios for the delivery of content in roaming situations.
Chapter 9 holds the Conclusions and Recommendations.

2. Problem statement

This chapter looks at the three most important aspects of the research question. First the subdivision in a three party Broker model is compared with the TINA Business Model to verify its relevancy. Secondly the concept of changing transport networks ('roaming') is described. The third part of this chapter deals with the implications of multi-domain service provisioning from the accounting perspective. It also elaborates on some of the concepts that will be used throughout this thesis, for instance what 'Content' is. Considerations and requirements for the problem statement conclude this chapter.

2.1. The Broker model vs. TINA

The Introduction of this thesis stated the choice for using a Broker party to mediate between subscribers, Transport Providers and Content Providers. This choice is based on the consideration that accounting could become a constraint in interconnecting networks of multiple wireless access techniques. Networks of the same type often use the same kind of accounting systems, which makes interoperability possible. When subscribers want to access a network of a different type (and have the equipment that could allow it), they are dependant of mutual agreements between their home provider and the foreign provider, both on the technical details as on the accounting. The GSM system is a good example for this, since GSM operators all over the world have made agreements to open their networks to foreign GSM subscribers, but interoperability with the CDMA operators in the USA has posed a huge problem for years. Now that additional technologies (UMTS, WLAN) become available on a large scale, combined with the introduction of Content Providers, interoperability becomes a lot more complex. Content sessions may have a very long duration (compared to GSM calls) and thus span multiple networks with different access and accounting technologies. The use of a Broker as an intermediate party avoids most of these problems, since it separates the content provisioning from the access technology. Furthermore, when network access is also brought under the control of the Broker, Transport Providers are no longer obliged to assure global access for subscribers, but instead can focus on their home network. This subchapter looks at aspects of the Broker model by comparing it to another model.

2.1.1. Tina

The Telecommunications Networking Information Architecture Consortium (TINAC) has defined a Business model for their TINA service architecture [2]. This Business model is very suitable for recognizing different roles in the architecture of this thesis. In short, the acting parties are called stakeholders. Each stakeholder can own one or several Business Administrative Domains (BAD). The sub domain description is left out of consideration, but can be found in the referenced document. Every BAD performs one or several business roles and interacts with other BADs through business relationships based on contracts. The roles that a BAD can assume are:

Consumer
A stakeholder in the consumer business role will consume and pay for the services offered in the TINA model.

Retailer
A stakeholder in the retailer role serves the stakeholders in the consumer role. It can range from a one-time-only service to a one-stop-shop and is the focal point of cash flows. The retailer role manages consumer service (de)registration, authorization prior to service usage, maintenance of session-level user service profiles, control and management of stream flow connections (supported by the connectivity provider) and the collecting of accounting information for the purpose of billing.

Broker
The role of the broker in the TINA model is to provide stakeholders with information that enables them to find other stakeholders (BAD) and services.
The broker should provide the following basic information:
- In response to a name provide a reference to BADs ('White Pages' function to retrieve instances)
- In response to a set of criteria provide names of matching services and a list of corresponding attributes ('Yellow Pages' function to retrieve services)

Third Party Service Provider
This stakeholder provides retailers or other third party providers with (whole sale) services. It has no direct contractual relationship with the consumer role.
It is primarily involved in the authoring, delivering and managing of content. If this stakeholder is mainly focused on generating content, it is also called a content provider. Several forms of the role of third party provider exist, but are not studied in the TINA system.

Connectivity Provider
A stakeholder in the connectivity provider role owns/manages a network. The network either transports data or is involved in a Distributed Processing Environment. 'The connectivity providers offer an interface to retailers and third party service providers which enables them to request connections between arbitrary end-points in the global network.' It is not likely that the transportation network is global, but segmented under the control of several BADs. BADs will have to federate to allow connections through multiple network segments, with the possibility that the network type is not matching. Tunneling ('wrapping') is given as a solution to counter network type mismatch.

Figure 2-1 shows the relationships between the 5 roles. Each business relationship is referenced in the TINA model by a branch and label (Bkr, 3Pty, etc) and the specific properties will not be repeated here. Though some references occur multiple times between different roles, the carried information of that reference point (RP) can be entirely different. All RPs have generic access interaction elements in common. Primarily these elements are:

- Initiate a dialogue between the BADs.
- Identify the peer BAD (possibly anonymous).
- Establish accounting/billing conditions in relation to,
- Service discovery and start
- Negotiate initial usage interactions (interfaces)

These roles and reference points can be identified in the Broker model used in this thesis. Figure 1-2 can then be interpreted as in Figure 2-2. Business relationships pointing to the roles itself have been ignored for reasons of clarity.
Using the Tina architecture for this thesis in stead of the proposed Broker model showed not to be appropriate for the following reason:

TINA documentation ([2]) states that TINA itself deals with all the interactions in the TINA service architecture, with the exception of those involving the Connectivity Provider. Since the Connectivity Provider is the main focus of this thesis, only the TINA Business model is used to clarify the role-play in the Broker model.

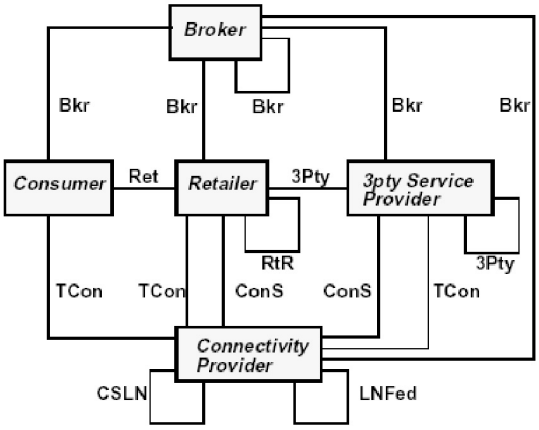

Figure 2-1: The TINA Service Architecture for its Business Model

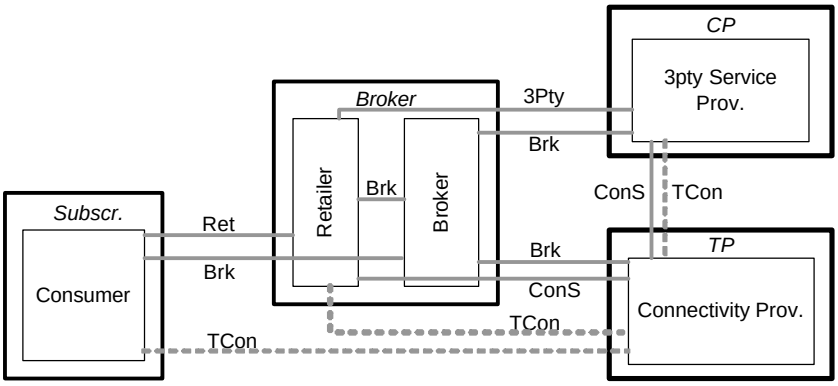

Figure 2-2: The Broker model confirms to Tina roles

In conclusion, the Broker model can be interpreted as the TINA Business Model, while considering that the Retailer role and Broker role are united in the Broker. The Broker model is therefore a somewhat simplified version of the TINA Business Model. Because this thesis focuses mainly on the Connectivity Provider/Transport Provider party, the Broker model is thus more suitable and distinctively different from TINA. By using the Broker model, complexity of content provisioning through transport network access is greatly reduced, since the accounting of the two is clearly separated. This ensures that accounting is not a limitation for content provisioning from the TP point of view.

2.2. Seamless Roaming

Traditionally telephony systems have been implemented as Circuit Switched (CS) connections. Later, Packet Switched (PS) technologies were developed based on chopping information data in small chunks and labeling each with a destination address and serial number. Both approaches have their own set of properties when it comes to describing the transport channel.
CS transport channels are primarily described by the destination and duration of a session. PS networks use properties like destination and duration, but also the quantity of transported data, and Quality of Service (QoS). These properties are the basis on which charging takes place.
When regarding these properties in the light of wireless access technologies, the PS domain offers the concept of 'always on'. In case a mobile is on and registered in CS networks like GSM, the mobile is either 'calling' or not used, 'standby'. Over time, the period that the mobile is used for calling is short with respect to the time it is in 'standby'. Because PS properties allow charging that is not strictly based on duration and destination, mobile terminals can keep established data sessions open over extensive periods of time. There may be periods in the session where no data is sent at all and consequently no charging takes place. When either party involved in the session chooses to send data after such a period, there is already a path available and no new session needs to be set up. Therefore the term 'always on' is used to indicate the fading borders between 'calling' and 'standby' modes. The 'always on' aspect has consequences for changing transport providers, since active sessions need to move together with the change. Before going into the matter of changing transport providers, a definition is given for transmitting states.

The 3rd Generation Partnership Project (3GPP) defined the three states that a (UMTS) mobile can be in for Packet Mobility Management (PMM) in [3], section 6.1.2. These are the PMM-DETACHED state, the PMM-IDLE state and the PMM-CONNECTED state.

- In PMM-DETACHED mode, the mobile is not in contact with the network and the network has no location information on the mobile. This state is left by performing a 'GPRS Attach' procedure.
- The PMM-IDLE mode is when the mobile has been registered and the network can page the mobile in the known routing area when necessary. No data can be sent since there is no designated radio channel. The PMM-CONNECTED state is entered after establishment of the PS signaling connection.
- In PMM-CONNECTED mode, the mobile is active and a radio path has been established to allow the transmission of data for one, or several data sessions.

Because of the 'always on' feature and subscriber mobility, the transport network needs to constantly adapt the wireless link to the mobile for optimal service. The next paragraphs describe three common terms used for mobility services.

Handovers
When a mobile is moving from one geographical area to another, the connection to the base station antenna might fade and the connection cannot be continued. The mobile then locates a better base station and requests its connection to be transferred for continuation of the call. This is known as a handover. Handovers within the area of one network provider can usually be done without disrupting the connection. During a conversation in mobile networks in CS mode, small parts of the call may be lost due to a handover and go unnoticed. Since such small disruptions are allowed for audio (voice) connections, there is no need to resend those missed parts later on. When considering PS data connections, every lost packet usually needs to be retransmitted for data consistency of the whole session. Some redundancy and buffering is in place in UMTS networks to prevent packet loss, though it is not flawless.

Roaming
If the mobile is moving not just outside the coverage area of the antenna it is connected with, but also outside of the boundaries of the network provider area, a more complex type of handover is required. A different operator will take over the services and the mobile is said to be roaming to a foreign network. In case of GSM/GPRS/UMTS the foreign network copies the settings from the home network and methods exist to transfer accounting information on the resource consumption from the foreign network to the home network in order to charge the subscriber. GSM/GPRS networks can currently only support roaming to a foreign network through PMM-DETACHED mode. This means that only after the connection with the serving network is completely dropped will the mobile start looking for alternative networks to roam to. In CS sessions this will mean that calls are completely dropped and once the mobile has re-attached itself, the calls cannot be automatically restored. The subscriber will need to redial and the call will be charged separately.

Seamless Roaming
In the PS domain dropout of the network is not necessarily a problem for ongoing sessions. As long as the sessions remain within time-critical boundaries, they can be copied to and continued in the foreign network. So in contrary to the CS situation where redialing is necessary, PS networks may allow sessions to survive roaming events. When transmission can be resumed without the subscribers notice, the term seamless roaming is used. Research is being conducted to find ways to facilitate fast roaming in order to allow all types of sessions to continue uninterrupted.
In some wireless systems, the mobile can foresee the necessity of a handover towards a new network and pre-register at that new network before the connection with the old network is lost. By doing so, the core network has some time to transfer ongoing sessions from the old to the new network and thus not lose any data packets due to fading.

Summarizing, migrating from base station antenna to base station antenna within one network is called a handover. Registering at and using a foreign network is called roaming. The goal of seamless roaming is that the subscriber may migrate to a foreign network without any notable loss of connectivity or session continuation.

2.3. Multi-domain Accounting Management

The two previous subchapters presented the Broker model and the concept of seamless roaming. This subchapter will look into the consequences of multi-domain service provisioning for the accounting system. It starts with a closer look on what Content Providers may provision. This is followed by a discussion on how the general Accounting Management structure, as described in the Introduction and in [1], applies to multi-domain accounting management. Subsequently Service Session Management and Accounting life cycles are discussed.

2.3.1. Content types

In previous (sub)chapters, the Content Providers were said to provide 'Content' or 'Information services', without regarding how those would manifest themselves. Henceforth, (only) the term 'Content' is used to describe any information that is sent to the subscriber by means of electronic transportation as part of a business agreement. For this thesis, the units of Content are called Content Elements. Therefore content can be a solitary item or part of a whole service. A (non-exhaustive) subdivision of content types is given with examples. The examples are of 'Mass media' or 'Personalized' nature, the former meaning one form for all buyers, and a customized form for each buyer for the latter.

- Streaming Content
  Streaming means that the use of the content starts before the whole content element has been received. The rate of reception matches the average playback speed. Also the content could have no denotable start or end and the subscriber may 'join' and 'leave' the content event.

  Mass media forms: (live) movie stream, audio stream, news ticker
  Personalized forms: peer-to-peer video/voice stream

- Content Service
  The Content may also be delivered as part of a subscribed service. The transferred Content Elements are in conformance with the agreed service.

  Mass media forms: online gaming, external data storage service (FTP)
  Personalized forms: digital agenda, newsletter service, online banking etc.

- Elemental Content:
  Content can also be purchased in singular form. This one Content Element is transferred between the subscriber and the Content Provider and after that the session ends.

  Mass media forms: pictures, downloadable music/movie files, E-Books
  Personalized forms: detailed horoscope, online medical counseling

The format of the content is likely to be in an open standard form, like MP3 for audio, MPEG/DivX for video, GIF/JPEG for graphics. Open standards are discussed in the lecture notes of the course 'Telematics Services' [4]. This summary shows that there can be many different forms of content. Some content elements are sent in an instance and use little transmission bandwidth. Others may require very long sessions and demand high bandwidth and data volume. For the remainder of this thesis, they will all just be referred to as 'content elements' without taking into account their particular demands or properties.

2.3.2. Accounting Management

The introduction of this document presented an accounting management model with six stages. When regarded in a single domain, these functions and their mutual relationships can often be recognized in a straightforward manner. The multi-domain accounting management on the other hand challenges the mutual relationships in the functional model. Depending on the agreements between the domain operators, multiple instances of charging and billing of the same service may occur across the domains, changing not the functions but rather the mutual relationships.
Subchapter 2.1 discussed the split in service provisioning and stated the choice to have the Broker in general control over both the content and the transport elements. Though alternatives can be conceived, it makes sense to organize the multi-domain accounting model in the same way. The choice for this thesis is to have TPs and CPs generate accounting records and forward those records to the Broker. The Broker subsequently combines the records that make up one multi-domain session. This means that only the Accumulation stage is investigated, with the goal to accumulate all partial records at the Broker in preparation for the Charging stage.

The coherence between the session management and the accounting management in a multi-domain environment can be shown by regarding the Service Session life cycle, Service Component life cycle and Service Accounting life cycle, as they are presented in [5]. This section continues with an abstracted description of such life cycles.

Figure 2-3 shows both the Service Session life cycle and the Accounting life cycle for a single domain service session (e.g. a phone call). The service session starts with the Session Invocation and the accompanying Accounting Invocation primarily as a result of a subscriber request. As soon as the service is provisioned, shown by Session Creation and Session Termination, the usage is metered for the duration of the session. After the service session is terminated, the Service Session life cycle is completed but the Accounting life cycle continues with the Collection and Accumulation stages. Eventually the resource usage is Charged to the subscriber, after converting the resource usage to the price. The life cycle finishes after the Billing stage has taken place, but since Charging and Billing are not regarded in this thesis they have been omitted from Figure 2-3. The combined accounting actions that occur between the Session Termination and the end of the Charging Process are also called the 'consolidation' of accounting information.

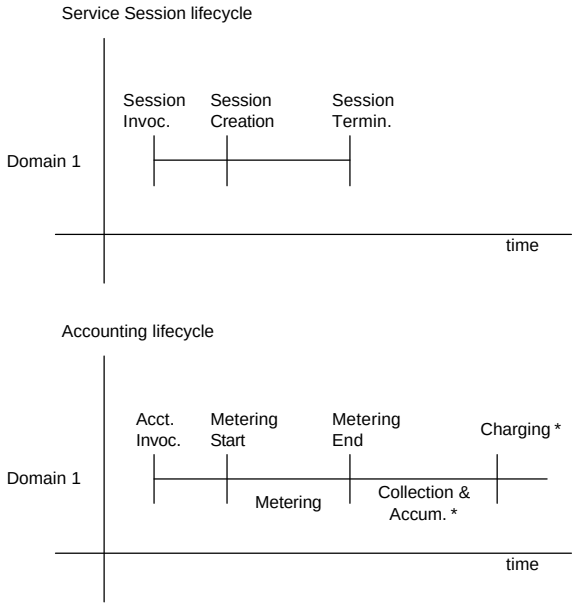

Figure 2-3: Life cycles of a service
*** Collection, Accounting and Charging together is Consolidation**

Multi-domain services

Multi-domain services are more complex, because the different parts of the service do not necessarily start and finish at the same time. Management is therefore split up into two parts. The part of a service that takes place within one domain will from now on be called a **session component**. For this thesis, the two session component types that will be regarded are the transport session components and the content session components, and the management of either is called session component management. The total composition of all components of one service will be called a **super session** and its management super session management. The super session life cycle is exemplified in Figure 2-4. It shows four domains, of which (only) Domain 1 is concerned with super session management. The life cycle starts with the Super Session Invocation (SSI) primarily as a result of a subscriber request. Subsequently a session component of Domain 2 is added by performing a Session Component Creation (SCC). As shown in Figure 2-3, Domain 2 provides the session component by performing a Session Invocation (SI) and a Session Creation (SC).

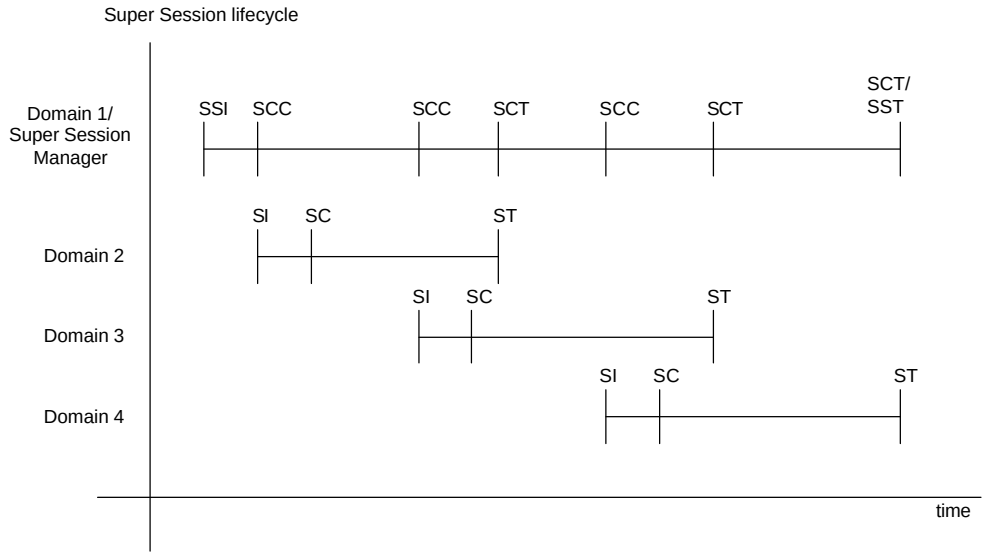

Figure 2-4: Super session life cycle

The addition of extra session components takes place in a similar way. The super session of Figure 2-4 consists of three session components and it shows that not all components last for the extent of the super session. Session components end with a Session Termination (ST) in their respective domain and a Session Component Termination (SCT) at the Super Session Manager. It is irrelevant whether the Super Session Manager or the Session Component Manager decides to terminate the session component.
A Super Session Termination (SST) occurs when the Super Session Manager decides to terminate the super session and this can only (but does not necessarily) take place when all components have been terminated first. Discussion of 'componentless' periods is postponed to the end of this section.

The corresponding multi-domain accounting life cycle may take two forms. Given that an Accounting Invocation is started simultaneously with the Session Invocation, the session component accounting life cycle can remain open until the super session is terminated, or it can be consolidated immediately after termination of the session component. Figure 2-5 exemplifies these situations. A Super Session Invocation will trigger a Super Session Accounting Invocation (SSAI). The creation of a session component will evoke an Accounting Component Creation (ACC).

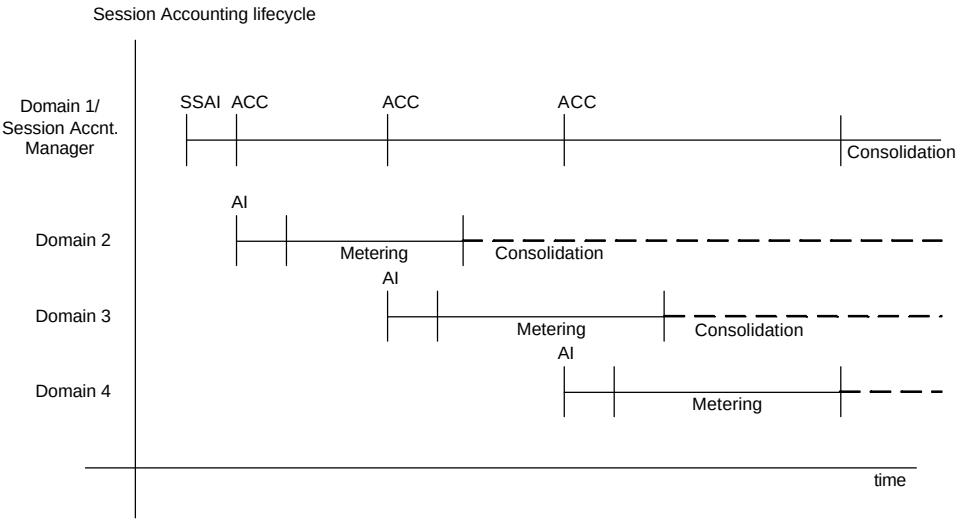

Figure 2-5: Session Accounting life cycle

Each domain starts its own accounting life cycle for the session component, similar to the single-domain situation of Figure 2-3. After the super session is terminated, the accumulated information from each component needs to be merged by an integral consolidation at the Super Session Accounting Manager. The choice for aggregated accumulation at the Super Session Manager has been discussed in the beginning of this section.
The question is, whether or not all session accounting components need to be prolonged until the whole super session is consolidated.
The main benefit is that simultaneous consolidation is relatively simple and straightforward since one party, the Session Accounting Manager, indicates when each component should present the accumulated accounting information to the aggregated accumulator, again the Session Accounting Manager.
The main disadvantage is that that situation would imply that session accounting components need to be prolonged unnecessarily at each domain. Because some super sessions may last very long and consist of many components it is unpractical and thus undesirable to postpone all consolidation activities until the super session closes. Secondary motivations are, that immediate component consolidation is less risky for domain entrepreneurs and that the subscriber can be informed during a super session of the partial charges to that point.

Component absence
Some statements need to be made about the closure of the Service Session life cycle. First of all, component sessions exist by the grace of the super session. When the Super Session Manager decides to terminate the super session, it should enforce the closure of all component sessions first. On the other hand, if all components happen to be terminated, it does not necessarily mean that the Super Session Manager should automatically close the super session. In stead the Super Session Manager could evoke new component sessions to continue the super session.
One of the partial research questions from the Introduction of this document stated that the transport resources from different networks must be correlated per content element. This means that the choice can be made to align the life cycle of the super session to the provisioning of a content element. The super session starts with the invocation of the content component. As soon as the content component is terminated, the Super Session Manager shall terminate all remaining transport components and subsequently the super session itself. This implies that super sessions do not encounter ‘componentless’ periods, since the content component is always present.

In summary, multi-domain Accounting Management is more complex than Accounting Management in a single domain because all accounting information for each super session must be combined. The Broker is the party to gather and combine all accounting information of super sessions for the subscriber and to initiate the Charging stage. Session accounting components may be consolidated and closed as soon as the session component ends since it is undesirable to postpone component accounting until the whole super session is closed.
Super sessions start with the Content component invocation and end when this component is closed. This ensures that super sessions have always at least one component.

2.4. Problem Statement Considerations

The proceeding parts of this chapter provided information on the background of the Broker model, the aspects of seamless roaming and multi-domain accounting. The assumptions to this point are listed in this subchapter. Also the goals are formulated for the accounting architecture that is to be developed in this research assignment. In conclusion, the relevancy of this research is discussed.

2.4.1. Research assumptions for the multi-domain accounting architecture

The following assumptions are made for the design of the multi-domain accounting architecture:

- It is assumed that the dominant form of multi-domain service management will involve a Broker party, as described by the Broker model. According to section 2.3.2, the accounting architecture developed in this research assignment will follow this model, by having the Broker accumulate all accounting information.
  Subchapter 2.1 discussed why the complexity of multi-domain accounting is greatly reduced by separating content provisioning from transport provisioning, thereby supporting the choice for brokerage.

- This thesis describes accounting management in the Collection and the Accumulation stages. It is assumed that subscriber Charging and Billing, along with mutual Charging and Billing between providers and Brokers, can take place based on the accumulated and correlated accounting information at the Broker.

- It is assumed that when a multi-domain accounting architecture can be designed for the UMTS and WLAN network types, other network types can also be fitted to support the multi-domain accounting architecture.

2.4.2. Goals for the multi-domain accounting architecture

The following goals are presented for this research assignment:

- The UMTS and WLAN networks are two distinctly different mobile networks. The accounting architecture must strive to not change the current network designs, or change as little as possible, to ensure that implementations will be feasible.

- The architecture should facilitate correlation of accounting information from several session components belonging to the same super session. The Broker should be able to correlate the accounting records as soon as all of them have been received. Robustness of the multi-domain accounting architecture should be pursued.

- Investigate the aspects of some of the accounting information exchange protocols that are commonly used and determine if there would be a particular preference with respect to the multi-domain accounting architecture.

- Investigate the aspects of double charging and estimate the impact on the accounting architecture. Also, investigate ways to avoid double charging.

2.4.3. The relevancy of developing a multi-domain accounting architecture

The value of finding a solution to multi-domain accounting issues can be imagined by looking at the possible benefits for the participants.

- Transport Providers do not need to add systems to their networks to technically interact with Content Providers, nor do they have to add systems that can handle the additional content accounting ('Value Added Service'). They do need to fit their network to accept instructions from the Broker party, as well as to exchange accounting information. Collaborating with a Broker means that all subscribers to that Broker can access the transport network.
- Content Providers do not need to collaborate with all Transport Providers to allow every subscriber to use content. Collaborating with a Broker means that all subscribers to that Broker can access the content.
- Service Brokers do not need own and maintain transport networks or content, but merely handle the accounting for their subscribers. Their benefits may lie in quantity discounts from providers due to their larger number of subscribers. Currently phone brokers like OneTel or DebiTel do business in this way in the Netherlands.
- Subscribers have the benefits of having a single party handling their mobile services. Charges can be presented in an organized matter to the subscriber.
-

These assumed benefits show the relevancy of a multi-domain accounting architecture. The desire for a combined accounting architecture for UMTS and WLAN networks in particular has been expressed in a number of recent publications, for instance in IEEE Spectrum magazine [6].

3. Service Provider Network Architectures

This chapter describes the network architectures of the chosen transport network types. First the UMTS network architecture is described. This is followed by a WLAN network architecture description. The descriptions include an identification of the network specific nodes, as well as a look at how sessions are provisioned. A description of the roaming principles of each network is also presented.
The third part of this chapter describes a model to explain the functioning of Content Providers.

3.1. The UMTS network architecture

Network architecture
The simplified network architecture for a UMTS network, as shown in Figure 3-1, consists of 2 domains: the Circuit Switched (CS) domain and the Packet Switched (PS) domain. Elements that build up a network are called logical nodes. The Mobile Switching Center (MSC) and the Gateway MSC set up voice connections from and to the mobile, while the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) route all data traffic to and from the mobile. The transceiver radio system of Base Stations (antennas) and Base Station Controllers (BSC) is called the UMTS Terrestrial Radio Access Network (UTRAN) or the GSM Base Station Sub-system (BSS), depending on the respective wireless technology.

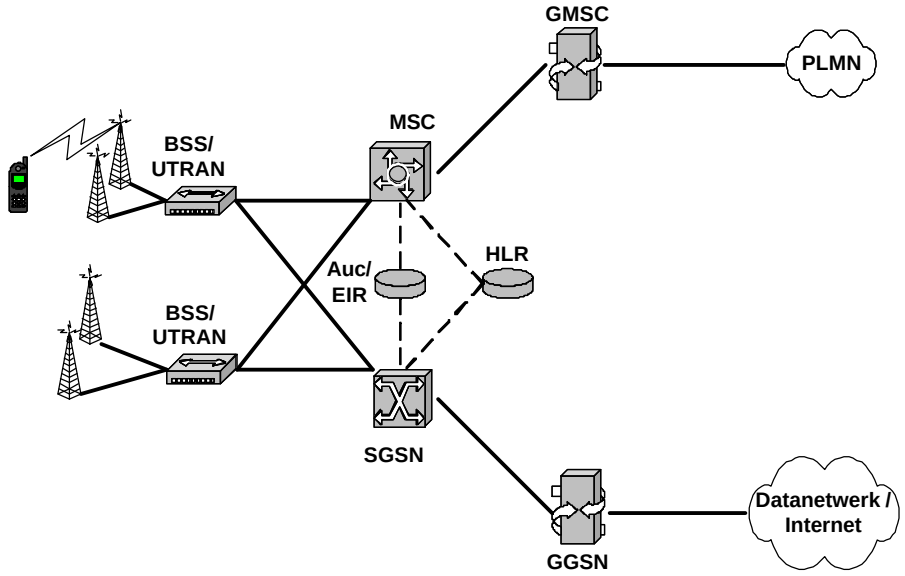

Figure 3-1: The UMTS Network Architecture

When a mobile is registering, the subscriber information is loaded from the Home Location Register (HLR) into the MSC/SGSN. The HLR contains information about the restrictions of the subscriber's subscription and security information. Also the mobile is authenticated upon registration by the Authentication Center (AuC). If the mobile is not under contract of the network, the HLR and AuC of the originating network are contacted for subscription and authentication information. The HLR and AuC support both the CS and the PS domain functions.
For this thesis, the PS domain is regarded primarily. Due to the long duration of sessions, this domain is much more involved in inter-system roaming issues than short-term CS (voice) sessions.

It is essential to realize that signaling data (like authentication, roaming and accounting information) and subscriber session data (like a file transfer or content session) are logically separated in the network.

Detailed registration and authentication procedures are not primary research targets of this thesis. It is assumed that the mobile will acquire one or several IP addresses from the network through the standardized registration process and that that will allow it to communicate over the Internet. Details on the registration and authentication process in GPRS/UMTS can be found in Chapter 6 of [3] (Iu mode for UMTS).

3.1.1. Session setup

The mobile network technology can be divided into two aspects. The first is the mobility aspect, which allows the network to track the location of each mobile.
The mobility aspect is represented by the establishment of a Mobility Management (MM) context at the serving SGSN to track the point of attachment of the mobile. By definition, a mobile can only have one MM context, which follows the mobile when it changes its serving SGSN.

The second aspect is the data traffic aspect, which allows a mobile to contact other entities inside and outside the serving network. A particular data traffic session is represented by the establishment of a Packet Data Protocol (PDP) context. Both the serving SGSN and GGSN maintain PDP contexts to track active data sessions.

The data traffic aspect is far more important for accounting than Mobility Management and therefore Mobility Management is only discussed in combination with roaming in section 3.1.3.

PDP context management
Upon PDP context setup, a mobile will receive a PDP address, which is unique in the network domain. PDP addresses are IPv4 or IPv6 addresses according to chapter 14.5 of [3]. More on PDP addressing can be found in [3], chapter 9.2: 'PDP Context Activation, Modification, Deactivation, and Preservation Functions'.

Each PDP context has at most one Traffic Flow Template (TFT) associated with it and they are located in the GGSN. A TFT consists of at least one, to at maximum eight packet filters, which can filter packets on sets of the following attributes:
- Source Address and Subnet Mask.
- Protocol Number (IPv4) / Next Header (IPv6).
- Destination Port Range.
- Source Port Range.
- IPSec Security Parameter Index (SPI).
- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.
- Flow Label (IPv6).

Secondary PDP contexts can be activated per PDP address. Secondary PDP contexts differ from the primary in QoS and TFT, but share the same destination Access Point Name (APN) and PDP address. The terms 'primary' and 'secondary' only denote the order in time that PDP contexts were created and after creation they are regarded being of equal status by the network. Therefore the primary PDP context can be terminated when desired, while the secondary context(s) remain in service.

A data path from a GGSN to a SGSN is also called a Tunnel. To allow reference to PDP Contexts, network nodes use Tunnel Endpoint Identifiers (TEID) according to

14.6 of [3]. The TEID is a unique identifier within one IP address or logical node and it is forwarded to the GGSN upon PDP Context Activation. The receiving end of a tunnel locally assigns a TEID value that the sending side must include in its messages regarding that PDP Context (e.g. activate, modify or deactivate messages).

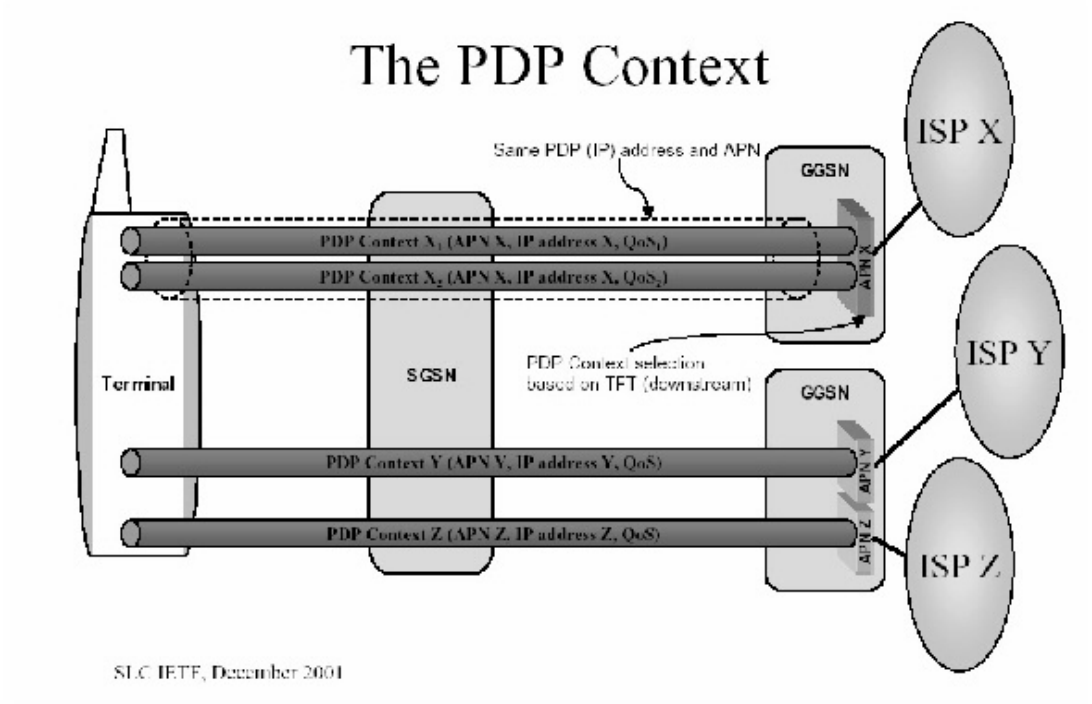

Figure 3-2: The PDP Context (presentation slide of SLC IETF)

Figure 3-2 visualizes the relationships of the elements of a PDP context. More on the PDP setup procedure can be found in chapter 9.2 of [3].

3.1.2. Network initiated sessions

Not only can a mobile request the establishment of a session. Any outside party may try to contact the mobile. In case packets arrive at the GGSN for a served mobile and no suitable PDP context is established, there would be no way of delivery for the GGSN. To counter this, the GGSN can initiate a 'Network Requested PDP Context Activation Procedure' as described in 9.2.2.2 of [3]. This procedure informs the mobile of new incoming packets by paging and solicits the mobile to initiate a PDP context activation procedure in order to deliver the incoming packets. This procedure only works when the GGSN has static PDP information about the PDP address. The GGSN does not initiate the creation of a PDP context on its own. It is expected that this is to allow the implementation some form of accept/decline policy for the subscriber. If the GGSN was allowed to initiate PDP context establishment directly, any outside source could send packets to the mobile without the subscriber's approval, while the subscriber still has to pay for the delivery.

3.1.3. Roaming in UMTS

The way of handing over the serving of a mobile from one SGSN to another SGSN is part of the Mobility Management and is transparent to the subscriber. The article of [19] (itself based on [3] and [20]) compares the Mobility Management principles of GPRS and UMTS. It states that CS cells are partitioned into Location Areas (LA) and for PS there are Routing Areas (RA). The LA is kept in a Visitor Location Register (VLR). The VLR is an HLR extension at the MSC to store a copy of HLR information from roaming users, obtained from the roaming user's own HLR. UMTS does not use a VLR for the PS domain. The SGSN stores RA information for the PS domain for all its attached users and the RA is the most precise type of location information available at the SGSN. The serving SGSN address is the most precise type of location information available at the HLR. Mobiles inform the network of their location through RA and LA update procedures both periodically and when they detect a change of their location.

RA Location Update
Now follows the RA location update scenario that takes place during roaming, for the PS-UMTS case based on the article [17] without regarding GPRS and the CS domain. The message flow of the RA Update scenario is illustrated in Figure 3-3. Each step is described in more detail in Table 1.

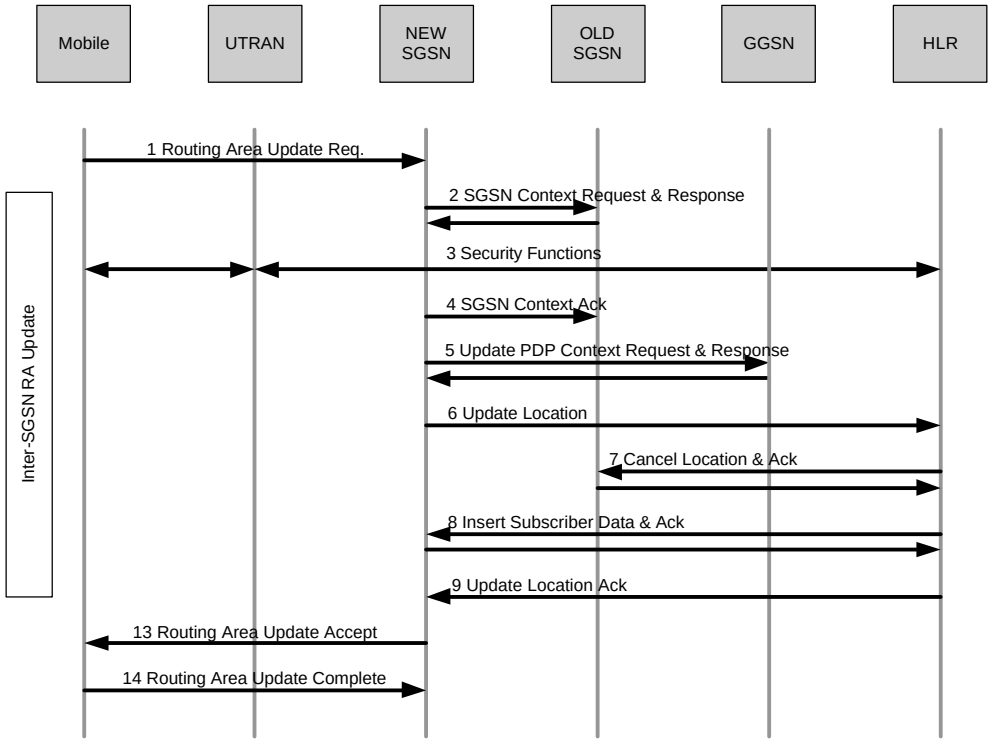

Figure 3-3: RA Update procedure (from [17])

	Source	Destin.	Description
Step 1	MT	New SGSN	The mobile sends the Routing Area Update request message to the new SGSN. It is not ciphered. It has a 'Follow on request' parameter to indicate if the UTRAN-SGSN connection should be kept for pending uplink traffic. In case of an inter-SGSN update, Steps 2-9 are executed or otherwise skipped.
Step 2	New SGSN	Old SGSN	The New SGSN contacts the Old SGSN by an SGSN Context Request message to receive the MM and PDP contexts of the mobile. The Old SGSN deletes the MM context after it receives 7 from the HLR AND a timer has expired. The timer is used to secure the MM context in case the mobile requests another inter-SGSN before the current procedure is completed.

Step 3	UTRAN	MT/HLR	Security functions are performed before starting step 4
Step 4	New SGSN	Old SGSN	The New SGSN acknowledges the reception of the SGSN Context. Note that no data packets are forwarded between the Old and New SGSN.
Step 5	New SGSN	GGSN	The New SGSN contacts the GGSN to update the PDP Contexts on the New SGSN address. The GGSN responds an acknowledgement
Step 6	New SGSN	HLR	The New SGSN sends the HLR an Update Location message to inform it on the SGSN change for the mobile.
Step 7	HLR	Old SGSN	The HLR cancels the MM and PDP Contexts at the Old SGSN. The Old SGSN doesn't delete the information until the timer mentioned in step 2 expires.
Step 8	HLR	New SGSN	The HLR inserts the subscriber data to the new SGSN. Each PDP Context is checked for activity, which demands extra SGSN tasks. E.g. QoS parameters should be met or modified for each PDP Context.
Step 9	HLR	New SGSN	After the Subscriber Data is acknowledged, the HLR acknowledges the completion of the RA Update on its side.
			Step 10-12 are omitted because they describe LA Updates for GPRS (but mentioned here for the sake of completeness)
Step 13	New SGSN	MT	The New SGSN sends the RA Update Accept message to the mobile.
Step 14	MT	New SGSN	The mobile sends the RA Update Complete message to the New SGSN to confirm the change.

Table 1: RA Update example

Packet forwarding on handover and Anticipated Handover
Packets are forwarded in the UTMS network through the chain of

GGSN – SGSN – UTRAN - Mobile Terminal

and vice versa. The UTRAN plays a key role in handovers. Is consists of Radio Network Controllers (RNC) that each controls one or several (usually bordering) broadcast cells. UMTS has the advantage that a mobile can be served by several cells at the same time to allow multiple radio paths. One RNC is in control over the cells that transmit to the mobile. Figure 3-4a shows such a multi-path for a mobile where RNC1 controls B1 and B2. If the mobile moves towards B3, the radio path between the mobile and B1 is lost due to radio path loss and the radio link between B3 and the mobile is established (Figure 3-4b). B3 belongs to a different RNC (RNC2) and therefore a ('Iur') link is established between RNC1 and RNC2 to forward the B3 signal to RNC1. This is merely a transparent forwarding of the radio signal received by B3 at (OSI) Layer 1 and partial Layer 2 (MAC). RNC1 combines the signals from B2 and B3 for optimal performance and forwards the derived packet data to SGSN1. In this case RNC1 is called the serving RNC (SRNC) and RNC2 is called the drift RNC (DRNC).

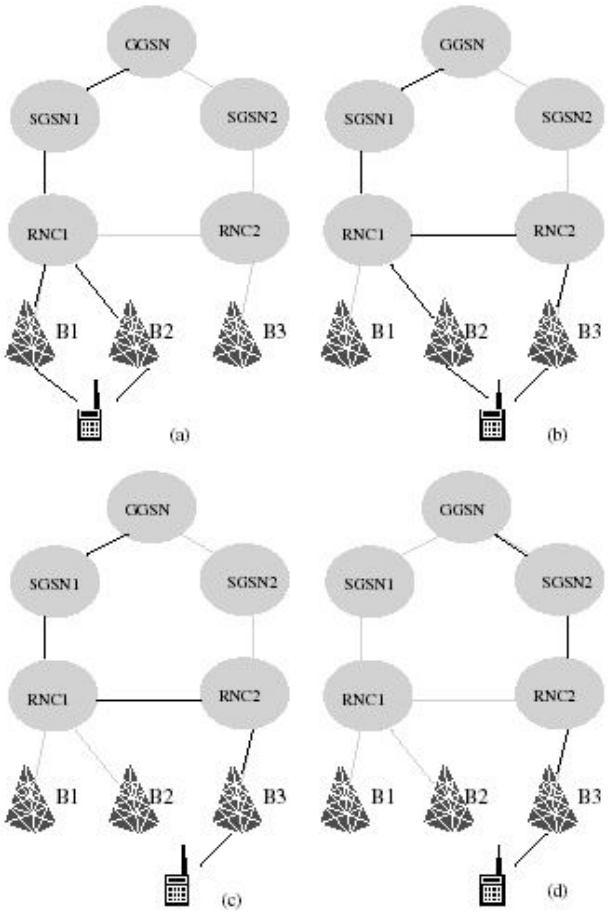

Figure 3-4: PS Serving RNC relocation (from article [17])

Figure 3-4c shows that the radio path link between B2 and the mobile has also been broken. The mobile does not communicate with any cell from RNC1 and therefore the data path from the mobile to the GGSN is no longer optimal. Suppose that RNC2 is connected to SGSN2. SRNC relocation now takes place to renew the data path as in Figure 3-4d to:

GGSN – SGSN2 – RNC2 - Mobile Terminal

The SRNC relocation procedure between Figure 3-4c and d is different for CS and PS. The article [17] gives the detailed SRNC relocation message flow for PS. It is described in short as RNC1 noticing that none of its own cells has a link with the mobile and therefore a SRNC handover is necessary (Figure 3-4c). It informs SGSN1 of its decision and SGSN1 determines if the (proposed) RNC2 is under its own service. If not, an inter-SGSN SRNC relocation is necessary and SGSN1 sends MM and PDP Context information to the SGSN of RNC2 (in this example SGSN2). SGSN2 sets up a data link to its RNC2 and after establishment it sends a request to SGSN1 to forward unacknowledged downstream packets that were buffered at RNC1. SGSN1 instructs RNC1 to stop sending packets to the mobile over the radio link (through B3) and commence with the forwarding of the downstream GGSN packets to RNC2. The new downlink path is now

GGSN - SGSN1 – RNC1 – RNC2 – Mobile Terminal

When the RNC2 detects a successful routing of downstream packets coming from RNC1, it instructs its SGSN2 to change the core network routing. Effectively RNC2 is now in control over the B3 - Mobile Terminal radio path link instead of RNC1. SGSN2 now updates the PDP Context routing in order to have the GGSN forward downstream packets to SGSN2 instead of SGSN1. After RNC2 detects that it has received all buffered packets in RNC1, it also instructs SGSN2 to notify SGSN1 to release the SGSN1-RNC1 data link for the Mobile Terminal. The transition to Figure 3-4d is now complete and the SGSN2 will follow the RA update procedure as described in the previous paragraph. The article states that the RA update procedure is picked up at step 8 ('Insert Subscriber Data & Ack'). This is probably a typo, since it is likely that the RA Update procedure is started at step 6 ('Update Location'). Steps 6 – 9 are one Update Location pair and should be carried out completely.

Through these RNC procedures packet loss is minimized. One major constraint is of course that RNC1 and RNC2 must be able to establish a link to allow the forwarding of packets over the UTRAN. This might be implemented for RNCs within the same Business Administrative Domain, but is certainly not necessarily in effect for adjacent RNCs of different BADs. Willingness of adjacent UMTS Providers to link their border RNCs together might turn out to be crucial for seamless roaming.

3.2. The WLAN network architecture

Network architecture
WLAN is also known as the IEEE wireless LAN family standard 802.11 and it comes in a number of variations according to the website [21] and article [22].

- **802.11** provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** is an extension to 802.11 and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as *802.11 High Rate* or *Wi-Fi*) is an extension to 802.11 that provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. This is currently the most widely present form.
- **802.11g** provides 20+ Mbps in the 2.4 GHz band and is still not fully standardized.

The mentioned data rates will not be achieved in the actual networks, but are the theoretical limits. An area with 2 or more wireless stations that have recognized each other and have established communications is called a Basic Service Set. In the most basic form there are just the two stations and is the network ad-hoc. Figure 3-5 shows such an Ad-Hoc network area where three Stations are within each other's transmission distance.
More commonly is the inclusion of a non-mobile Access Point (AP). The AP bridges the wireless and wired networks and all Stations in range communicate through it instead of in ad-hoc mode. When there are several overlapping APs, it is said to be an Extended Service Set (ESS). The APs are interconnected through some distribution network, commonly Ethernet LAN, and a Network Access Server (NAS) is needed to enable Stations to exchange messages over the Internet.

Figure 3-6 shows such a configuration. An Authentication server will authenticate Stations that are within an AP broadcast area. Similar to the description of the UMTS network, the authentication and registration processes are not under investigation in this thesis. The article [23] describes both processes and provides additional references. A common form of an authentication server is a RADIUS server, which is discussed in section 4.2.1.

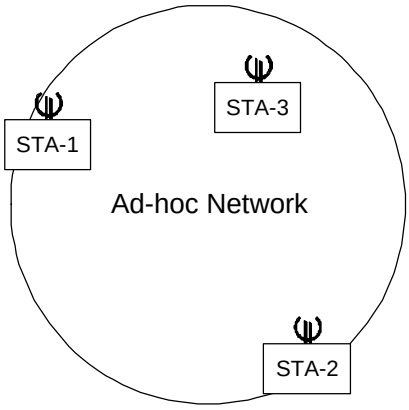

Figure 3-5: Visualization of an Ad-Hoc wireless network consisting of three Stations

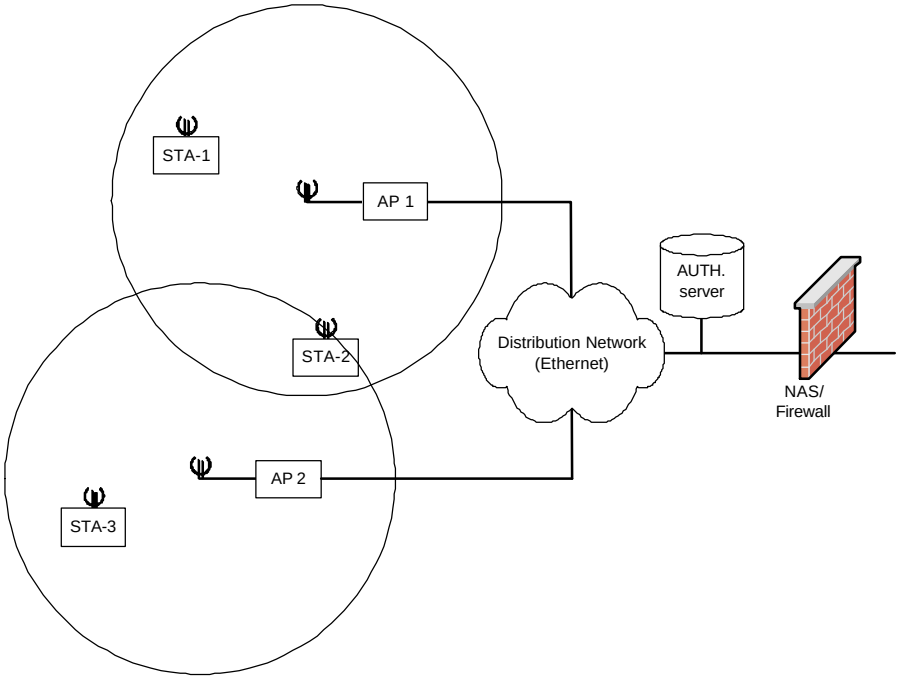

Figure 3-6: 2 APs are linked together and allow Internet access through a firewall. Mobiles may migrate from AP to AP without loss of connection.

In comparison with UMTS, there is no denotable equivalent of a PDP Context session. The mobiles receive an IP address upon registration and can usually access the Internet without much trouble. Sometimes the gateway to the Internet is equipped with a Firewall for security. A Firewall can be configured in many ways, but it usually blocks all unsollicitated incoming data packets and it may be used to shield off home network user information to the outside. More information on Firewalls can be found in [24]

Roaming
Several frequency subsets are defined within the 802.11 frequency bands and each neighboring AP is broadcasting at one, or a small number of other frequency sets to minimize interference. A Station will always register at the AP with the best signal-to-noise beacon frequency of its set. As soon as the Station detects that the signal is fading, or a better AP is present, it will switch to that stronger AP. There was no initial standardized roaming protocol developed for 802.11.
Therefore some vendors have developed their own protocol. Aironet, Lucent Technologies, and Digital Ocean have developed the Inter-Access Point Protocol (IAPP) to allow roaming between their Access Points. IAPP defines the messages and data for exchange between Access Points and between the IAPP and higher layer management entities for roaming. TCP is used for inter-Access Point communication and UDP for RADIUS authentication request/response exchanges (for RADIUS, see also section 4.2.1 or the article [23]). It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices. The IAPP specification has not been made available to the public.

The IEEE has acknowledged this initiative and a working group has been started to adapt the IAPP for standardization under the code 802.11f. The roaming protocol is supposedly not only being developed for roaming within an ESS, but also between different ESSs (article [22]). It is unknown at this point if it also includes a method of seamless roaming between two ESSs.
The 802.11f standardization has not been disclosed during this thesis. Publication is expected in the course of 2003.

3.3. The Content Provider Architecture

Content Providers come in a great variety of different architectures. For this thesis it is assumed that the Content Providers operate on the Internet, and each implementation is customized for the type of offered service. The term ‘Content’ is to be taken in the broadest sense. A summary of several content types has been presented in section 2.3.1. Several assumptions are made to come to a general model for Content Providers.

- The Content Provider is operating according to the Third Party Service Provider role of the TINA architecture, as described in subchapter 2.1.
- The Content Provider operates primarily on the Internet and its transmission standards are in conformance with the TCP/IP suite. It may have additional private network links.
- The Content delivered to the subscriber originates from a Single Point-Of-Attachment (SPOA) on either the Internet or through the private network links. The Content may come from different internal locations.
- Additional features, like encryption for security, do not change the general model.
- Content is delivered in a one on one session. Broadcast or multi-domain sessions are not regarded.

The model for the Content Provider Domain, as shown in Figure 3-7, constitutes of three elements. First is the Single Point-Of-Attachment server. This element makes sure that the QoS demands for each session are met. It decides the network and/or route (or first hop) to the destination to achieve that goal. It may also listen for incoming session requests in case Content sessions are set up by the other peer party.

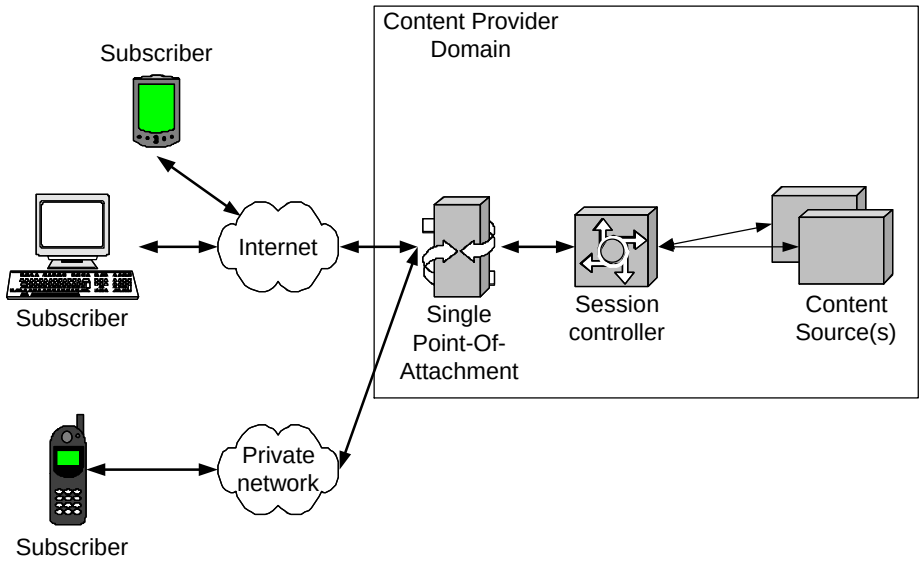

Figure 3-7: The Content Provider Model

The second element is the Session Controller. This element deals with the handling of requests for Content Sessions. It also controls the session on behalf of the subscriber. E.g. the handling of a pause request from the subscriber of a movie stream session, or the decision of sending a news item to subscribed news tickers. The third item is the Content Source. This can be an electronic storage facility in case of movies/music, but also the link to the live video feed of a sports event/concert, or a press agency's editorial board.
It is the task of the Session Controller to electronically format the Content Element appropriately before it is being sent.

This model can be fit to most known business implementations of Content Providers and therefore it is useful for describing the behavior of CPs in this thesis.

4. Service Provider Accounting Architectures

Several types of accounting architectures accompany the network architectures of the previous chapter and they are explained in this chapter. The well-documented accounting architecture of UMTS already allows UMTS operators to settle the costs amongst themselves for roaming users. For WLAN multiple solutions exist for accounting issues. There are also several protocols developed that are used for the exchange of accounting information between operators. A comparison is made between some of the most common ones to be able to check if and how they are able to carry the necessary accounting information that was mentioned in section 2.4.1.

4.1. UMTS Accounting Architecture

To accommodate for accounting in the UMTS network, interfaces are in force between relevant network elements and the billing system.
Those logical nodes report network usage by users to the Billing System through Charging Data Records (CDRs, in traditional CS standardization also referred to as Call Detail Records). Each logical node has its own type of CDR. In the CS domain, the MSC sends one of two types of CDRs for every CS connection it services. The MSC sends 'Mobile Originated CDRs' (MOCs) for calls that were dialed by the subscriber, or 'Mobile Terminated CDRs' (MTCs) in case the subscriber was called by another party. See [7] for more details on CDRs in the CS domain. In the PS domain, where sessions can last for long periods of time, the SGSNs and GGSNs send their respective S-CDRs and G-CDRs to an intermediate Charging Gateway Function (CGF). The CGF combines and stores the CDRs in non-volatile memory and formats the information conveniently for the Billing System. The CGF may be located in a separate physical network element or resident in the SGSN/GGSNs in a distributed way.
The Accounting architecture is added to Figure 3-1 and depicted in Figure 4-1. The possible locations of the CGF are depicted in Figure 4-2.

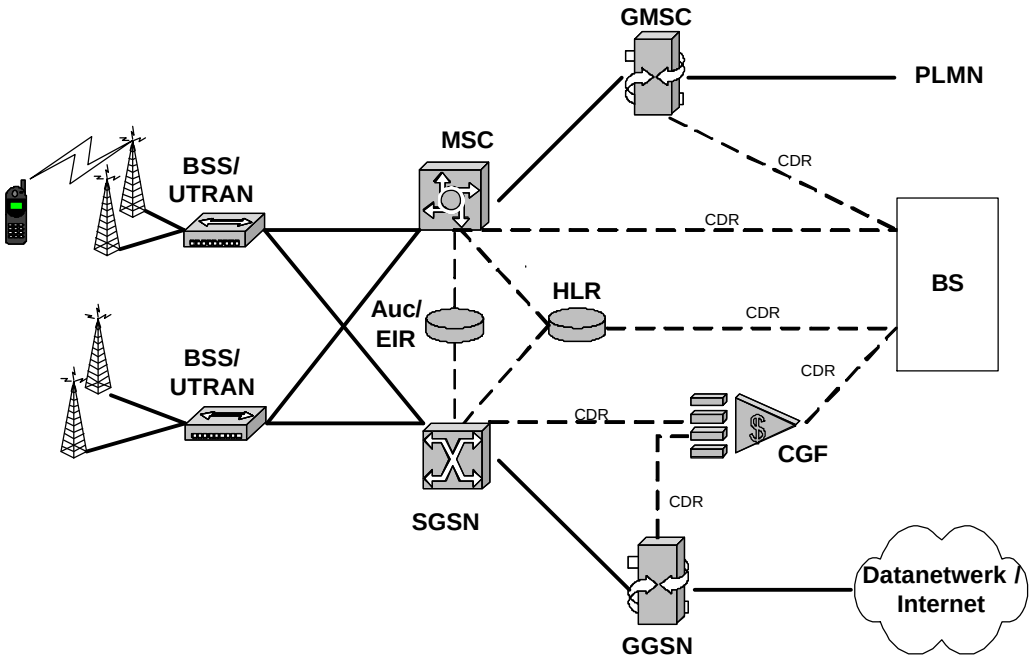

Figure 4-1: Accounting in a UMTS Network
(crossing lines do not imply a merger of communications)

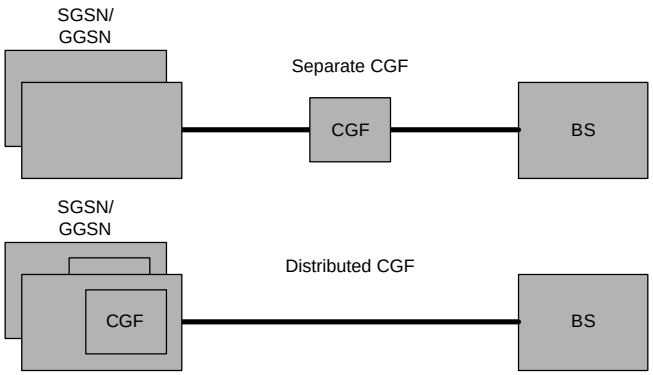

Figure 4-2: Charging Gateway Function Alternative Locations

This subchapter continues with a closer look at the types of CDRs and the information that they contain that is relevant to accounting.

4.1.1. CDRs in the PS domain ([9])

Five types of CDRs are in use in the PS domain:

- S-CDR records report radio and core network usage per PDP context at the SGSN
- G-CDR records report external and core network usage per PDP context at the GGSN
- M-CDR records report user mobility related activities at the SGSN
- SMS Mobile Terminated-CDRs
  These records report received Short Message Service events at the SGSN (SMS is not regarded in this thesis)
- SMS Mobile Originated-CDRs
  These records report sent Short Message Service events at the SGSN (SMS is not regarded in this thesis)

The S-CDR and G-CDR are used for reporting data quantity information, and will therefore be further examined. The full CDR description is given for both node types in Appendix A and each record field is described in short. Important aspects from those CDR fields are described in more detail in the next section.
The field definition includes the field name, description and category. For performance improvements, an operator is allowed to eliminate some of the fields from their records if they are not essential for their operation. The category of the field shows if the field may be omitted. The categories are:

- 'Mandatory' (M). The field is mandatory and shall always be present in the CDR.
- 'Conditional' (C). The field shall be present only when certain Conditions are met. These Conditions are specified as part of the field description.

All other fields are designated as 'Operator' (O) provisionable. Those fields that an operator wishes to be present are further divided into mandatory and conditional categories:

- 'Operator mandatory' (Om). The field, if provisioned by the operator, shall always be present.
- 'Operator conditional' (Oc). The field, if provisioned by the operator, is present only when the required Conditions are met.

Regardless of the type of CDR, each one of them comes in one of three different formats:

- A Fully Qualified CDR (FQC): A record consisting of all M, C, Om and Oc fields
- A Fully Qualified Partial CDR (FQPC): A record consisting of all M and C fields, plus all the Om and Oc fields enabled by the PLMN operator.
- A Reduced Partial CDR (RPC): A record containing only M fields and those containing information that changed since the last CDR.

A session can be reported by using several Partial CDRs. The first CDR will always be a FQPC, and subsequent CDRs will be RPCs. When the Billing System requires FQPCs, either the SGSN and GGSN both need to report in FQPCs, or the CGF needs to transform each RPC into FQPCs by completing the omitted fields with information from the previous RPCs or the primary FQPC.
For example, location information does not need to be repeated in each CDR if the mobile does not move, and can thus be omitted to reduce storage space and network resources.

4.1.2. Important S-CDR/G-CDR aspects

The previous section already referred to Appendix A for the full list of information from the S-CDR and G-CDR. What follows is a closer look at the most important items for the accounting process in the view of multi-domain accounting management.

'International Mobile Subscriber Identity'
To identify a user/subscriber on the network, each mobile stores an International Mobile Subscriber Identity (IMSI) of the user/subscriber. On the home network this is used to identify the user at the SGSN. In foreign networks, a Packet Temporary Mobile Subscriber Identity (P-TMSI) is allocated at first registration as an alias for the IMSI due to security and confidentiality restrictions. The IMSI consists of 3 parts: Mobile Country Code (mcc), Mobile Network Code (mnc) and the Mobile Subscriber Identification Number (msin). The msin is unique within the mnc, and the mnc is unique within the mcc. More on the IMSI/P-TMSI can be found in [8]

'Charging Identity'
To allow correlation of CDRs from the SGSN and GGSN for each session, the GGSN issues a Charging ID (C-ID) for each new PDP context. It includes this C-ID with the Context response to the requesting SGSN and the C-ID will be valid for the entire session, even if the mobile roams to a different SGSN during the session. A PDP Context may migrate between SGSNs, but cannot change GGSN. The Charging ID is unique within the scope of a particular GGSN over an extensive period of time (about 100 days), which makes the combination of a C-ID and the GGSN address globally unique over the same time period.
More on the Charging-ID can be found in chapter 5.8 of [9].

'Access Point Name Network/Operator Identifier' [8]
An Access Point Name (APN) is a reference to a GGSN. To support inter-PLMN roaming, the internal GPRS/UMTS DNS functionality is used to translate the APN into the IP address of the GGSN. The APN is composed of two parts as follows:
- The APN Network Identifier identifies to which external network the GGSN is connected to and optionally to a requested service by the MS. This part of the APN is mandatory. In order to guarantee uniqueness of APN Network Identifier within the GPRS/UMTS PLMN(s), an APN Network Identifier containing more than one label corresponds to an Internet domain name. This name should only be allocated by the PLMN to an organization that has officially reserved this name in the Internet domain. Other types of APN Network Identifiers are not guaranteed to be unique within the GPRS PLMN(s).
- The APN Operator Identifier, identifies in which PLMN GPRS backbone the GGSN is located. The APN Operator Identifier is composed of three labels. The last label shall be "gprs". The first and second labels together shall uniquely identify the GPRS PLMN, using the IMSI mcc and mnc codes in the format "mnc<MNC>.mcc<MCC>.gprs"

This is also explained in [3], chapter 14.4.

I.e. to retrieve the file 'http://www.utwente.nl/index.html', a PDP context setup request will reach the SGSN for APNNI www.utwente.nl. The SGSN will determine the appropriate GGSN and forward the request to that GGSN. The GGSN will query the internal DNS server, which will translate this Internet domain name into the corresponding IP address. The mobile either supplied its static IP address as source (PDP) address, or it is appointed one by the GGSN at this point. Once the PDP context is established, the mobile can send an HTTP GET request for file ~/index.html to the www.utwente.nl server through the PDP context with the GGSN.
For as long as the context exists and the packet filters allow, any consecutive traffic to and from the www.utwente.nl server can use this PDP context.

'List of Traffic Data Volumes' [9]
This list includes one or more containers, each with the following attributes:
- Data Volume Uplink/Downlink; number of transmitted octets during the period of this container
- Change Condition; reason of change for closing the container, such as 'tariff time change', 'change of QoS' or closing of the CDR.
- Change Time; time stamp of the moment of closing.

The first container and all containers created due to a 'change of QoS' will optionally have a 'QoS Requested' and 'QoS negotiated' field. Table 2 is an example of a container list caused by one QoS change and one tariff time change.

QoS Requested = QoS1 QoS Negotiated = QoS1	QoS Requested = QoS2 QoS Negotiated = QoS2	
Data Volume Uplink = 1 Data Volume Downlink = 2	Data Volume Uplink = 5 Data Volume Downlink = 6	Data Volume Uplink = 3 Data Volume Downlink = 4
Change Cond. = QoS change Time Stamp = TIME1	Change Cond. = Tariff change Time Stamp = TIME2	Change Cond. = Record close Time Stamp = TIME3

Table 2: Traffic Data Volume Container List Example

'Charging Characteristics'
The Charging Characteristics ('Annex A' of [9]) can be supplied by the HLR to the SGSN as part of the subscription information. The SGSN supports three default configuration types in case the HLR does not supply characteristics:

- The home default profile for subscribers of the SGSNs PLMN
- The visiting default profile for visitors using a GGSN belonging to the same PLMN
- The roaming default profile for visitors using a GGSN belonging to the visitors home PLMN

Optionally the SGSN may support several visiting and roaming default charging profiles based on the MNC/MCC combination of the subscriber. In case of non-home subscribers, the SGSN can be configured to apply the charging characteristics of the subscriber's home HLR, if received, or to apply one of the three default configurations mentioned above.
If the SGSN does receive HLR characteristics, it forwards them with the PDP context setup request to the GGSN, even if it has ignored them itself. The GGSN will also apply charging characteristics to the PDP context; either the SGSN supplied parameters or its own pre-configured set for the home, visited or roaming case. If the GGSN does not receive the charging characteristics through the SGSN, it assumes the MS is 'not-subscribed'. In this way forwarding of the charging characteristics is implicitly denoting a subscriber to the home domain.
The charging characteristics contain Profile information and Behavioral information bits. The first identify which Charging Characteristics Profile is applicable for the particular subscriber and the second can be freely assigned by operators for particular charging behaviors. The Profiles can also be defined by the operator and consist of information on when to send CDRs (e.g. time limit, volume limit) as well as an optional field of the preferred CGF address.

'External Charging Identifier'
A Charging Identifier received from a non-GPRS/UMTS, external network entity. When inter-working with an IP Multimedia Subsystem (IMS) this is the IMS Charging Identifier as received from the IMS network by the GGSN. The IMS system is still subject to standardization by the 3GPP.

'RNC Unsent Downlink Volume'
The SGSN counts the number of octets in the payload of all packets sent on the downlink to the mobile. Upon PDP activation the SGSN can request the RNC in the UTRAN to count packets that didn't make it to the mobile over the radio interface and that were subsequently discarded. For instance packets that are still buffered in the RNC upon release of the Radio Access Bearer (RAB, radio channel) due to roaming are possibly counted twice by the SGSN, which causes overcharging. On RAB release, the RNC sends the Unsent Downlink Volume to the SGSN, which can include it in the S-CDR. Due to high implications on the RNC the standardizations prohibit a SGSN to request intermediate packet counts from the RNC. It is unclear how distinctions are made in unsent packet counts with respect to tariff changes during the PDP context.

This concludes this subchapter on the accounting system within UMTS networks. The next subchapter describes several accounting architectures that can operate in WLAN networks.

4.2. WLAN Accounting Architecture

Several initiatives have been undertaken to allow accounting in IP-based networks. The main challenge is the metering process of data quantity per subscriber. Due to the high data rates, much higher than in UMTS, the amount of processing power required for fully metering all simultaneous data through nodes is substantial. Therefore, the first commercial WLAN networks often relied on time-based accounting. Since WLAN is based on best-effort transmission techniques, QoS support has proven to be a great obstacle for WLAN operators. The more subscribers that access a WLAN network simultaneously, the more the transmission service degrades and the accounting overhead increases.
Some major parties are promoting the RADIUS standard as the accounting system for WLAN, for instance Microsoft [10]. Therefore RADIUS accounting is presented first. Diameter is the successor of RADIUS and some of the differences are also discussed. The article recommends SNMP MIB support for common management, and since a MIB is also a commonly adopted method of metering, it is included in this research.

4.2.1. RADIUS

Subchapter 3.2 already mentioned the Authentication function in a WLAN network. The Remote Authentication Dial In User Service (RADIUS) combines Authentication, Authorization and Accounting services for data networks and works in combination with a Network Access Server (NAS). The NAS facilitates a data session for the subscriber and maintains accounting information on that session. The RADIUS receives the accounting information from the NAS for consolidation.

Accounting functionality within RADIUS is specified in a RfC 2866 [11]. RADIUS Accounting works in a client/server model with ‘request’ and ‘response’ messages. The document [11] mainly describes these messages, that are exchanged between the RADIUS (server) and the NAS (client) or another RADIUS (either in client or server mode). A number of attributes can be sent with either the request message or the response message. A basic set of attribute formats have been described, and ‘new attributes can be added without disturbing existing implementations of the protocol’. The basic set of RADIUS attributes is:

- Acct-Status-Type
- Acct-Delay-Time
- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Session-Id
- Acct-Authentic
- Acct-Session-Time
- Acct-Input-Packets
- Acct-Output-Packets
- Acct-Terminate-Cause
- Acct-Multi-Session-Id
- Acct-Link-Count

A message is either a request or response and contains zero or more attributes. Response messages do not contain any basic attributes other than those used for proxy status (unspecified), and can optionally carry vendor-specific attributes. RADIUS accounting messages are only sent at the beginning or at the end of a subscriber session and not during a subscriber session.

'Acct-Status-Type'
This attribute indicates whether an Accounting-Request marks the beginning of the subscriber service (Start) or the end (Stop).

'Acct-Delay-Time'
This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.)

'Acct-Input-Octets'
This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop (i.e. at the end of the subscriber session).

'Acct-Output-Octets'
This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

'Acct-Session-Id'
This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session must have the same Acct-Session-Id. An Accounting-Request packet must have an Acct-Session-Id. An Access-Request packet may have an Acct-Session-Id; if it does, then the NAS must use the same Acct-Session-Id in the Accounting-Request packets for that session.

'Acct-Authentic'
This attribute may be included in an Accounting-Request to indicate how the subscriber was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Subscribers who are delivered service without being authenticated should not generate Accounting records.

'Acct-Session-Time'
This attribute indicates how many seconds the subscriber has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

'Acct-Input-Packets'
This attribute indicates how many packets have been received from the port over the course of this service being provided to a subscriber ('Framed User'), and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

'Acct-Output-Packets'
This attribute indicates how many packets have been sent to the port in the course of delivering this service to a subscriber ('Framed User'), and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

'Acct-Terminate-Cause'
This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

'Acct-Multi-Session-Id'
This attribute is a unique Accounting ID to make it easy to link together multiple related sessions in a log file. Each session linked together would have a unique Acct-Session-Id but the same Acct-Multi-Session-Id.

'Acct-Link-Count'
This attribute gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated. The NAS may include the Acct-Link-Count attribute in any Accounting-Request which might have multiple links.

A session is described as:
'Each service provided by the NAS to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the NAS supports that, with each session generating a separate start and stop accounting record with its own Acct-Session-Id'. Therefore, the actual definition of a session depends on the type of NAS and can in principle be custom defined by the operator.

Concluding, RADIUS Accounting offers a simple method of transferring accounting information from the metering equipment to the accounting server after a subscriber session ends. The definition of what a subscriber session at the NAS constitutes is not specified. RADIUS supports volume-based accounting, the inclusion of a session ID and even a multi-session ID, but currently no QoS information is taken into account.

4.2.2. Diameter

Diameter is the successor of RADIUS and described as an Internet Draft working document in [12]. (This document is expected to change status to a RfC soon, since it has recently been approved by the IESG).
Diameter servers and clients must support the base protocol that includes accounting and this is backwards compatible with the RADIUS accounting protocol. The most important enhancements of Diameter over RADIUS are:

- Some Diameter accounting applications have been described and the (non-base protocol) Attribute-Value Pairs (AVP) of the Diameter messages of those applications have been standardized.
- Diameter clients or servers must implement the failover mechanism, which is a safeguard against loss of accounting information in case the peer party or the intermediate network fails. RADIUS does not have a failover mechanism.
- Diameter supports event-based accounting records, which are singular records. RADIUS only supported Start and Stop messages of events.
- Also, Diameter supports the sending of interim accounting records upon instruction of the authorization process. Interim accounting records contain cumulative accounting information for existing accounting sessions.
- Support for server-initiated messages in RADIUS is optional. This support is mandatory for Diameter.
- All Diameter accounting records must include a **Session ID** that is globally and eternally unique. Its mandatory part starts with the sender's identity (e.g. NAS) and is followed by a portion that the client can guarantee is eternally unique (e.g. time code + sequence number). Optionally, an implementation-specific value may be included. The Diameter entity that starts the accounting session constructs the Session ID. If a Diameter entity possesses a Subscriber ID, it must always be included in the accounting

record. A Diameter application may require multiple accounting sub-sessions. Such applications would send messages with a constant Session ID, but with a different Accounting Sub Session ID. A **sub-session** represents a distinct service provided to a given session. These services may happen concurrently or serially. Changes in sessions are tracked with the **Accounting-Sub-Session-Id**. Also, when sessions with a different Session ID need to be correlated, applications may use the Accounting-Sub-Session-Id for such correlation.
A **multi-session** represents a logical linking of several sessions and this link can be tracked by the **Acct-Multi-Session-Id**. The Acct-Multi-Session-Id is of the same format as the Session-Id. It must be used in all accounting messages for the given session(s).

- Diameter accounting records contain a record number that, in combination with the information whether a document is a Start, Interim or Stop record, shows how many accounting documents exist for a particular accounting session.
- Upon setup of an accounting session, the Diameter server can state whether real-time accounting is in effect, and what the client should do if the connection with the Diameter server is lost during the accounting session.

This concludes the description of the accounting aspects of the Diameter base protocol.

4.2.3. SNMP/the MIB

According to both [10] and [13], the Simple Network Management Protocol is a widely used protocol for management of distributed system elements. The latest version of SNMP is Version 3. It allows management of a system in a Manager-Agent structure. The Agent represents an entity inside or near the system that is being managed and it monitors the system and/or saves important information of managed objects. The Manager retrieves or receives information from the Agents and can take actions based on the received information. The information about managed objects is saved in a repository called a Management Information Base (MIB). The data inside the MIB has a tree structure and each branch has a structured Identifier. The Manager can retrieve or set information in the MIB by using the proper Identifier.

Meter-MIBs
MIBs can be used to do measurements in a network and are then called Meter-MIBs. The MIB has a list of rules to define measurements. The Manager can add a new measurement by first adding an entry to the rules list of the MIB. After that, it has to activate that rule in the MIB for as long as it wants the system to do the measurement. When desired, the Manager can retrieve the metered information from the MIB.

The investigation of SNMP and Meter-MIB in this thesis has been limited due to time restraints.

4.3. Content Provider Accounting

This subchapter deals with accounting processes that are common in Content Providers. By model definition, the Content Provider is not subject to transport accounting (which is the scope of this thesis), but is nevertheless discussed for completeness of the Broker model.

Section 2.3.1 listed the different types of Content Elements that Content Providers may supply. When there is a form of charging in effect, it is usually done by purchasing a login that allows access for a certain time period (pre-paid) or based on a subscription service (post-paid).
Pre-paid billing is often done by entering credit-card details over the web and the login information (username, password and website) is (e)mailed to the subscriber after successful charging of the credit card. The login/password combination is blocked after the usage period expired, or when the maximum number of logins is reached. For example, a lot of digital erotic content has been made available in this way since the beginning, using credit-card information.
One widely spread example of a subscription service is online banking. This allows subscribers to view and control their bank accounts from anywhere over the Internet. Subscribers are often given a device for security measures that facilitates the authorization process based on a challenge-response exchange at the login process. The charges for the subscription to online banking can be taken directly out of the bank account of the subscriber, since the supplier of the Content Element also controls (part of) the subscriber's financial resources.

Concluding, there is no single accounting system in effect when it comes to Content Providers, but the dominant form of Billing has been through credit-cards.

4.4. Accounting Information Exchange Protocols

Accounting systems are often shielded from the outside world because they contain all the valuable information that generates revenue. Since some interaction between accounting systems of different BADs is necessary, for instance in roaming situations, BAD stakeholders allow accounting information exchange in a controlled manner. Internal accounting record formats are transformed into special accounting exchange records to conceal the inner network structure of the BAD from competition. This subchapter looks at three exchange protocols. In conformance with the general order of presentation in this thesis, the Transferred Account Procedure (TAP) exchange protocol for GSM/UMTS is regarded first. It is followed by IPDR which is developed more for general data networks. The third exchange protocol under investigation is the newly developed mobile eXchange Protocol (MXP), which is said to be specifically for mobile internet and m-Commerce inter-company billing exchange.
TAP and IPDR are open standards (free to use), while using MXP requires an annual subscription from the publishers of the protocol.

4.4.1. Transferred Account Procedure (TAP)

The most recent version of TAP that is in use between GSM/UMTS operators is TAP3. The article [14] explains the operational field of TAP3 in GSM networks. The article states:
'TAP3 is used for billing between GSM to GSM Operators, GSM to non-GSM Operators (supporting Inter-Standard Roaming) and GSM to Satellite Operators. From November 2001 it will also support billing between GSM Operators and their Service Providers and in the future will be developed to support billing between Non-GSM-to-Non-GSM Operators.'
It also mentions that TAP3 can be used for data traffic, but that this must be further developed 'when GPRS becomes more popular'. The latest version of the protocol shows only minor changes to the version at the time of writing of the article on this point, according to the author of the article in a personal response.
Value Added Services, billing for content and Customized Application Mobile Enhanced Logic (CAMEL) services are also listed to be included in TAP3.
TAP3 supports the Inter Operator Tariff (IOT) Charging Principles, which allow inclusion of price information in TAP3 records e.g. transaction costs and applied discounts. Since April 2001 TAP3 also supports a 'Reject and Return policy', which allows an operator to return faulty TAP3 record parts to the originator and to process correct records in a timely manner.

The statements in the article can be verified in the TAP3 standardization document [15]. The TAP3 record item terminology is mostly the same as the terminology used for CDRs, which is explained in section 4.1.2 and Appendix A of this thesis. The standardization document is built up in a branched type structure, beginning with the top level group 'Data Interchange'.

The relevant sub-branches will be listed below with the corresponding section number mentioned between brackets. If only one or some sub branches are of interest, they are mentioned after the label of a branch. A * following the label of a branch denotes that that branch is not further explored.

The Data Interchange (3.1) contains a Notification branch and a Transfer Batch branch, of which only the latter is of interest. The Transfer Batch (3.2) contains a number of branches, including:

- 'Batch Control Information' *
- 'Accounting Information' (3.4) : Taxation, (Applied) Discounting, Currency Conversion *
- 'Network Information' : Recording Entity Information *
- 'Call Event Details'

'Call Event Details' contains **only one type of** the following relevant branch types. A record may hold multiple instances of that type in a batch though.

- 'Mobile Originated/Terminated Call' *
- 'Supplementary Service Event (3.17)' : Supplementary Service Used (3.11 : Third Party Information, Charge Information (3.10)) *
- 'Value Added Service' (3.19): VAS Used, (GSM) Chargeable Subscriber *
- 'GPRS Call'
- 'Content Transaction'

Summarizing before continuing, a TAP3 record contains one or several Call Event Details. A Call Event Detail describes a single event in a specific event description. The descriptions 'GPRS Call' and 'Content Transaction' are relevant for this thesis and will subsequently be regarded:

GPRS Call

A 'GPRS CALL' (3.20) holds the following relevant branches:

- 'GPRS Basic Call Information'
- 'CAMEL Service Used' *
- 'GPRS Location Information' *
- 'GPRS Service Used'

- The 'GPRS Basic Call Information' (3.21) contains:
  - 'GPRS Chargeable Subscriber' : Chargeable Subscriber, PDP type, PDP address, Charging Characteristics *
  - 'GPRS Destination' : Access Point Name NI/OI, remote PDP address *
  - 'Call Event Start Timestamp' *
  - 'Total Call Event Duration' *
  - 'Network Initiated PDP Context' *
  - 'Charging ID' *

The 'GPRS Service Used' (3.22) contains:

- 'GPRS Service Usage' : GPRS usage Timestamp, QoS requested/used, Data Volume Incoming, Data Volume Outgoing *
- 'Charge Information' (3.10) : Call Type Group, Charge Detail (type, units), Tax Information, Discount Information *

Content Transaction

A 'Content Transaction' (3.24) holds the following relevant branches:

- 'Charged Party Information' *
- 'Serving Parties Information' : Content Provider, Internet Service provider, Network *
- 'Content Service Used'

The 'Content Service Used' (3.27) contains:

- multiple transaction descriptions *
- 'Transaction Identifier' *
- 'Data Volume Incoming' *
- 'Data Volume Outgoing' *
- 'Charge Information' (3.10) *

In conclusion, this section has compared the statements from the article [14] with the TAP3 specification. The accounting elements of interest for this thesis concerning TAP3 have also been identified within the TAP3 specification. The following section presents a similar investigation of IPDR accounting exchange

4.4.2. Internet Protocol Detail Record (IPDR)

The name Internet Protocol Detail Record is actually derived from the Charging Data Record (CDR) that is used in GSM/UMTS networks. A number of documents have been published for IPDR of which [16] is the most important one. It describes the IPDR reference model and how it relates to the Telecommunication Management Forum's (TMF) telecommunication operation map (TOM), which is a well-known and accepted organizational model of telecommunication operations business. The Network Data Management (NDM) component of the TOM is primarily under investigation of IPDR. It is named the NDM-Usage (or NDM-U) within IPDR and a reference model is shown in Figure 4-3.

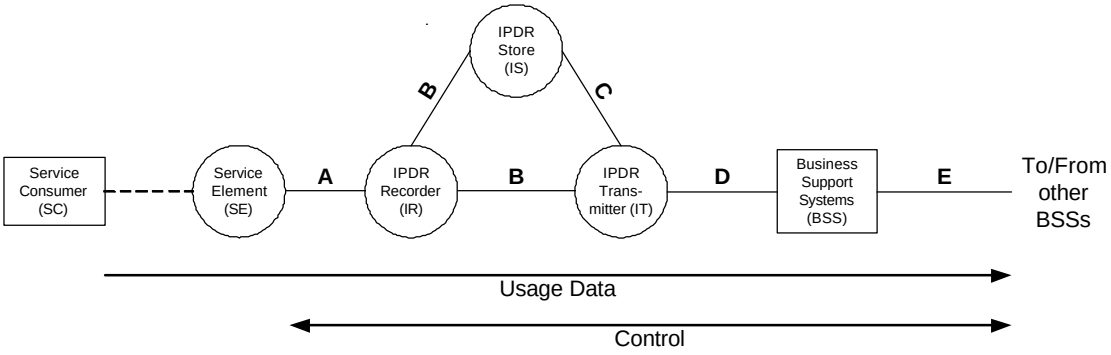

Figure 4-3: NDM-U Reference Model

The reference model has the following nodes:

- A Service Consumer (SC), which can request one or several Service Elements.
- A Service Element (SE), which is a set of equipment and software that provides a valuable service to SCs. The IPDR reference model applies to any type of Service Element that is capable of generating accountable usage records.
- An IPDR Recorder (IR) has two functions; mediation of proprietary protocols and data transactions from a SE, and producing IPDRs of that data. IPDR Recorder packages usage information from one or several SEs into IPDRs and forwards them to an IPDR Store/Transmitter.
- An IPDR Store (IS) stores IPDR-records in non-volatile memory and also provides a repository function for IPDR Documents (IPDRDocs).

- An IPDR Transmitter (IT) transforms IPDRs from either an IS or an IR into IPDRDocs, organizes the IPDRDocs into Groups of each service type, and delivers IPDRDocs from Groups to one or more Business Support Systems by using one of a set of transfer protocols.

The standardization document describes the interfaces A until E. From those, the D interface is also completely specified. Work in progress is the investigation of the interfaces A and E, where A deals with the collection of metering data and E deals with the exchange of IPDRDocs between Business Support Systems. The interface A transfers the metering data in an unrestrained form and this form could be Script-MIB data, CDR data, or any vendor-specific form. The IR in a Script-MIB environment would be considered the 'Manager' (section 4.2.3) and in an UMTS environment it would be the Charging Gateway Function (subchapter 4.1).
IPDR Documents are defined in XML and contain one or several IPDRs. An IPDR may in principle be any record that is specified in XML and conforms to the general format of [16]. Some IPDRs have been designed and published for specific purposes like Voice over IP and email, but in principle anyone can construct an IPDR document in XML to be used in a particular system. This makes IPDR a very flexible method of exchanging accounting information. Unlike TAP3, a closer look at the information that an IPDR contains is unnecessary, because of the liberty to construct IPDRs in any desired format.

4.4.3. Mobile eXchange Protocol (MXP)

The MXP is a recent initiative of the Cibernet Corporation, which is a wholly owned subsidiary of Cellular Telecommunications & Internet Association (CTIA) according to the article [17]. The CTIA is known for developing the accounting exchange protocol CIBER, which is a commonly used standard between mobile operators in mostly North America. The CTIA recognized that mobile operators often support more than one air interface and network architecture as well as IP based services. Traditionally, accounting systems were developed from a network perspective, rather than from a Billing perspective. With the development of MXP comes an accounting exchange protocol that incorporates labels for all standard network, equipment, subscriber and service identifiers. "The important thing to distinguish MXP from any other usage record is the intention to execute the business relationship based on predefined terms and rates with revenue sharing as a goal." The protocol supports standardized naming conventions, but does not dictate any particular business model. Three record types are denoted in MXP: service, aggregate and reject types. The service records describe customer-specific records. Aggregate records provide a means to exchange non-customer specific usage. Reject records are sent in response to non-acceptable service or aggregate records. The usefulness of aggregate records can be exemplified by considering that a particular Content Provider could possibly not be interested in the subscriber details for its wireless service. The CP would rather compare the total amount of times it provisioned the service to subscribers of a wireless network with the count from the network operator and clear those service instances as a whole instead of separately.
On a final note, apparently there have been ongoing negotiations between Cibernet and the IPDR organization because both systems would be complementary. Both protocols support more than wireless networks alone, but the IPDR organization has difficulties in dealing with exchange between business systems (the 'E interface' of IPDR) due to their focus on the delivery from the infrastructure rather than between back-office systems.

Though the MXP is not an open standard, these statements can be compared to the product description [18]. MXP has been described in XML, just as IPDR. Singular records are called 'messages', while documents containing multiple records are called 'envelopes'. The proposed means of exchanging messages and envelopes is secure FTP (or CD-ROMs in case of unavailability of FTP) within the standard MXP age limits, but bilaterally agreements on this are encouraged.

Figure 4-4 shows a graphic representation of the basic MXP record structure as presented in the standardization document [18]. Each MXP file contains two sections that summarize the MXP records: the Transmission Information section and the Audit Information section.

- The Transmission Information section contains Sender, Receiver information, as well as unique Identification numbers (575,999,424 unique record identification numbers each day for any given sender/receiver pair.
- The Audit Information section records the number of records and the total charges of the MXP file. For Envelopes, this will be the total of all MXP record sections. For Messages, this will be the total for the MXP record in the file.

Each MXP record is either a Service type, Aggregate type or Reject type.

- Service type records contain billing exchange details for a subscriber service. This category supports TAP3 and CIBER record types, but also includes other service types for which settlement is expected (i.e. digital content, data network usage, m-commerce, micro payment, SMS/MMS, or credit transactions).
- Aggregate record types support bulk billing details between entities into a single record without subscriber-specific information.
- Reject type records allow the return of Service and Aggregate Records for invalid data or disputed charges. The default is to return the record for the total amount of the charge, though partial credits are also allowed. A partner may use partial credits, for example, when a service is provided at a lower quality of service than stipulated in the business agreement. The whole MXP file is returned and additional fields indicate the reason of rejection (e.g. non-conformance of the file to the agreed MXP record format).

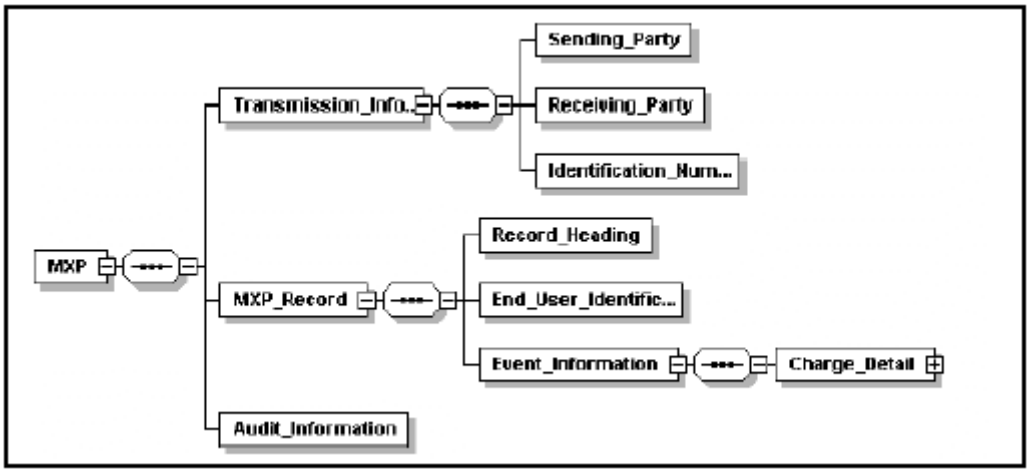

Figure 4-4 Basic MXP Structure

Every MXP record starts with a Record Heading. The Record Heading contains information specific to a given record within the envelope such as record type, charge information, offsets, and start dates for the given record. In case of a partial record, the sender has the option to populate a Link ID that allows all partial records to be linked together more easily at the destination. This assists the receiver in reconstructing all of the applicable session or call information. Also the total charges and taxation may be included here.
Service type records also include an End User Information section. Aggregate records do not include this field. The End User Information section includes information about the subscriber who initiated or received the services. This information may include the IP address, MIN or the IMSI, as well as the equipment identifier for the wireless device utilized by the subscriber.
The Event Information of the MXP record contains one or several Event Type (e.g. Mobile Originated Voice, Packet Data), Charge Type (e.g. Air, Incoming Packets, Total Packets) and Rate Element (e.g. duration based, volume based). Partial records may omit one or several of these fields as long as all information is present in at least one of the partial records. The Link ID aids in correlating partial records.

Concluding, the MXP accounting exchange structure adds functionality to current exchange protocols by supporting their original record formats. On top of that it allows wholesale accounting information exchanges, in case individual subscriber information is irrelevant to the receiving party. Since the standard is relatively new and disclosed (not an open standard) it is difficult to predict if MXP is the answer to the issues of multi-domain accounting. No information has been found on which parties have adopted MXP, nor how they value using MXP. The different approach does make MXP an interesting protocol.

5. Design of a Multi-domain Accounting architecture

The previous chapters have described UMTS and WLAN as Transport Provider systems and their accounting architectures. Also a model for Content Providers and some available accounting information exchange protocols have been described. This chapter proposes an architecture which allows multi-domain service provisioning and multi-domain accounting for the Broker model.

5.1. Analysis

Chapter 2 described the choices of using the Broker model for both the service provisioning architecture as the accounting architecture. The separation of transport and content provisioning combined with the choice of accumulating the multi-domain accounting information at the Broker leads to the conclusion that each provider must transfer their part of the accounting information to the Broker. As a result, transport accounting records do not contain indication information of the provided content component and vice versa.
To come to a multi-domain accounting architecture in which transport components can be linked to one particular content component, two requirements must be discussed:

Firstly, a transport accounting record must reflect transport resources used for only one content component, despite the fact that the transport network has no knowledge of content component provisioning information. If this requirement is not met and the record contains mixed information on several transport components, the Broker is unable to untangle the transport accounting information for each content component.

Secondly, the Broker must have information that allows identification of each transport component accounting record, in order to determine to which content component the record belongs. Such correlation information could be maintained at a central point, or could be distributed amongst the components and presented to the Broker when correlation takes place. The latter case implies that component accounting records hold enough multi-domain accounting information for the Broker to correlate records from different providers without any prior administration. This is impossible for the combination of the following two reasons: a) it was stated above that providers do not have indicative information on correlated components from other providers. Such information can only be included in component records if it is sent by a party that does maintain correlation information, but b) this case stated that the Broker does not maintain such correlation information. These two reasons show that if the Broker does not maintain correlation information, and the providers do not maintain it, it is obvious that correlation cannot take place. As a result of this reasoning, it is required that the Broker is the central point for maintaining correlation information.

These requirements of having each accounting record describe one component and having the Broker maintain the correlation information form the basis of the architecture description in this chapter.

Correlation information management
As described in the previous paragraph, the Broker needs to maintain information on the association between transport components and content component. This paragraph describes the way correlation information will be managed in the accounting architecture proposal.

Section 2.3.2 defined that the composition of all correlated session components is called a super session. To distinguish multiple super sessions within the Broker domain, they shall be denoted by a unique **Super Session IDentity** (**SSID**). Subsequently, to distinguish multiple session components within one super session, they shall be denoted by a unique **Session Component IDentity** (**SCID**). The Broker shall register for each of its subscribers each SSID upon the start of a super session and list all SCIDs of added components in a Profile. For coherent administration, the Broker must maintain the status of every component. A SCID is defined to be 'open' while the session component is active and 'closed' when the session component is terminated. Section 2.3.2 described how a super session life cycle starts and ends with the content component life cycle, which ensures that super sessions always have active components in their session life cycle. This shows the importance of maintaining component statuses, since the decision of commencing correlated accumulation can be based upon the notice that all SCIDs of a particular SSID are 'closed'.
The Broker also needs to register every incoming component accounting record within the proper Profile, within the proper super session for the proper SCID. A super session is ready for correlated accumulation as soon as all the SCID accounting records for a closed super session are received.

A situation may occur where a component accounting record will not be received by the Broker. Such a failure disrupts the correlated accumulation process, since the accumulated information shall not be presented to the Charging stage before all component accounting records are received. Some countermeasures can be conceived, for instance a deadline for component providers to send their accounting records to the Broker after closure of the super session, but such a failure policy is considered outside the scope of this research. It is assumed that all component accounting records arrive at the Broker with an acceptable delay.

The previous description assumed that incoming component accounting records can be linked to the corresponding SCID. This is not automatically achieved. Since it was assumed in the beginning of this subchapter that component providers do not include distributed multi-domain accounting information in their accounting records, some element in the record must bridge the component accounting information to the correlation information. This can only be achieved when this element has previously been shared between the Broker and the component provider. Two solutions were considered to counter this sharing issue:

1. A session component provider constructs and passes on a 'component ID' to the Broker at the beginning of the component provisioning procedure. This 'component ID' can be network type specific. When the 'component ID' is exchanged during the setup procedure of a component, it can be combined with the SCID when the SCID is created at the Broker. The SCID and the 'component ID' can then be added to the Profile simultaneously.
   It would be impossible to use the 'component ID' directly in the SSID, since such an ID is network type specific and thus not guaranteed to be unique in the Broker domain.

2. The Broker constructs the SCID and passes it on to the component provider at the start of the component provisioning. The component accounting records must then include the SCID. Subchapter 4.4 showed that the three accounting exchange protocols allow inclusion of 'external charging identifiers' like the SCID. Additionally, inclusion is also allowed in the UMTS accounting system (section 4.1.2) while the WLAN accounting systems do not exclude the addition of extra information such as a SCID in the accounting records.

The choice in this research is to follow solution 2, considering that having one less conversion step (from component ID to SCID) and less identifier information in the Profile (only SSID and SCID instead of SSID, SCID and 'component ID') simplifies the description of the correlation information management at the Broker. This implies that it is up to the transport network to include the SCID that is issued at the start of the component provisioning in the corresponding accounting record(s) for that component.

Subscriber Identity
Subscribers in the UMTS transport network are identified by their International Mobile Subscriber Identity (IMSI) or Packet Temporary Mobile Subscriber Identity (P-TMSI) in UMTS accounting according to section 4.1.2. In WLAN this identification is done by MAC address or login name. It goes beyond saying that it must be clear to each party at any time which subscriber is targeted in accounting records for proper billing. Two possible approaches have been considered with the Broker model in mind. Either one unambiguous naming convention should be adopted throughout all parties (a 'Global User Identity'), or one or multiple name translations must take place between parties. In [8], section 13 'Numbering, addressing and identification within the IP multimedia core network subsystem' this issue is addressed and it formats a temporary private or public identity for a subscriber based on the IMSI.

Though identity issues are very relevant in the field of seamless roaming and accounting, it will not be addressed further in this research thesis. It is assumed that either a unique identity exists, or that the Broker holds separate appropriate aliases for its subscribers for each different transport network type. The identity of the subscriber will henceforth only be referred to as the Subscriber Identity (SID).

Summary
The Broker maintains correlation information in a Profile, by registering a SSID for each super session. Components that are added to a super session are given a SCID, which is registered to the SSID in the Profile. The Broker maintains both the provisioning status of each session component as well as the corresponding accounting records reception status. The Broker starts correlated accumulation for a super session when all session components are closed and all accounting records have been received. The consequences of the failure of reception of one component accounting record for the correlated accumulation of the other records is not regarded. Each accounting record may only contain information on one session component and the SCID that was issued by the Broker at the start of the session component provisioning must be included.
Subscriber identification is assumed to be consistent across the different domains and subscribers will be addressed by a SID in the multi-domain accounting architecture.

5.2. General description of the multi-domain accounting architecture design

To come to the design of the multi-domain Accounting architecture, a general overview is presented in this subchapter. First, a description is given for the general functions of the Broker. Subsequently the interfaces between the parties of the Broker model are presented and the way of requesting content by the subscriber is discussed. The combined functionality will be described at the end of this subchapter.

5.2.1. Broker functions

Subchapter 5.1 emphasized that the Broker has to maintain the accounting correlation information to be able to properly accumulate component accounting records. The correlation is accomplished by inserting SCIDs in component accounting records and by registering the records that have been received in the Profile. The creation, registration and distribution of SCIDs occur upon the start of a session component. As a result, the design of the Broker will be split in two parts. There will be Session Identity Management (SIM) for distributing SCIDs and there will be Accounting Records Management (ARM) for correlated accumulation, depicted in Figure 5-1. The SIM involves session management and communicates with the session management part of the component providers. The ARM communicates with the accounting management part of the component providers.

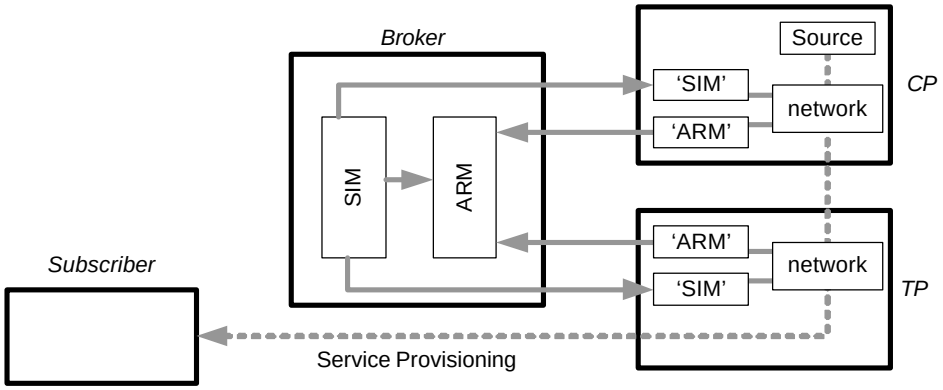

Figure 5-1: Session Identity Management and Accounting Record Management functions

The paragraph 'Correlation information management' of subchapter 5.1 emphasized that the SSIDs and SCIDs will be listed in a Profile. Since both the SIM and ARM use Profile information, it is chosen to split the Profile information in a Subscriber Profile at the SIM and a Super Session Profile at the ARM.

- The Subscriber Profile shall maintain session management information of super sessions and session components during the Super Session life cycle (see also section 2.3.2).
- The Super Session Profile shall maintain information on received component accounting records and is used to determine when a super session is ready for correlated accumulation.

To determine when a super session is ready for correlated accumulation, the Super Session Profile needs information from the Subscriber Profile on

- which super sessions are issued and to which subscriber they belong
- which SCIDs are issued for the super session
- when a super session is closed, since this means that no additional SCIDs will be added

It is chosen that the SIM function must send notification messages to the ARM function on these events to keep super session information consistent in the Subscriber Profile and the Super Session Profile.

On a final note, both functions SIM and ARM used in this thesis for multi-domain accounting are considered to be included in a new defined function referred to in this thesis as the '**Open Connectivity Control Function**' (OCCF). Provider-specific OCCF elements are referred to as the 'Broker OCCF', the 'CP OCCF' and the 'TP OCCF'.

5.2.2. Interface definitions

To structure the multi-domain architecture design description, the various communication interfaces between functions are given an index. The detailed design description in coming subchapters defines exactly which sub-functions within the SIM, the ARM and the provider functions communicate over these interfaces. A general description suffices at this point.

A. Interface A handles registration of the subscribers at transport networks. As soon as a subscriber tries to access a transport network, the Broker will authenticate the subscriber for the network over this interface. This is a form of session management and therefore it is included in the SIM function at the Broker.

B. Interface B connects the SIM function at the Broker to the transport networks and it handles transport session component management. This includes passing the SCID to the transport network along with the transport session component setup.

C. Interface C represents the communications between the subscriber and the Broker. A transport network needs to facilitate this Interface. The subscriber negotiates service provisioning, such as the ordering of content over this interface with the Broker. Alternatively, this interface shall also be called the 'Home Broker Session'.

D. Interface D connects the SIM function at the Broker to the content provider networks and it handles content session component management. This includes passing the SCID to the Content Provider along with the content session component setup.

E. Interface E is used for transferring accounting records from the component providers to the Broker. Both the TPs and the CPs send records to the ARM at the Broker in the same manner and therefore it is chosen that one Interface represents these exchanges.

F. Interface F represents the interaction between the subscribers's mobile and the serving transport network. This includes presenting registration information, upload and download of data packets and all other regular transport network interactions as for instance described in chapter 3.

Since the data communications between the TP and CP during content delivery do not carry anything other than the content data packets, they are not considered to be a separate interface.

5.2.3. Content Identity

Super sessions consist of a single content component and one or several transport components, as described in the paragraph 'Component absence' of section 2.3.2. This implies that the subscriber must be able to communicate to the Broker for each particular content element it desires. The communication channel has previously been defined as Interface C, or alternatively the 'Home Broker Session'. The way of specifying a particular content element is considered outside the scope of this research, since it does not directly involves accounting management. This problem is similar to the problem of the subscriber identity, addressed in subchapter 5.1. For the design in this thesis, it is assumed that every content element has a unique identity called the **Content Identity** (CID). For instance, this could be an electronic tag that can be downloaded by the subscriber from a CP web page. The tag holds particular information to allow the Broker to determine which content element the subscriber requests from a CP when the Broker receives this tag over the Home Broker Session. This assumption suffices for the description of the multi-domain accounting architecture and extra considerations on the acquisition and use of the CID are presented in the Intermezzo section of Chapter 8.

5.2.4. Expected behavior of the OCCF

The expected behavior of the OCCF is described here as a goal. Chapter 8 contains three examples that show that the OCCF operates according to the expectations. Each of the following three examples shows a different usage scenario:

Example 1: A mobile is registered at a UMTS network and establishes a Home Broker Session to the Broker. The subscriber acquires a Content ID and passes it on to the Broker to order. The Broker subsequently sets up the delivery. After termination of delivery, all partial accounting records flow to the Broker where they are correlated and passed on to the Billing System.

Example 2: Under the same initial assumptions and actions as Example 1, the subscriber receives the ordered content element. During delivery, the wireless connection is lost and the mobile registers at a different UMTS network. The delivery continues and after termination of delivery, all component accounting records are sent to the Broker where they are correlated and passed on to the Billing System.

Example 3: Under the same initial assumptions and actions as Examples 1 and 2, the subscriber receives the ordered content element. During delivery, the mobile also registers at a WLAN network. The Broker initiates the redirection of delivery from the UMTS network to the WLAN network. As soon as the UMTS transport component is terminated, its accounting records are transferred to the Broker. After termination of delivery, the remaining accounting records at the CP and WLAN TP are sent to the Broker where they are correlated and passed on to the Billing System.

The Home Broker Session
The Home Broker Session is vital for the subscriber for communicating with the Broker. It is therefore expected that the subscriber/mobile initiates a Home Broker Session to the Broker as soon as it registers at a transport network.
The Home Broker Session shall be accounted at the TP as a transport component. No content can be transported over the Home Broker Session after establishment, since the transport accounting record would reflect both the subscriber to Broker traffic as the content traffic and this is not allowed according to section 2.3.2.

Therefore two types of super sessions are expected: those who start with a transport session component and those who start with a content session component. For either type, only transport components can be added to the super session.

Multi-domain service setup
It is expected that when the subscriber sends a CID to the Broker, the Broker will create a super session for this request. This corresponds to the Super Session Invocation described in section 2.3.2. The super session is given a SSID, to be registered at the Subscriber Profile in the SIM and the Super Session Profile at the ARM. Subsequently, the Broker will first set up the content session component. A SCID is created at the Broker, included in the Subscriber Profile and sent to the CP together with the content component Session Invocation. The CP configures its system for delivery of the content element and then confirms the content component invocation to the Broker. The next step for the Broker is to set up a transport component and a SCID is created and registered for this component. The Broker sends a transport component Session Invocation to the TP, which includes the SCID for the transport component. The TP configures the transport network to facilitate the transport component and then confirms the transport component invocation to the Broker. The Broker then activates the content component by sending an activation message to the CP, after which the delivery takes place.

As a result of the multi-domain provisioning, component accounting records are sent to the Broker over the E Interface during and after the super session life cycle. Every component accounting record shall be stored by the Broker when it is received and the SCID of that record shall be retrieved from the record. The Broker must register the reception of the accounting record at the Super Session Profile by using the SCID. In the case that both the super session is closed and all the component accounting records are received must the Broker commence with correlating the stored component accounting records for that super session.

Roaming
When during a super session the subscriber changes its TP, the Broker must create a clone transport component at the new transport network. Alternatively, when a subscriber is registered at multiple transport networks, the Broker may decide to move the transport component to another network by creating a clone transport component at the new network. The term 'clone' means that the transportation properties (source, destination, QoS etc.) must be the same as the original transport component (or at least appropriate for the super session), but with a new SCID. The new SCID must be registered at both the Subscriber Profile and the Super Session Profile with the corresponding (existing) SSID.

As a result of roaming, the ARM function shall receive multiple transport component accounting records, each with a unique SCID.

5.3. Detailed description of the multi-domain accounting architecture design: Sub-function and Interface definition of the OCCF

The sections in this subchapter identify the sub-functions of the Broker-, TP- and CP OCCF. The Interfaces listed in section 5.2.2 are linked to these sub-functions. The relationships and interworking between the sub-functions are not discussed here, but rather in the next subchapters.

5.3.1. Sub-function definition

Broker OCCF SIM sub-functions
Four sub-functions can be identified from the functional description in the previous subchapters that deal with Super Session Management at the Broker. The most important section is 5.2.4, which described the expected behavior of the service session management. The sub-functions fall under the responsibility of the SIM function of the Broker OCCF, and their interworking shall be discussed in subchapter 5.4.

- Content component management: The SIM function must be able to receive content requests from the subscriber and subsequently negotiate the delivery with the CP. The sub-function that manages content requests on behalf of the subscriber shall be named the **Client Session Manager** (CSM).

- Transport component management: The SIM function must be able to request transport component setup and termination with the TP. The sub-function that manages transport components shall be named the **Network Session Manager** (NSM).

- Subscriber Profile management: The SIM function must be able to create and register SSIDs and SCIDs in a Subscriber Profile. Additionally, the ARM function must be notified of the creation of and the additions to the super sessions. The sub-function that manages the Subscriber Profile and the ARM notifications shall be named the **Subscriber Profile Manager** (SPM).

- Network registration: The SIM function must also be able to support registration procedures at transport networks. The sub-function that manages transport network registration shall be named the **Network Registration Manager** (NRM).

Broker OCCF ARM sub-functions
Four sub-functions can be identified from the functional description in the previous subchapters that deal with Accounting Management at the Broker.
The most important section is 5.2.4, which described the expected behavior of the component accounting management. The sub-functions fall under the responsibility of the ARM function of the Broker OCCF, and their interworking shall be discussed in subchapter 5.4. Please note that transport accounting records have previously been abbreviated as CDRs (Charging Data Records).

- Incoming record management: The ARM function must be able to receive component accounting records and retrieve the SCID from those records. The sub-function that manages record reception and SCID retrieval shall be named the **CDR Receiver** (CDR-R).

- Session component identity management: The ARM function must be able to receive notifications from the SIM SPM sub-function on the creation and active status of SSIDs and the creation of SCIDs. Additionally, the ARM function must be able to register which component accounting records have been received. The sub-function that manages such SSID and SCID information at the ARM function shall be named the **CDR Profile Manager** (CDR-PM).

- Record storage: The SIM function must be able to store the received component accounting records until the moment of correlated accounting. The sub-function that manages record storage shall be named the **CDR Store** (CDR-S).

- Correlated accumulation: The SIM function must combine the component accounting records when the super session is terminated and all accounting records have been received. The correlated accounting information must be presented to the Charging stage. The sub-function that manages the correlation shall be named the **CDR Processor** (CDR-P).

TP OCCF sub-functions
The TP OCCF is situated at the transport network. The TP OCCF sub-functions are described in detail in subchapter 5.5.

Two sub-functions can be identified from the functional description in the previous subchapters that deal with transport component management at the Broker and two other sub-functions are presented here.

- Transport component management: The TP OCCF must be able to receive transport component setup and termination requests from the Broker. Additionally it must be able to request a SCID from the Broker as a result of a request from the mobile, for instance upon setup of the Home Broker. Session. The sub-function that manages the exchange of these requests shall be named the **Network Session Control** (NSC)

- Accounting record management: The TP OCCF must be able to send the accounting records to the Broker. The sub-function that manages the exchange of these records shall be named the **Accounting Session Control** (ASC)

- Network activity management: The TP OCCF must be able to interact with the transport network in order to facilitate transport component setup and termination. The sub-function that bridges the TP OCCF to the transport

network shall be named the **Session Transformation Function** (STF)

- Network accounting management: The TP OCCF must acquire the component accounting records from the transport network. The sub-function that bridges the TP OCCF to the transport network for accounting shall be named the **Accounting Transformation Function** (ATF)

CP OCCF sub-functions
The CP OCCF is situated at the content provisioning network. The CP OCCF sub-functions are described in detail in subchapter 5.6.

Two sub-functions can be identified from the functional description in the previous subchapters that deal with content component management at the Broker and two other sub-functions are presented here.

- Content component management: The CP OCCF must be able to receive content component setup and termination requests from the Broker. The sub-function that manages the exchange of these requests shall be named the **Content Session Control** (CSC)

- Accounting record management: The CP OCCF must be able to send the accounting records to the Broker. The sub-function that manages the exchange of these records shall be named the **Accounting Session Control** (ASC)

- Content activity management: The CP OCCF must be able to interact with the content provisioning network in order to facilitate content component setup and termination, similar to the TP OCCF. The sub-function that bridges the CP OCCF to the transport network shall be named the **Session Transformation Function** (STF)

- Content accounting management: The CP OCCF must acquire the component accounting records from the content provisioning network, similar to the TP OCCF. The sub-function that bridges the CP OCCF to the content provisioning network for accounting shall be named the **Accounting Transformation Function** (ATF)

5.3.2. Interfaces linked to the sub-functions

The defined sub-functions are presented here per interface. The Interfaces were first introduced in section 5.2.2. Figure 5-2 shows the general OCCF locations and the outlined sub-functions per interface. The SIM and ARM functions are not shown, but the sub-functions only. Please note that transport accounting records have previously been abbreviated as CDRs (Charging Data Records).

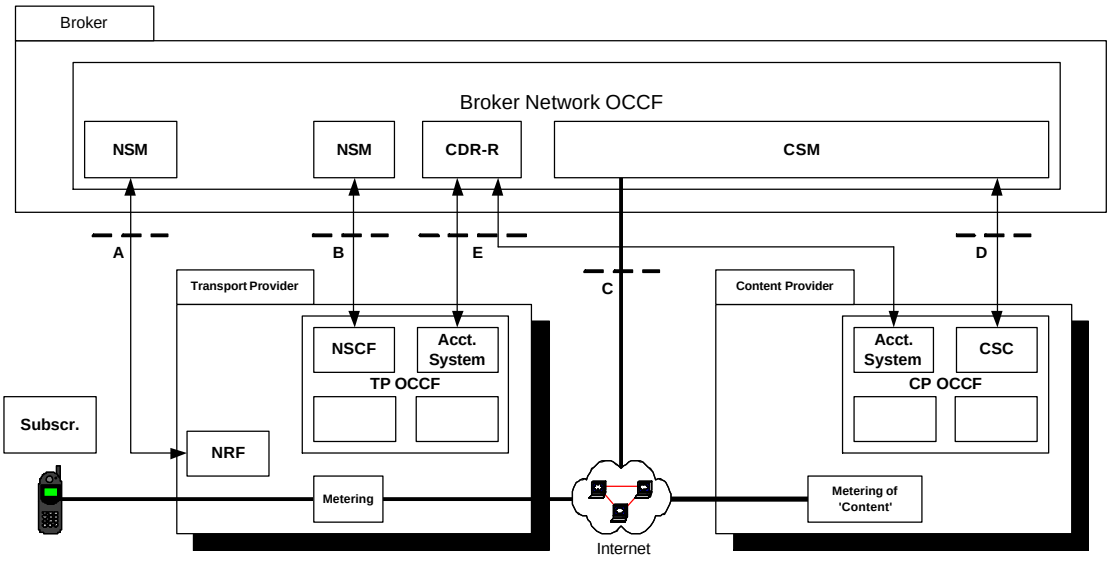

Figure 5-2: the OCCF locations and Interfaces

Interface A is the interface between native registration elements (Network Registration Function, NRF) and the Network Registration Manager (NRM) of the Broker. The type of native registration element determines which protocol is used over the A interface to register the subscriber. The NRF is NOT part of the TP OCCF.

Interface B is used to set up transport session components and to transfer the proper SCID for the CDRs of the TP. The two parties involved are the Network Session Control function (NSC) at the transport network and the Network Session Manager (NSM) at the Broker.

Interface C is used to communicate between the mobile and the Client Session Manager (CSM). The communications are facilitated by the transport network, and therefore this interface represents a transport session component. The mobile sends the CID tag of the requested content element to the CSM over this interface, which has also been named the Home Broker Session.

Interface D is used to set up content session components and to transfer the proper SCID for the CDRs of the CP. The two parties involved are the Content Session Control (CSC) at the CP and the Client Session Manager (CSM) at the Broker.

Interface E is the interface between the Accounting Session Control (ASC) of both the TP and CP, and the Broker. Both the TP and CP send their accounting records to the CDR Receiver (CDR-R) at the Broker OCCF, where they will be processed further.

The **F Interface** is the radio link between the mobile and the transport network, exchanging the data packets. Besides the regular transport component data, the packets can also contain registration information for the NRF, or they can contain the Home Broker Session (Interface C) data packets. The F Interface will not be further regarded, since the important elements have been captured in the A and C Interfaces, and data transmission properties depend on the type of transport network.

5.4. Detailed description of the multi-domain accounting architecture design: The Broker OCCF

The Broker OCCF is split up in the two aforementioned parts of Session Identity Management (SIM) and Accounting Records Management (ARM). The first part deals with the setup and termination of all data sessions of the subscriber in the transport networks and at the Content Providers. It also issues and registers the SSIDs and SCIDs for each subscriber to all providers of the session components.
The second part receives and processes all incoming accounting records from Transport Providers and Content Providers.
Not belonging to the Broker OCCF, but still part of the Broker is the Billing system, which receives the aggregated CDRs from the ARM. Figure 5-3 shows the sub-functions of the Broker OCCF and their mutual relationships that will be discussed in this subchapter.

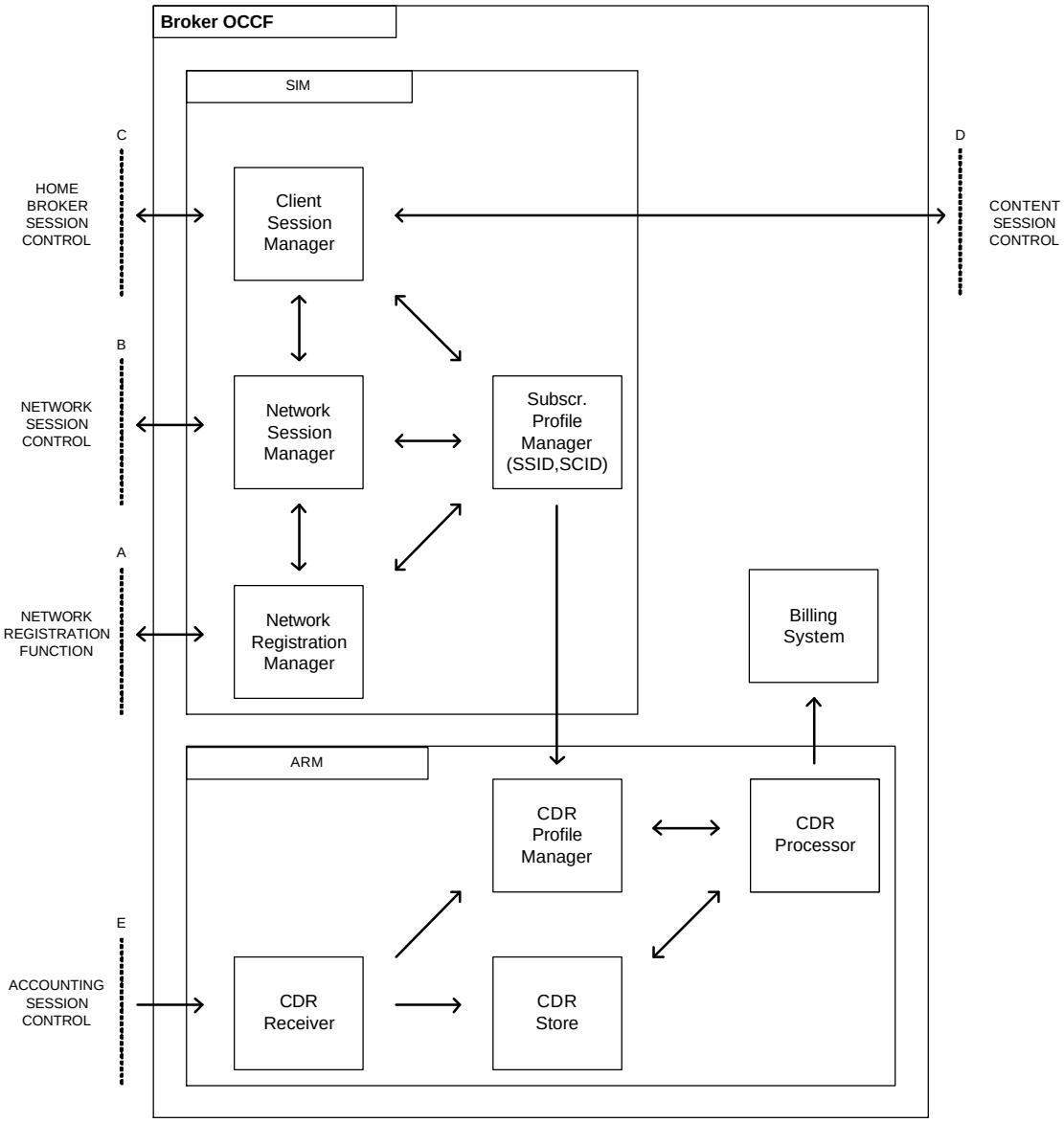

Figure 5-3: The Broker Functional Diagram

This subchapter is organized in the following way:

- Section 5.4.1 discusses the SIM sub-functions.
- Section 5.4.2 presents SIM setup procedures for
    - registration at the transport network
    - setup of the Home Broker Session
    - registration of the subscriber at the Client Session Manager (CSM)
    - content component setup as a result of a content request
    - transport component setup as a result of a content request
    - content delivery
- Section 5.4.3 presents SIM termination procedures for
    - NSM initiated sessions (possibly as a result of TP initiated termination)
    - CSM initiated sessions
- Section 5.4.4 discusses the ARM sub-functions.
- Section 5.4.5 presents ARM Super Session Profile procedures as a result of the SPM notifications. Exemplifying events are defined here that are used for the ARM description
- Section 5.4.6 presents ARM CDR management based upon the exemplifying events

5.4.1. SIM Functional Elements

The SIM is communicating with TPs and CPs over the interfaces A, B and D. It also communicates with the subscriber through the C interface. Further refinement of the functionalities of the SIM is presented in this section and mainly follows the implications of the four interfaces. One function handles registrations of the Subscriber at transport networks; another handles the communications with the transport network on transport component setup and termination. A third is communicating with the Subscriber and manages its requests for Content with the Content Provider. Finally, a centralized function is maintaining the Subscriber Profile and since content usage spans multiple parties, the management of component identifiers for accounting is collocated with the Profile. These four functions are defined subsequently and shown in Figure 5-4.

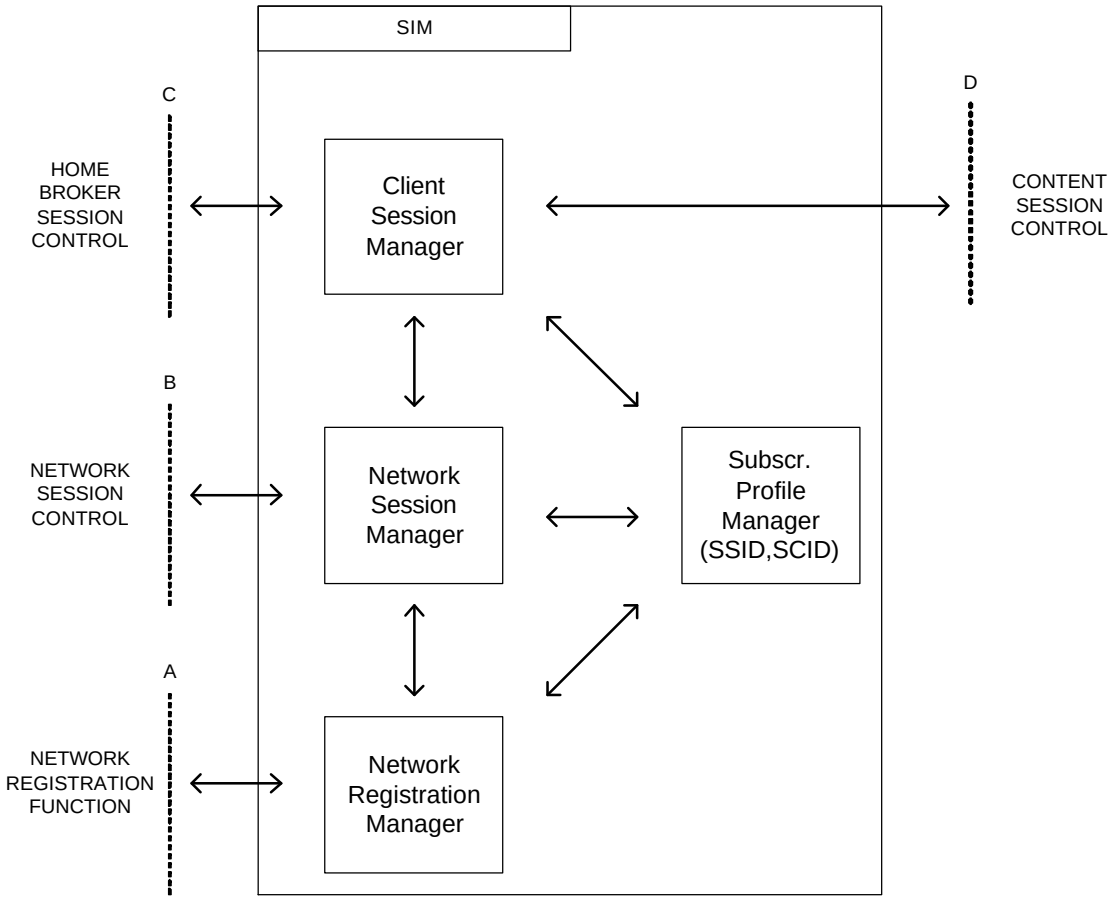

Figure 5-4: SIM Functions

The **Network Registration Manager** (NRM) facilitates the registration of subscribers at transport networks in order to use the services of the transport network. Examples of the NRM are the Home Location Register (UMTS) or a RADIUS server (WLAN). The Network Registration Manager address can be derived from the information presented by the mobile upon registration by the transport network.

The **Network Session Manager** (NSM) communicates with transport networks to support two features: in case a mobile requests a transport component from the transport network, it presents the transport network a SCID for that service. This service will consist of transport components only and no content components can be added. Secondly, the NSM can instruct the transport network to set up a transport component to the mobile. It presents the SID, the source address of the incoming data, and the SCID to be included in the accounting of this component. For clarity, the NSM has no interactions with the mobile itself, only with the transport network.

The **Subscriber Profile Manager** (SPM) maintains information on the subscribers in a Subscriber Profile. The SPM generates the SSIDs and the SCIDs. The Subscriber Profile includes the SID, Subscription info, Authentication info, and information on active super sessions. When the Client Session Manager or the Network Session Manager request the establishment of a new super session, a new SSID and SCID is generated for the initial request and the SSID and SCID are listed in the Subscriber Profile. Subsequent transport components receive an additional SCID, which are also registered in the profile with the corresponding super session. The Subscriber Profile indicates which session components are

open (active) and which are closed. When all SCIDs are closed, the SSID is closed. The closed SSID is then purged from the Subscriber Profile.

The SPM also instructs the CDR Profile Manager to create a Super Session Profile for each new SSID. The SPM notifies the CDR Profile Manager of every additional SCID it issues for a super session (not shown in Figure 5-4).

The **Client Session Manager** (CSM) facilitates the provisioning of content services to the mobile based on the CID it receives from the mobile. It communicates with the CP on the delivery of the content to the mobile and it instructs the Network Session Manager to set up a transport component for that delivery. The CSM requests the creation of a super session from the Subscriber Profile Manager and forwards the proper SCID to the Content Provider. The CSM also forwards the SSID to the Network Session Manager when it requests a transport component. That ensures that the transport components will be registered under the proper super session.

5.4.2. SIM Setup Procedures

This section exemplifies the registration process, the establishment of the communications between the mobile and the CSM, and the ordering and setup of content delivery. The example shows how the accounting identifiers SSID and SCID are handled within the SIM. Each paragraph shows part of the example and functional blocks that are not involved in that part are omitted for clarity.

Network Registration
This part exemplifies the handling of the registration process at the Broker of a mobile at a transport network. The SPM maintains the Subscriber Profiles. At the start of this example, the Subscriber is not registered at any transport network. If the transport network is UMTS, the NRM will act as a Home Location Register. If the transport network is WLAN, the NRM could be a RADIUS server (see Figure 5-5).

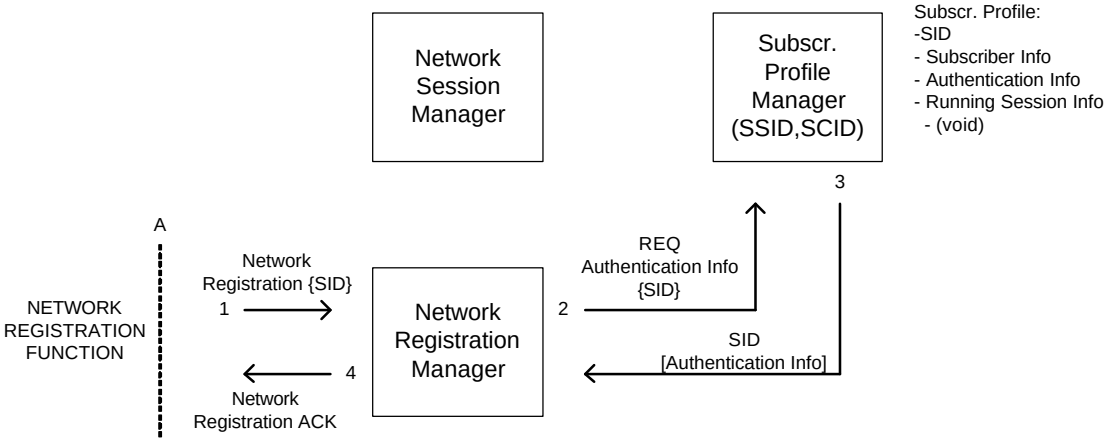

Figure 5-5: Network Registration

1. When a mobile enters a transport network, it tries to register. The transport network derives the NRM location and presents the registration request of the mobile to the NRM.

2. The NRM fetches the authentication information from the subscriber profile at the SPM.
3. The SPM returns the authentication information to the NRM.
4. The NRM authenticates the mobile at the transport network and from that point on the mobile can start requesting services of the transport network.

Network Service establishment

The now registered mobile requests its first service at the transport network. It requests to be connected to its CSM at the Broker and it presents the transport network with the CSM address that it knows. The NSC is requested a SCID by its provisioning network element (not shown). It is assumed that both parties have made previous agreements (Service Level Agreement, or SLA) on service provisioning and that the location of the NSM of the Broker is known at the NSC of the transport network. If there were no SLA, the mobile wouldn't be allowed to register in the first place, because the TP wouldn't be sure of getting paid for its services (see Figure 5-6).

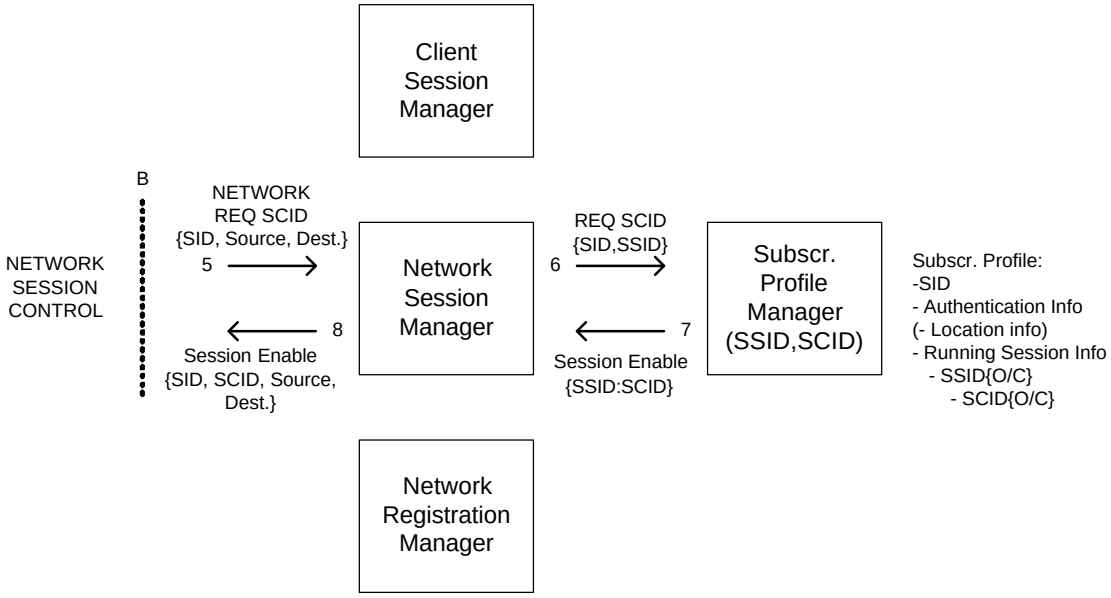

Figure 5-6: Network Service Request needs a SCID

5. The mobile requests its first service from the transport network and it presents the destination address. The NSC sends a request for a SCID to the NSM that includes the SID, the source address (=mobile) and the destination address (=CSM)
6. The NSM sends a request for a SCID to the SPM. No SSID exists for this transport component, so the SSID parameter in the request is void. A later example will show when a SSID can be included.
7. The SPM constructs a SSID and a SCID for this request. It adds them to the Subscriber Profile and returns them to the NSM. The SPM also notifies the CDR-PM of the creation of the SSID and SCID (not shown in the figure, postponed to the ARM description starting in section 5.4.4)
8. The NSM sends a Session Enable message to the NSC to instruct it to set up a transport component for the Subscriber. It includes the SID and the SCID, the Source and the Destination address. (Not shown is a possible TP confirmation message)

After this procedure, the TP sets up the transport component from the mobile to the CSM and the TP will include the SCID in all accounting records that result from this particular session component.

Client Registration

The previous paragraph described that the mobile requested a transport component to connect to its CSM. The transport component has been set up and the corresponding SSID and SCID are listed in the Subscriber Profile. The mobile will now try to connect to the CSM. The CSM will first authenticate the mobile to ensure that it is communicating with the correct party, and also to load Subscriber Information about what kind of usage restrictions apply for this particular subscriber (see Figure 5-7).

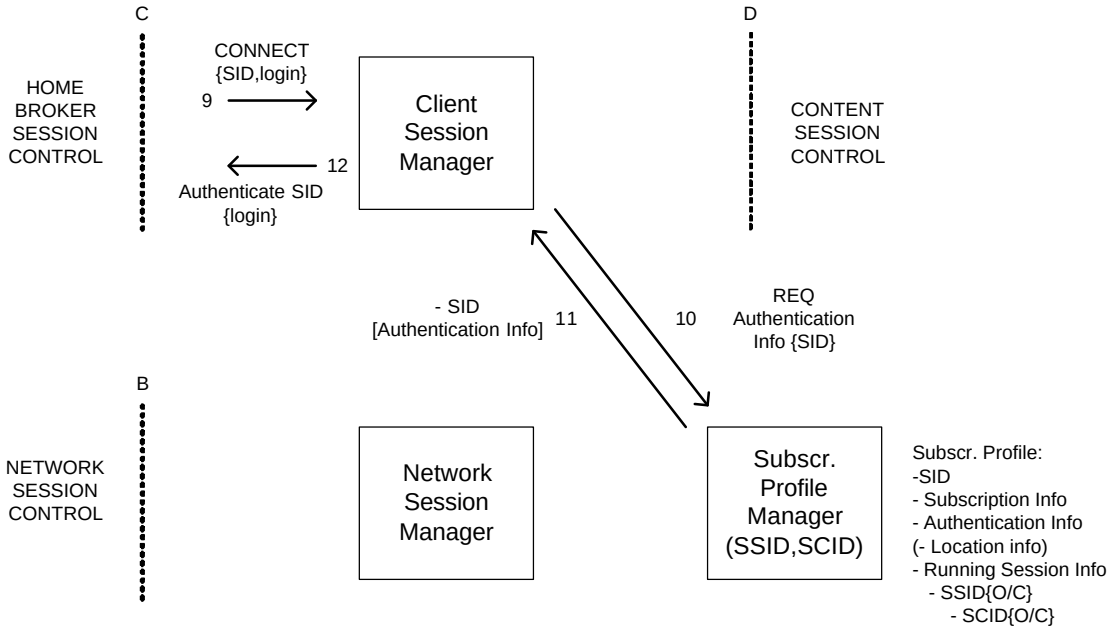

Figure 5-7: Client Registration

9. The mobile presents its SID and authentication information to the CSM.
10. The CSM fetches the corresponding Authentication Information from the SPM, along with the Subscription Information on the rules that apply for this subscriber. This is different authentication information than the one that was used in steps 1-4! Network registration is done by authentication procedures inherent to the network type, while the CSM authentication may be a challenge-response procedure or simply a password.
11. The SPM presents the requested Authentication and Subscription Information to the CSM.
12. The CSM authenticates the mobile, after which the CSM is able to receive and process requests for content from the mobile.

Content Component Setup
It is assumed that the mobile possesses a CID of the content element that the subscriber requests and the mobile presents the CID to the CSM. This order needs to be appointed a SSID and the CP needs to be contacted to set up the content component. The ways of obtaining a CID by the mobile are discussed in the Intermezzo of Chapter 8. See Figure 5-8.

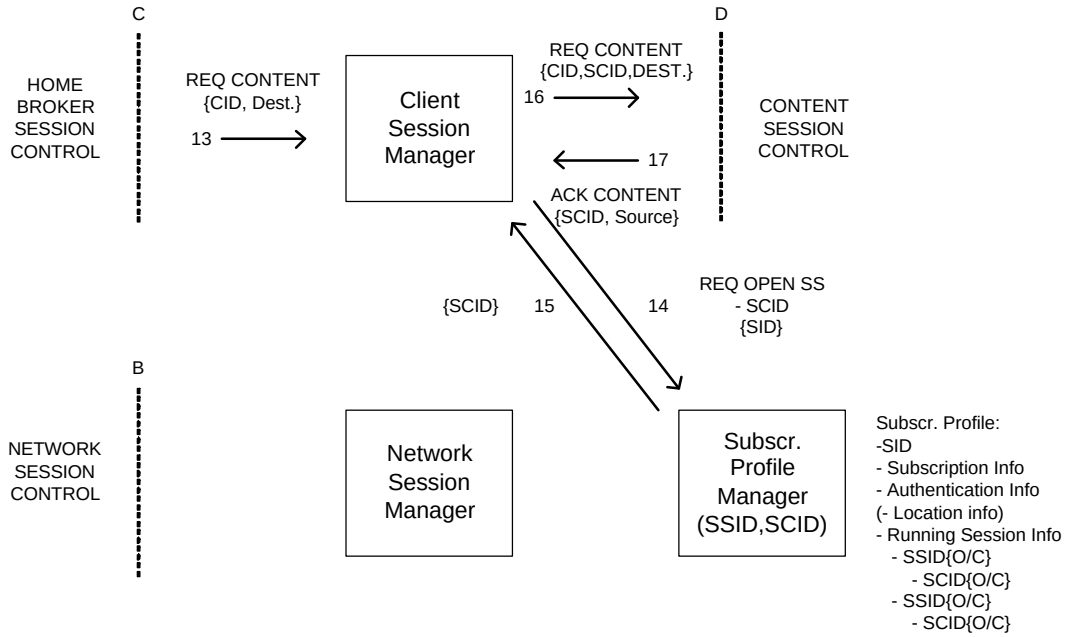

Figure 5-8: Content Component Setup

13. The mobile presents the CID and the address that it wishes to receive the content on to the CSM.
14. The CSM requests the opening of a super session at the SPM under which the session components can be registered. In the request, the CSM includes the SID as well as the notification that it needs a SCID for the content component.
15. The SPM creates a SSID and SCID and includes them in the SID profile. It returns the SCID to the CSM to be used for the content component. (Note that the SSID can be derived from the SCID, so the SCID suffices). The SPM also notifies the CDR-PM of the creation of the SSID and SCID (not shown in the figure, postponed to the ARM description starting in section 5.4.4).
16. The CSM contacts the CSC of the CP (CSC location possibly derived from the information in the CID), requesting the particular content element by including the CID and the Destination address, as well as the SCID to be used in the CP accounting records.
17. The CSC verifies the request for availability, prepares the content component delivery and returns an acknowledgement to the CSM in which it includes the Source address that will be used for the content component.

For clarity, there has been no direct information exchange between the CP and the mobile up until this point.

Transport Component Setup

The CSM now has enough information to order the transport component setup. It has the SSID (derived from the SCID for the content component), the initial Source and Destination address for the transport component and the CP waiting to be triggered for the delivery (see Figure 5-9).

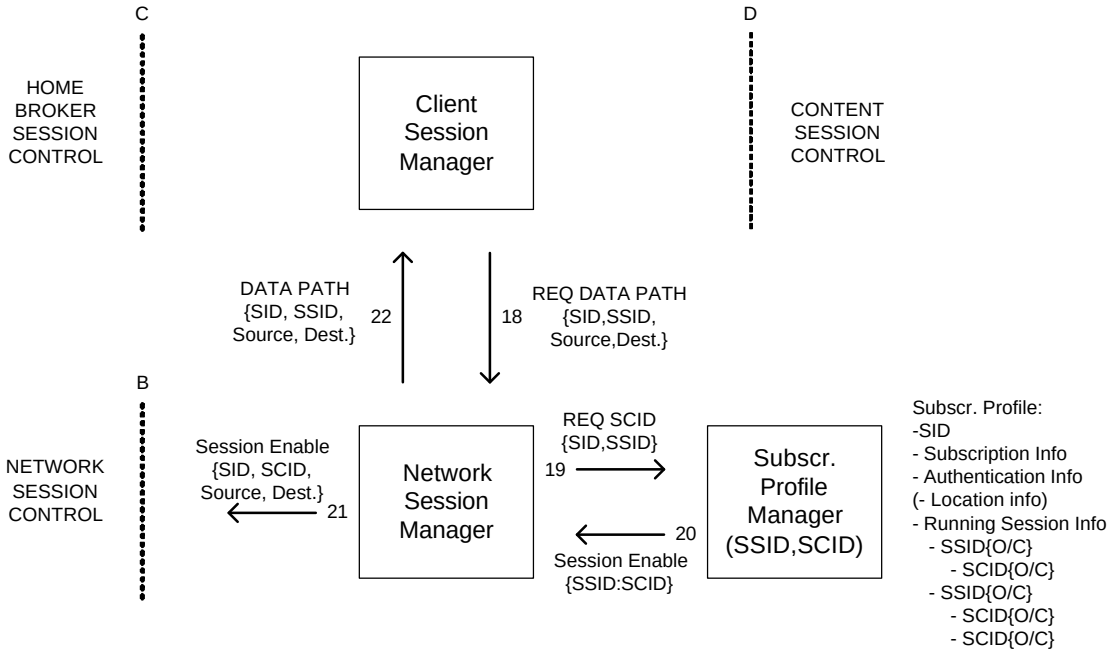

Figure 5-9: Setting up the transport component for Content Delivery

18. The CSM sends a request for a transport component to the NSM, including the SID, the Source and Destination address and the SSID.
19. Similar to (6), the NSM sends a request for a SCID to the SPM. With the SID and now included SSID parameter, the SPM can correlate the transport component to the proper super session in the Subscriber Profile. (not shown is the notification to the CDR-PM)
20. The SPM creates a SCID for the transport component according to the SSID, adds the SCID entry to the Subscriber Profile and returns the SCID to the NSM.
21. Similar to (8), the NSM sends a Session Enable message to the NSC. It includes the SID and the SCID, the Source and the Destination address. The TP sets up the transport component and includes the SCID in all corresponding accounting records. (Not shown is a possible TP confirmation message)
22. The NSM informs the CSM that the transport component setup was successful.

Content Delivery

The CSM is now ready to enforce the content delivery. Both the TP and the CP have been given proper accounting information to be able to correlate their component accounting records when the Broker receives them (see Figure 5-10).

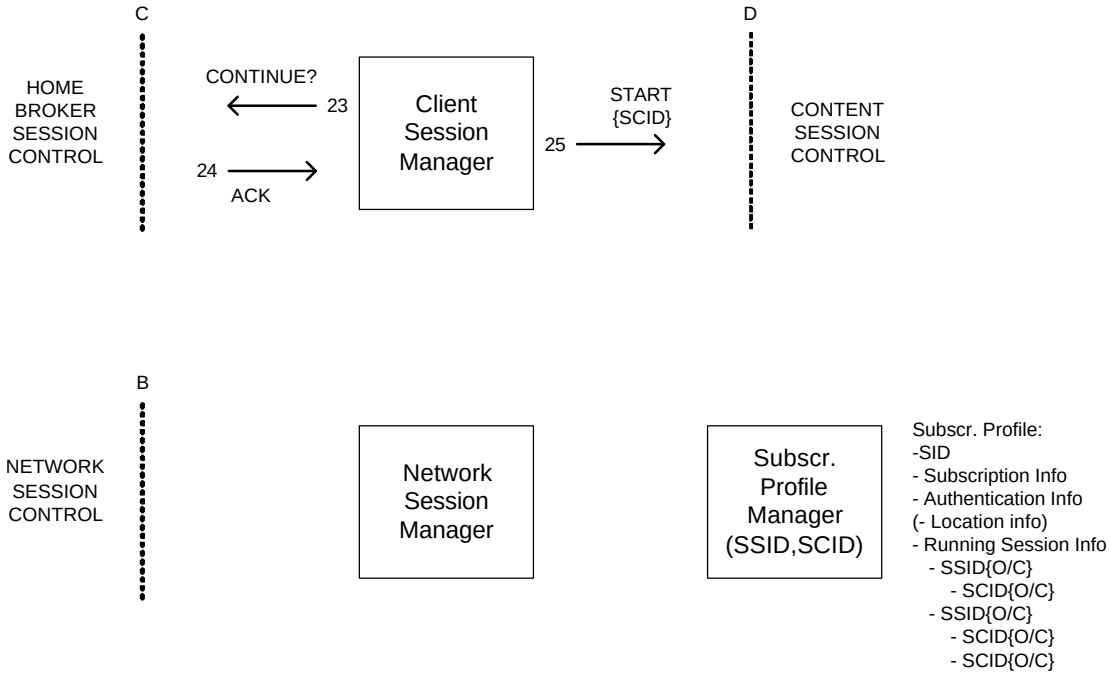

Figure 5-10: Enforcement of the Content Delivery

23. Before the content delivery takes place, it seems wise to prompt the subscriber with the question to confirm or roll back the request.
24. If the subscriber has changed its mind and cancels the request, the CSC can be instructed to roll back and purge the accounting information. Since in that case there will be no content delivered, it can be assumed that no charge will take place at the CP. Additionally, the NSC can order the termination of the transport component in the transport network. Since there has not been any data exchange between the CP and the mobile over the transport component, it can be assumed that there will not be any charge at the TP for this part. This example continues with the acknowledgement of the delivery.
25. Upon the acknowledgement of the subscriber, the CSM instructs the CSC to start the delivery of the content.

The setup procedure is completed and the mobile receives the content from the CP.

5.4.3. SIM Termination Procedures

The previous section 5.4.2 described that two methods of initiating super sessions exist: the Network Session Manager Initiated sessions and the Client Session Manager Initiated sessions. Both types have multiple procedures to close a super session, mainly depending on the party that is requesting the termination.

The accounting process is indifferent to the way that session components are torn down. Therefore all common termination procedures are mentioned, but only typical ones are exemplified.

First the termination procedures for NSM Initiated sessions are explained, followed by the procedures for CSM Initiated sessions.

NSM Initiated Session Termination Procedures
NSM Initiated sessions are by definition super sessions consisting of transport components only. The Home Broker Session from the subscriber to the CSM is one example. Browsing through free web pages could be another.
From the Broker point of view, the only two parties that can issue a termination of a transport component are the TP and the NSM. This is due to the fact that it is irrelevant to the Broker if the mobile ordered the termination in the transport network, or the TP itself ordered it. The NSC shall in both of the latter cases inform the NSM of the termination through a Closed Session message. This is not further explored in this section, but addressed in section 5.5.2.

The example in Figure 5-11 shows how the NSM orders the termination of a (one) certain transport component. Later examples will show that this may take place during roaming situations or when a corresponding content component has been terminated.

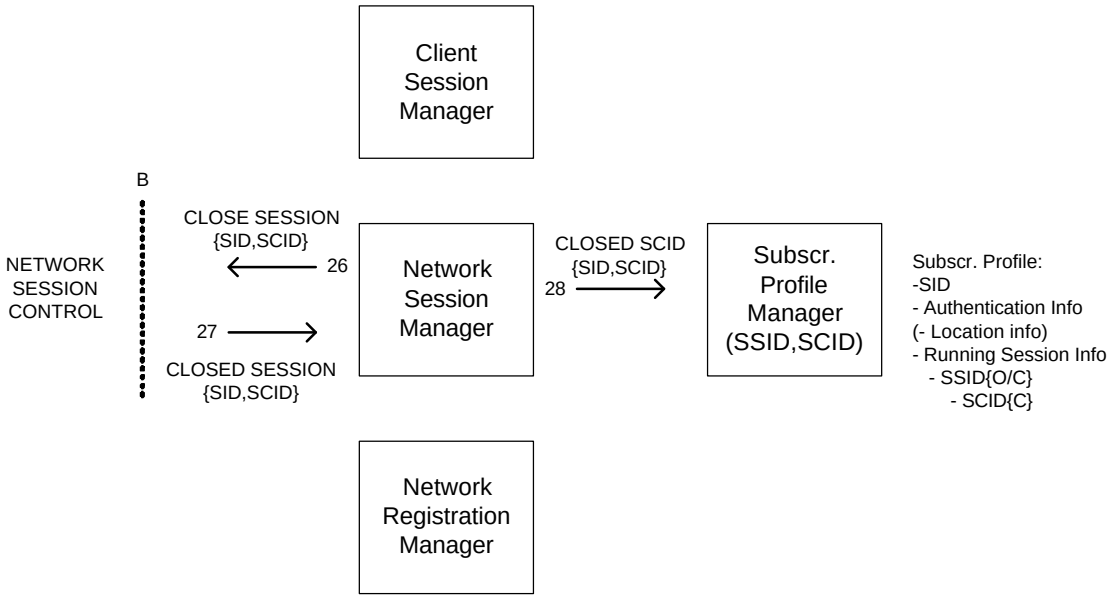

Figure 5-11: NSM Initiated Termination

26. The NSM is triggered to apply a termination procedure for a particular transport component. It sends the NSC a message requesting the close of that component, denoted by the SID and SCID.

27. The NSC initiates the termination of the transport component in the transport network and when it succeeds in doing so, it sends back an acknowledgement to the NSM. The accounting records of this particular transport component will be constructed at the TP and eventually sent to the CDR-R at the Broker (not shown)
28. The NSM sends an update message to the SPM that it has terminated the transport component denoted by the SID and SCID. The SPM now closes the SCID from the Subscriber Profile and if this was the last or only open SCID, it also closes and removes the SSID. The SPM notifies the CDR-PM of the close of the SCID and possibly the removal of the closed SSID (not shown).

It may be the case that the network connection has been lost. For the Broker OCCF, this is also considered a NSM Initiated Session termination. In that case, the NSC is informed trough a similar message as step 27 and step 26 is simply omitted. Example 2 in subchapter 8.2 digresses further on this issue.

CSM Initiated Session Termination Procedures

Since the sessions that are set up by the CSM are almost always consisting of multiple components, the termination procedures are also more complex. The CSM acknowledges triggers for the termination of a super session from several parties. These parties are:

- The subscriber may request the termination of a super session from the CSM when it decides not to continue the use of a particular content element.
- The CSC may inform the CSM that it has terminated the delivery of the content element in most cases probably because it 'finished' (like a movie). More reasons could be considered, which would all result in the same 'Ceased Session' message. This message implies that the accounting process at the CP has commenced for the content component and that it is not possible to resume it without re-ordering (and thus starting a new super session).
- The CSM itself may decide to terminate a super session, for instance when the credit of the subscriber has run out.

All these triggers result in the same CSM Initiated Session Termination Procedure, shown in Figure 5-12.

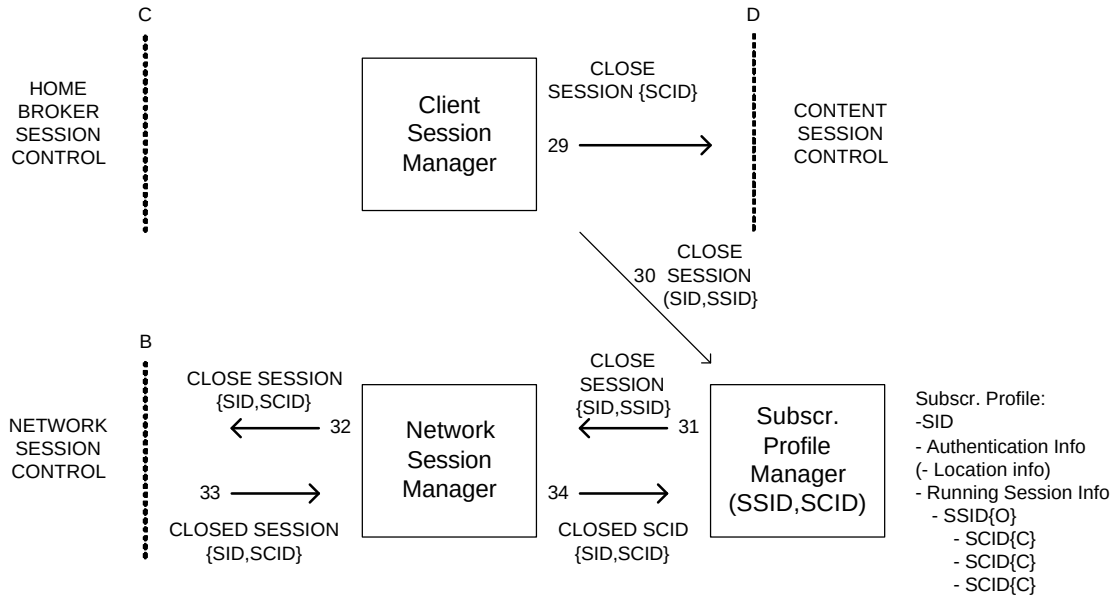

Figure 5-12: CSM Initiated Termination

29. In case the trigger to close the super session has not been sent by the CSC, the CSC is instructed to terminate the content component provisioning and to complete the accounting records and send them to the Broker.

To instruct the termination of the corresponding transport components, the CSM could either instruct the NSM directly to terminate the components, or instruct the SPM to terminate the super session (which in its turn lets the SPM instruct the NSM to close all transport components). There is no difference in the amount of message exchanges. Therefore no specific preference exists for either method, but only the latter is exemplified.

30. The CSM informs the SPM that it has terminated the content component and since there can only be one content component for each super session, it implicitly instructs the SPM to terminate all corresponding transport components.
31. The SPM instructs the NSM to terminate all network sessions that belong to the super session by including the SID and the SSID. (alternatively, the SPM may include all open SCIDs in this message)
32. The NSM checks all active transport components of the subscriber for membership of the SSID and subsequently instructs the NSC to terminate the transport component. This is compliant with 26. Generally speaking there is only one transport component active at a time per super session, but during roaming a (temporary) situation may exist where there are two simultaneous transport components active on different transport networks for a super session. Because in such a situation two transport components at different TPs must be terminated, it follows that the CLOSE SESSION instruction must be issued for more than one transport component. (It is indifferent to use the SCID or the SSID in the instruction, but the SCID was chosen to be consistent with the Session Enable request of 21).
33. Similar to 27, an acknowledgement is sent to the NSM of the termination of the transport component. It includes the SCID of the terminated transport component.
34. Similar to 28, the NSM sends an update message to the SPM for each SCID it terminated. The SPM terminates each component in the Subscriber Profile until all components have been terminated.

The previous steps of the example did not mention the SCID and SSID termination notifications that the SPM sends to the CDR-PM. These notifications will be regarded at the ARM description starting in the next section (5.4.4).

The example until now has shown the setup and termination procedures for super sessions and the creation and distribution of corresponding accounting identifiers. The next section shows the handling of the incoming accounting records and the way that they are eventually properly correlated for the Billing System.

5.4.4. ARM Functional Elements

The Accounting Record Management (ARM) function receives the component accounting records from TPs and CPs over the E interface and processes them for the Billing System. The component accounting records are also referred to as Charging Data Records (CDRs). Further refinement of the functionalities of the ARM is presented in this section. One function handles the reception of the incoming CDR. Since this thesis mainly regards multi-domain sessions and multiple CDRs need to be correlated, a storage function needs to be present to temporarily store CDRs until all of them have been received. A third function

maintains a registry of expected CDRs and determines if all CDRs of a particular super session have been received. When all CDRs of a particular closed super session have been received, a forth function will retrieve them from storage and process them into a format suitable for the Billing System. These four functions are defined subsequently and shown in Figure 5-13.

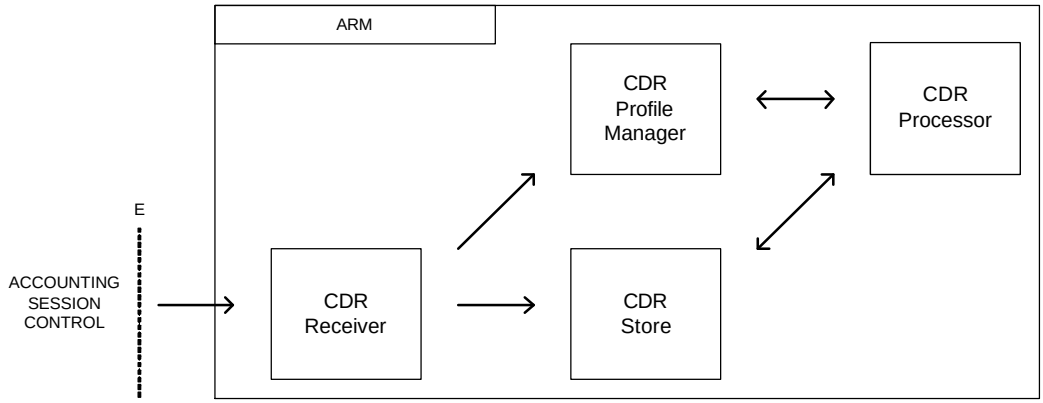

Figure 5-13: Accounting Control Functions

The **Charging Data Record Receiver** (CDR-R) receives CDRs from TPs and CPs according to agreements made in the Service Level Agreement between the Broker and the respective provider. The CDR-R labels each incoming record with a Storage Identity (STID) and extracts the SCID from the record. The CDR-R forwards the CDR to the CDR Store function and notifies the CDR Profile Manager of the reception.

The **Charging Data Record Store** (CDR-S) receives CDR files from the CDR-R and stores them under the accompanying STID. It retrieves the CDR files when asked to by the CDR-P.

The **Charging Data Record Profile Manager** (CDR-PM) maintains the Super Session Profile for each super session that has been created by the SPM. The SPM also notifies the CDR-PM of additional SCIDs, which are included in the Super Session Profile at the CDR-PM. A notification of the close of a super session from the SPM means that no more components will be added to the Super Session Profile. When the CDR-PM has receives notifications that a super session has been closed and eventually that all corresponding CDRs have been received and stored, it forwards the –now also closed- Super Session Profile to the CDR Processor. (The interactions with the SPM are not shown in Figure 5-13, but will be introduced first in the next section)

The **Charging Data Record Processor** (CDR-P) receives Super Session Profiles from the CDR-PM. The CDR-P presents the STIDs that are listed in the Super Session Profile to the CDR-S in order to receive those records. The CDR-P processes the information from the CDRs and formats them into one record that is suitable for the Billing System.

5.4.5. ARM Super Session Profile Procedures

This section described the creation, maintenance and closure of the Super Session Profiles as well as the flow of CDRs from the point of reception until they are processed for the Billing System. The description is given with the aid of an example. The example shows how the SSID and SCID are handled within the ARM. Each paragraph shows part of the example and sub-functions that are not involved in that part are omitted for clarity. Events in this example occur in the following order:

Suppose two subscribers (SID '1' and '2') are registered at a TP. Active super sessions are denoted by a letter (SSID 'A') and session components are denoted by an additional index (SCID 'A1').
First Subscriber 1 starts a Home Broker Session to its Client Session Manager. Then Subscriber 2 does the same. Subscriber 1 orders content and this is eventually closed after using one transport component. Subscriber 2 terminates its (transport) network connection without ordering any content.
All components are accounted by only one CDR, with the exception of the Home Broker Session of Subscriber 1.

Super Session Profile Management: Profile Creation
This part exemplifies the management of the Super Session Profile by the CDR-PM based upon the information it receives from the SPM. The first event, as shown in Figure 5-14, creates a Super Session Profile:

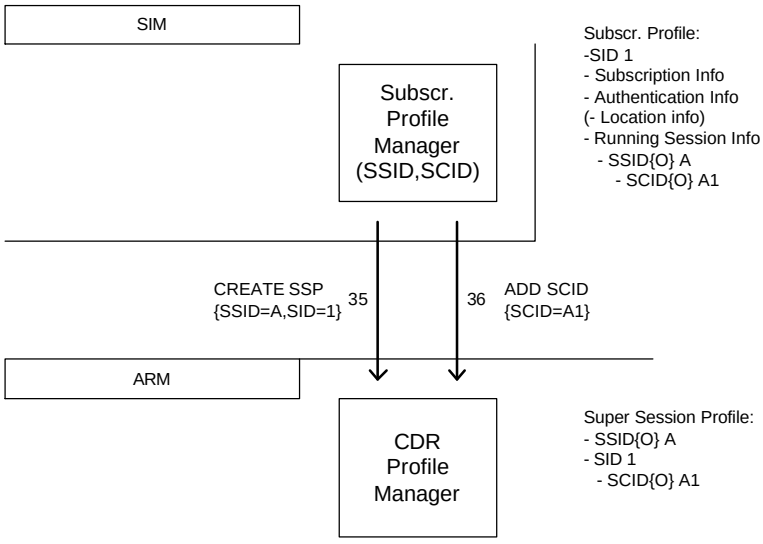

Figure 5-14: Super Session Profile Creation

35. The SPM creates a SSID and SCID for the transport component of Subscriber 1 at the NSM. The SPM adds the two identifiers to the Subscriber Profile. The SPM instructs the CDR-PM to create a Super Session Profile and includes the SSID and the SID for which the super session was issued. Inclusion of the SID here will show to be eventually necessary information for the CDR-P.
36. The SPM instructs the CDR-PM to add the SCID to the Super Session Profile. Including just the SCID in the message is sufficient, since the SSID can be derived from the SCID.

Combination of these two messages into one is very well possible, but to distinguish between SSID and SCID notifications they are issued separately in this example.

After these two steps, the CDR-PM is ready to register the storage of all CDRs for SCID A1. In the continuing example, shown in Figure 5-15, Subscriber 2 also follows the steps in this paragraph and both the SPM and the CDR-PM have two open Super Session Profiles.

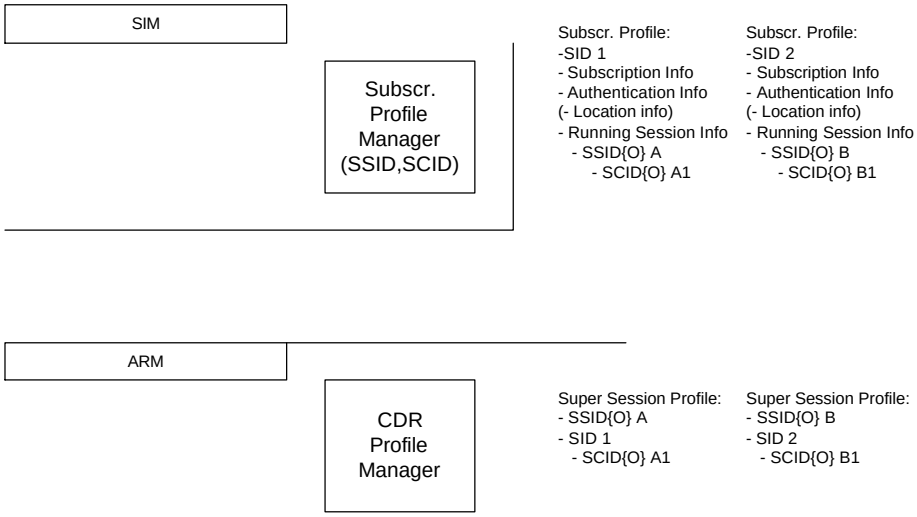

Figure 5-15: Creation of Profiles for Subscriber 2

Super Session Profile Management: Content Ordering

Both Subscribers now have access to the CSM and the CDR-PM is awaiting notification of the arrival of the corresponding CDRs from the serving TPs. The example continues with the ordering of content by Subscriber 1. The paragraph 'Content Component from section 5.4.2 described that the SPM will create a new SSID plus a SCID for the content component of the super session. The SPM orders the creation of a new Super Session Profile at the CDR-PM after it adds the information to the proper Subscriber Profile (see Figure 5-16).

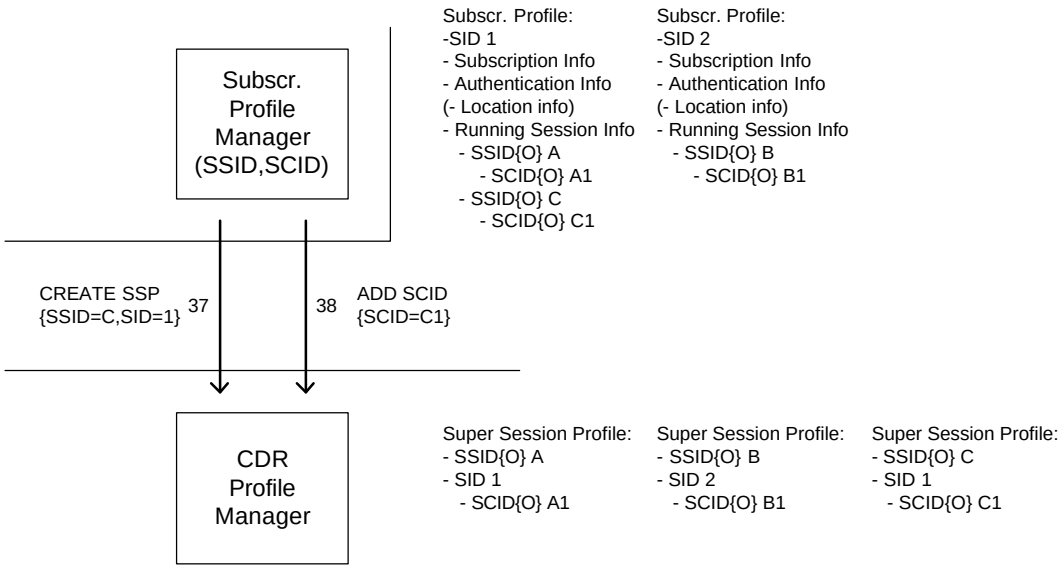

Figure 5-16: Adding a Super Session Profile for a Content Session

37. The SPM issues the next SSID for the new Content Session and creates the SCID for the content component. It includes them in the Subscriber Profile of Subscriber 1. The SPM orders the creation of a new Super Session Profile from the CDR-PM and passes on the SSID and SID.
38. The CDR-PM creates a new Super Session Profile like it was ordered to. The SPM sends a second order to include the SCID of the content component to the Super Session Profile. The CDR-PM adds the SCID to the Super Session Profile.

The CDR-PM is now ready to register notifications from the CDR-R on the new super session. The example continues with the addition of the SCID of the transport component of the content session, as described in section 5.4.2, paragraph 'Transport component Setup' (see Figure 5-17).

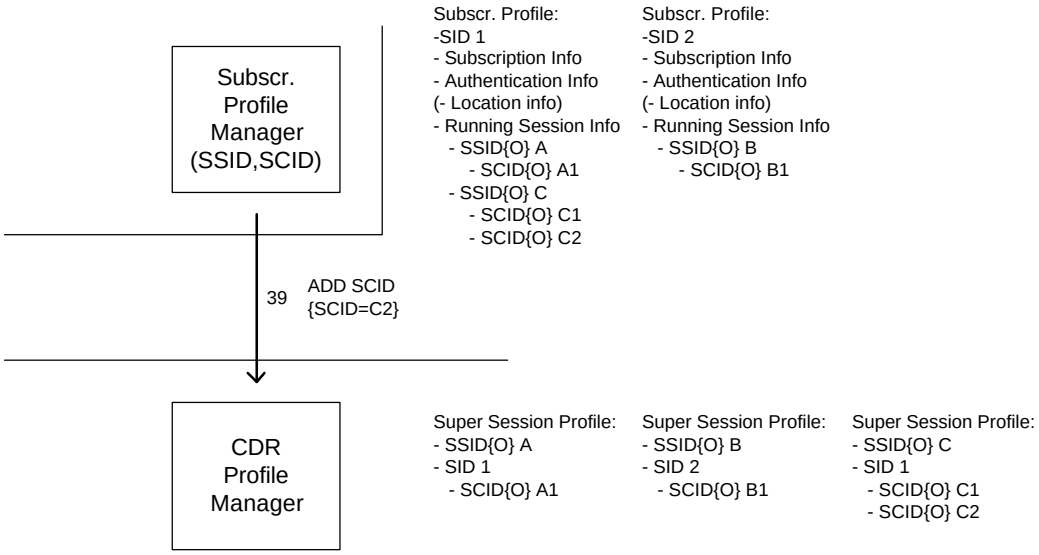

Figure 5-17 Transport component SCID added to Super Session Profile

39. Once the transport component SCID is added to the SSID in the Subscriber Profile, the SPM orders the addition of the SCID to the Super Session Profile at the CDR-PM. The CDR-PM derives the SSID from the SCID and adds the entry to the proper profile.

CDRs from both the serving TP and CP will be registered at the same profile at the CDR-PM. The event sequence also stated that the delivery of the content was done by using two transport components. It suffices to mention that the addition of the second transport component takes place in the same way as the first in step 39. To complete the focus on the SPM and CDR-PM interactions, the example continues in the next paragraph with the termination of a super session.

Super Session Profile Management: Profile closure
The example continues with the Subscriber 2 turning off its mobile device without having used any content. The only active session it had was the Home Broker Session and the transport component will be accounted for by the TP. The SPM will notify the CDR-PM of the termination of the super session to indicate that there will be no additional components to this super session. See Figure 5-18.

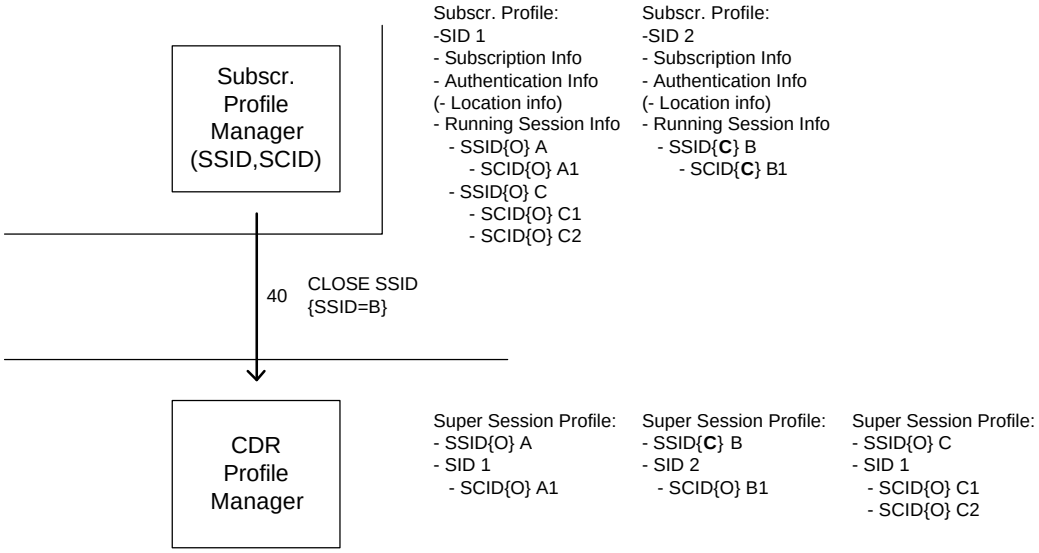

Figure 5-18: Closing a Super Session

40. The SPM closes the SCID and SSID in the Subscriber Profile and informs the CDR-PM of the close of the super session. The CDR-PM changes the status of the Super Session Profile to 'closed' to indicate that no component SCIDs will be added and that the profile can be forwarded to the CDR-P once all CDRs have been received.

Remarkable may be the fact that the CDR-PM is notified of the termination of super sessions, but not of the termination of session components. These notification messages have been omitted because they hold no value to the accounting process. The Broker (as a whole) has no prior notice of the number of fractional CDRs a TP or CP will send for a service component unless it previously agreed a number in the SLA. The TP or CP may even send information on several service components in one CDR. Subchapter 4.4 indicated that most common CDRs provide information on consecutive records by including a sequence number and/or flag that states if the record is the last one for a particular service. This is reliable information for the CDR-PM to judge if all records have been received, and on which it will close the corresponding service component in the Super Session Profile. The notification from the SPM of the termination of a super session is only necessary to be sure that no extra components will be added and that closed Super Session Profiles of which all component CDRs have been received can be forwarded to the CDR-P.

The example until now has shown the Super Session Profile management at the CDR-PM and all notification messages that the CDR-PM receives from the SPM. In the next section, the SPM will be omitted and the functioning of the Accounting Record Manager as a whole will be described, according to the Super Session Profiles stored at the CDR-PM.

5.4.6. ARM CDR Management

In this section, the handling, storage and processing of incoming CDRs is exemplified. The SSID and SCID will show their value in correlating the CDRs and a storage identifier, the STID, will be introduced.

ARM: Receipt of a CDR for Subscriber 2

The example in the previous section ended with the termination of a super session in SIM and the notification message that the CDR-PM received of that event. This means that an accounting record for that session is being sent by the TP to the Broker over the E interface and the example continues with this reception (see Figure 5-19).

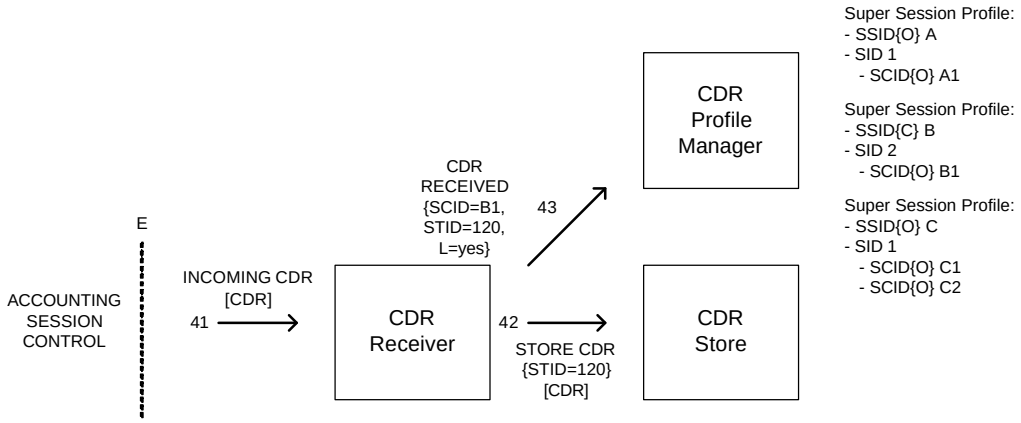

Figure 5-19: Reception of a CDR for Subscriber 2

41. A CDR is received by the CDR-R. The CDR-R generates a STID for the CDR (randomly chosen to be '120' for this example). The CDR-R also retrieves the SCIDs and sequence number from the record. In this example, the CDR is for SCID B1 only and the record is the only one for this component (no succeeding CDRs for this component).
42. The CDR-R forwards the CDR to the CDR-S for non-volatile storage under the storage number (STID). It is assumed that the CDR-R can maintain its own incremented list of STIDs for incoming records and that it does not need to query the CDR-S for one.
43. The CDR-R notifies the CDR-PM of the reception of a CDR. The CDR-R includes the SCID it retrieved from the record, the STID it labeled the CDR with, and the parameter ('flag') that states that the record was the last one for this component (since it was the only one).

ARM: Processing of a closed Super Session Profile

The CDR-PM receives the notification from the CDR-R, adds the STID to the SCID, closes the SCID in the Super Session Profile and determines if all components have been closed. When this is the case, the CDR-PM forwards the Super Session Profile to the CDR-P. The CDR-P fetches the proper CDRs from the CDR-S and subsequently processes them for the Billing System (see Figure 5-20).

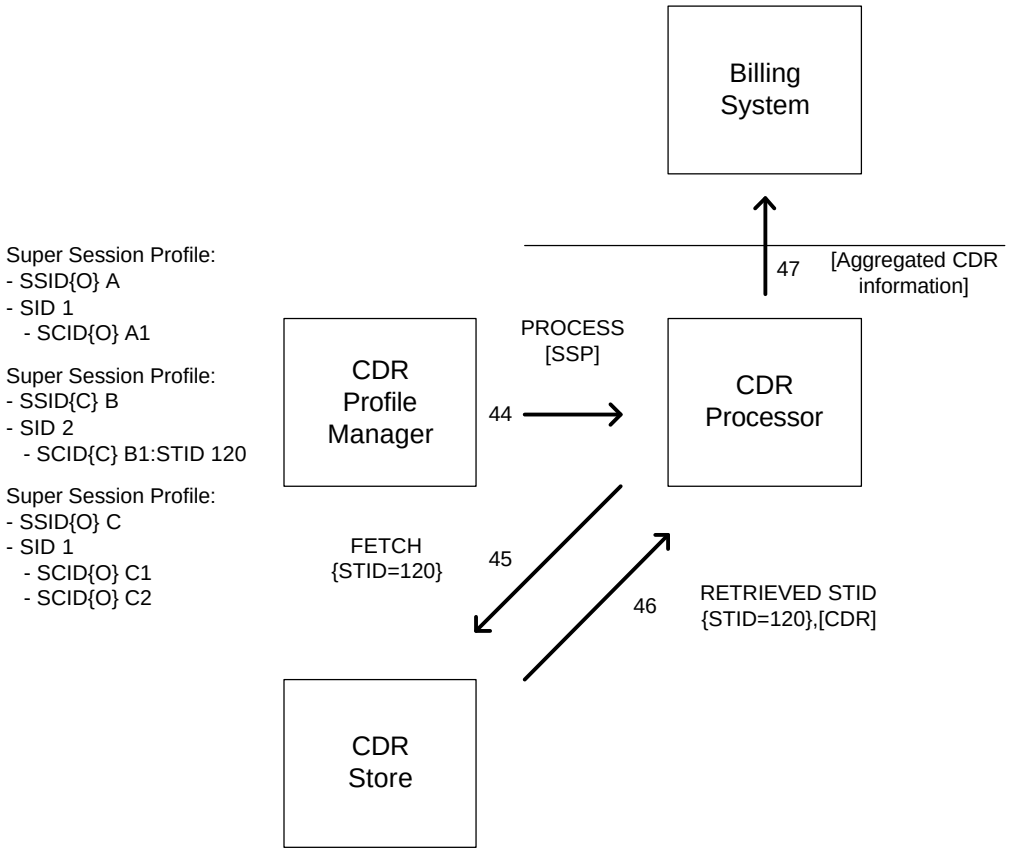

Figure 5-20: Super Session Profile Processing

Please note that a 'closed SCID' in the SIM has a different meaning than in the ARM. In the first it indicates that the session component service has ceased and in the latter it states that all relevant CDRs have been received for that session component.

44. The CDR-PM adds the STID to the SCID in the Super Session Profile and since it was marked as being the last STID, the SCID is closed. If the STID is not the last STID, the SCID will remain 'open' until the last STID is received. Also, since the SSID was already closed by notification from the SPM in step 40, the Super Session Profile is now ready to be processed. The CDR-PM orders the processing of the Super Session Profile by sending it to the CDR-P. For the sake of simplicity it is assumed that closed Super Session Profiles are purged from the CDR-PM.
45. The CDR-P collects all the STIDs from the profile (one in this example) and it requests the corresponding CDR from the CDR-S.
46. The CDR-S retrieves the CDR from its non-volatile storage and sends it to the CDR-P.

One may argue if the CDR should be deleted after being fetched, but two arguments are against that: First it could be assumed that the Broker only has one facility of non-volatile storage and that is the CDR-S. Deleting records from this storage will imply that they will be lost for future reference (e.g. auditing). Second and even more important, one CDR may hold information on several SCIDs, which will show in the continuation of the example. When the record is deleted after the first section was processed, subsequent profiles would be deprived of their CDR information. Therefore it is assumed that all received CDRs will remain in the CDR-S (forever) and issues of reusability of storage space and STIDs will remain inconclusive in this thesis.

47. The CDR-R now has all necessary CDR information and it may start processing that information for the Billing System. In parallel with common standardization procedures (e.g. UMTS), the way of processing and preparing the information for the Billing System will not be regarded, since it is up to the operator to decide on what and how to bill the subscriber. Also, the method of revenue sharing (clearing) between involved sub-contractors is not discussed.

Though it may be wise for future reference to store the aggregated CDR information and/or the Super Session Profile in non-volatile storage, no such action is included in this example. This is again considered a choice that the entrepreneur must make and it is not necessarily subject to standardization. All necessary information (SCIDs) is still available at the CDR-S for retrieval purposes.

The example until now has shown that the Broker can create a super session for a Subscriber, the transport component can be given an accounting identifier and the corresponding accounting records can be received and processed. Thus far the super session consisted of only one session component. Following the previously stated events of section 5.4.5, the next paragraph will show the more complex situation of a super session with several components.

ARM: Handling of multi-component sessions.
This paragraph presents the last and most complex part of the ongoing example: the situation of multiple session component providers sending multiple component CDRs for an ongoing super session. For clarity, the event sequence as it was presented in section 5.4.5 is refined and focused on the ARM part:

The previous paragraph showed that the activities of Subscriber 2 have ceased and how the accounting process handled the corresponding CDR.
The CDR-PM now holds only two Super Session Profiles with information of Subscriber 1. One profile was for the Home Broker Session and the second one was for a content session containing a content component plus a transport component.

The content session will close, and two CDRs will be sent to the Broker. The CP will send one CDR for the content component. The TP will send one accounting record containing two CDR cells (e.g. a TAP3 file in batch mode, see section 4.4.1). One CDR cell describes the transport component that was used for the content session and the second cell contains a partial CDR record on the transport component of the Home Broker Session.

Figure 5-21 shows the notification of the SPM to the CDR-PM on the termination of the content session.

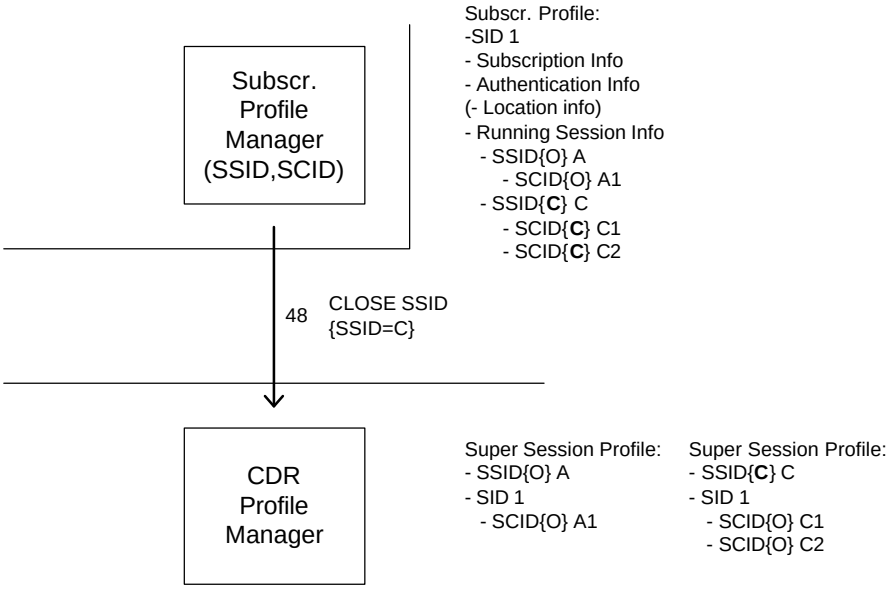

Figure 5-21: Closure of the content session

48. Similar to 40, the SPM notifies the CDR-PM that it terminated a super session and the CDR-PM changes the status of the corresponding Super Session Profile to 'closed'.

Figure 5-22 shows the reception of the first CDR.

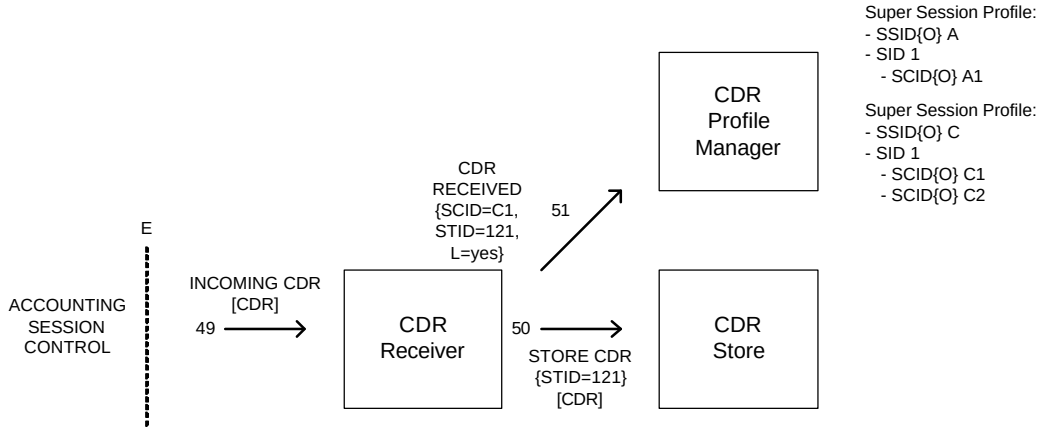

Figure 5-22: First incoming CDR for the content session

49. Similar to 41, a CDR is received by the CDR-R. This one originates from the CP. The CDR-R generates a STID for the CDR (successively being '121'). The CDR-R also retrieves the SCID and sequence number from the record.
50. Similar to 42, the CDR-R forwards the CDR to the CDR-S for non-volatile storage under the storage number (STID).
51. Similar to 43, the CDR-R notifies the CDR-PM of the reception of a CDR. The CDR-R includes the SCID, the STID it labeled the CDR with, and the parameter ('flag') that states that the record was the last one for this component (since it was the only one).

The CDR-PM now adds the STID to the corresponding SCID in the Super Session Profile and then closes the SCID. Not all components have been received yet, so the Super Session Profile remains in the CDR-PM. Figure 5-23 shows the arrival of the second CDR, containing information on both transport components.

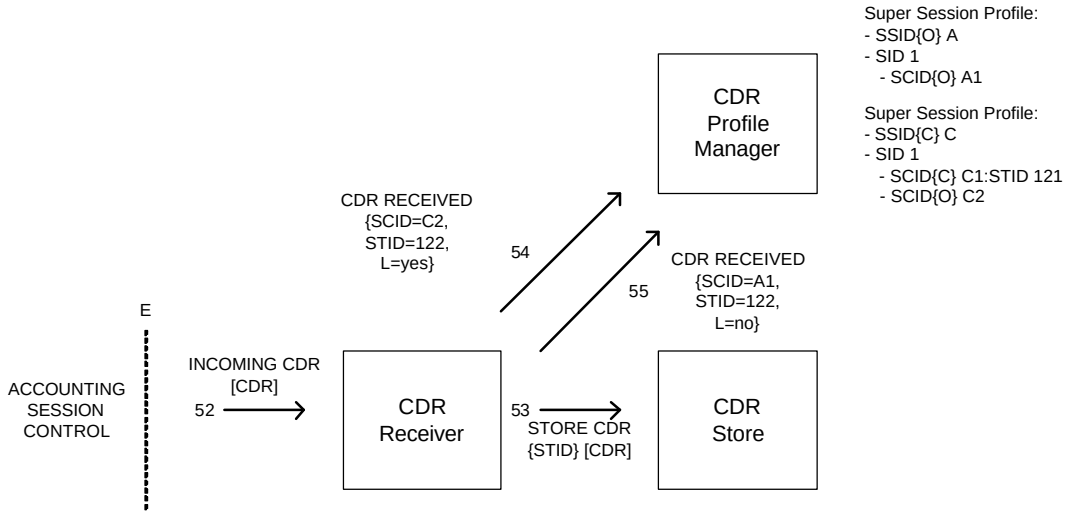

Figure 5-23: Second incoming CDR for the content session

52. Similar to 41 and 49, a CDR is received by the CDR-R. This one originates from the TP. The CDR-R generates a STID for the CDR (successively being '122'). The CDR-R also retrieves the SCIDs and sequence number from the record. The record contains two CDR cells, so two SCIDs are included.
53. Similar to 42 and 50, the CDR-R forwards the CDR to the CDR-S for non-volatile storage under the storage number (STID).

For simplicity, the two CDR cells are announced at the CDR-PM in two separate notification messages, both similar to 43 and 51. Combining these two notifications is very well possible, but not further explored in this thesis. The notification for the CDR cell concerning the content session transport component is arbitrarily sent first, followed by the notification of the reception of the partial CDR for the Home Broker Session.

54. The CDR-R notifies the CDR-PM of the reception of a CDR. The CDR-R includes the SCID, the STID it labeled the CDR with, and the parameter ('flag') that states that the record was the last one for this component (since there was only one transport component for the content session).
55. The CDR-R sends a second notification to the CDR-PM for the reception of the next CDR. The CDR-R includes the SCID, the (same) STID and the parameter ('flag') is set to state that it is a partial record (since there will be a second partial record coming in the future for this SCID).

After step 54, the CDR-PM is ready to forward the Super Session Profile to the CDR-P. This is similar to Figure 5-20, but for the sake of completeness this process is repeated in Figure 5-24. The difference between both figures lies in the open profiles at the CDR-PM.

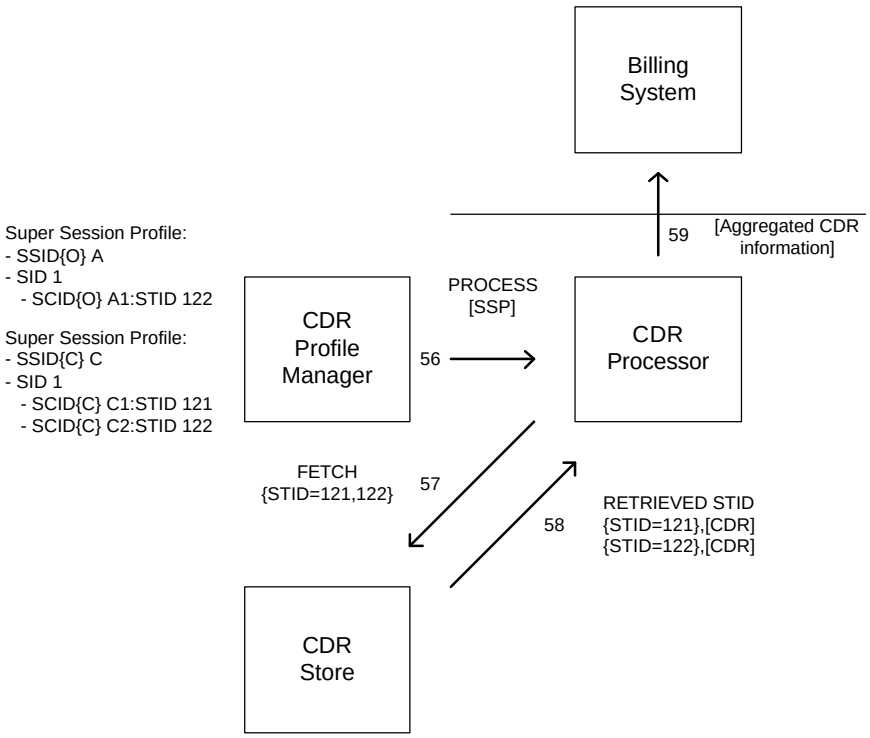

Figure 5-24: Super Session Profile processing (2)

56. Similar to 44, the CDR-PM forwards the Super Session Profile to the CDR-P. The profile contains the two SCIDs and the respective STIDs
57. Similar to 45, the CDR-P collects the STIDs from the profile and requests the corresponding records from the CDR-S.
58. Similar to 46, the CDR-S retrieves the CDRs from its non-volatile storage and sends them to the CDR-P.
59. Similar to 47, the CDR-P now interpreters the information from both records (ignoring the cell in the one CDR on the transport component of the Home Broker Session), accumulates all information, formats a correlated record and sends it to the Billing System.

This concludes the description and the functionality example of the Broker OCCF. This subchapter described the functionalities of both the SIM and ARM functions of the Broker OCCF. It exemplified the setup of both kinds of super sessions; a single (network) domain and a multi (content and network) domain super session. The distribution of accounting identifiers to session components and their use in correlating the corresponding component CDRs was shown.

5.5. Detailed description of the multi-domain accounting architecture design: Transport Provider OCCF

This subchapter describes the OCCF addition to a general Transport Provider. The Network Registration Function, the Network Session Control and Accounting Session Control functions have already been presented and their interactions with the Broker OCCF have been described.

The subchapter is organized in the following way:

- Section 5.5.1 lists TP OCCF requirements as derived from the Broker OCCF description in the previous subchapter as well as the TP OCCF sub-function descriptions.
- Section 5.5.2 describes TP OCCF setup and termination procedures and the resulting accounting procedure.
- Section 5.5.3 discusses several remaining TP OCCF considerations.

5.5.1. TP OCCF requirements

The following requirements are derived from the Broker OCCF description in the previous subchapter:

1. Registration of the mobile needs to be performed. It has already been stated that this is performed by native registration functions in the network and therefore this is not considered a part of the TP OCCF. The only requirement of transport network registration functions is that they must recognize that the mobile belongs to a Broker and they must be able to determine how to contact the NRM at the Broker OCCF. It is assumed that agreements on registration are made a priori by means of a SLA between the TP and the Broker.

2. The TP OCCF must be able to receive Session Enable {SID, SCID, Source, Destination} requests from the Broker over the B interface and subsequently facilitate the setup of that transport component. It must ensure that the SCID is included as a parameter in all relevant accounting records.

3. In case that the mobile requests a transport component through transport network specific ways, the TP OCCF must notice the request, pause the enabling, request a Session Enable and execute the Session Enable according to point 2 (in this particular order).

4. In case of external requests for a data connection with the mobile ('incoming network sessions'), the TP OCCF must perform the same actions as listed in point 3 (including those from point 2).

5. The TP OCCF must be able to receive Close Session {SID, SCID} requests from the Broker over the B interface and subsequently terminate the corresponding transport component.

6. When a network initiated termination or a dropped connection occurs, the TP OCCF must notice the event and subsequently inform the NSM over the B interface of the termination of the SCID.

7. Any internal accounting record that is constructed due to TP OCCF involvement includes a SCID. The TP OCCF must gather those records and format them in a previously agreed way for transfer to the Broker over the E interface.

8. Considering that a TP may interact with several Brokers, some form of registration is also necessary of which Broker to notify for a transport component termination.

TP OCCF Functional Elements
The following sub-functions have been described in section 5.3.1:

The **Network Registration Function** (NRF) is already discussed previously and will not be a focal point in the remainder of the TP OCCF description. The registration process is assumed to be performed independently and therefore the NRF is not part of the TP OCCF. The NRF may be queried by TP OCCF sub-functions for presenting the BrokerID for a particular SID. The NRF and the corresponding A interface are depicted in Figure 5-25.

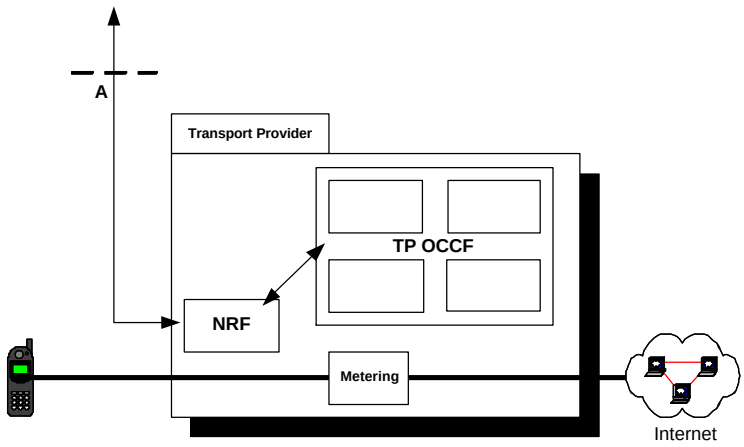

Figure 5-25: The Network Registration Function

The **Network Session Control** (NSC) has been included in the description of the Broker OCCF, with respect to the interactions they have over the B interface. The NSC exchanges orders and notifications with the Brokers and the Session Transformation Function. The necessity of maintaining a local cache of SID-BrokerID pairs will show in a later example. The NSC is shown in Figure 5-26.

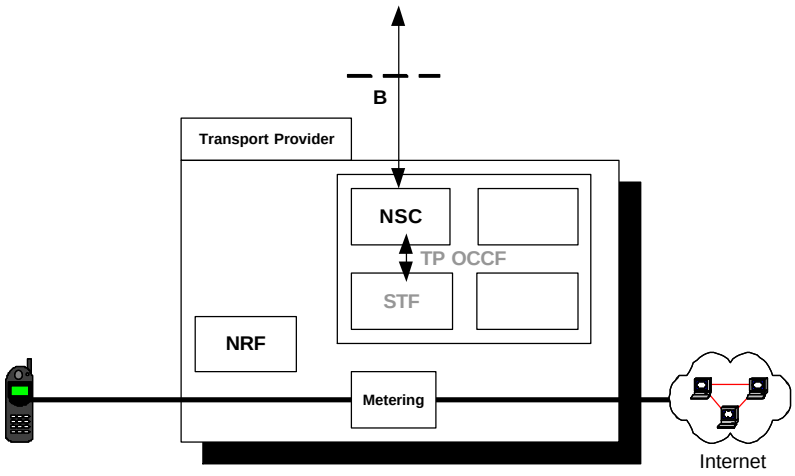

Figure 5-26: The Network Session Control

The **Session Transformation Function** (STF) is partially embedded in the transport network in a way that it can transform the Session Enable/Close Session requests into transport network actions. These actions result in the transport component setup or closure. The STF is also responsible for handing out the appropriate SCIDs to accounting elements within the transport network. Furthermore, the STF is responsible for intercepting mobile initiated and network initiated session requests, and transport component termination. The STF must accordingly notify the NSC of any of these events. The STF is chosen to maintain Broker Profiles, in which it registers the active transport components of SIDs per Broker, combined with any corresponding network type dependant session identifier that is linked to a particular SCID. This translation is necessary because native network nodes are not expected to be able to cope with orders based on a 'SCID'. They need to receive orders in their own (network type dependant) way. The functioning of the STF as a transport network node is not discussed here since it is network type dependant. Chapter 6 will show how the STF can interact with UMTS and WLAN network nodes. Figure 5-27 shows the STF within the TP OCCF.

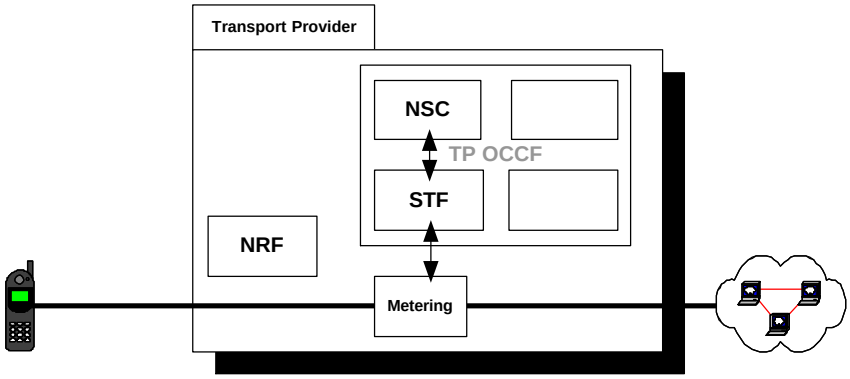

Figure 5-27: The Session Transformation Function

The **Accounting Transformation Function** (ATF) actively or passively gathers the accounting information, labeled by a SCID, from the network and formats it in an appropriate way for the ASC. The interval of this gathering is network type dependant and possibly also under influence of the respective SLA. With respect to the Accounting Management, the ATF performs the Collection stage and possibly the Accumulation stage within the TP domain. Figure 5-28 shows the ATF within the TP OCCF.

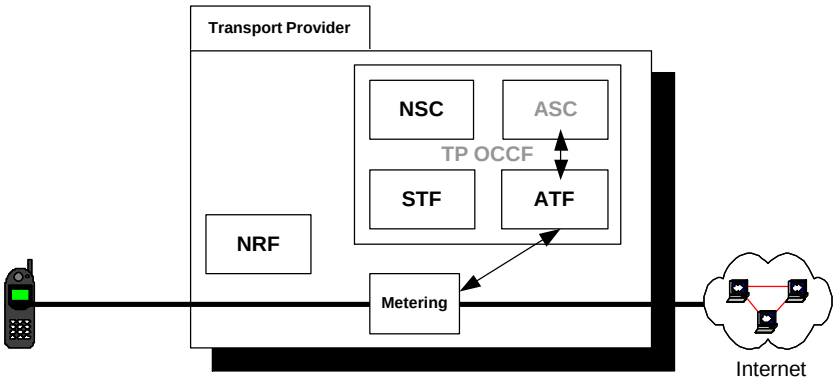

Figure 5-28: The Accounting Transformation Function

The **Accounting Session Control** (ASC) formats and sends CDRs to the Broker OCCF in a previously agreed manner over the E interface. The CDRs have been received from the ATF with the SCID label included and some information may be added, e.g. price information. It is assumed that the ASC can determine from the SID or SCID which Broker OCCF should receive the accounting information, similar to the NRF being able to determine which Broker OCCF to contact for registration information (section 5.4.1). The ASC is shown in Figure 5-29.

(In case that the ASC cannot determine the proper Broker OCCF from the SID/SCID, a list must be maintained of which SID belongs to which Broker. The NRF may be polled for the BrokerID in case it cannot be derived and it is not available in the locally cached list)

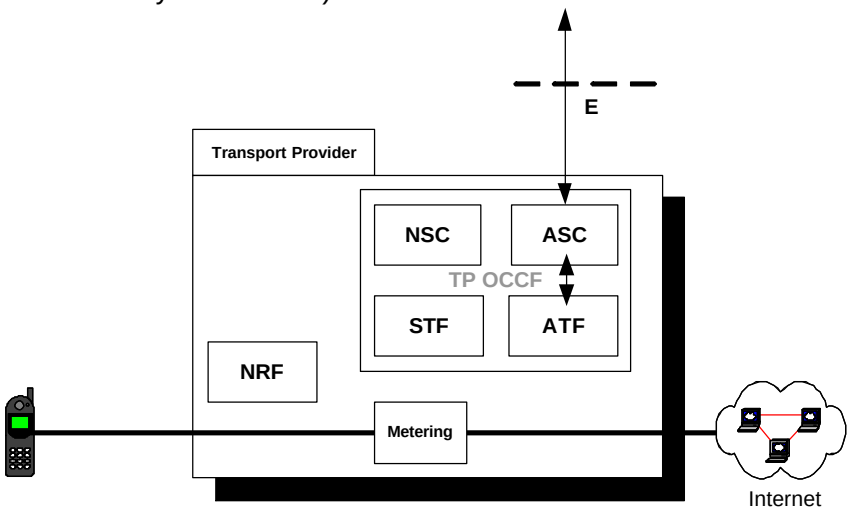

Figure 5-29: The Accounting Session Control

5.5.2. TP OCCF Procedures

This section describes the functioning of the TP OCCF. The core management is handling of Session Enable and Close Session requests from the Broker and the corresponding accounting records. Additionally, notifications must be sent to the Broker on network initiated sessions, which result in the Session Enable procedure. The focus lies on the TP OCCF and it is outlined in Figure 5-30. The double arrows denote interacting sub-functions. The TP OCCF description shall make use of the example described in section 5.4.5 by using the same SCID and SID labels.

The five procedures that are discussed in this section are the Session Enable procedure, the Session Close procedure, the accounting procedure, the handling of Network Initiated sessions and the handling of Network Initiated terminations

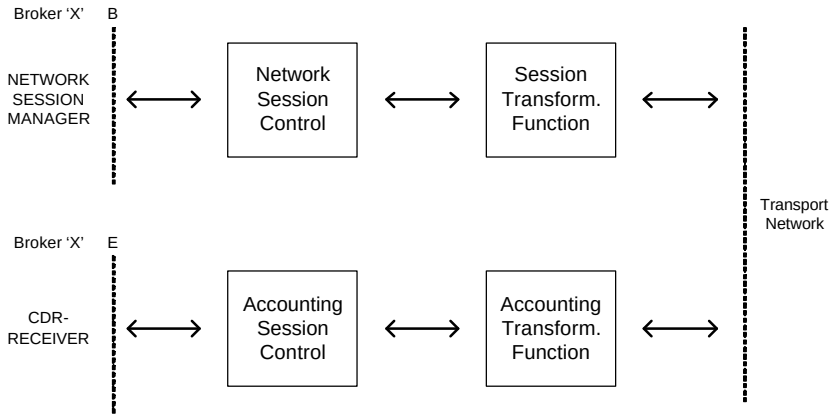

Figure 5-30: The TP OCCF

TP OCCF: Session Enable

It is assumed that the B interface is available for the NSC and NSM to exchange messages. This paragraph shows the handling of a Session Enable message (see Figure 5-31).

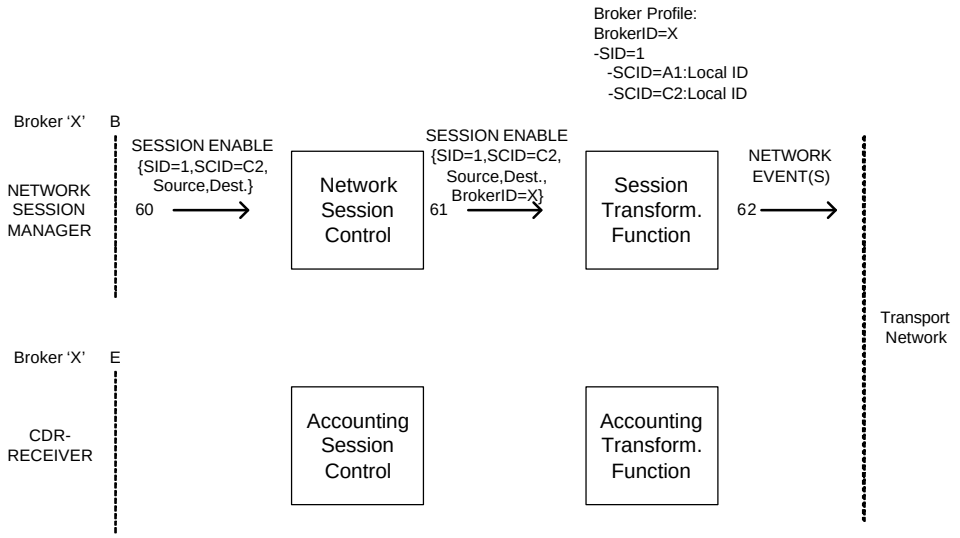

Figure 5-31: An incoming Session Enable message

60. The Session Enable message is received over the B interface from the NSM. It contains the SID, SCID, and Source and Destination address coherent with step 21 (and also 8) and uses the labels from step 39. (SCID 'A1' was used there to denote the Home Broker Session and is therefore already present in the Broker Profile)
61. The NSC forwards the request to the STF and adds a Broker identifier for the requesting Broker OCCF. This BrokerID is necessary at the STF in case of network initiated termination.
62. The STF facilitates the request and the transport network elements are instructed to include the SCID in their accounting records. Upon succeeding, the STF adds the SCID entry to the Broker Profile. At this point it is assumed that the SCID cannot be used within the transport network elements as a proper identifier and therefore the Broker Profile links the SCID to a corresponding network-particular identifier. Not regarded is any kind of notification message of success or failure back over the B interface.

The transport component is now enabled.

TP OCCF: Session Close

The NSM also issues Close Session messages for SCIDs. These messages need confirmation since the termination of session components is necessary information for consistent Subscriber Profiles at the Broker OCCF. The event is shown in Figure 5-32.

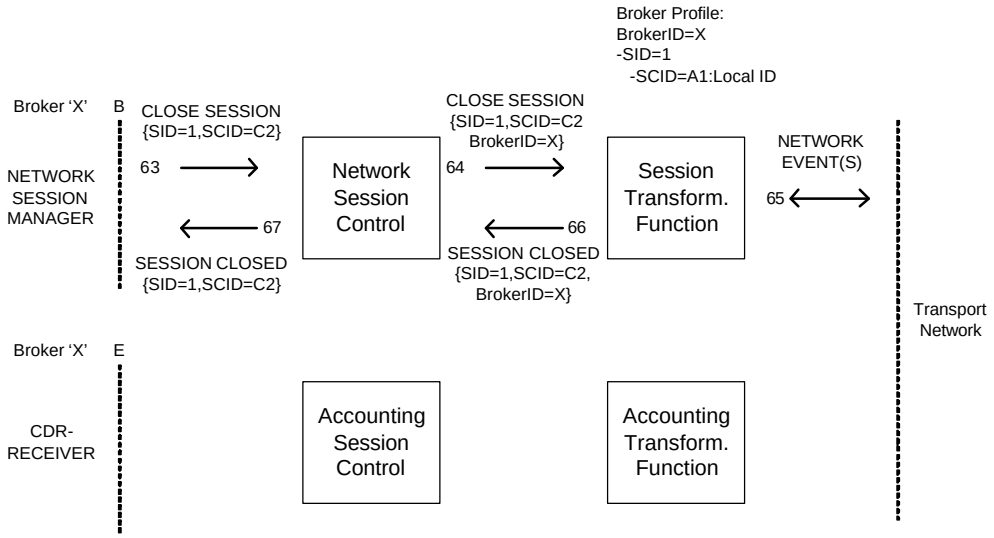

Figure 5-32: A Close Session event

63. A Close Session message is received in conformance with step 26. The NSC adds the Broker identifier to the message and forwards the message.
64. The STF receives the Close Session message.
65. The STF terminates the provisioning of the transport component through network type dependant ways. Subsequently it deletes the SCID entry from the Broker profile.
66. The STF sends a notification of the successful termination.
67. The NSC forwards the notification to the proper Broker network, which conforms to step 27.

The transport component provisioning has now terminated and the accounting process will automatically commence. The accounting records are either (actively) intercepted by the ATF, or they are sent there automatically (passively).

TP OCCF accounting procedure

The accounting information reaches the STF, either actively or passively, and the STF formats them into CDRs of an appropriate (intermediate) format. Eventually the CDRs are sent to the CDR-R. The intermediate CDR and the CDR that is sent to the Broker OCCF are not necessarily equal. The ASC may accumulate intermediate CDRs, add extra information or even change the record format if the internal CDR structure differs from the in the SLA agreed CDR format (see Figure 5-33).

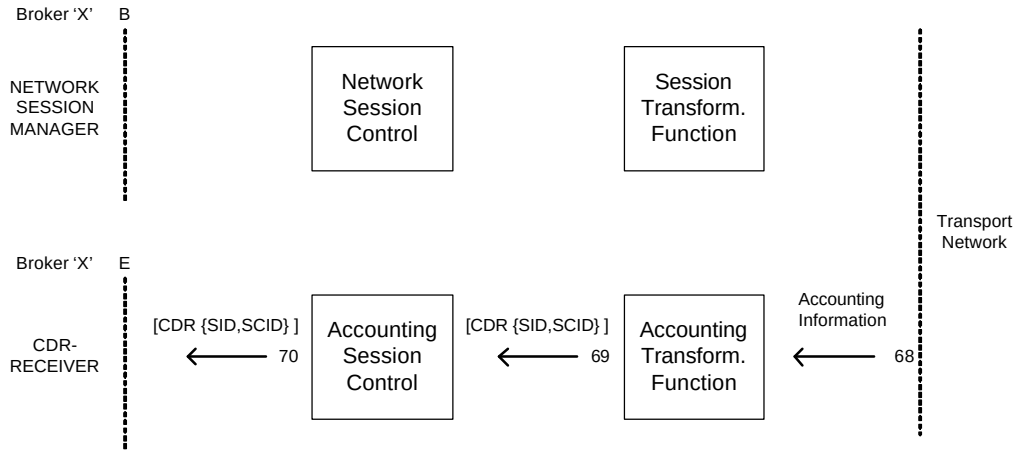

Figure 5-33: The accounting process within the TP OCCF

68. The accounting information is gathered at the ATF during or at the end of the transport session.
69. At a certain point in time, the CDR is completed and sent to the ASC. The decision of completing and sending a CDR is dependant of a number of aspects. E.g. the transport component could be terminated, a deadline for sending partial session information is reached, or the maximum value (monetary or data volume) of a CDR is reached. These triggers are operator specific and are likely to fall under the agreements of a particular SLA between the TP operator and the Broker.
70. The ASC is assumed to be able to determine where to send the CDR, based on the information within the CDR or static Broker information within the ASC itself. This assumption is discussed in the considerations at the end of this section. The CDR is forwarded to the proper CDR-R. It is unspecified if the ASC keeps a copy of the CDR for the TP administration or clearing process since this is a choice for the operator to make.

The accounting record(s) have been forwarded to the proper Broker and this completes the description of the TP OCCF for Session Enable/Close Session messages and their corresponding accounting process.

TP OCCF Network Initiated sessions

The Home Broker Session description in section 5.2.4 discussed super sessions that consist of only transport components. This applies to both the mobile initiated- and network initiated session requests. Both of these request types are referred to as 'network initiated' in this section for convenience, since they both originate from within the transport network. This paragraph and Figure 5-34 show how the network initiated session request results in a corresponding Session Enable message.

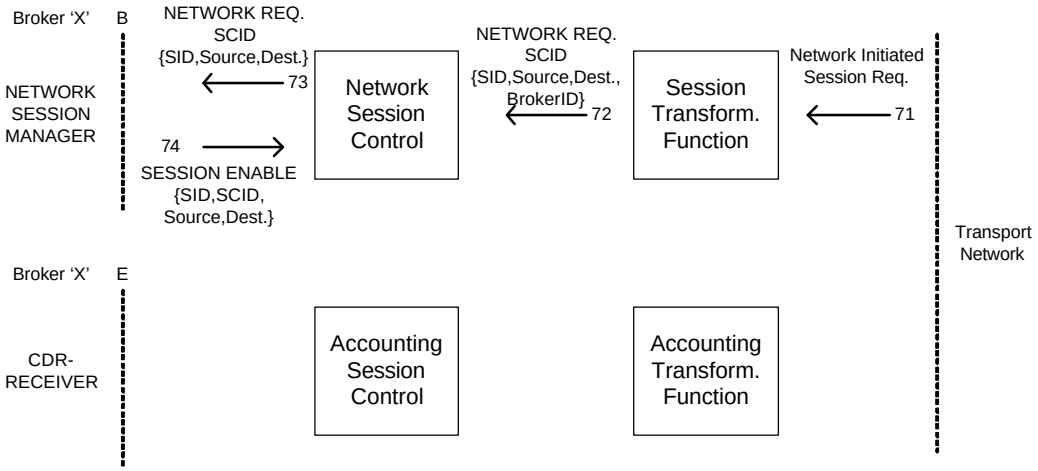

Figure 5-34 Network initiated session request

71. The Network Initiated Session Request reaches the STF through transport network specific means.
72. The STF sends out a Network Request for a SCID to the NSC, including the SID and the Source and Destination parameters. Also the BrokerID is included for proper reference. (See also the considerations in section 5.5.3.)
73. The 'Network Request for SCID' message is sent to the proper NSM in conformance with step 5.
74. The NSM returns the Session Enable command in conformance with step 8.

From this point on, the events are similar to the regular Session Enable message, as was described in the 'TP OCCF: Session Enable' paragraph at the beginning of this section. It is network type dependant if the STF needs to maintain some form of linkage between the network request and the subsequent Session Enable message. This will not be further considered here.

TP OCCF Network Initiated termination

This paragraph describes the Network Initiated session termination for the sake of completeness (see Figure 5-35).

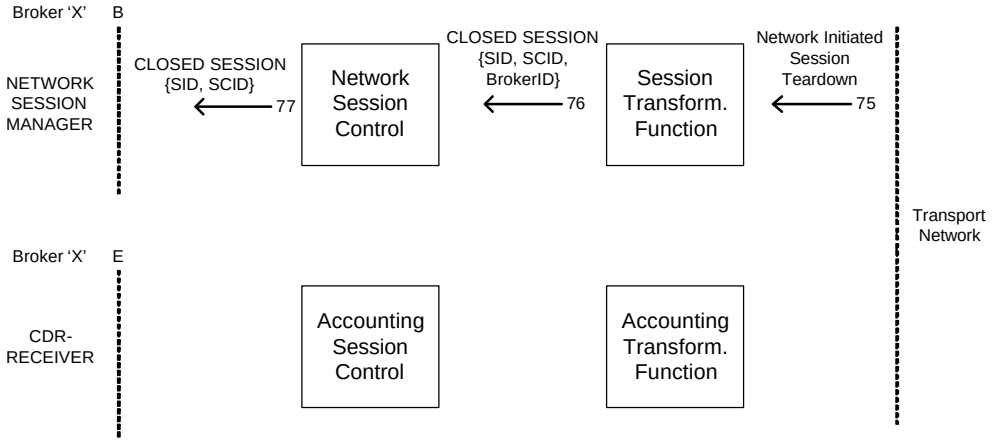

Figure 5-35 Network initiated session termination

75. Through network type dependant ways, the STF is aware of a network initiated session termination.
76. The STF deletes the corresponding SCID entry from the Broker Profile (not shown) and sends the notification message to the NSC.
77. The NSC notifies the appropriate Broker OCCF of the termination event.

5.5.3. TP OCCF considerations

Three additional considerations on the TP OCCF architecture are presented in this section.

First is the necessity of allowing the TP OCCF to query the NRF for BrokerID-SID combinations. This is undesirable since the NRF was stated to remain a native transport network element. One way to avoid this problem is to construct the SID in such a way that the Broker identity can be derived from it. Section 5.4.1 stated that 'the Network Registration Manager address can be derived from the information presented by the mobile upon registration by the transport network'.

Only when
a) this 'presented information' is not included in the accounting information gathered from the transport network and
b) there is no SID - Broker Identity combination available from previous SID accounting events at the TP OCCF sub-function in question and
c) no such link is available at any of the other sub-functions,
then the sub-function may query the NRF for the SID-Broker identity combination.
There is one situation imaginable when considering this TP OCCF architecture design where this problem occurs and this is the establishment of the Home Broker Session. The Home Broker Session is a network initiated session request for a SID that has no entry in any Broker Profile. Therefore a query may take place from the STF. Henceforth, other TP OCCF sub-functions may query the STF for the desired combination if necessary. Step 72 assumed that the BrokerID was available under this consideration.

A second consideration is that at step 62 the matter of confirmation messages was addressed. They add in reliability, but they are not essential for Session Enable messages and therefore they are omitted in this thesis. Additionally, the parameters mentioned in the messages contain only the bare essential information. It could be very handy for instance to include a reason of termination to termination messages over the B interface. Again, this is not a bare essential parameter and therefore not included here.

The third and final point of consideration is what kind of information is sent between the ATF and the ASC. The description did not make a clear choice for this issue. The accumulation of the transport provider accounting information may either be performed at the STF or the ASC. Factors outside the scope of this thesis (e.g. sub-contracting issues, real time billing issues, or even the choice of intermediate and final accounting information format) influence this choice and therefore no conclusion is drawn at this point.

These considerations conclude the description of the TP OCCF design.

5.6. Content Provider OCCF

The Content Provider architecture is not a direct subject of investigation in this thesis. But since the Content Provider is a very important party in the multi-domain session provisioning, this subchapter is included to describe the CP OCCF. The Content Session Control and Accounting Session Control are part of the CP OCCF and have already been mentioned in subchapter 5.3.

The subchapter is organized in the following way:

- Section 5.6.1 lists CP OCCF requirements as derived from the Broker OCCF description in subchapter 5.4 as well as the CP OCCF sub-function descriptions.
- Section 5.6.2 describes the CP OCCF content component setup and termination procedures and the resulting accounting process.

5.6.1. CP OCCF requirements

The following requirements can be derived from the Broker OCCF description in subchapter 5.4:

1. The CP OCCF must be able to receive Request Content {CID, SCID, Destination} requests from the Broker over the D interface and subsequently facilitate the setup of that content component. It must ensure that the SCID will be included as a parameter in all relevant accounting records. The CP OCCF must acknowledge the Request Content message and provide the source address of where the content component will be provisioned from. This is necessary information for transport components.

2. The CP OCCF must start the content provisioning when a Start {SCID} message is received from the Broker OCCF.

3. The CP OCCF must stop the content provisioning when a Close Session {SCID} message is received from the Broker OCCF.

4. The CP OCCF must send a Closed Session {SCID} notification message to the Broker OCCF over the D interface in case it terminates the content component by itself.

5. During or after a content session, the CP OCCF must gather, format and send the accounting CDRs (including the SCID) to the Broker OCCF over the E interface in a previously agreed way (SLA).

6. Considering that a CP may interact with several Brokers, some form of registration is also necessary of which Broker to notify for a content component termination.

When this is compared to the number of restrictions for the TP OCCF (section 5.5.1), it shows that the CP OCCF has fewer restrictions.

CP OCCF Functional Elements

The CP OCCF sub-functions show a strong similarity with the TP OCCF sub-functions. It is chosen for convenience that the transformation functions at the CP OCCF bear the same name as those in the TP OCCF. The difference between TP and CP counterparts is described where applicable.

The **Content Session Control** (CSC) has been included in the description of the Broker OCCF, with respect to the interactions they have over the D interface. The CSC exchanges orders and notifications with the Brokers and the Session Transformation Function (STF). The CSC is shown in Figure 5-36.

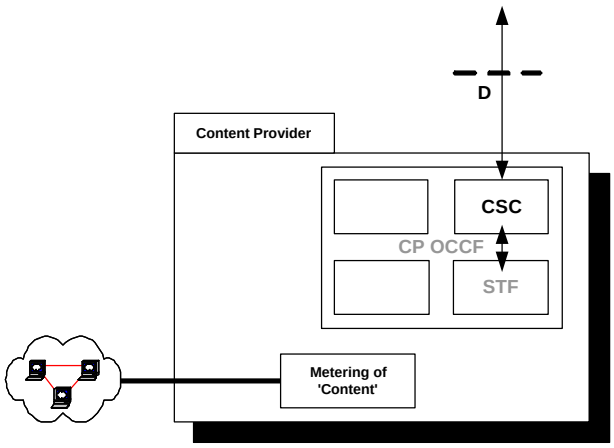

Figure 5-36: The Content Session Control function

The **Session Transformation Function** (STF) is the bridge between the CP OCCF and the content provisioning network. The STF can transform content session requests into network actions that result in the desired content component. Similar to the TP STF is the CP STF also responsible for handing out the appropriate SCIDs to accounting elements within the content provisioning network. Also content component termination is noticed by the STF and it subsequently sends out a Closed Session notification. Similar to the TP STF, the CP STF is chosen to maintain a profile in which SCIDs are linked to BrokerIDs. Note that the CP OCCF does not receive or maintain any individual subscriber identity information (SID).

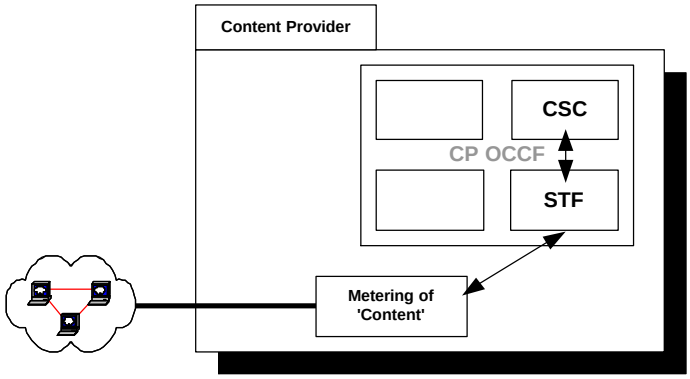

Figure 5-37: The Session Transformation Function

The **Accounting Transformation Function** (ATF) holds the (exact) same properties as the ATF at the TP OCCF. It gathers accounting information actively or passively and formats it in an appropriate way for the Accounting Session Control. The same remarks on the collecting interval and on Accounting Management stages can be made here as were described in section 5.5.3 . Figure 5-38 shows the ATF at the CP.

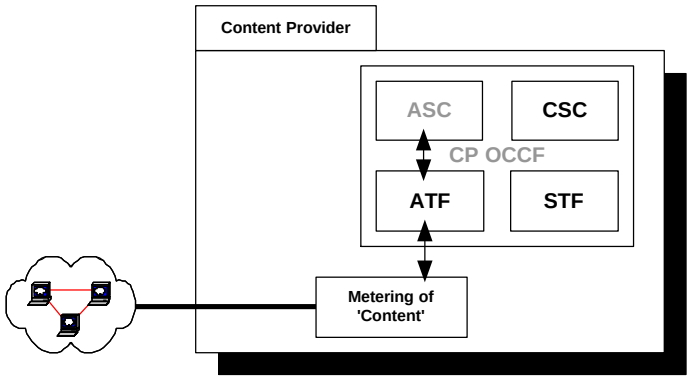

Figure 5-38: The Accounting Transformation Function

The **Accounting Session Control** (ASC) exchanges the accounting records with the Broker and this sub-function possibly differs from the TP ASC at only one point. The SCID is the only Broker information in the accounting records, since there is no SID present at the content provisioning network. In case that the BrokerID cannot be derived from the SCID, querying of the CP STF Broker Profile is allowed in order to retrieve the proper Broker identity. The ASC is depicted in Figure 5-39.

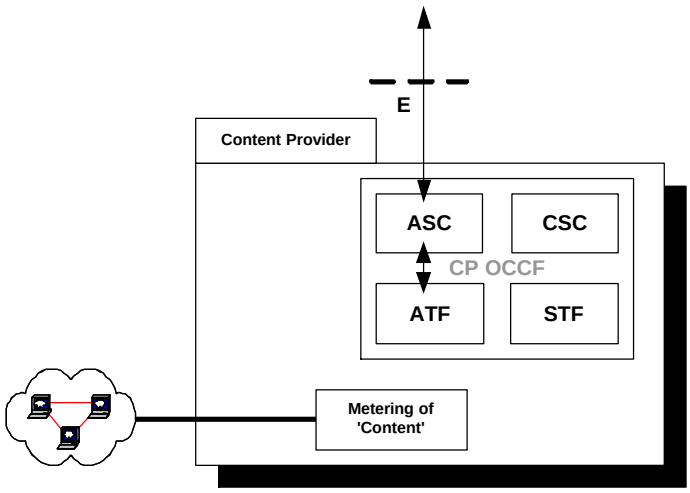

Figure 5-39: The Accounting Session Control

5.6.2. CP OCCF Procedures

This section describes the functioning of the CP OCCF. This example is simpler than the TP OCCF examples since only one party (the Broker) may request the provisioning of a content component. In some sense, the Broker is the 'subscriber' to the Content Service.

CP OCCF: session setup
The initial request for a content component creation comes from the Broker over the D interface. The actions at the CP OCCF are shown in Figure 5-40.

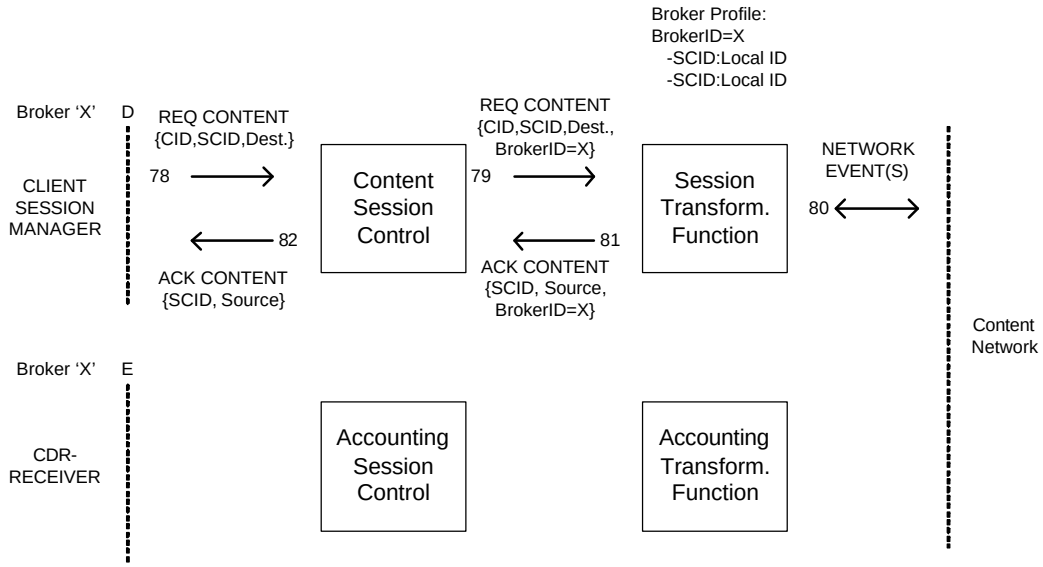

Figure 5-40: Content Session Component Setup

78. In conformance with step 16 is the CSC asked to provision a content component. The CID describes which content element is requested and the destination address is also included in the request.
79. The CSC forwards the request to the STF and adds the BrokerID to the request.
80. The STF sets up the delivery of the content element and targets it to the Destination address included in the request. Upon successful invocation it registers the SCID of the request in the Broker profile.
81. The STF sends a confirmation message back to the CSC and includes the source address of the content component. It should be noted that no content provisioning has commenced yet, since the Broker still needs to set up a transport component for delivery.
82. The CSC forwards the acknowledgement to the appropriate Broker OCCF to indicate that the content provisioning may be started. Upon failure of provisioning, this message will be a reject message, but this is not further explored in this thesis.

The CP now has the requested content element ready for provisioning and is waiting for a Start request from the Broker OCCF.
The CSC forwards the Start {SCID} request (step 25 in section 5.4.2) to the STF upon reception and the STF subsequently starts the content component. This is not depicted since the Start message is just forwarded unaltered.

The accounting procedure is identical to the TP OCCF accounting procedure, which was described in section 5.5.2, 'TP OCCF accounting procedure'. The only difference exists on the BrokerID lookup procedure. This procedure was described in the description of the Accounting Session Control in section 5.5.1.

CP OCCF Session Close

The CP OCCF requirements show that termination of a content component is initiated either by the Broker or by the CP. The first is shown in Figure 5-41 and the second in Figure 5-42.

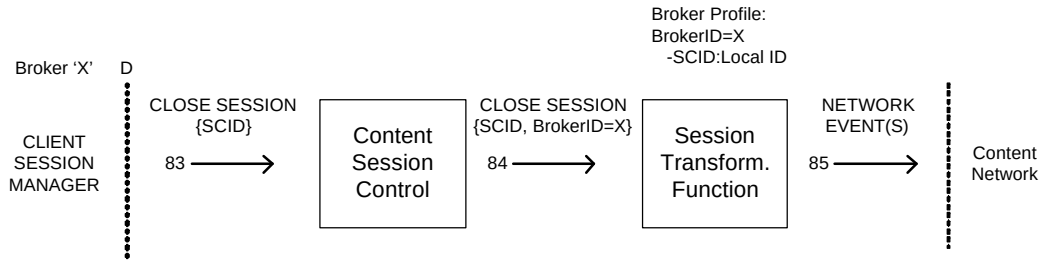

Figure 5-41: Broker initiated session termination

83. The Close Session request is received by the CSC.
84. The CSC adds the BrokerID and forwards the request to the STF.
85. The STF interacts with the content provisioning network in such a way that the content provisioning is terminated and the accounting process automatically commences. The STF subsequently deletes the SCID entry form the Broker profile.

One may argue that a confirmation message of the termination to the Broker will add in reliability, but since they are not essential for Close Session messages, they have been omitted in this thesis. The following example of Network Initiated Session Termination, as shown in Figure 5-42, could be useful as a confirmation message as well.

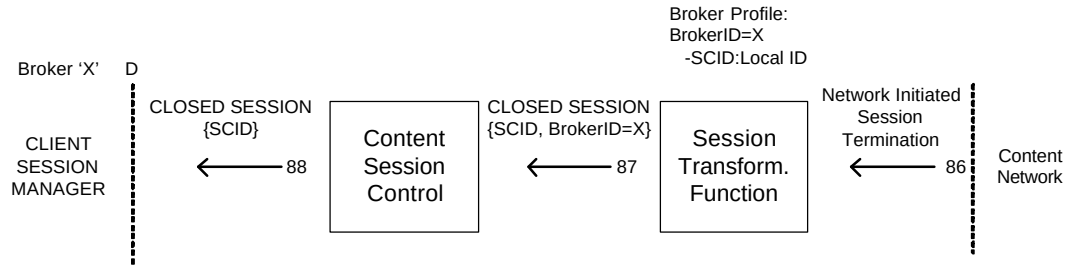

Figure 5-42: CP initiated session termination

86. The STF notices a termination of a particular content component through network type specific means. It is assumed that the accounting process is started automatically.
87. The STF looks up the SCID according to the local identifier of the content component and deletes the SCID entry from the Broker Profile. The STF sends a notification message of the termination to the CSC.
88. The CSC sends the notification of termination to the Broker OCCF over the D interface.

The assumption was made in both cases that the accounting process was started automatically. This should be included in the design of the content network and both transformation Functions. Since such a (content network) design is not part of this thesis, this matter remains unspecified and it is assumed that the CDRs (including the SCID) are eventually sent to the Broker over the E interface. This is depicted without specifications in Figure 5-43, which is similar to the TP case of Figure 5-33.

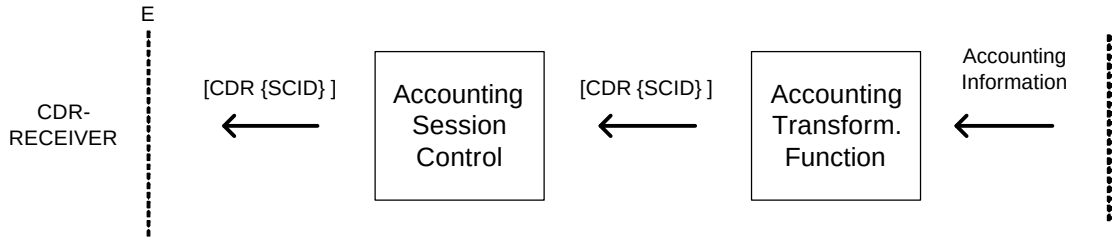

Figure 5-43: Accounting records creation

This concludes the description of the general design of the OCCF at the Broker, the Transport Provider and the Content Provider in this chapter. Their interfaces have been described and the message exchange has been shown through the ongoing example(s).

6. TP OCCF mapping into transport networks

The previous chapter described the proposed multi-domain accounting architecture for general Transport Providers and Content Providers. The description is refined by regarding the inclusion of the proposed TP OCCF to actual transport network architectures. The two chosen transport network technologies of UMTS and WLAN have been described in chapters 3 and 4.
The TP OCCF requirements applicable on transport networks are presented in subchapter 6.1. The TP OCCF mapping into the UMTS and WLAN transport networks is presented in subchapters 6.2 and 6.3, respectively.

The TP OCCF
Subchapter 5.5 discussed the TP OCCF without including a particular transport network architecture. In the description, the TP OCCF consisted of four sub-functions. Two were described as uniform for every TP that uses the multi-domain accounting architecture. These two were the Network Session Control (NSC) and the Accounting Session Control (ASC); see the TP OCCF model in Figure 6-1. The two other sub-functions transform the OCCF commands into actions within the transport network and they were named the Session Transformation Function (STF) and the Accounting Transformation Function (ATF).

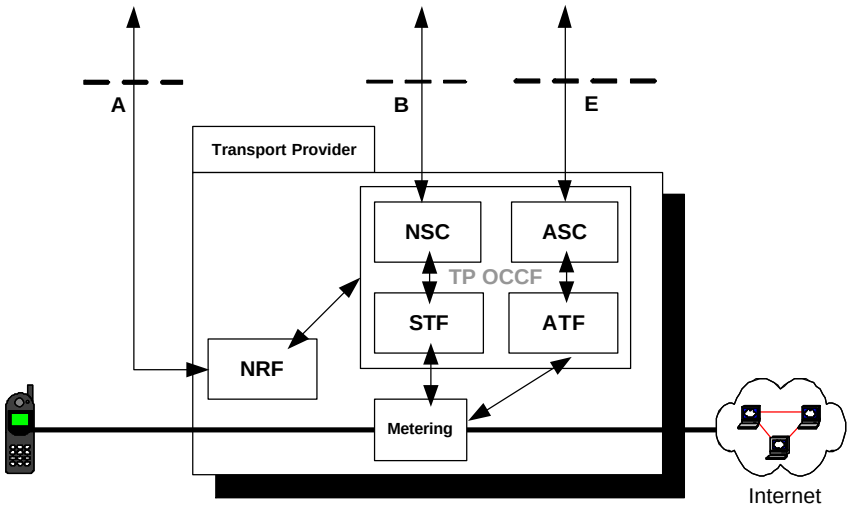

Figure 6-1: The TP OCCF model

This chapter regards the interactions between the STF and the transport network (in Figure 6-1 depicted by a 'Metering' element) and the ATF and the accounting system of the transport network.

6.1. TP OCCF Requirements

The STF and ATF interact with the transport network-specific elements to ensure the proper working of the OCCF multi-domain accounting architecture.
The requirements for both the STF and ATF to facilitate the proper working of the OCCF with the transport network are listed below and they will be addressed by number in the next subchapters.

Requirement 1: STF identifier administration
If necessary, the STF should maintain a list (Broker Profile) of network-particular session identifiers and the corresponding SCID. This occurs when the SCID generated in another (Broker) domain cannot be used as a network session identifier in the TP domain. This has also been mentioned at step 62, section 5.5.2.

Requirement 2: STF session setup
The STF should facilitate the setup of a Broker requested transport session component from the available information of the SID, the Source and the Destination address. This corresponds to the Session Enable command described in step 61, section 5.5.2, and the succeeding step 62. The BrokerID does not hold any value outside the TP OCCF, since it is only used in the STF Broker Profile. Therefore it is not included in this setup requirement (see also Requirement 3).

Requirement 3: STF accounting setup
The STF should facilitate the setup of the accounting process for transport components and make sure that the SCID is included in the accounting records. This requirement comes in combination with Requirement 2 and is also a result of step 62, section 5.5.2.
No requirement is included on the interval of accounting, or any other (time) restrictions that apply to the accounting setup, since they are operator dependant or under the influence of a particular Service Level Agreement.

Requirement 4: STF Session closure
The STF should facilitate the closure of a transport component from the available information of a SID, SCID and BrokerID triplet and, if applicable, the corresponding local network session identifier. This corresponds to step 65 of section 5.5.2. Closure of a transport component implies that the accounting process for the session is also consolidated within the network according to the method that was decided upon setup (see Requirement 7).

Requirement 5: STF mobile/network initiated session requests
The STF should be notified of mobile initiated and/or network initiated session requests and must subsequently fetch a SCID for that session request. This corresponds to step 71, section 5.5.2. The alarming network element must not activate the transport component until the STF has received the SCID (as a result of the Session Enable message), since all accounting records must contain the SCID. Premature provisioning undermines this accounting requirement.

Requirement 6: STF mobile/network initiated session termination
The STF should be notified of mobile initiated and/or network initiated session termination. As a result, the NSC must inform the Broker OCCF of termination of the transport component for consistency in the Subscriber Profile. This was shown in step 75 of section 5.5.2.

Requirement 7: ATF accounting record reception
The ATF is required to either actively or passively gather accounting records from the transport network nodes. Active gathering may take place for instance upon notice of a session closure. Passive gathering may take place when the STF instructs the network nodes to send their accounting records to the ATF during the session as well as upon (component) session closure.

These seven requirements have been derived from the TP OCCF description in subchapter 5.5 as necessities to have a transport network support the multi-domain accounting architecture. Also, **any** transport network that supports these

requirements and includes the TP OCCF in their network may participate in the accounting architecture.

6.2. TP OCCF mapping into the UMTS architecture

This subchapter describes the embedding of the TP OCCF into an UMTS core network. The goal is to minimize the necessary changes to the standardized elements of the core network while supporting all the requirements that were stated in the previous subchapter. The UMTS network and its elements are described in subchapter 3.1 and accounting in UMTS in subchapter 4.1. One solution that meets the requirements is described, yet several other solutions could be developed. The proposed UMTS solution is evaluated in the concluding paragraph of this subchapter.

The STF and ATF in an UMTS Network
Before describing the solution to each requirement, the location of the TP OCCF is discussed. Since the TP OCCF adds new functionalities to the UMTS network that should not interfere with regular UMTS operations, the proposed location for this solution is in a separate network element on the backbone network. The SGSN and GGSN are the two metering elements and they normally send their accounting records to the CGF. This is depicted in Figure 6-2, and it only shows the STF and ATF since they are the only OCCF parts that communicate with the network elements. The TP OCCF does not participate in the common UMTS operations like PDP Context management or data transfer, nor does it participate in regular UMTS signaling messaging.

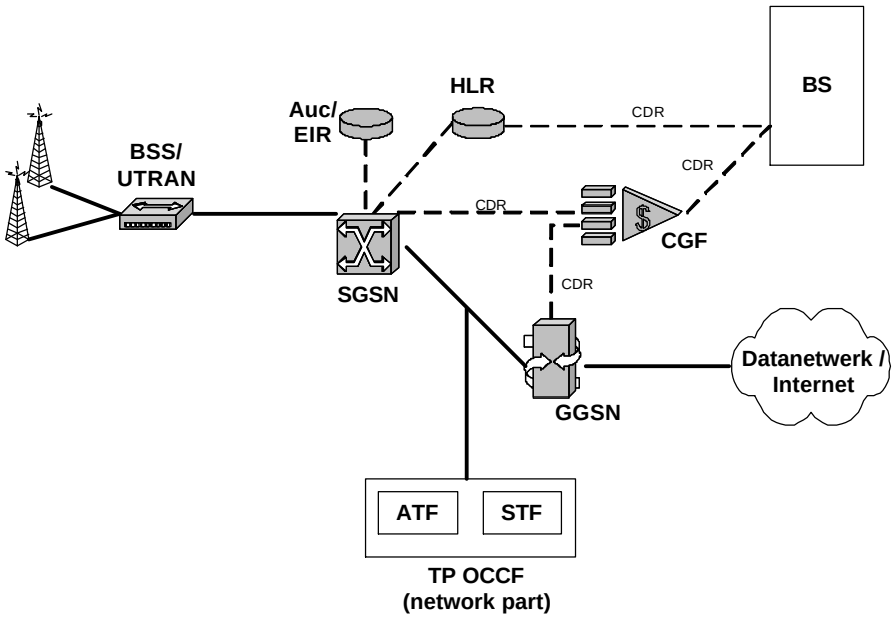

Figure 6-2: the TP OCCF as a backbone network element

The requirement descriptions make use of the interactions between an STF agent application at the GGSN and the STF. PDP Context sessions always stay at the same GGSN during the provisioning, and therefore it is logical to have TP OCCF

interactions with this network element. The choice for this solution shall be evaluated after each requirement is fulfilled:

Fulfilling Requirement 1: STF identifier administration
It is questionable whether or not the STF agent can use the SCID to point to a particular PDP Context in the GGSN. This would require that the GGSN must base its PDP Context management information on a foreign identifier. Normally the Tunnel Endpoint IDentifier (TEID) is used within the GGSN to identify a PDP Context, as described in section 3.1.1. Since a PDP Context does not change the serving GGSN during its life cycle, the TEID at the GGSN can be used to address PDP Contexts. The translation between the SCID and the TEID takes place at the STF by use of the Broker Profile, as was shown in step 62 of section 5.5.2 to keep the SCID out of the UMTS session management.

It is therefore concluded that the TEID is a proper identifier for PDP Context reference between the STF (agent) and the GGSN.

Fulfilling Requirement 2: STF session setup
To initiate a PDP Context setup as a transport component, the STF triggers a UMTS 'Network Requested PDP Context Activation Procedures' at the GGSN by presenting the SID and the Source and Destination Address of the mobile to the Agent application. Section 9.2.2.2 of [3] states that the GGSN needs to have static PDP Address information in order to initiate such a procedure. It is assumed that providing the PDP Address through the STF (as Destination Address, received by the Broker from the mobile over the Home Broker Session) is equal of status to static PDP Address information. If this is not the case, the GGSN may perform a lookup in its PDP Context table for the PDP Address belonging to the Home Broker Session, since the latter uses the same Destination address as presented in the request.

The new PDP Context shall often not be a secondary PDP Context, since section 9.2.2.1.1 of [3] states that secondary PDP Contexts share not only the PDP Address, but also the Access Point Name (APN). If one APN denotes the Broker network or a particular Content Provider network, then it is obvious that different networks have different APNs. Therefore no secondary PDP Context could point to a Content Provider network if the primary PDP Context points to the Broker Network.

In the Network Requested PDP Context Activation Procedure that is used here, a 'PDU Notification Request' {IMSI, PDP Type, PDP Address, APN} message is sent by the GGSN to the SGSN. The SGSN solicits the mobile to request the PDP Context by presenting this information, which the mobile subsequently does.
Normally this procedure is then finished, but for TP OCCF compatibility, the GGSN must return the TEID it appointed to the STF request for inclusion in the Broker Profile.

It is therefore concluded that by triggering the Network Requested PDP Context Activation Procedure at the GGSN, the STF agent can set up Broker requested transport components.

Fulfilling Requirement 3: STF accounting session setup
The SCIDs need to be included in all relevant CDRs of the SGSN and the GGSN. Step 4 of section 9.2.2.1 of [3] states that when the GGSN adds the PDP Context to the PDP Context table, it also generates a Charging ID. It is assumed that at

this point the 'External Charging Identifier' is also added to the first (and possibly subsequent) G-CDR(s). Since the GGSN function does not use External Charging Identifiers for its own functioning, it is assumed that they are included as a result of additional GGSN applications requesting the inclusion.
The Requirement 3 can be met by including the SCID in the G-CDRs as External Charging Identifier. The SCID must then be included in the PDP Activation information from Requirement 2. The STF agent is the GGSN application that presents the External Charging Identifier.

The pending STF agent setup request must be maintained throughout the Network Requested PDP Context Activation Procedure until the PDP Context is created in order to include the SCID as External Charging Identifier. For unambiguous correlation, only one STF Network setup request per SID may be presented to the GGSN simultaneously. It will then be impossible that the GGSN includes the wrong SCID in the CDRs. Please note that Requirement 2 also demanded to maintain the agent setup request in order to return the TEID to the STF.

It is therefore concluded that by presenting the SCID with the setup request to the GGSN, the GGSN can include the SCID as External Charging Identifier in its G-CDRs and that this is sufficient to correlate the S-CDRs and G-CDRs (when combined by the CGF) with the SCID. Figure 6-3 shows the accounting record collection from the SGSN and GGSN by the ATF and the management relationship between the STF and the STF agent at the GGSN.

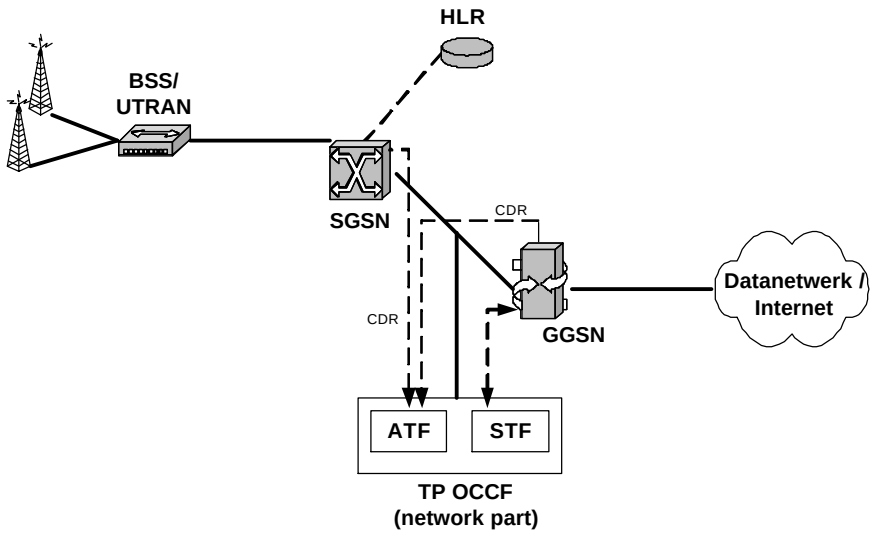

Figure 6-3 The TP OCCF

Fulfilling Requirement 4: STF Session closure
Upon the reception of a Session Close message from the NSC, the STF can look up the corresponding TEID for the SCID in the Broker Profile. The STF passes the request on to the agent. The STF agent can now present the TEID with a termination request to the GGSN. The GGSN subsequently initiates a 'GGSN-initiated PDP Context Deactivation Procedure' as described in section 9.2.4.3 of [3]. Termination of a PDP Context is assumed to be an automatic trigger for the SGSN and GGSN to construct and send their respective CDRs to the CGF.

It is therefore concluded that presenting the TEID in the termination request to the GGSN is sufficient for termination of a transport component and that the accounting records are subsequently constructed and collected at the CGF.

Fulfilling Requirement 5: STF mobile/network initiated session requests
It has already been stated that normal Network Requested PDP Context Activation Procedures solicit the mobile to initiate a PDP Context Activation Procedure.
Therefore the interception of PDP Context activation at the GGSN for including a SCID only needs to take place upon mobile initiated activation procedures. The 'worst case' scenario occurs when the mobile requests a PDP Context for the Home Broker Session. It is then that the GGSN needs to recognize that the request originates from a Broker subscriber and that it needs to acquire a SCID before facilitating the (any) PDP Context request.
One solution is that the GGSN recognizes the Broker subscriber from the SID in the request. If this is not possible, another way of forwarding this information is to make use of the operator-specific ('Behavioral') part of the Charging Characteristics. Section 4.1.2 already showed that a Charging Characteristics Profile is loaded at the SGSN from the HLR upon registration of the mobile. The HLR (as Network Registration Function) must therefore present a Broker subscriber specific Charging Characteristics Profile to the SGSN that includes such an identifier. Please note that the proposed Charging Characteristics do not tell WHICH Broker is involved, but only that the subscriber makes use of a Broker. Resolving which Broker is to be contacted is not part of the STF to GGSN interactions and this has already been considered in section 5.5.2.

Assuming that either solution is effective, the GGSN is aware that it needs to address the STF for a SCID for inclusion in the CDRs. The SCID request must include not only the local TEID identifier, but also the Source (mobile) address and the Destination (e.g. Broker network) address, and of course the SID (IMSI) of the mobile. Apart from the TEID all the necessary information is available from the original 'Create PDP Context Request' coming from the SGSN (step 4 of section 9.2.2.1 of [3]). The GGSN must initiate a SCID request procedure after constructing its TEID and before responding to the Create request of the SGSN.

It is therefore concluded that the GGSN has a single point at which it must request a SCID from the STF agent for a particular mobile initiated transport component setup in order to properly facilitate that setup. The necessity of adding information to the Charging Characteristics is dependant on derivation of the BrokerID from the SID (IMSI), but very well possible in the operator-defined space.

Fulfilling Requirement 6: STF mobile/network initiated session termination
Also network initiated termination of a PDP Context must be reported to the STF. All deactivation procedures involve the GGSN according to 9.2.4 of [3]. The solution to this requirement is that the GGSN sends an alert to the STF agent upon termination (closure) of a PDP Context. The message includes the TEID that was in use, and possibly the SID (for faster lookup in the Broker Profile if the SID and the BrokerID are related).

It is therefore concluded that this requirement can be fulfilled with a single alert from the GGSN to the STF agent upon termination of a PDP Context.

Fulfilling Requirement 7: ATF accounting record reception
Accounting records (CDRs) are sent to the CGF by the SGSN and the GGSN either at the termination of a PDP Context, or as a result of a trigger event. The trigger events are described in the Charging Characteristics Profile (Annex A of [9]) and are operator-dependant. The Charging Characteristics Profile optionally includes the preferred CGF address.

This requirement is met when the ATF operates as an additional CGF node in the UMTS network and every Broker subscriber is given the Charging Characteristics Profile in which the ATF address is listed as the mandatory CGF. The ATF will then automatically receive all CDRs that are related to Broker subscribers. The ATF can (like any CGF) correlate the S-CDRs to the G-CDRs through the Charging ID and since the SCID is listed as an External Charging Identifier in the G-CDRs it can gather all accounting information for a particular transport component. Section 5.5.2 already described the rest of the accounting process within the TP OCCF.

The ATF-CGF operates independently from the other CGFs, thus not disturbing their legacy function. It is therefore concluded that by including the ATF address as the mandatory CGF in the Charging Profile of Broker subscribers, all relevant CDRs are sent to the ATF. The ATF may subsequently accumulate all accounting information by using the Charging ID and the SCID.

Solution discussion
The solution for adding TP OCCF functionality to UMTS networks in the way that was described above introduces a primitive third-party setup procedure. This has not yet been facilitated within the UMTS network in any other way. A third-party setup procedure is defined as an outside party issuing a connection between two peer parties. This procedure is necessary if the Broker is to be in control of transport component management.

The solution proposed the use of TEIDs in GGSN-STF communications. This was done since the GGSN administers its PDP Contexts by TEID. The TEID structure is not defined since it is intended for private GGSN use only. Therefore, when a UMTS network consists of multiple GGSNs and TEIDs are not defined unambiguously within the network, the TEID might not be suitable as a local identifier in the Broker Profile at the STF. Alternatively, the Charging-ID could be used. The Charging-ID has been defined as a combination of the GGSN address and a random number, unique within a time frame of approximately 100 days (‘Charging Identity’, section 4.1.2). However, it is unclear if and how the GGSN is able to trace the Charging-ID back to the corresponding PDP Context and choosing between either the TEID or the Charging-ID (or possibly another alternative) could remain an implementation choice.

The communications between the STF and the STF agent at the GGSN require a protocol. This protocol has not been further investigated due to time restraints. Also, it is not a critical accounting issue which protocol is used, as long as the SCID is passed on to the GGSN as External Charging ID. The SNMP protocol described in section 4.2.3 could be a candidate to facilitate the message exchange between the STF and the STF agent, but this has not been investigated further.

The paragraph ‘Correlation information management’ of subchapter 5.1 discussed the choice of having the Broker construct a SCID over the use of the local identifier (TEID, Charging-ID, etc). The proposed solution for the UMTS network shows that this choice has a performance impact. Instead of immediate provisioning for mobile initiated or network initiated transport sessions, the provisioning must wait until the SCID is present. If the local identifier were to be used in the Broker OCCF, the provisioning could take place without interruption since such a mobile initiated or network initiated transport session setup would only require a notification to the Broker OCCF of the provisioning. Valuing the benefits and disadvantages of either choice can be based upon the consideration of which event occurs the most. Generally the mobile starts with the Home Broker Session, which is a mobile initiated session setup. Further study needs to be done to be able to conclude how the extra complexity of the Broker OCCF stands to the extra delay for the mobile initiated or network initiated sessions.

Conclusions

This subchapter proposed a solution for mapping the TP OCCF into a UMTS transport network. The requirements for supporting the multi-domain accounting architecture by transport networks as described in subchapter 6.1 have been discussed and each of the requirements has been met. The alterations and/or additions to the UMTS architecture are:

- The TP OCCF is located at a separate network element.
- The HLR must recognize subscribers from a Broker and resolve the BrokerID from the registration information (preferably from the presented SID).
- A separate Charging Characteristics Profile must be defined in which the Accounting Transformation Function is listed as mandatory Charging Gateway Function. If necessary, the operator specific space of the Charging Characteristics must include an identifier that says that the subscriber uses a Broker.
- The GGSN must interact with a Session Transformation Function agent application on transport component setup and termination, as well as on SCID exchange. The SCID must be included in the G-CDRs as an External Charging Identifier. The Tunnel Endpoint IDentifier (TEID) of the GGSN is chosen to distinguish PDP Contexts in the interactions with the STF and the Charging-ID is mentioned as an alternative for this.
- The Accounting Transformation Function at the TP OCCF must operate within the UMTS network as a Charging Gateway Node in order to receive all relevant CDRs.

These alterations modify as little as possible of the current UMTS architecture for facilitating transport components and communications with the Broker.

6.3. TP OCCF mapping into a WLAN architecture with Diameter

This subchapter presents *one of several* possible mapping methods of the TP OCCF into a WLAN transport network. WLAN networks have been discussed in subchapters 3.2 and 4.2. The proposed solution for adding TP OCCF functionalities to the WLAN network includes the use of the Diameter protocol described in section 4.2.2. Diameter allows the collection of resource usage information at the Diameter server and will show that inclusion of the required SCID in the accounting records is possible. Also, Diameter offers the possibility of intermediate accounting records, which will also show its necessity in this subchapter. The Diameter base protocol in the referenced form ([12]) is still 'work in progress', but this document is expected to be submitted soon in an almost integral form as an RfC. Therefore the description of the TP OCCF addition in this subchapter is based on [12] in anticipation of the soon-to-be released RfC. The proposed solution of using Diameter is evaluated in the concluding paragraph in this subchapter.

The AAA ('Authentication, Authorization and Accounting') working group of the IETF compared four AAA protocols according to a set of requirements and published these in the RfCs 2989 ([25]) and 3127 ([26]). The Diameter protocol achieved a slight preference over the other three protocols in the end conclusions. Ventura [27] also concluded that 'the Diameter protocol is going to be the most widely used AAA protocol of the Next Generation on the market'. Both these conclusions support the choice for Diameter as a possible AAA mechanism in WLAN. This choice does not exclude the use of any other accounting system in WLAN networks, but merely shows that the Broker model and OCCF system can work with at least one type of accounting system. Only the Accounting part of the Diameter protocol has been investigated in this report due to time restraints.

The STF and ATF in a WLAN Network with Diameter

Before describing the solution to each requirement, the location of the TP OCCF is discussed. The limited research that has been done for this thesis in the Diameter protocol as mentioned above puts some important constraints on the location of the TP OCCF and the interactions it has with the WLAN network elements.
For instance, the question of what Diameter considers a 'session' has not been sufficiently researched. Since the Diameter accounting is based upon the 'session' concept, it is critical for the TP OCCF design to know if a 'session' either embodies all data communications of the mobile, or if a mobile can have multiple 'sessions' to support accounting for separate transport components. Since no sufficient answer has been found to this matter, it is assumed that the mobile has only one 'session' and that a solution must be found within Diameter to describe accounting for separate transport components.

It is clear however, that the Accounting part of the Diameter base protocol operates on a 'push' model. This means that the Network Access Server (NAS) sends the accounting records to the Diameter server for storage and processing, and that the server has no means of initiating an accounting session. Such initiative could be embedded in the Authentication and Authorization part of Diameter, but this has not yet been researched. Therefore the transport component session management cannot be described by using the accounting part of the Diameter protocol. The session management is necessary to transform the Broker OCCF Session Enable requests into provisioning and accounting for that session component. The described TP OCCF solution in this subchapter shall

therefore consist of the Diameter server-client model for the accounting record handling (Accounting Transformation Function, ATF) and an additional abstract server-client model is described to handle the session management (Session Transformation Function, STF). Where possible, requirements for the latter are described and the implemented protocol could be the Diameter Authentication and Authorization protocol, or alternatively the SNMP protocol that was also mentioned in the UMTS OCCF solution in subchapter 6.2. The proposed location of the TP OCCF as separate network element, consisting of a Diameter server and an unspecified STF manager is shown in Figure 6-4

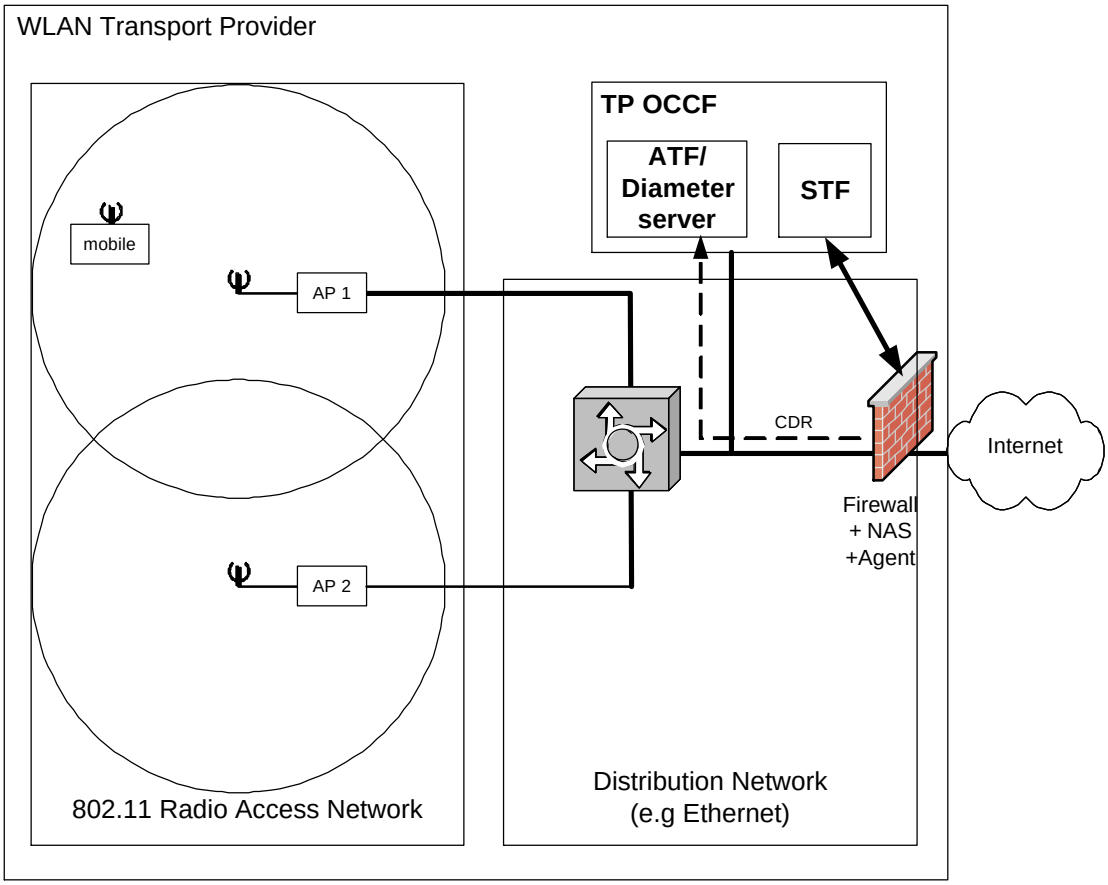

Figure 6-4: TP OCCF WLAN and Diameter

On a final note, in consistency with requirement 2 of the general TP OCCF requirements from section 5.5.1, all accounting records from the NAS to the Diameter server must include the SCID of the transport component. This requirement shall be addressed further in the solution discussion at the end of this subchapter.

With the discussed restraints in mind, the description of the TP OCCF solution for a WLAN network with Diameter Accounting is described by fulfilling the requirements that have been presented in subchapter 6.1.

Fulfilling Requirement 1: STF identifier administration
It is questionable whether or not the STF agent at the NAS can use the SCID to point to a particular session or sub-session of the mobile. This would require that the NAS must base its session management information on a foreign identifier. Section 4.2.2 discussed the various session identifiers that are already present in

the Diameter base protocol. It is assumed that the NAS bases its session management information on three of these identifiers (Attribute-Value-Pairs, or AVPs).

- The **Session-Id** is issued by the client (NAS) upon authentication and used throughout the duration of the session. It allows the addition of an optional field that could be the SCID. Since it is unclear if the 'session' concept of Diameter is appropriate for describing transport components, it is assumed that the Session-Id is not usable. If a session represents all data traffic of the mobile and the Session-Id is the same for all the records, different SCIDs cannot be included in the Session-Id.
- The next denominator that is used in the base protocol is the **Accounting-Sub-Session-Id**. It is included in intermediate accounting records to allow one intermediate record to describe a particular sub-session within the ongoing session. This fits the description of a transport component and the inclusion of the SCID in this field would be appropriate if the *format* of the Accounting-Sub-Session-Id was acceptable. Unfortunately, the Diameter base protocol prescribes that the Accounting-Sub-Session-Id is monotonically incremental by one for each new sub-session and this excludes addition of a semi-random SCID.
- The third AVP is the **Acct-Multi-Session-Id**. This Id is used in the base protocol to combine several legs of a particular session when several accounting entities file their individual accounting records. The Acct-Multi-Session-Id is unsuitable to describe a particular transport component to the NAS, since the NAS only maintains this information as a parameter for the accounting records and not all sessions use this Id.

To fulfill this requirement, it is assumed that the NAS maintains transport component information according to the Session-Id and Sub-Session-Id, since that seems to be the method of distinguishing several parts within a subscriber session. The combination of Session-Id and Sub-Session-Id is proposed here to be used as the local identifier in the STF(Agent)-to-NAS communications. The format of the Sub-Session-Id (monotonically increasing by one for each new sub-session) has predictability, which can be used by the STF to indicate new sub-sessions to the NAS. Including the last constructed Sub-Session-Id, incremented by one, in the STF(Agent)-to-NAS communications would imply that a new sub-session is requested from the NAS.
The STF must then maintain information on the last appointed Sub-Session-Id for each subscriber session, since the Broker Profile only lists active transport components. Looking up the highest Sub-Session-Id in the Broker Profile by the STF upon sending a request to the NAS does not suffice, since the highest Sub-Session-Id may have already been removed.

In conclusion, the combination of the Session-Id and Sub-Session-Id is used in the STF(Agent)-to-NAS communications as a local transport component identifier. This allows the STF to predict what the local identifier will be for new transport components (as requested by the Broker OCCF) without consulting the NAS.

Fulfilling Requirement 2: STF session setup
When the STF receives a request from the NSC to set up a new transport component, the STF must first determine the local identifier for this request. This is the Session-Id linked to the SID, in combination with the highest used Sub-Session-Id incremented by one. This local identifier must be presented to the STF Agent at the NAS, together with the Source and Destination address of the sub-session and the SCID. The STF Agent application must then instruct the NAS to set up the sub-session with the given parameters. Either the method of

requesting could indicate that a new sub-session is requested, or the NAS could derive this from the new Sub-Session-Id that is presented.

It is therefore concluded that the STF can set up Broker requested Transport components by determining the local identifier and sending the appropriate parameters to the STF agent application at the NAS for facilitation.

Fulfilling Requirement 3: STF accounting session setup
The SCIDs need to be included in all relevant accounting records of the NAS. These records are all of the type INTERIM, as described in section 4.2.2 and the records include the Sub-Session-Id of the transport component that they represent. Requirement 1 described the Acct- Multi-Session-Id as an optional Id to indicate that records from several accounting entities belong together. The same AVP format is used for the Acct-Multi-Session-Id as for the regular Session-Id, including the optional field. The base protocol description is interpreted as that an accounting record holds only one Acct-Multi-Session-Id, but that several intermediate records may hold different Acct-Multi-Session-Ids. This would allow the SCID to piggy-back on the Acct-Multi-Session-Id in the optional fields to indicate if the particular intermediate record belongs to a transport component.
If for some reason the SCID cannot be part of the Acct-Multi-Session-Id, a new SCID-AVP could be defined. The base protocol states that a Diameter application may define non-mandatory AVPs in addition to the predefined AVPs. Defining a new AVP is preferred, since presence of that AVP in accounting records would indicate that the subscriber is a Broker user and no confusion could exist with WLAN operators that already use the Acct- Multi-Session-Id. Yet it is unclear from the base protocol ([12], chapter 1.2) if the SCID-AVP will fall under the condition of a 'new AVP' and whether a request must be sent to the IANA organization for approval.

In conclusion, multiple methods exist to include the SCID in the transport accounting records. A new AVP could be defined, or it might be that the Acct-Multi-Session-Id (or even the 'Error message' AVP) can be re-used for the purpose of SCID inclusion. This remains subject for further study.

Fulfilling Requirement 4: STF Session closure
Once the STF receives a 'Close Session' request from the Broker OCCF, it must look up the local identifier corresponding to the SCID in the request. The STF must request termination of the sub-session from the NAS through the STF agent application by presenting the local identifier in the request. It is assumed that the termination results in an INTERIM record to the Diameter server. The Diameter base protocol did not describe the indication of the termination of a sub-session in the (INTERIM) accounting record when the session itself continues. Three alternatives are presented, without stating a preference for either one:

1. An accounting record is only sent for a sub-session after the transport component is terminated. This implies that each transport component is accounted for by only one record. The ASC indicates in the record sent to the Broker that the record is the only (or last) one for the transport component.
2. The ATF (or ASC) performs a lookup in the Broker Profile to see if the SCID is still active when an accounting record is received. The ASC may either send each accounting record immediately to the Broker OCCF or buffer the Diameter records until the transport component is terminated. In either case must the record that is sent to the Broker contain an

identifier that states if the record (for the sub-session) is an interim record or a final record.

3. Sub-sessions are not terminated until the session itself is terminated. Again, the record sent to the Broker must contain an identifier to state that the record is the only one (or last one) for the transport component.

In conclusion, the accounting record reaches the Broker OCCF and contains all necessary information in any of the three alternatives. All three need additional ASC intervention for inserting the record status, which rules out simple forwarding of the Diameter accounting record.

Requirement 5: STF mobile/network initiated session requests

The NAS is required to obtain a SCID before it provisions any session requests from the mobile or from outside parties. This requirement is very hard, if not impossible to meet since the NAS functioning is only described in the capacity of a Diameter client. The internal functioning of the NAS is not described and presumably different for each implementation.

Given that the NAS notices a mobile initiated or network initiated transport component request, the NAS must hold the provisioning and interact with the STF agent to obtain a SCID. The STF agent subsequently contacts the STF to obtain the SCID. The STF then forwards the request to the NSC and awaits the arrival of the corresponding Session Enable message. This has been shown in steps 71 until 74 of section 5.5.2.

The NAS could include the local session identifier in the request to the STF agent, but it is not strictly necessary since the STF can determine the local identifier from the last-issued (highest) local identifier.

In conclusion, recognizing mobile initiated or network initiated session requests at the NAS is difficult to describe. It is assumed that the NAS can request the SCID from the STF for inclusion in the accounting records.

Requirement 6: STF mobile/network initiated session termination

Just as the requirement 5, noticing the termination of a transport component by the mobile or its peer party is very difficult. This is due to the fact that WLAN does not have a strict session management like UMTS. One initiative to add such session management has been found in RfC 2868 ([31]), but time restraints prevented the exploration of the RfC.

Usually, a re-authentication procedure verifies the presence of the mobile (around once every 10 minutes). A new authentication/authorization procedure must be initiated when the wireless connection with the mobile is dropped, which also starts a new session. Failure of the mobile to respond to re-authentication messages results in deregistration.

When the background of this requirement is examined, it turns out that the implications of not meeting this request are small. In regular use, the Broker will notice the termination of a super-session from the CP. Subsequently it orders the termination of the corresponding transport component.
When the termination of the transport component occurs first, in general it is caused by one of two events:

- The mobile terminates the transport component and subsequently the Broker terminates the content component.
- The (wireless) connection to the mobile is lost and all running transport components are terminated by the transport network and subsequently the Broker terminates the content component.

While the first is not possible to meet directly in WLAN, the second is always noticed by failure of the mobile to answer the periodical re-authentication request. Assuming that the mobile will be turned off or lose connectivity at some point in time, the obsolete transport components will be terminated eventually.
It should be noted that in case that the termination time of a content element is relevant for its price and also that the mobile wants to terminate the super session, it is preferred that the mobile requests termination from the Broker OCCF through the Home Broker Session rather than to just terminate the transport component.

This issue shows undeniably an undesired feature of WLAN networks in this configuration but, recalling the statement of section 5.4.3, the accounting process is independent of the way of terminating session components. It suffices to say that when the transport component is (eventually) terminated, the accounting information is sent to the Diameter server and the ATF and subsequently reaches the Broker OCCF.

It can therefore be concluded that even though there is no timely response of this particular WLAN network configuration to mobile terminated transport components, eventually these components will be terminated. Further study of these issues is recommendable for a complete overview of the operational possibilities of the WLAN network.

Fulfilling Requirement 7: ATF accounting record reception
Accounting records (CDRs) must be constructed by the Accounting Transformation Function based upon the accounting information from the network nodes. The Diameter protocol already specifies that client nodes must send accounting information (e.g. byte counts, packet counts) in the messages of the type INTERIM_RECORD and STOP_RECORD. Requirement 3 already stated that the SCID must be included in every record of either type when the subscriber makes use of a Broker. The Diameter server recognizes that the record must be passed on to the ATF application by either the SID (which it had authenticated previously) or the presence of the SCID. This allows for handling AAA facilities for both regular users and Broker users at the Diameter server.

Solution discussion
The requirement of including the SCID in every accounting record complicates the design of the solution. Actually, since the local network identifier (Session-Id plus Sub-Session-Id) is predictable for the STF, an alternative solution would be to not include the SCID in the Diameter accounting records. The records need additional processing anyway (requirement 4) so this could also involve adding the SCID from the information from the Broker Profile. The Broker Profile must then

maintain its SCID-local Id pair information after transport components have been terminated and not purge it like it does now.

The method of communicating between the STF and STF agent has not been investigated thoroughly due to time restraints. It is recommended that further study should go into this matter when an implementation is made.

Conclusions
Not all necessary requirements have been met for the WLAN configuration combined with a Diameter accounting architecture. It has been shown though how the SCID could be included in the accounting records once it is linked to a transport component at the NAS. The method of metering separate transport components also remains subject to further study and a reference to a possible solution has been given in [31].

Lack of well developed methods for third-party setup, handover and session component recognition in WLAN heavily influenced the proposed architecture in this subchapter. Yet sufficient facilitation of such methods is required when a WLAN network has to support multi-domain service accounting.

7. Roaming issues and double charging

The previous chapters have discussed in general and in detail the events that occur at a particular network from the registration to the termination phase as well as the accompanying accounting process events. When all these events are regarded integrally over several (transport) parties, some session management problems occur. These issues have no direct effect on the accounting process, since every party accounts for its own portion, yet there is a threat of several parties accounting for parts of the same service when overlap occurs. Measures need to be taken in session management to prevent such double charging.
These, and other recognized complications are discussed in the following order:

- Session Management: Overlapping and non-overlapping roaming
- Session Management: Addressing issues with roaming; MobileIP
- Session Management: Broker network preference policies
- Accounting Management: Double charging due to single link packet loss
- Accounting Management: Double charging due to roaming

Subchapter 2.2 discussed the aspects of roaming.
Roaming was defined there as a way of continuation of service when the mobile user is moving and the transport provider is changed. The multi-domain accounting architecture proposed in chapters 5 and 6 has been developed to support the combination of accounting records from the various transport networks when the subscriber is roaming among these transport networks

7.1. Session Management: Overlapping and non-overlapping roaming

Section 2.3.2 discussed the principles of session and accounting life cycles and how session component life cycles make up super sessions. Three transport provider migration policies emerge when this is compared to the principles of roaming of subchapter 2.2.

- First is the policy that a mobile remains on one network at a time and only starts to look for other networks when the ongoing connection is dropped or terminated.
- The second policy is that the mobile attempts to register automatically at every transport network that it detects and that a palette of transport network choices exists for the Broker OCCF to set up transport components.
- The third policy is a combination of both, where the subscriber registers at a limited number of networks.

In all policies exists the possibility that, even though it is already connected to a particular network, the mobile will keep ‘listening’ on the dedicated wireless control frequencies of all network types it supports for other networks that the mobile could roam to. The policies have of course advantages and disadvantages and they are compared by the following (non-exhaustive) listing:

Advantages of the first policy:

- Being registered at one network at a time simplifies the functioning of the Broker OCCF by making transport component management straightforward. There is only one network to facilitate components.
- This policy is already automatically in effect in geographical areas with scarce (single) network coverage, which could justify using this policy without regarding the geographical location.

Disadvantages of the first policy:

- A period of time exists between deregistration at the serving network and re-registration at the subsequent network in which no data transfer can take place. If this period is short enough, the switch may occur without human notice and thus pass the criteria of seamless roaming. There is a distinct possibility that this is not the case and that seamless roaming is not possible.
- If the registered period at a particular network is to last until the subscriber moves out of the coverage area, or if changing transport networks is prone to active subscriber intervention, the Broker OCCF is left in offside position when it comes to supporting optimal access. One of the benefits of subscribing to a Broker service should be that a Broker can pick for instance the cheapest or fastest network available at any time in conformance with the subscription and this benefit is severely downgraded by this policy.

Advantages of the second policy:

- The mobile tries to register at every network it encounters. Assuming that networks without OCCF support will reject registration and that registration alone does not result in charges to the subscriber, this offers the best reliability for subscribers. Several simultaneous registrations at different networks will overcome loss of connectivity in a particular network. This policy supports seamless roaming the best, since changing a data traffic flow from one transport network to another can be done in a minimal time span.
- The Broker OCCF can compare every transport component request to the transport network characteristics of every active registration. The Broker OCCF can then pick the best network to facilitate the transport component in conformance with the subscription criteria.

Disadvantages of the second policy:

- It has been stated that the mobile must establish a Home Broker Session at every transport network that it registers at. This Home Broker Session is a transport component and will be accounted for. Registering at transport networks that will not be used for other transport components due to the presence of better alternatives will result in unnecessary charges for the surplus Home Broker Session.
- Dense urban regions (e.g. Manhattan, NY) may see a large number of transport networks at a given location and managing registration procedures at every one of them may have a big impact on overall performance (let alone on the excess costs mentioned in the previous point).

Advantages of the third policy

- The mobile is registered at a few networks (e.g. 3) for redundancy in service provisioning in case one the coverage of one of the networks ceases unexpectedly. The mobile communicates with the Broker over the primary Home Broker Session which alternative networks are available. The advantage is that redundant provisioning is achieved without excess charges from networks that will probably not be used for service provisioning.

Disadvantages of the second policy:

- Communicating registration options over the Home Broker Session introduces excess data traffic. This traffic is charged to the subscriber which could be difficult to explain. The Home Broker Session charges could be substantial in areas where a large number of Transport Providers operate.

No conclusions are drawn on the preference of either policy at this time, since concealed issues may arise during deeper investigation of this topic.

7.2. Session Management: Addressing issues with roaming; MobileIP

Wireless mobile network services are an extension of the regular Internet when they are used in the Broker model. The mobile and the Content Provider run peer applications and the transport provider merely facilitates the exchange of data packets between the mobile and the Internet. The Internet Protocol Suite, as described in 2.4 of [4], deals with the protocol stack, that allows interworking of computer systems on the Internet. The four layers of the protocol stack and example elements are shown in Figure 7-1. The interface between two stacked layers is predefined, which allows elements in the layers to be interchangeable. For instance, the Internetworking layer is operating independent of the type of Network Interface that is used, whether it is fixed (X.25 or Ethernet) or wireless (WLAN). The benefit of this approach is that as long as each underlying layer is transparent to the upper layer, systems of a total different architecture can still communicate with each other.

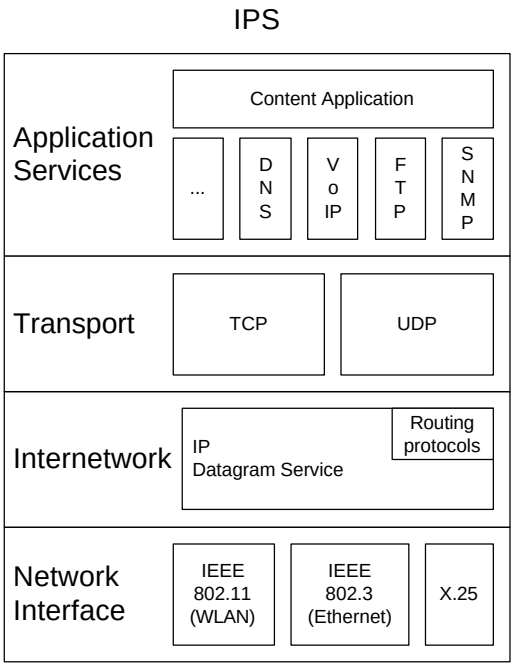

Figure 7-1: Internet Protocol Suite (IPS) structure (based on Figure 2-12 of [4])

A second advantage is the principle of *stratification*, or 'networks over networks' (5.7 of [1]). This means that layers may also be stacked repeatedly to provide connectivity. *Concatenation* also occurs when the borders of domains of the same layer elements are linked together.

The IP Datagram service that is described also incorporates a routing mechanism for the data packets. The packets do not contain a detailed fixed routing schema towards their destination but routing is rather done 'hop by hop', based on the destination address. This means that intermediate machines only need to determine the next machine that the packet needs to be sent to, which greatly simplifies their operation. IP has been developed for internet access at fixed locations (e.g. a physical jack in a wall).

Now, the problem that arises with multi-domain transport service provisioning is that when a mobile migrates to another network, it has to change it IP address. This requires that the end to end Transport layer supports changing of the IP address during ongoing content element delivery!

One of the most important solutions to this problem is the use of what is called Mobile IP. It is subsequently described, since it is likely to be a key feature in multi-domain service provisioning with implications for the Broker domain.

Mobile IP

Mobile IP is a standard proposed by a working group within the Internet Engineering Task Force. It was designed to solve the IP addressing problem described above, by allowing the mobile node to use two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment. Mobile IP can be used on top op both IP version 4 and 6. An 'Ericsson Open Report' [28] was found that summarizes the working of Mobile IP, mainly based on [29]. The Open Report states that there are two versions, Mobile IPv4 and Mobile IPv6.

The Mobile IP model defines three entities: the Home Agent (HA), the Foreign Agent (FA) and the Mobile Node (MN) and it is completely transparent to transport and higher layer protocols. See Figure 7-2. The MN has two IP addresses. One is the (static) home address and the other is called the care-of address. The addresses can be of either the IPv4 or IPv6 type. The home address is maintained by the HA and the care-of address is managed by a FA. When a MN is roaming away from its home domain, it contacts the FA in the new domain to acquire a new care-of address. The MN then notifies the HA of its new address. All incoming data at the HA (step 1) is tunneled to the FA over the Internet (step 2). The FA strips the IP packets from tunneling information (headers) and delivers the packets to the MN (step 3). When the MN roams to a different network it obtains a new care-of address and updates the HA, after which the incoming packets are forwarded to the new destination, etc. In this way the corresponding hosts do not notice that the MN is roaming, because they communicate with the home address that is located at the HA. Return packets from the MN to the corresponding hosts are sent directly, and not through the HA (step 4). This is called triangle routing.

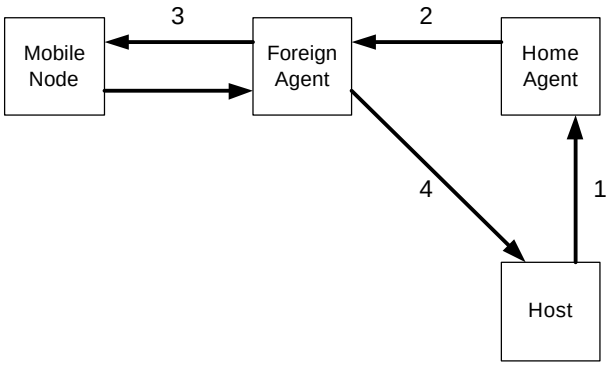

Figure 7-2: Mobile IPv4

IPv4 addresses have a fixed format. An extension for Mobile IP in combination with IPv4 was described in Internet Draft [30], dealing with route optimization. With this extension, packets were sent directly to the MN without passing through the HA. Upon roaming, the corresponding host receives a binding update message from the HA to inform it of the new care-of address. The corresponding host stores the binding information in its cache and tunnels it own IP packets directly to the care-of address. In this way the triangle routing situation is eliminated.

Mobile IP with IPv6 was developed to make use of the new features of the IPv6 protocol with respect to the more flexible way that IPv6 addresses are defined. The route optimization has become a fundamental part op Mobile IPv6. Also, IPv6 features like Neighbor Discovery and Address Autoconfiguration have replaced the function of the FA. A proposition is presented in [32] in the form of an Internet Draft document to develop a Diameter application in combination with Mobile IP. The development of Mobile IP for the IPv6 protocol ensures that this is a viable option for mobility facilitation for the years to come. All hosts that use IPv6 will be able to handle subscribers that change their care-of address during sessions without affecting upper-layer protocols.

Mobile IPv4 in its basic form can always be used, as long as Transport Providers offer Foreign Agent services. For instance, the FA function in UMTS is warranted through chapter 5.7 of [3] and co-located in the GGSN. The other required element is the Home Agent and this function evokes a conflict of concepts.

The Mobile IP Home Agent
The Broker model is based on the splitting of data transport and accounting. In principle, the Broker domain is only used for the exchange of accounting and signaling messages between the different parties that facilitate the multi-domain service to the subscriber. The actual content elements are not routed through the Broker domain and the subscriber has no distinct 'home domain' transport network. Mobile IP does not function without such a home domain to situate the Home Agent. The same issue arose when the registration function was discussed, since registration usually also involves a 'home domain'. That issue was bypassed by integrating registration with the Broker OCCF under the consideration that registration is a signaling function. Since the HA may be involved in routing all data traffic to the mobile, integrating it within the Broker domain may have severe implications. Routing of all data connections of all subscribers (e.g. for a million subscribers) through the Home Agent of the Broker would require large investments in Home Agent equipment and goes against the idea that the Broker only handles signaling traffic for the session components and their accounting process.

To combat this paradox of the model versus the practical demands, a special Content Provider is proposed that one Broker may subscribe to for all its subscribers. Through the Broker Model, this special CP is used to facilitate Home Agent services to all subscribers of the Broker, thus relieving the Broker domain from handling all the traffic flows from CP to the mobile. Figure 7-3 shows such a cascading form of Content Providers. This is not the only solution that can be conceived, but it is shown here as an example.

In practice, this special CP may very well belong to the Broker's own Business Administrative Domain and therefore be an integral part of the Broker subscription, but it may also be that a provisioning entrepreneur chooses to offer (only) Mobile IP HA services at its BAD for Brokers. Therefore the choice of offering HA services or outsourcing them is up to the Brokers.

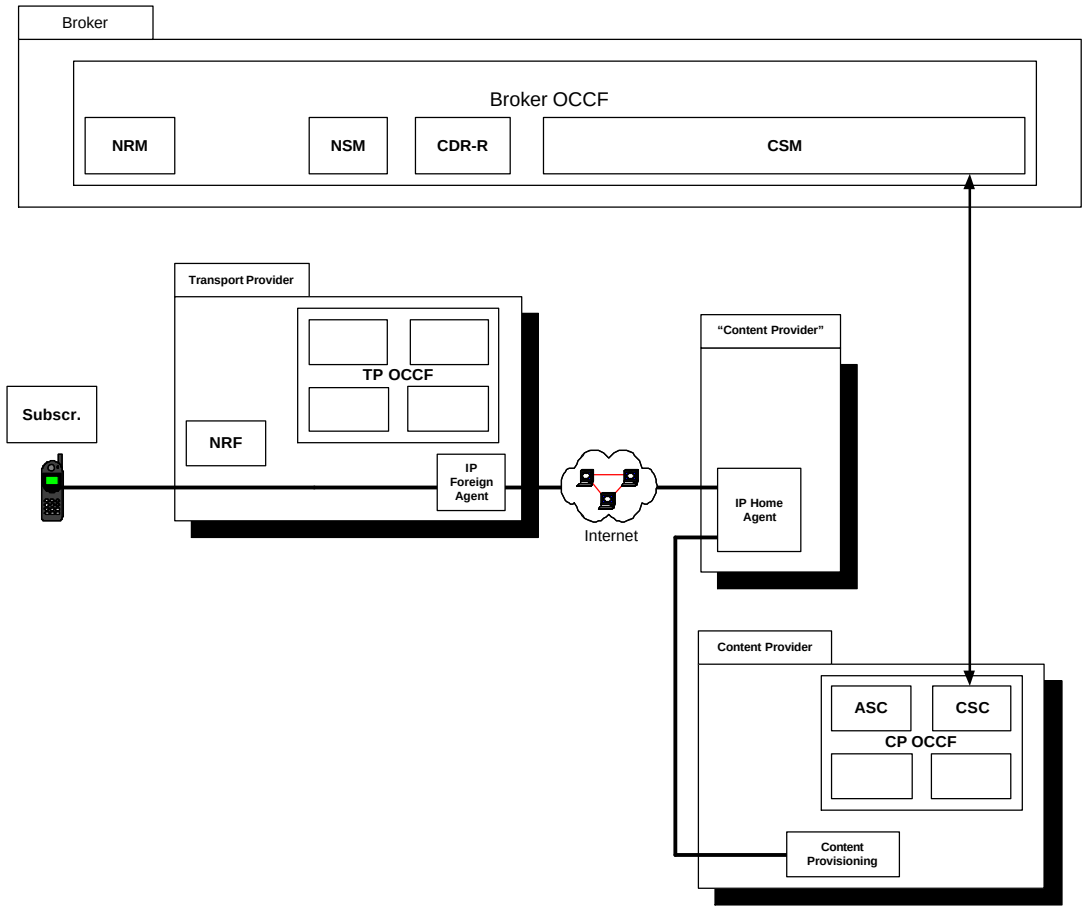

Figure 7-3: Cascading of Content Providers

Another solution could involve the Client Session Manager. As soon as the mobile changes its IP address, the Network Session Manager updates the Client Session Manager of this event. The Client Session Manager may then forward this update to the respective Content Session Controls of all Content Providers involved.

On a final note and related to the last point, it may also be useful to define suspend and resume messages in the communications between the CSM and the CSC. This allows the Broker to pause content provisioning in case the mobile loses all connectivity. Ongoing content sessions may then be resumed when connectivity is restored and thus minimize loss of 'content'.

7.3. Session Management: Broker network preference policies

The third aspect of session management in this chapter deals with the difficulties and possibilities of being registered at multiple networks at the same time. Ignoring the possibility that content may even be delivered over several transport components simultaneously, one element in the Broker OCCF must decide and steer the transport components that carry the content element. This may also be considered unforced migration, since no external conditions necessitate changing the main provider. In all, the following questions shall be answered:

- Which part of the Broker OCCF has sufficient information to decide if switching transport providers for content delivery is possible?
- Which part of the Broker OCCF has sufficient information to decide if switching transport providers for content delivery is necessary?
- Which part of the Broker OCCF has sufficient abilities to command the setup of replacement transport components in the newly preferred transport provider and termination of obsolete transport components?
- How could the migration take place?

Migration possibility
Two interfaces were defined in section 5.2.2 that are relevant to solve this question: The A Interface, which handles registration, and the C interface that makes up the Home Broker Session. The corresponding SIM sub-functions are the Network Registration Manager (NRM) and the Client Session Manager (CSM) respectively. Both sub-functions have knowledge of which networks are available to a particular subscriber. Steps 1 to 4 of section 5.4.2 show that the Subscriber Profile Manager (SPM) is involved in every registration event of the NRM. Inclusion of registration information as well as deregistration events in each Subscriber Profile would give the SPM also all necessary information.

Migration necessity
The three identified elements that have knowledge of the available networks must also be in a position to decide which transport components might be up for migration. Obviously the NRM fails this requirement since it holds no information on transport components of any kind. The CSM only holds part of the information since it is only involved in super-sessions that contain a content component. Network initiated super-sessions are not noticed by the CSM. The SPM on the other hand does know the amount of super-sessions and corresponding session components that are active. Not included in the Subscriber Profile definition was information whether a session component was of the network type or content type nor which particular provider supplies session components. This information shows to be necessary when a decision policy is to be added.

Migration initiation ability
The remaining SPM sub-function also proves to be able to command the enabling and termination of transport components. Step 7 and 20 of section 5.4.2 show that the SPM may issue a Session Enable message to the NSM to construct a transport component. The necessary information with this request, in addition to the already listed SCID, must be the SID and since multiple transport networks are possible, also a TP identifier must be included.
Closure of transport components can be done by using step 31, section 5.4.3. Merely presenting the already listed SID and SCID with this request suffices to have the proper component terminated.

Example of enforcing a migration policy
The three previous paragraphs show that the SPM is the only sub-function in the presented Broker OCCF that could check, maintain and enforce migration policies for each subscriber, given some minor additions to the Subscriber Profiles.
These additions consist of:

- Including information on Transport Providers on which migration decisions can be made. This information could be based on a Service Level Agreement between the Broker and TP and can then be considered semi-static.
- Including information on which networks a subscriber is registered at.
- Including information whether a SCID is issued for a content or transport component.
- Including information for which TP a (network) SCID is issued.
- Allowing the message of step 7 and 20 to include the SID and TP identifier to indicate the order of setting up a new transport component

Effectuating migration may then evolve from the following situation:
The mobile is registered at Network 1 and one or several transport components are in effect. The mobile co-registers at Network 2 and the SPM now compares its subscriber policy to the information (e.g. pricing) of both Network 1 and 2. When Network 1 is still preferred over Network 2, the SPM does not initiate anything until new events occur. Network 2 then only serves as a backup network in case Network 1 fails. When Network 2 is preferred, the SPM initiates a sequence of events. For every transport component that is up for migration, a clone component is set up in Network 2 by issuing a message like step 7 and 20 with the additional information mentioned above. The clone components receive new SCIDs that fall under the same SSID as the original SCIDs. The actual method of switching the packet stream from the CP from the original transport components to the clone components depends on the way packet routing is set up. For instance if Mobile IP is in effect, the mobile must make its new care-of address known to the Home Agent, as described in the previous subchapter.
As soon as the clone components take over, the original ones are terminated through the process started by step 31 and their accounting records are sent to the CDR-R.

Several successive registrations may lead to an unlimited amount of unforced migrations as long as the SPM finds a preference of one TP over another, for instance caused by differences in tariff structures.

In conclusion, Session Management may be extended with a TP preference policy and the best location would be the Subscriber Profile Manager since almost all necessary information is present there.

7.4. Accounting Management: Double charging due to single link packet loss

Subchapter 7.2 showed the Internet Protocol Suite that is in use for Internet connectivity. An end to end Transport Layer is used between the Content Provider and the mobile. This transport layer makes sure that all IP packets from the Internetworking layer arrive at the destination by keeping track of the sequence of packets. Packets that are lost or become corrupt along the way are retransmitted to guarantee full data integrity. These retransmissions have implications for the charging of TPs, especially for wireless transport providers. Since the end to end control over these retransmissions is beyond the view of the transport network, there is no way that the charging entities can distinguish duplicate from original packets. It should be noted though that packet loss on wireless links is usually much greater than packet loss in fixed lines. Duplicate packets contain the same information as the original ones and therefore the subscriber is charged double for the same information if no countermeasures are undertaken. For instance, a subscriber may be charged for 1.1 MB while it downloaded a 1 MB file due to 10% retransmissions. The unpredictability of retransmissions makes it hard for a subscriber to estimate in advance how much the cost for downloading a particular file will be.

It makes sense that a (wireless) TP only tries to combat the problem of this type of double charging within its own network since it is very hard, if not impossible, to take measures outside the own B.A.D. The concept of stratification then comes in handy, since the TP may then take the incoming and outgoing packets as a given property. The transport network can ensure that it delivers all packets and prevent double charging for its part of the link. This becomes more and more important if the provider holds a wireless link, since that is often the part where most information is lost or corrupted. Section 4.1.2 already showed that this is included in the UMTS accounting architecture. The UTRAN keeps track of the amount of packets that do not reach the mobile and this count is included in the S-CDRs. It is assumed that this count is subtracted from the sent packet counts of the SGSN and GGSN. It is obvious that the reverse situation does not need compensation, since packets from the mobile that do not reach the UTRAN are never accounted for by the SGSN/GGSN.
No such compensating method has been developed for WLAN yet, since volume accounting has only recently come to the table.

In conclusion, end to end retransmissions are often inherent to proper information exchange, but also mostly obscure for wireless transport providers. Each concatenated transport party should ensure that is does not account for retransmissions, but it is almost impossible to not account for excess traffic in a particular network if that traffic stems from another party. It is recommended that at least the wireless part of the end to end connection is guarded against accounting for retransmissions, since this is the part where data loss is the most likely.

7.5. Accounting Management: Double charging due to roaming

The second cause of double charging is associated with retransmissions due to the mobile switching to another Transport Provider. The end-to-end link may be considered as a conduit through which IP packets travel (ignoring multiple routing possibility that is inherent to IP). There is a distinct time span between the moment of sending and the moment of reception of a packet. If a seamless handover is done properly, no packets will be lost. If the roaming action is caused by a dropped connection, or if the sequence of switching is not optimal, packets that are on route to the destination may not reach the mobile, evoke retransmission requests and cause double charging. First let's take a look at the ideal situation:

Assuming Mobile IP is used, packets are transmitted from the Content Provider (Host) to the mobile (Node) through the Home Agent. The location of the Mobile IP Home Agent has been discussed in subchapter 7.2. The Foreign Agent 1 (at the gateway of the TP network) sends the packets directly from the mobile to the Content Provider. The mobile may then migrate towards the transport network of Foreign Agent 2 (FA2), as can be seen in Figure 7-5.

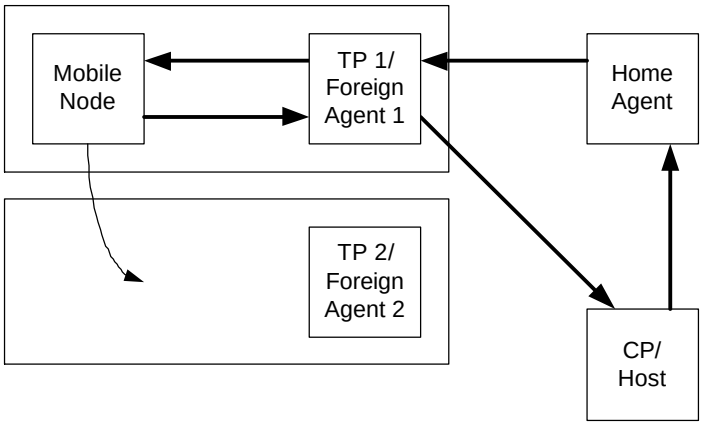

Figure 7-5: A mobile node with Mobile IP

During migration, the mobile registers at the FA2 and the FA2 notifies the Home Agent of the new care-of address. The mobile still receives incoming packets from the FA1. This is depicted in Figure 7-6. The FA1 still transmits packets from the mobile that are buffered. The mobile node sends new packets to the FA2 for transmission.

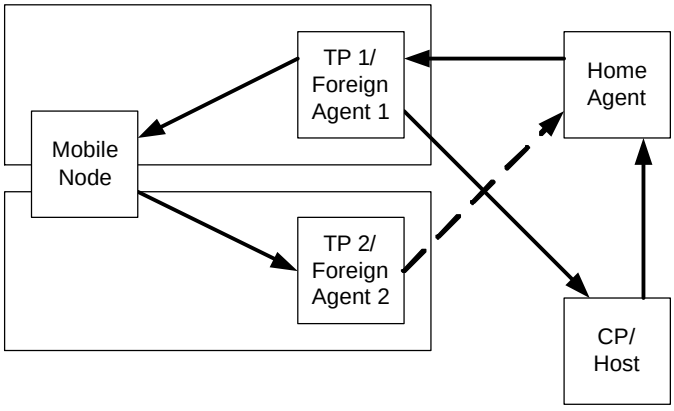

Figure 7-6: The mobile is registered at two networks

The Home Agent redirects the packet stream from FA1 to FA2, which can be seen in Figure 7-7. After a certain period of time, the FA1 does not receive any more packets that were still en route from the HA. The registration at the FA1 can be terminated once the FA1 has sent these last packets to the mobile. The mobile is now fully residing in the network of FA2 and the migration has taken place without notice of the host and without excess packet loss.

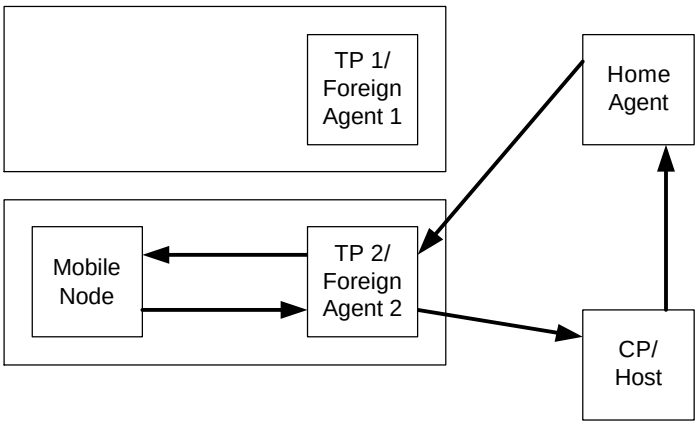

Figure 7-7: Completion of the migration process

As long as all these steps are taken in this order, no excess packets are lost in Mobile IP. Defects in this procedure may be:

- The mobile is detached from Network 1 before registering at Network 2. This results in packets arriving at Network 1 that fail to be delivered. Network 1 may still charge for these packets if the charging entity is not immediately aware that the connection has dropped. The lost packets have to be re-sent once the connection is restored at Network 2 and they will be charged again. Thus excess double charging occurs.
- During migration and if the data transfer makes use of an acknowledgement protocol, the transfer time for acknowledgement packages may be longer than initially expected by the Host. The Host will re-send the packets that did arrive correctly again and these unnecessary packets will also be charged. Thus excess double charging occurs.
- In a similar way, if the mobile transmits packets before the connection with Network 1 is dropped, it may miss the returning acknowledgement packets from the Host. Once the mobile registers at Network 2, it will re-send the same packets, which causes charges for the same information in both networks.

In conclusion, there are several situations conceivable in which (part of the) transported information is charged double to the subscriber. This is of course an undesired effect, but unfortunately inherent to the way that the IP Suite is designed. Some countermeasures can be taken to combat particular aspects, for instance keeping track of failing packets or following proper roaming procedures. The IETF standardization body is currently working on specifying an accounting architecture for roaming users. This architecture is supported by the Diameter concept and roaming is supported by the Mobile IP protocol, see [32]. Currently, charging issues associated with roaming are also being studied by this standardization body.

8. Multi-domain Accounting Example Scenarios

To support the descriptions of the proposed multi-domain accounting architecture of this thesis, this chapter holds three example scenarios that show the expectance of common use. Each example shall start with an abstract description of event groups after which a combination of detailed description and references completes the example. Since the main research topic of this thesis is accounting management and not session management, most attention will go to the former aspect. Chapter 5 already contained a detailed example on how a single Transport Provider interacts with the Broker OCCF. This will form the main basis for the examples in this chapter. The three examples that are shown are:

Example 1: A mobile is registered at a UMTS network and establishes Home Broker Session to the Broker. The subscriber acquires a Content ID and passes it on to the Broker to order. The Broker subsequently sets up the delivery. After termination of delivery, all partial accounting records flow to the Broker where they are correlated and passed on to the Billing System.

Example 2: Under the same initial assumptions and actions as Example 1, the subscriber receives the ordered content element. During delivery, the wireless connection is lost and the mobile registers at a different UMTS network. The delivery continues and after termination of delivery, all component accounting records are sent to the Broker where they are correlated and passed on to the Billing System.

Example 3: Under the same initial assumptions and actions as Examples 1 and 2, the subscriber receives the ordered content element. During delivery, the mobile also registers at a WLAN network. The Broker initiates the redirection of delivery from the UMTS network to the WLAN network. As soon as the UMTS transport component is terminated, its accounting records are transferred to the Broker. After termination of delivery, the remaining accounting records at the CP and WLAN TP are sent to the Broker where they are correlated and passed on to the Billing System.

Intermezzo: Obtaining a Content ID (CID)

One hiatus in the description of ordering content until now has been the acquiring of the CID. It has been assumed that the mobile simply has a CID to send to the Broker and this intermezzo gives some examples for obtaining the CID. The description of the CID was given in subchapter 5.2.3.

Method 1: through free internet pages
As previously mentioned, a Content Provider company may set up dedicated (free) web pages that list all available content elements. Visiting such a website (like any other web page) can be regarded as a network session, which is accounted for as a separate super session. The definition of the super session in section 2.3.2 (and also the Home Broker Definition in section 5.2.4) stated that no additional content components can be added to an already established network session, which clearly separates the accounting for any web surfing and the accounting for the particular content element.

The CID tag is listed or downloadable with the description of a particular content element on such a web page. The software in the mobile must respond to an 'order' command from the subscriber by either sending the URL of the CID to the Client Session Manager (CSM), or by downloading the CID and forwarding it to the CSM. Sending the URL or the CID to the CSM corresponds with step 13 of section 5.4.2.

Method 2: through a CID Repository at the CSM
The Broker operator may hold as a policy that subscribers may only order content that the Broker previously negotiated with Content Providers. The CSM is then linked to a CID Repository, as shown in Figure 8-1. The mobile then requests (part of) the list of available CIDs from the CSM. The CSM fetches the list (and possible descriptions of each CID) from the Repository and presents it to the mobile. The subscriber can then choose a particular content element and send the corresponding CID to the CSM as step 13 of section 5.4.2.

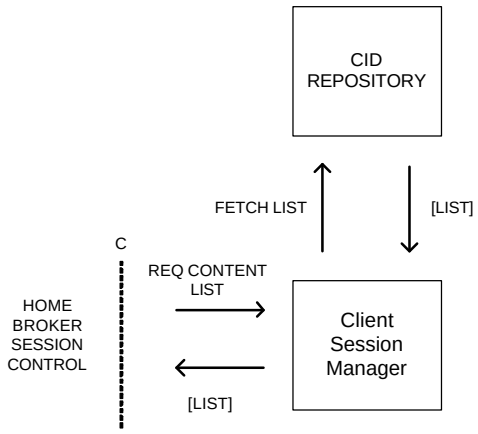

Figure 8-1: A CID Repository

Of course other methods could be developed for obtaining a CID, but this goes beyond the outline of this thesis. No conclusions can or shall be drawn here as to which method is preferred, since it is outside the scope of the thesis. Brokers may choose to facilitate either or both of the methods, or develop alternative methods. This concludes the intermezzo.

8.1. Example 1: Ordering of Content on a UMTS network

It is assumed that the mobile is registered and operating in a UMTS network. The first action that the mobile undertakes is to establish a Home Broker Session. After this is established, the mobile sends a CID to the CSM to order a particular content element. The Broker sets up the delivery of this content element with the CP and TP. All relevant accounting records flow towards the Broker OCCF after the delivery is terminated and they are subsequently correlated. Figure 8-2 shows four denotable phases and each phase is subsequently described.

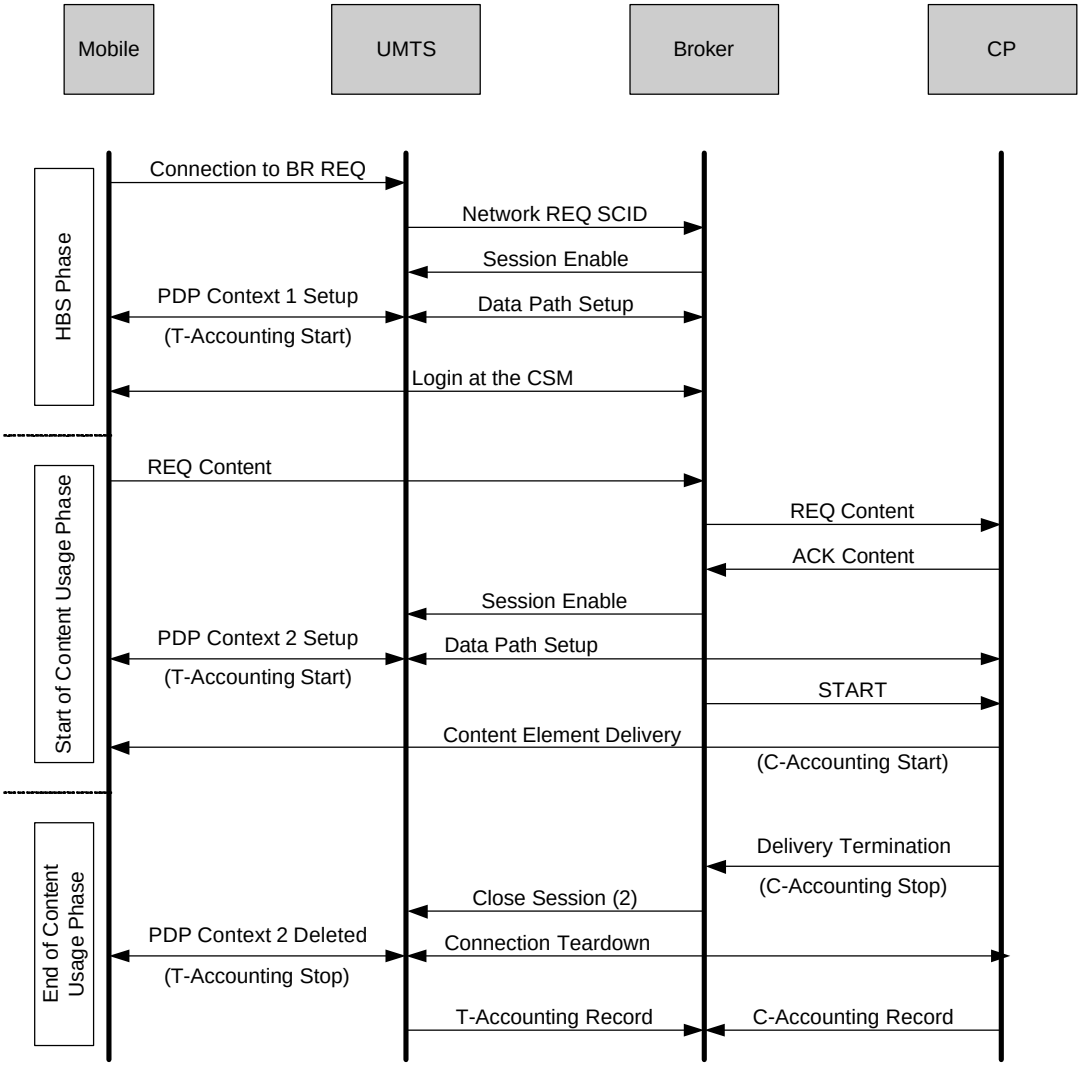

Figure 8-2: Example 1

8.1.1. Home Broker Session Phase

UMTS Network:
: First the mobile initiates a PDP Context Setup, as described in section 3.1.1. This request reaches the GGSN, who contacts the STF (agent) according to Requirement 2 of subchapter 6.2 to obtain a SCID for the transport component.

UMTS/Broker OCCF:
: The STF passes the request on to the NSC according to the procedure started at step 71 in section 5.5.2. The NSC contacts the proper Broker NSM.

Broker OCCF:
: The SCID request reaches the NSM according to step 5 and the SCID is issued for a new super session. The CDR-PM receives the super session and SCID information along steps 35 and 36, which makes the ARM ready for reception of accounting records for this transport component.

UMTS/Broker OCCF:
: When the Session Enable message reaches the NSC (step 74 and/or step 60), the STF presents the SCID to the STF agent at the GGSN for inclusion in the G-CDRs as 'External Charging Identifier' in conformance with Requirement 3 of subchapter 6.2.

UMTS Network:
: The GGSN completes the PDP Context Setup procedure and the mobile may now exchange packets with the CSM. The accounting for this transport component takes place according to regular UMTS accounting described in subchapter 4.1.

Mobile/Broker OCCF:
: The mobile sends a Connect message to the CSM according to step 9 of section 5.4.2. The mobile is then ready to request content after the authentication procedure succeeded.

This concludes the Home Broker Session Phase.

8.1.2. Start of Content Usage Phase

Mobile/Broker OCCF:
: The mobile presents a Content-ID to the Client Session Manager. This corresponds to step 13 of section 5.4.2. The Intermezzo in the beginning of this chapter listed some methods of obtaining a CID.

Broker OCCF:
: Steps 14 and 15 of section 5.4.2 initiate the construction of a new super session and SCID at the SPM. The CDR-PM receives the super session and SCID information along steps 35 and 36, which makes the ARM ready for reception of accounting records for this content session.

Broker OCCF/CP:
: After the super session is created, the CSM requests the content delivery from the CSC at the Content Provider through steps 16 and 17 of section 5.4.2. Between these steps, the CSC sets up the content delivering entity and the accompanying accounting process of which the latter includes the presented SCID in all accounting records.

Broker OCCF/UMTS Network:
: The CSM requests the setup of a transport component from the NSM according to steps 18 until 22 of section 5.4.2. Step 21 corresponds with step 60 of section 5.5.2.

UMTS Network:

Successive steps 61 and 62 register the transport component at the Broker Profile at the STF. The STF initiates a UMTS 'Network Requested PDP Context Activation Procedure' and corresponding accounting process as described in Requirements 2 and 3 of subchapter 6.2.

Broker OCCF/CP:

With the transport component established (recall step 22), the CSM may prompt the subscriber with an acknowledge request and subsequently start the content element delivery (step 25).

This concludes the Start of Content Usage Phase.

8.1.3. End of Content Usage Phase

CP/Broker OCCF:

The CSC notifies the CSM that it terminated the content delivery as well as the corresponding accounting process. This has been listed as one of the possible triggers for termination in section 5.4.3 and surpasses step 29.

Broker OCCF:

The CSM initiates a closure of the super-session, which in total is described by steps 30 until 34 of section 5.4.3. Before describing the transport component termination, the super-session termination results in an update message to the CDR-PM in step 40. The CDR-PM now knows that once all outstanding accounting records are received, the super-session is ready for consolidation by the CDR-Processor.

UMTS Network:

The Close Session message of step 30 corresponds to step 63 of section 5.5.2. Requirements 4 and 7 of subchapter 6.2 describe the termination of the PDP Context and the flow of accounting records towards the ATF. The ATF prepares the accounting information for the ASC according to steps 68 until 70.

UMTS Network/Broker OCCF:

The accounting information flows to the CDR Receiver in a predetermined manner, as described in both steps 41 and 70.

CP Network/Broker OCCF:

The CP starts to construct and send the accounting CDRs as soon as the CSC signals the termination of the content session component. This is depicted in Figure 5-43.

Broker OCCF:

Both the accounting CDRs from the TP and CP arrive at the CDR-Receiver at a given time. Individual receptions initiate steps 41 until 43 of 5.4.6. Since the Super Session Profile only holds two SCID entries, the CDR-PM initiates the processing of the combined accounting information according to steps 44 until 47.

Since the Home Broker Session is still active, more Start of Content Usage Phases and corresponding End of Content Usage Phases can be initiated by the subscriber. This concludes the first example.

8.2. Example 2: Ordering of Content on a UMTS network in a roaming environment

Again it is assumed that the mobile is registered and operating on a UMTS network. Similar to the previous example, the first action that the mobile undertakes is to establish a Home Broker Session. After this is established, the mobile sends a CID to the CSM to order a particular content element. The Broker sets up the delivery of this content element with the CP and TP. During delivery, the wireless connection is lost and the mobile registers at a different UMTS network. The accounting record from the first transport component flows towards the Broker OCCF. When the delivery of content is terminated, also the accounting records of the CP and the second TP are sent to the Broker. When all accounting records are received, they are combined and prepared for the Billing System. Figure 8-3 shows the phases that make up this example, where similar phases as Example 1 are shown in a simplified manner.

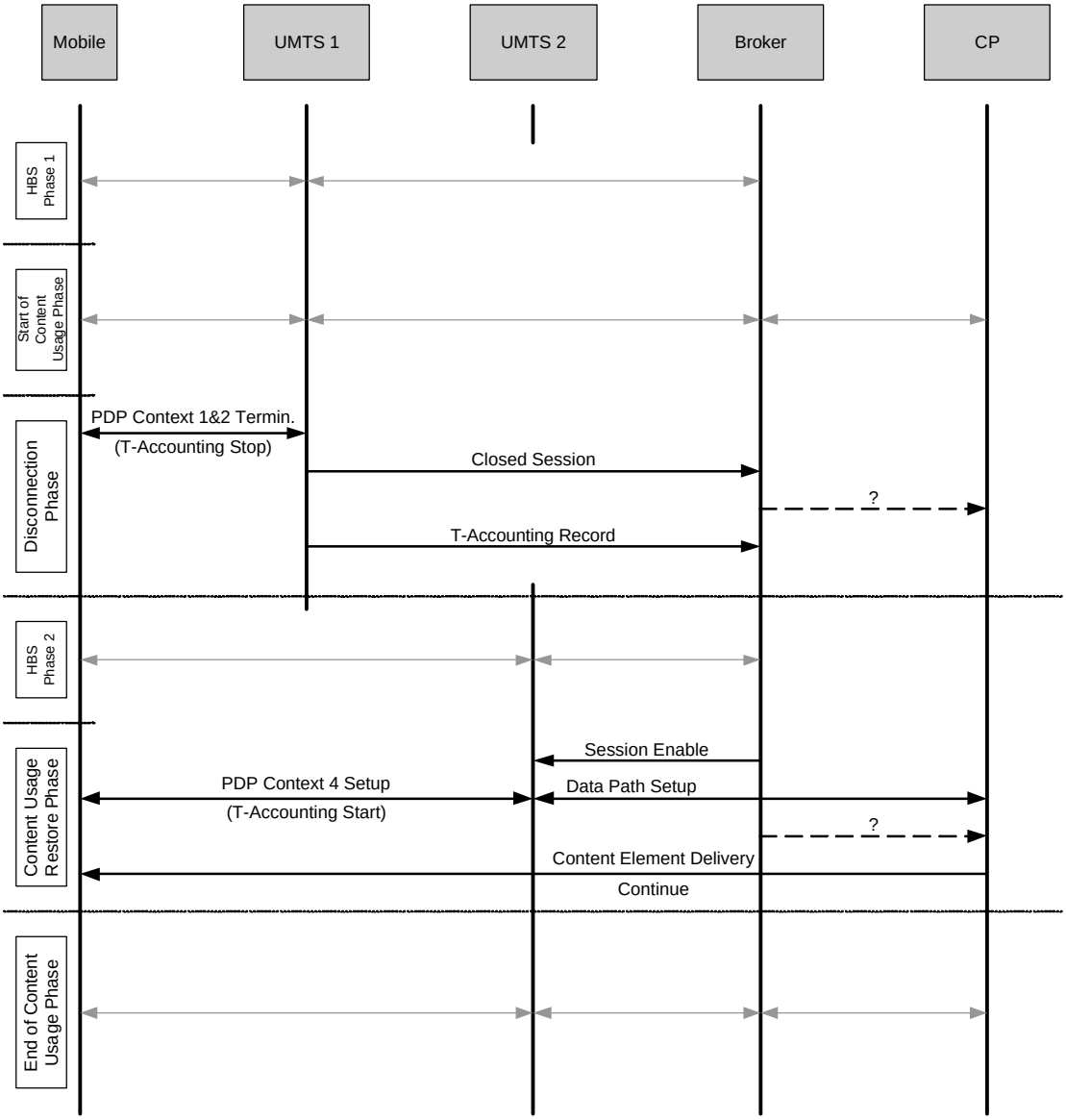

Figure 8-3: Example 2

8.2.1. Home Broker Session Phase 1

This phase shows the establishment of the Home Broker Session at UMTS network 1 and is identical to section 8.1.1. The PDP Context in use is labeled 1.

8.2.2. Start of Content Usage Phase

This phase shows the ordering of a content element and delivery setup in an identical manner as described in section 8.1.2. The new PDP Context is labeled 2.

8.2.3. Disconnection Phase

UMTS Network:

Since the connection to the mobile is lost, the two PDP Contexts for the Home Broker Session and for the content component are deleted. Requirement 6 of subchapter 6.2 stated that the STF must notice these events and contact the NSM.

UMTS Network/Broker OCCF:

The NSM is notified of the termination of both transport components.
This is described as comments with steps 27 and 28 of section 5.4.3. For the Home Broker Session this means that the super-session is also closed with the SCID closure and the CDR-PM is updated through step 40. The super-session for the content element remains open for the time being.

Broker OCCF/CP:

The policy for handling this type of event is part of the session management policy and outside the scope of this thesis. It is closely tied with the roaming policies described in subchapter 7.1, which also remained inconclusive. It is very well imaginable that when all network connectivity is lost, the CSM orders the CP to ‘pause’ the content delivery until the mobile succeeds in restoring connectivity. This has also been discussed at the end of subchapter 7.2.

UMTS Network/Broker OCCF:

Requirement 7 of subchapter 6.2 describes the automatic flow of accounting records towards the ATF in the UMTS network. The ATF prepares the accounting information for the ASC according to steps 68 until 70. The accounting information is sent to the CDR Receiver in a predetermined manner, as described in both steps 41 and 70.

This concludes the Disconnection Phase

8.2.4. Home Broker Session Phase 2

This phase shows the establishment of the Home Broker Session at UMTS network 2 and is identical to sections 8.1.1 and 8.2.1. The PDP Context in use is labeled 3.

8.2.5. Content Usage Restore Phase

Broker OCCF/UMTS Network:

Once the CSM notices that the connectivity is restored (for instance through the re-establishment of the Home Broker Session in Network 2) it orders a new transport component for continuing the content delivery. This is shown in steps 18 until 22 of section 5.4.2. Step 21 corresponds with step 60 of section 5.5.2.

UMST Network:

Successive steps 61 and 62 register the transport component at the Broker Profile at the STF. The STF initiates a UMTS 'Network Requested PDP Context Activation Procedure' and corresponding accounting process as described in Requirements 2 and 3 of subchapter 6.2. This PDP Context is labeled 4.

Broker OCCF/CP:

In case that the content delivery was paused, the CSM shall send a 'resume' message to the CSC as soon as the transport component 4 is established.

CP/Mobile:

The content delivery is continued.

This concludes the Content Usage Restore Phase.

8.2.6. End of Content Usage Phase

Once the content delivery is terminated, the accounting records for the content component and transport component 4 flow to the CDR-R. This phase is identical to section 8.1.3.

In conclusion, this second example showed a more complex case where a connection is lost and restored in another UMTS network. Considerations whether or not the content component needs to be paused in the connectionless period are beyond this thesis. The accounting record(s) for transport component 1 and 2 are sent to the Broker before the whole content super-session is completed. This conforms to the considerations on accounting life cycles given in section 2.3.2.

8.3. Example 3: Ordering of Content in a multi-domain roaming environment

Similar to the previous two examples, it is assumed that the mobile is registered and operating on a UMTS network. Again the first action that the mobile undertakes is to establish a Home Broker Session. A CID is sent to the CSM to order a particular content element and the Broker sets up the delivery of this content element with the CP and TP. During delivery, the mobile co-registers at a WLAN network. The mobile established a second Home Broker Session through this new WLAN. Due to a particular subscription policy at the Broker, the SPM decides that the active transport components must be transferred from the UMTS network to the WLAN. Such a policy and unforced migration aspects have been discussed previously in subchapter 7.3. Once the clone transport component has been established at the WLAN network, the content provisioning can be redirected. Termination of the original transport components completes the migration. The termination of the whole content session is also included for sake of completeness. Example 3 is shown in Figure 8-4.

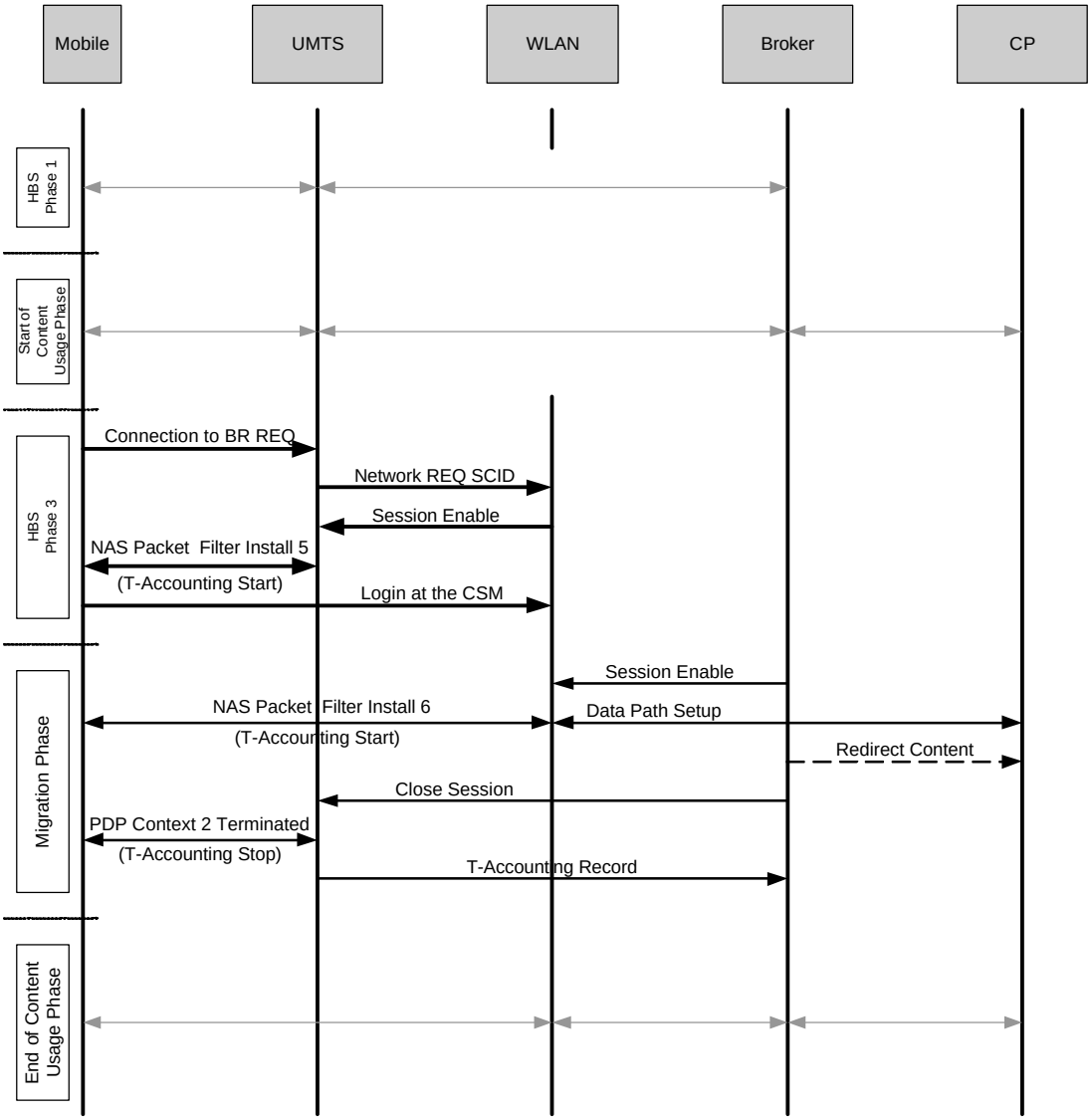

Figure 8-4: Example 3

8.3.1. Home Broker Session Phase 1

This phase shows the establishment of the Home Broker Session at UMTS network 1 and is identical to section 8.1.1 and 8.2.1. The PDP Context in use is still labeled 1.

8.3.2. Start of Content Usage Phase

This phase shows the ordering of a content element and delivery setup in an identical manner as described in section 8.1.2 and 8.2.2. The PDP Context is again labeled 2.

8.3.3. Home Broker Session Phase 3

WLAN Network:

First the mobile tries to contact the CSM. The NAS recognizes that the data packet destination IP does not conform to any active packet filter (since there isn't one yet). The NAS should obtain a SCID for the passing of this packet and meanwhile it must not discard the packet. These three rules are presented as an example of a solution to Requirement 5 of subchapter 6.3. Requesting a SCID from the STF corresponds to step 71 in section 5.5.2.

WLAN Network/Broker OCCF:

The STF passes the request on to the NSC according to the procedure started at step 71 in section 5.5.2. The NSC contacts the proper Broker NSM.

Broker OCCF:

The SCID request reaches the NSM according to step 5 and the SCID is issued for a new super session. The CDR-PM receives the super session and SCID information along steps 35 and 36, which makes the ARM ready for reception of accounting records for this network session.

WLAN Network/Broker OCCF:

When the Session Enable message reaches the NSC (step 74 and/or step 60), the STF presents the SCID to the NAS for inclusion in the Diameter accounting information as an AVP in conformance with Requirements 3 and 4 of subchapter 6.3. The Sub-Session-Id is of value 1 (the assumed starting value). The NAS sets up the metering for this sub-session and subsequently passed the buffered packets. The accounting records concerning this sub-session are sent as Interim records to the Diameter server.

Mobile/Broker OCCF:

The Connect message from the mobile now passes the NAS and reaches the CSM according to step 9 of section 5.4.2. Once the login procedure is completed, the mobile is ready to request content.

This concludes the Home Broker Session Phase for the WLAN network.

8.3.4. Migration Phase

Broker OCCF:

The mobile is registered at both transport networks. Subchapter 7.3 discussed the aspects of an unforced migration policy, which lead up to the execution of the migration process of this example.

Broker OCCF/WLAN Network:

In conformance with subchapter 7.3, step 21 shows the Session Enable message to the WLAN network. This corresponds with step 60 of section 5.5.2 for the TP OCCF.

WLAN Network:

When the Session Enable message reaches the NSC (step 60), the STF (agent) presents the SCID to the NAS for inclusion in the Diameter accounting records as an AVP in conformance with Requirements 2 and 4 of subchapter 6.3. Since the previous Sub-Session-Id was of value 1 (the Home Broker Session), the STF concludes that the new Sub-Session-Id is of value 2. The NAS meters the packet flow for this sub-session and the accounting records are sent as Interim records to the Diameter server.

Broker OCCF/CP:

The key procedure of the session management is the redirection from the packet stream from the original transport component in the UMTS network towards the clone transport component in the WLAN network. This may take place by using Mobile IP, as described in subchapter 7.2. Other methods have not been described, but are not excluded. The packet stream is assumed to ‘switch’ at the source (CP or Home Agent) towards the WLAN network and after a certain period of time, all packets that were on route towards the UMTS network will have reached the mobile. After this period it can safely be assumed that no more packets will reach the mobile over the UMTS network and the UMTS transport component can be terminated.

Broker OCCF/UMTS Network:

The SPM issues a Close Session order to the NSM as shown in steps 31 until 34. The Close Session message of step 32 corresponds to step 63 of section 5.5.2.

The policy under which the unforced migration takes place may demand that the mobile de-registers from the UMTS network as a whole. In that case the Home Broker Session 1 transport component is also terminated in a similar fashion, or the NRM must become involved to request deregistration from the UMTS network. This is not further pursued in this research assignment.

UMTS Network:

Requirements 4 and 7 of subchapter 6.2 describe the termination of the PDP Context and the flow of accounting records towards the ATF. The ATF prepares the accounting information for the ASC according to steps 68 until 70.

UMTS Network/Broker OCCF:

The accounting information flows to the CDR Receiver in a predetermined manner, as described in both steps 41 and 70.

This concludes the Migration Phase

8.3.5. End of Content Usage Phase

This Phase is included in this Example for the sake of completeness. Eventually the content delivery is terminated, the accounting records for the content component and transport component 6 flow to the CDR-R for further processing. This phase is identical to sections 8.1.3 and 8.2.6.

In conclusion, this third Example has shown the procedures that lead to unforced migration. A comparison with Example 2 shows that way of changing the Transport Provider during content delivery is indifferent to the multi-domain accounting management. This introduces a form of robustness for the accounting process, since the local accounting procedures of individual content or transport components are not dependant of other parties for successful consolidation at the Broker OCCF. This has been described as one of the goals of this research assignment in section 2.4.2.

9. Conclusions and Recommendations

Conclusions
This thesis describes a method of administrating content and transport accounting records from different providers in a way that allows correlation of those records for one-party billing. The method is designed particularly to allow a subscriber to change its transport network operator during the use of content. The additions that are needed to effectuate this method in transport networks are described for two chosen types of networks without restricting the use to these two types.
With this, the thesis complies with its main research question, which was stated in Chapter 1.

The chosen transport network types are UMTS and WLAN (in combination with the Diameter accounting protocol), which are, or will soon be, globally available for a large number of mobile subscribers. It is expected that they will mainly co-exist and therefore allowing roaming between them is seen as a good business opportunity, especially when it includes seamless provisioning of Content. Currently, interconnectivity between WLAN and UMTS networks is scarce. The proposed Broker model may form the bridge between both technologies when operators add OCCF functionalities to their networks.

The partial research questions that were stated in Chapter 1 have been addressed in the following way:

- How do the chosen mobile networks facilitate connectivity to their subscribers?

  The network architecture of UMTS has been described in subchapter 3.1, including the native procedures of seamless roaming between two UMTS networks. The network architecture of a WLAN is not as restricted as UMTS is, and therefore further choices have been made in subchapter 3.2 on the elements that make up a WLAN implementation. These choices have been made on the access technology (IEEE 802.11b), the core network (Ethernet) and the authentication and registration services (Diameter)

- How do the chosen mobile networks apply Transport Accounting?

  Subchapter 4.1 discussed the transport accounting method for UMTS networks in detail, mainly focusing on the Charging Data Record structures. CDRs are generated at the SGSN and GGSN and collected by the CGF for preparation for Billing. WLAN networks have a broader choice of applying transport accounting systems of which three alternatives have been described. These three were RADIUS, Diameter and SNMP/the MIB.

- How can the transportation resources that belong to a specific content element be registered and passed on to the Broker?

  Starting with the latter, three accounting information exchange protocols have been discussed in subchapter 4.4.
  - TAP3 is a standard which is currently in use in the GSM world, but extensions have made it also suitable for packet data networks like GPRS and UMTS. TAP3 records consist of pre-formatted elements.
  - The IPDR standard defines the framework of the accounting records. Some record elements have been pre-formatted, but the record elements that contain the accounting information on particular events are not defined, but left open for definition between the exchanging partners.

- The MXP protocol does not have its own pre-defined accounting information elements. MXP allows inclusion of TAP3, IPDR or any other accounting record format in a standardized exchange policy. This allows accounting systems to transfer any type of record in a uniform way. The downsides are that it is rarely used yet and has high adoption costs (est. $30.000 per year), whereas TAP3 and IPRD are open standards.

Each protocol could gain an advantage over the others in a particular exchange scenario and therefore this research remains inconclusive on the preferred accounting exchange protocol.

The registration of transport network usage is typically a matter of choice for the network operator and surely dependant of the type of transport network. Chapter 4 discussed common accounting procedures in UMTS and WLAN. The proposed OCCF design of chapter 5 and 6 included the interception of accounting information from regular network accounting entities and preparation of the information for exchange with the Broker party. This system relies on the assumption that 'Broker subscribers' can be recognized from regular subscribers upon registration.

- How can several partial transportation resource records from different networks, but belonging to the same content element, be correlated by the Broker?

  Chapter 5 included an analysis of the requirements of multi-domain accounting and described an architecture that can accomplish this.
  The proposed multi-domain accounting architecture groups **session components** into **super sessions**. Each component provider receives a Session Component ID (SCID) upon the setup of the component. That SCID must be included in the accounting records for the component. Once the accounting records are received by the Broker, they can be combined with the other session component accounting records by using the included SCID.
  The accounting architecture allows the Broker to approach every TP equally, regardless of the particular transport network architecture.

  Chapter 6 described methods for including the SCID in the TP accounting records for both UMTS and WLAN (with Diameter) networks.

- How does double charging occur and can it be avoided?

  Chapter 7 discussed the causes of double charging and also the closely related mobility issues. The wireless link is a great cause of packet loss in an end-to-end session. Transport Providers should prevent double charging due to packet loss or corruption over that wireless link, but cannot be held responsible for extra traffic due to packet loss or corruption originating from other parts of the transmission path. It is therefore concluded that packet loss or corruption inevitably leads to double charging when packets need to be resent. The wireless link is very susceptible to packet loss and therefore compensation for double charging is strongly recommended for good business practice.

Section 2.4.2 presented several goals for this assignment.

- The first goal was to not change the design of current transport network architectures. The proposed UMTS network addition utilized the native accounting record flow, which does not change the architecture. Additionally, an STF agent application needs to run on the GGSN. The interactions between this application and the GGSN have been described. All events that originate from the Broker OCCF have been mapped onto existing GGSN events or actions, which changes little of the native GGSN functioning. It is therefore concluded that supporting the multi-domain accounting architecture by an UMTS network is feasible.

  The chosen WLAN network with the use of a Diameter accounting server showed to be able to include the necessary SCID in the accounting records. Alternatively, a method was described to manage the Diameter accounting system in such a way that inclusion is not necessary and the SCID can be linked after the record has been received by the Diameter server.
  The method of third-party session setup, which is necessary for support of the multi-domain accounting design, has not been described in detail. This is because further research needs to be done in session management for Diameter in order to be able to conclude if Diameter is a suitable third-party session setup method. SNMP has been named as an alternative, but this has also not been researched into detail for this matter. It is therefore concluded that supporting the multi-domain accounting architecture by using the Diameter protocol is likely, but not proven. Further study needs to be done to prove proper provisioning can take place.

- The second goal of being able to correlate session components at the Broker has been achieved. The description of the accounting architecture in chapter 6 shows that once the SCID is present in the accounting records, the SSID can be retrieved. Once all component accounting records have been received, correlation commences.

- The third goal targeted the accounting exchange. Two common and one new accounting information exchange protocols have been investigated. No particular preference in either protocol can be concluded from the research, since all three support inclusion of the SCID and inclusion of the resource usage.

- The fourth and final goal was about double charging. Double charging has been discussed in chapter 7. Double charging is related to the way the Internet Protocol Suite functions. The only two parties that notice and control retransmission of IP packets are the two sending peers. Intermediate nodes operate on a lower layer and therefore they cannot distinguish original IP packets from duplicate ones without extensive packet analysis. As a result, duplicate packets are counted together with the original ones and charging takes place based upon this count. Hence double counting results in double charging. The answer to the partial research question on double charging already mentions that transport networks can at most prevent the occurring of double charging within their own domain. It is concluded that double charging is unavoidable

It is important to note that the proposed TP solutions do not exclude regular operation of the networks, but rather stimulates co-existence. Moreover, adoption of OCCF Functionalities within transport networks is scalable. Development and testing of such functionalities could take place in operating networks. For instance a UMTS network could be equipped with separate test-OCCF and test-GGSN machines. The usage scenarios within the TP network can be developed by (manually) feeding 'Broker OCCF commands' into the test-OCCF and verify that the proper actions are undertaken within the network elements (SGSN/test-GGSN). In general, development of implementations for transport networks could be done in an iterative manner. Several implementations are feasible, as long as each one makes the transport network comply with the requirements stated in chapter 6.1.
A second notice must go to the validity of the multi-domain accounting architecture, as presented in chapter 5. The architecture in this thesis has been developed iteratively, hence without formal modeling methods. Such validation must take place before any implementations of the TP(/CP) OCCF, Broker OCCF or the communication protocol between the two are developed.

Overall concluding, the main and partial research questions have been answered in this thesis and the goals have been achieved to a great extent. The proposed multi-domain accounting solution allows correlated accumulation by the Broker in a way that is independent of a particular wireless-access technology and robust in content delivery. The UMTS and WLAN (with Diameter) technologies can be adapted to support the multi-domain accounting architecture, though some issues still remain. The most important issues are the suitability of the Diameter protocol for session management and finding an appropriate method for session management in the UMTS GGSN.

Recommendations
The description of the multi-domain accounting architecture has a number of issues that need further study.

1) In order to successfully develop this architecture further, a worldwide influential standardization organization should adopt it. The recommended organization is the Internet Engineering Task Force, since they already do a lot of research in this field of work.

2) It is recommended that the multi-domain accounting architecture description is verified for correctness. This can be done by transforming it into a state machine and/or by using formal modeling methods.

3) The session management methods at the UMTS and WLAN (with Diameter) networks that should facilitate third-party setup and termination have not been researched to a great extent in this thesis. They are vital to the multi-party accounting architecture though, since they should make sure that every transport component is linked to a SCID. It is recommended that further study should be done in the session management features of Diameter and SNMP for suitability to come to a complete description of how UMTS and WLAN (with Diameter) can support the multi-domain accounting architecture.

4) This thesis assumes that Brokers already have existing agreements on the method of exchange of accounting data, on the applicable tariffs and also on

the clearing of costs between the Provider and the Broker. It is recommended that more research has to be done on these assumptions, given the expected growth of the number of Content and Transport Providers worldwide. Protocols could be developed that allow two parties to negotiate such agreements automatically upon the first encounter.

5) Several operational aspects have not been explored. The most important ones are:
    a. A global subscriber identity, which can be used to identify a subscriber in all types of network. Networks should be able to derive subscription to a Broker from this identity.
    b. A global Broker identity, which Transport Providers can use to contact the proper Broker when a subscriber is trying to access their network.
    c. A proper Home Broker Session protocol to enable subscribers to communicate with their Broker network on which Content they want to order, to assist in roaming etc.
    d. A proper Broker-Provider protocol that allows the exchange of the message information described in the accounting architecture.
    e. Security functions must be implemented that mutually identify subscribers or Transport Providers with the Broker. The ordering of a content element must be non-repudiational.

It is recommended that these aspects are researched since uniformity amongst all parties of these aspects is necessary for interoperability.

6) The proposed solution to the WLAN network with Diameter accounting would greatly benefit from a ‘session’ concept. A session concept similar to the PDP-Context in UMTS would be very useful from the accounting point-of-view, especially when it comes to session component termination. It is recommended that this is researched further. The Diameter accounting protocol supports segregation into sub-sessions, but no operational implementation has been found. RfC 2868 ([31]) describes a Tunnel protocol proposal for RADIUS. Since this protocol seems to introduce a more detailed session concept and Diameter evolved from RADIUS, this solution could be applicable. Unfortunately it has not been researched further in this thesis due to time restraints.

10. Glossary

APN	Access Point Name
AuC	Authentication Center
ARM	Accounting Records Management
ASC	Accounting Session Control
ATF	Accounting Transformation Function
AVP	Attribute-Value-Pair
BAD	Business Administrative Domain
BSC	Base Station Controller
BSS	Base Station Subsystem
C-ID	Charging Identity
CAMEL	Customized Application Mobile Enhanced Logic
CDMA	Code Division Multiple Access
CDR	Call Detail Record, or Charge Data Record
CDR-P	CDR Processor
CDR-PM	CDR Profile Manager
CDR-R	CDR Receiver
CDR-S	CDR Store
CGF	Charging Gateway Function
CID	Content Identity
CP	Content Provider
CS	Circuit Switched
CSC	Client Session Control
CSM	Client Session Manager
Diameter	Not an abbreviation, successor of RADIUS
DNS	The Domain Name System
FQ(P)C	Fully Qualified (Partial) CDR
G-CDR	GGSN-CDR
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HLR	Home Location Register
IEEE	the Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IMSI, (P-)	(Packet) International Mobile Subscriber Identity
IPDR	Internet Protocol Detail Record
LA	Location Area
mcc	Mobile Country Code
MIB	Management Information Base
MM	Mobility Management
MSC	Mobile Switching Center
msin	the Mobile Subscriber Identification Number
MXP	Mobile eXchange Protocol
NAS	Network Access Server
NDM	Network Data Management
NRF	Network Registration Function
NRM	Network Registration Manager
NSC	Network Session Control
NSM	Network Session Manager
OCCF	Open Connectivity Control Function
OSI	Open Systems Interconnection (Reference Model)
PDP	Packet Data Protocol
PLMN	A Public Land Mobile Network
PMM	Packet Mobility Management

PS	Packet Switched
QoC	Quality of Service
RA	Routing Area
RAB	Radio Access Bearer
RADIUS	Remote Authentication Dial In User Service
RfC	Request For Comments
RNC	Radio Network Controller
RP	Reference Point
RPC	Reduced Partial CDR
S-CDR	SGSN-CDR
SC	1) Session Component 2) Session Creation
SCC	Session Component Creation
SCID	Session Component IDentity
SCT	Session Component Termination
SGSN	Serving GPRS Support Node
SI	Session Invocation
SID	Subscriber IDentity
SIM	Session Identity Management
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPM	Subscriber Profile Manager
SSI	Super Session Invocation
SSID	Super Session IDentity
SST	Super Session Termination
ST	Session Termination
STF	Session Transformation Function
STID	STorage IDentity
TAP(3)	Transferred Account Procedure version 3
TEID	Tunnel Endpoint IDentifier
TFT	Traffic Flow Template
TINA(C)	The Telecommunications Information Networking Architecture (Consortium)
TOS	Type Of Service
TP	Transport Provider
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrial Radio Access Network
VAS	Value-Added-Service
VLR	Visitor Location Register
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

References

[1] Goede, L. de, 1998, *Operational Management of Telematics Systems and Services,* [Lecture notes], Universiteit Twente, Enschede.

[2] TINA-C, 1997, *TINA Business Model and Reference Points version 4.0*, [Online], Available from: <http://www.tinac.com/specifications/documents/bm_rp.pdf> [visited 2002].

[3] *General Packet Radio Service (GPRS) Service Description*, TS 23.060 V5.2.0, The 3rd Generation Partnership Project (3GPP).

[4] E.F.Michiels, M.J.van Sinderen, I.A.Widya, 2002, *Telematics Services,* [Lecture notes], Universiteit Twente, Enschede.

[5] M. van Le, B.J.F. van Beijnum, B.L. de Goede, *Real-time Service Accounting*, IEEE Workshop on IP Operations and Management, Oct. 29-31, 2002, Dallas, TX, USA.

[6] Blau, John, 2002, *Wi-Fi Hotspot Networks Sprout Like Mushrooms,* IEEE Spectrum, September issue, p. 18-20.

[7] *3G Charging data description for the CS domain*, TS 32.205 V5.1.0, The 3rd Generation Partnership Project (3GPP).

[8] *Numbering, addressing and identification,* TS 23.003 V5.4.0, The 3rd Generation Partnership Project (3GPP).

[9] *3G Charging data description for the PS domain,* TS 32.215 V5.1.0, The 3rd Generation Partnership Project (3GPP).

[10] *Recommendations for IEEE 802.11 Access Points* (April 2002), [Online], Microsoft Corporation, Available from: <http://www.microsoft.com/whdc/hwdev /tech/network/802x/AccessPts.mspx> [visited 2002].

[11] Rigney, C., *RADIUS Accounting*, RfC2866, June 2000, [Online].

[12] Calhoun et al, *Diameter Base Protocol*, Work in Progress, December 2002, Version draft-ietf-aaa-diameter-17.txt, [Online].

[13] Marsman, R., 2000, *Development of prototype-scripts for the Script-MIB*, MSc thesis, Universiteit Twente, Enschede.

[14] Gullstrand, C[hrister] (2001), *Tapping the Potential of Roaming*, [Online], TADIG, the GSM Association, Available from: <http://www.gsmworld.com/using/billing/potential.shtml> [visited 2002].

[15] PRD TD.57, *Transferred Account Procedure Data Record Format Specification Version Number 3,* V3.9.0, GSM Association, [Online], Available from: <http://www.gsmworld.com/using/billing/whatis.shtml> [visited 2002].

[16] IPDR Inc, 2002, *Network Data Management – Usage (NDM-U) For IP-Based Services*, Version 3.1, [Online], Available from: <http://www.ipdr.org> [visited 2002].

[17] Schwartz, Susana, 2002, *Cibernet Releases MXP Standard for Mobile IP Revenue Settlement*, Billing World &OSS Today, August issue, [Online], Available from: <http://www.cibernet.com/images/BW_Cibernet_Aug02_p.pdf>.

[18] Cibernet Corp. 2002, *MXP Product Description*, version 1.3, [Online], Available from: <http://www.cibernet.com/images/MXPProductDescription.pdf>.

[19] Lin, Haung, Chen, Chlamtac, 2001, *Mobility management: From GPRS to UMTS*, Wireless Communications and Mobile Computing 2001; **1**: 339-359.

[20] *UTRAN Iu Interface RANAP signaling for Release 1999*, TS 25.401 V3.4.0, The 3rd Generation Partnership Project (3GPP).

[21] www.80211-planet.com: *The Source for 802.11 Business and Technology*, [Online], Available from:<www.80211-planet.com> [visited 2002].

[22] *Mobile Communications* [Lecture Notes], Universiteit Twente, included the article *IEEE 802.11 Tutorial*, by Zyren and Petrick without further references.

[23] Levijoki, Sami (26-05-2000), *Authentication, Authorization and Accounting in Ad Hoc networks*, [Online], Department of Computer Science, Helsinki University of Technology, Available from: <http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/authentication/aaa.htm> [visited 2002].

[24] Michiels, E.F., 2000, *Telematics Systems Security,* [Lecture Notes], Universiteit Twente, Enschede.

[25] Aboba et al, *Criteria for Evaluating AAA Protocols for Network Access,* RfC2989, November 2000, [Online].

[26] Mitton et al, *Authentication, Authorization, and Accounting: Protocol Evaluation*, RfC3127, June 2001, [Online].

[27] Ventura, Håkan, 2002, *Diameter next generation's AAA protocol*, MSC thesis, University of Linköping, LiTH-ISY-EX-3232-2002.

[28] Karagiannis, G., Heijenk, G. (21-12-2000), *Mobility support for ubiquitous Internet access*, Ericsson Open Report number 11/0362-FCP NB 102 88 Uen.

[29] Perkins, C. E. (ed), *IP Mobility Support*, RfC2002, October 1996, [Online].

[30] Perkins, C. E., Johnson, B. J., *Route Optimisation in Mobile IP*, Work in progress, Nov. 2000, Version draft-ietf-mobileip-optim-10.txt, [Online].

[31] Zorn et al, 2000, *RADIUS Attributes for Tunnel Protocol Support*, RfC 2868, June 2000, [Online].

[32] Calhoun, Johansson, Perkins, *Diameter Mobile IP Application*, Work in progress, April 2003, Version draft-ietf-aaa-diameter-mobileip-14.txt, [Online].

Appendix A

Charging Data Record Formats of the SGSN and GGSN
The S-CDR and G-CDR fields are explained more extensively in [9].

'M' fields are Mandatory
'C' fields are Conditional
'Om' fields are Mandatory if supported by the Operator
'Oc' fields are Conditional if supported by the Operator

SGSN PDP context data (S-CDR)

Field	Category	Description
Record Type	M	SGSN PDP context record.
Network Initiated PDP Context	O_C	A flag that is present if this is a network initiated PDP context.
Served IMSI	M	IMSI of the served party
Served IMEI	O_C	The IMEI of the ME, if available.
SGSN Address	O_M	The IP address of the current SGSN.
MS Network Capability	O_M	The mobile station Network Capability.
Routing Area Code (RAC)	O_M	RAC at the time of "Record Opening Time"
Location Area Code (LAC)	O_M	LAC at the time of "Record Opening Time"
Cell Identifier	O_M	Cell identity for GSM or Service Area Code (SAC) for UMTS at the time of "Record Opening Time".
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs
GGSN Address Used	M	The control plane IP address of the GGSN currently used. The GGSN address is always the same for an activated PDP context.
Access Point Name Network Identifier	O_M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	O_M	PDP type, i.e. IP, PPP, IHOSS:OSP
Served PDP Address	O_C	PDP address of the served IMSI, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
List of Traffic Data Volumes	O_M	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per QoS/tariff period. Initial and subsequently changed QoS and corresponding data volumes are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this SGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the SGSN.
SGSN Change	C	Present if this is first record after SGSN change.
Cause for Record Closing	M	The reason for closure of the record from this SGSN.
Diagnostics	O_M	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number in this SGSN. Only present in case of partial records.
Node ID	O_M	Name of the recording entity
Record Extensions	O_C	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	O_M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	O_M	An index indicating how the APN was selected.
Access Point Name Operator Identifier	O_M	The Operator Identifier part of the APN.
Served MSISDN	O_M	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
System Type	O_C	Indicates the type of air interface used, e.g. UTRAN. This field is present when either the UTRAN or GERAN air-interface is used. It is omitted when the service is provided by a GSM air interface.

CAMEL Information	O_C	Set of CAMEL information related to PDP context. For more information see Description of Record Fields. This field is present if CAMEL service is activated.
RNC Unsent Downlink Volume	O_C	The downlink data volume which the RNC has not sent to MS. This field is present when the RNC has provided unsent downlink volume count at RAB release.
Charging Characteristics Selection Mode	O_M	Holds information about how Charging Characteristics were selected.
Dynamic Address Flag	O_C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.

GGSN PDP context data (G-CDR)

Field	Category	Description
Record Type	M	GGSN PDP context record.
Network initiated PDP context	O_C	A flag that is present if this is a network initiated PDP context.
Served IMSI	M	IMSI of the served party
GGSN Address used	M	The control plane IP address of the GGSN used.
Charging ID	M	PDP context identifier used to identify this PDP context in different records created by GSNs
SGSN Address	M	List of SGSN addresses used during this record.
Access Point Name Network Identifier	O_M	The logical name of the connected access point to the external packet data network (network identifier part of APN).
PDP Type	O_M	PDP type, i.e. IP, PPP, or IHOSS:OSP
Served PDP Address	O_C	PDP address, i.e. IPv4 or IPv6. This parameter shall be present except when both the PDP type is PPP and dynamic PDP address assignment is used.
Dynamic Address Flag	O_C	Indicates whether served PDP address is dynamic, which is allocated during PDP context activation. This field is missing if address is static.
List of Traffic Data Volumes	O_M	A list of changes in charging conditions for this PDP context, each change is time stamped. Charging conditions are used to categorise traffic volumes, such as per tariff period. Initial and subsequently changed QoS and corresponding data values are listed.
Record Opening Time	M	Time stamp when PDP context is activated in this GGSN or record opening time on subsequent partial records.
Duration	M	Duration of this record in the GGSN.
Cause for Record Closing	M	The reason for the release of record from this GGSN.
Diagnostics	O_M	A more detailed reason for the release of the connection.
Record Sequence Number	C	Partial record sequence number, only present in case of partial records.
Node ID	O_M	Name of the recording entity.
Record Extensions	O_C	A set of network operator/manufacturer specific extensions to the record. Conditioned upon the existence of an extension.
Local Record Sequence Number	O_M	Consecutive record number created by this node. The number is allocated sequentially including all CDR types.
APN Selection Mode	O_M	An index indicating how the APN was selected.
Served MSISDN	O_M	The primary MSISDN of the subscriber.
Charging Characteristics	M	The Charging Characteristics applied to the PDP context.
Charging Characteristics Selection Mode	O_M	Holds information about how Charging Characteristics were selected.
IMS Signalling Context	O_C	Included if the PDP context is used for IMS signalling
External Charging Identifier	O_C	A Charging Identifier received from a none-GPRS, external network entity