International Telecommunication Union

ITU-T Technical paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(06/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION-NETWORKS

Multiple radio access technologies

Preface

Mobile/cellular networks, as currently deployed worldwide, lack the ability for both user equipment (UE) to utilize more than one radio access technology at-a-time. Similarly, they lack the ability to manage reciprocally the concurrent multi-connections in the mobile and NGN networks. ITU-T recognized this technological gap towards the end of 2008. Afterwards, other standards forums became aware also of the potential for standardization and development of a new architecture in the smart phone (MUE), mobile radio and core networks. Closing this gap could offer a number of interesting new scenarios for the mobile subscriber.

Multi-connection is the term utilized in ITU-T Study Group 13 to define this new architecture. It encompasses and supports both the NGN functional architecture and the mobile network architecture infrastructure to take advantage of a variety of use cases, scenarios, and applications in today's mobile smart phone market success.

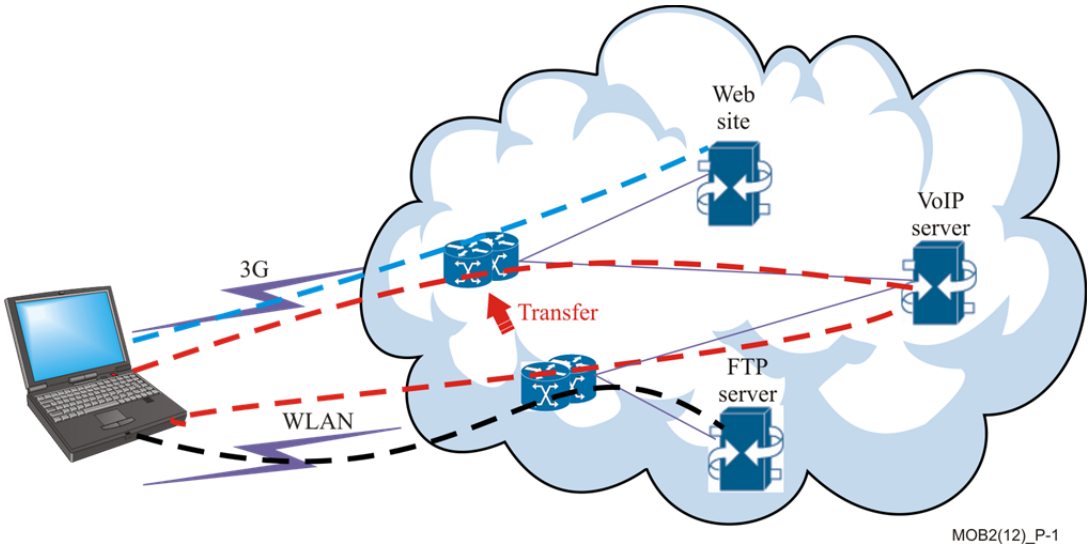

Figure P-1 – Service transfer

Take as an example, a smart phone subscriber who may want to use multi-connection with multiple radio connections simultaneously, feeding a single application in order to get an aggregated bandwidth. If she is at the airport and her flight is about to leave while she is still downloading a file, she may accelerate the file downloading process by utilizing in parallel 3G-cellular access and WLAN access at the airport's hotspot.

Likewise, multi-connection may offer "service reliability". Consider a subscriber holding a video conference with her business partners on the PC via both an ADSL link and a WLAN link simultaneously been used. It might happen that the WLAN connection abruptly breaks down due to an unstable hotspot. In this case, the active ADSL connection avoids the interruption of the video conference; thus, the subscriber can continue holding the conference entirely via the ADSL connection. The multi-connection feature was paramount. Other use cases enabled by the multi-connection architecture are also presented in this technical paper.

The technical paper provides the fundamental principles of the multi-connection architecture within the scope of ITU-T NGN and ITU-T future networks, the scenarios and use cases covered and the technical requirements already defined to achieve this goal.

It also presents the design techniques that allowed the development of this functional architecture and the emerging standards behind this subject area. This is done by providing a comprehensive reference list related to the questions under study by ITU-T concerning multi-connection, including its relation to ITU-R standards.

It is expected that the technical paper will appeal to other groups inside and outside ITU-T interested in additional development of signalling flows and specification of testing scenarios for the multi-connection architecture. Such an audience should include those ITU-T delegates, researchers, designers, engineers, and academics working on multi-connection mobile networks.

This technical paper is intended for researchers and staff of operators of NGN networks, mobile network and multiple radio access technology heterogeneous networks - those future networks evolving from the merge of these network systems. It portrays scenarios and use cases from which operators and users can draw conclusions on the direction of multi-connection services and the technological direction of this new mobile industry.

Emphasis is placed on the current state of maturity of multi-connection architecture, since there are still unanswered questions to pursue on the design principle from which it started. In particular, the alignment of multi-connection architecture with recent technological developments in the techniques used for concurrent network accesses in standards forums like IETF, and IEEE.

This technical paper provides topics, ideas and techniques drawn from such forums to convey gaps in the multi-connection network elements, behaviour, interfaces, and reference points. Thus, it provides guidance on further steps to achieve a more mature ITU-T multi-connection, functional architecture.

Table of Contents

1 Introduction

1.1 Principles and objectives

The technical paper collects the principles on which the ITU-T multi-connection architecture and related topics, throughout the several multi-connection recommendations, have progressed since its inception in 2009.

These principles maintain that multi-connection networks shall support a range of cell sizes in concert with a multi-connection core infrastructure, both allowing seamless interworking among multiple radio access technologies. They shall operate using novel scalable self-organizing and self-optimizing techniques, adhering as much as possible to the models in order to diminish operator's investments. As for cell sizes, they cover macro, micro, pico, and femto cells. The multi-connection core network infrastructure shall cover existing core carrier-grade backhaul, commercial grade wired backhaul, DSL, cable, and in-band wireless backhaul; i.e., relays, and out-of-band wireless backhaul. So far, the radio access technologies include 2G, 3G, LTE, Wi-Fi, WiMAX, and other unlicensed technologies coupled with LTE and LTE-A radio access networks, Ref. [27].

The self-organizing and self-optimizing techniques apply e2e QoS, QoE, and Policy and Charging new techniques with effects on both, radio access network and core network.

A paramount aspect of multi-connection networks is that they shall support seamless mobility, and IP flow mobility to control traffic data paths in the user plane with different accesses-connectivity.

A major goal is to develop a common architecture and infrastructure for service delivery across the entire network. Specifically, the multi-connection core network pursues to support an unconstrained combined radio evolution to meet the every-day changing subscriber needs.

1.2 Terminology

A number of terms are being used to describe the technology concerning with mobile terminals and networks with the capability to communicate with each other through different accesses - simultaneously.

Multi-connection is the term used in the context of ITU-T standardization. Multiple PDN Connection to the same APN is the terminology used in the context of 3GPP; and in some areas of the industry Multi-RAT Heterogeneous Networks.

In this technical paper, multi-connection is the preferred term.

2 Multi-connection Scenarios

A number of use cases were developed to argument the usefulness of the multi-connection architecture and provide requirements for it. In the following Clauses these cases are presented, following Ref. [6]. The current functional architecture emphasizes on some use cases and their implementation for instance the Aggregation use case, while some use cases need additional functionality still to be implemented. The models, such as Policy and Charging Control (PCC), IP flow mobility, and QoS mechanisms among others, are shown within the technical paper as a guide for compatibility and alignment purposes.

2.1 Multimedia Division Use Case

This use case presents a MUE accessing multimedia services through multiple connections; i.e., multimedia services can be divided and delivered through different data paths.

Alice has to attend a video conference with business partners via her mobile phone when she is walking to her office. On the way to her office, some WLAN hot-spots are available, so Alice decides to initiate the video flow through the WLAN link in order to benefit from higher bandwidth and cheaper cost, whereas she sends and receives the audio flow through the 2G/3G link in order to guarantee the audio flow to be uninterrupted.

2.2 Load Balance Use Case

In this use case a MUE separates a flow between multiple connections simultaneously.

Alice switches the video-conference from her mobile phone to her personal computer, after she arrives at her office. The personal computer can access Internet via asymmetric digital subscriber line (ADSL) and via a public WLAN in the building. Alice would like to use the WLAN link because it is free, but a colleague tells her that the WLAN link is too unstable to keep video-conference continuity today. Alice then decides to use the ADSL link in order to mitigate the load on the WLAN link, but still keeps the WLAN link active.

2.3 Reliability Use Case

This use case emphasizes on the multi-connection capacity to offer simultaneous accesses in order to improve service reliability upon the network or MUE failure.

Alice holds a video-conference with her business partners using a personal computer via ADSL link and WLAN link simultaneously. After a while, the WLAN connection abruptly breaks down due to an unstable situation. Fortunately, the active ADSL connection avoids the interruption of the video-conference and Alice continues to hold the conference entirely via the ADSL connection.

2.4 UE Initiated Network Selection Use Case

In this use case the MUE automatically selects the currently best connection, according to a pre-configured policy, and activates it.

After the video-conference, Alice decides to eat lunch in a nearby restaurant which provides a WLAN link to customers (hot-spot). While waiting, Alice enjoys the MP3 from her favourite on-line music channel through the WLAN link. Suddenly, Alice realizes that she had not checked her corporate email box earlier that morning. Based upon the configured policy; e.g., using a security class, the MUE automatically chooses the 3G link to download her email through her corporate VPN, even though the WLAN is free.

2.5 Network-initiated Network Selection Use Case

In this case, the multi-connection network is capable to select and provide to the MUE the best available connection.

After finishing lunch, Alice enjoys a cup of coffee and the on-line MP3 in the restaurant over the restaurant's WLAN hot-spot link. At that time, Alice's boss calls her using VoIP over WLAN to discuss a business emergency. The network immediately recognizes that the VoIP call needs stricter QoS assurance than the VoIP session over WLAN can provide, and chooses a 3G access rather than the WLAN link to establish a VoIP connection with Alice.

2.6 Service Continuity Use Case

This use case shows that, in multi-connection, if one of the connections is lost, then the service can use another connection to maintain the service without any interruption. Consider the following case.

Alice has both a 3G connection and WLAN connection in her home. She uses the video call service through 3G, and the peer-to-peer (P2P) downloading through WLAN so that the download does not affect her voice service. After a while, she leaves home with a video call active. When the WLAN connection is lost, the network senses the change and automatically starts delivering the P2P data over the 3G connection without restarting the P2P downloading service, and Alice is informed by the network of the change.

2.7 Bandwidth Aggregation Use Case

This use case shows that the MUE can use multiple connections simultaneously to serve a single application in order to get an aggregated bandwidth.

Alice uses a WLAN connection to download a film in the airport. Then she finds there is not enough time to finish downloading before the flight, so she must accelerate the download to save time. So she sets up the 3G connection, and lets the downloading service use both the WLAN and 3G simultaneously to achieve a wider aggregated bandwidth in order to speed up the download.

2.8 Service Transfer Use Case

This use case shows that the service can move among multiple connections according to the network's policies.

Alice launches a voice call through a WLAN connection, and browses web pages through the 3G connection at the same time. Then she starts a file transfer protocol (FTP) session to download software through the WLAN connection. She feels the WLAN connection becomes congested due to the large number of file transfers, therefore, she chooses to move the voice call to the 3G connection, and this transfer is transparent to her voice call.

2.9 Service Flow Duplication Use Case

In this use case, the service flow duplication is used to avoid disruptions created by handover. In other words, a subscriber requires the involvement of another MUE in the on-going session; i.e., the duplication of the current session. The multi-connection network and involved MUEs have the advantage compared to the "single-connection" network to allocate the required number of simultaneous connections in the MUE, thus providing ahead of time a smooth set-up of the duplicated session.

Alice watches a music concert with her family via her multi-connection MUE1 (for instance, a large screen) connected at her home via WLAN or fixed access. Subsequently, she decides to duplicate the on-going session to her multi-connection MUE2 with WLAN and 3G connections, using her MUE1. Instead of using MUE1 to request a classical service transfer to MUE2, she invokes the

network operator's service "service flow duplication"; she will avoid interruptions and/or glitches, for instance, delayed video and audio frames or IP packets created by a classical service transfer or HO. Once the multi-connection network performs the service flow duplication and the session run simultaneously in MUE2, Alice has the option to either:

1) Release the 3G connection in MUE2, and only maintain the WLAN connection.
2) Preserve both connections in MUE2 simultaneously. When she moves out of WLAN coverage leaving home, the network automatically shall maintain the service using the 3G connection, without service disruption.

2.10 Data Transmission Rate Adjustment Use Case

In this use case, when the MUE uses bandwidth aggregation, the service flow can be transmitted through different connections by adjusting their bit rate according to the access network's price and speed.

For example, Alice is enjoying Internet Protocol Television (IPTV) via her mobile phone when she is walking to her office. As she moves, she finds that there are some WLAN hot-spots available. So Alice decides to initiate the WLAN link in order to efficiently deliver over two interfaces. Then the server divides and delivers a single stream through the different data paths, adjusting the bit rate for each connection. If a MUE has two connections; e.g., one has three times the bit rate availability than the other, then the server adjusts the bit rate of one or both streams.

3 Architectural overview

The multi-connection functional architecture is based on a collection of multiple layers which objective is to enhance the current NGN architecture. Figure 1 shows the functional general architecture [1].

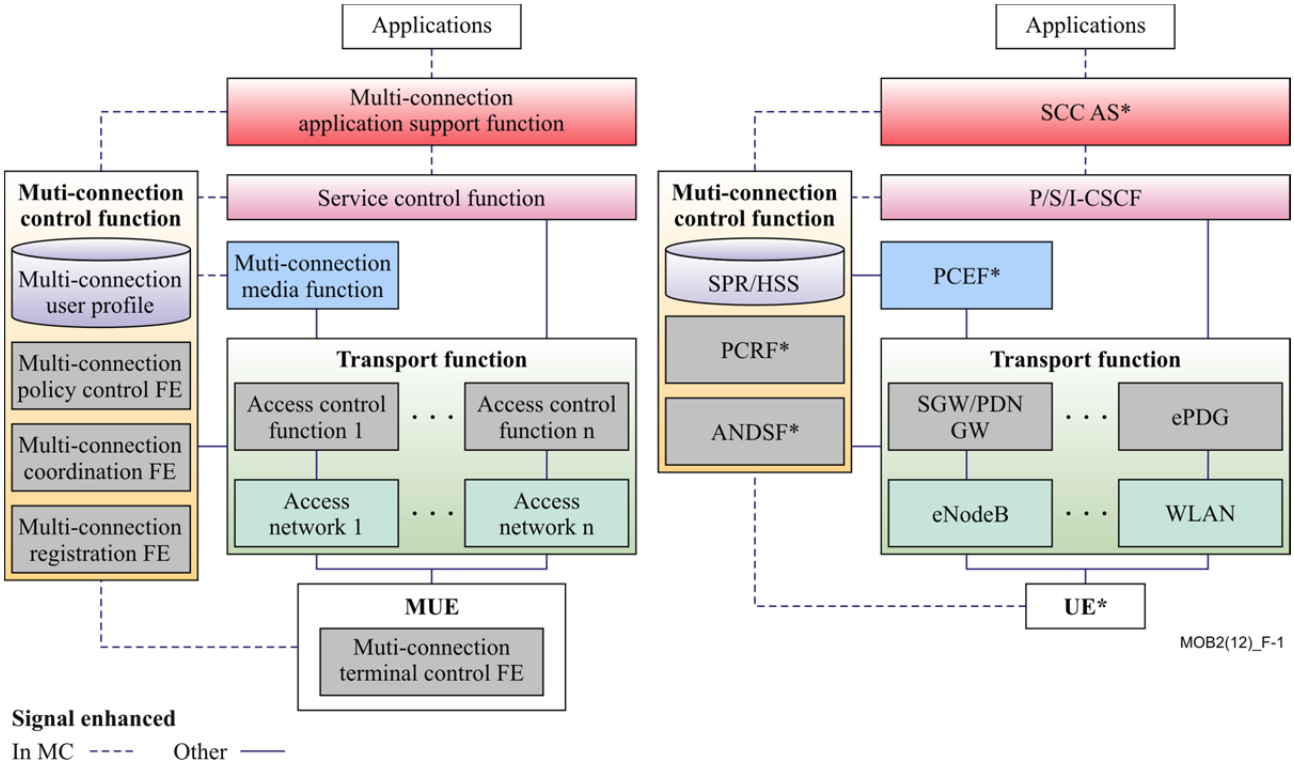

Figure 1 - Multi-connection Functional General Architecture [1]

The functional entities include new independent elements with interfaces and related multi-connection signalling, which enhance the existing functionality in NGN.

These functions have as objective, among others, to:

- Enforce the multi-connection access policy and maintain information on the available connections of the multi-connection User Equipment, such as session time length, bandwidth, connection status, and other important information;
- Manage multi-connection session initiation, session transfer, session release, and session update for the related connections;
- Provide multi-connection mobility management and flow-based traffic transport services;
- Provide multi-connection session continuity for services that so require it;
- Provide integrated statistical or dynamic policy control and mapping for specific services to certain accesses;
- Support Authentication, Authorisation, and Accounting (AAA) functions for multi-connection services assisting AAA relative events for each access;
- Support mechanisms for service composition and service decomposition by generating and merging multiple flows

3 *Architectural overview*

The multi-connection architecture enhances the current NGN functional architecture to support multiple concurrent sessions between a multi-connection UE (Multi-UE or MUE) and the multi-connection network in a coordinated manner. A paramount objective while designing and specifying the multi-connection architecture was to allow legacy single-connection networks to be supported, and furthermore to be backwards compatible with present deployed single-connection networks.

4 Description of functions, functional entities and reference points in multi-connection

This Section describes the various functions and specifically the Function Elements, as well the reference points among them in the multi-connection architecture.

4.1 Description of functions and functional entities

The Functions in the network infrastructure are:

1. Transport Function.
    a. Network Access.
    b. Access Control Functional Entity (AC-FE).
2. Multi-connection Media Function (MMF).
3. Service Control Function (SCF).
4. Multi-connection Application Support Function (MAS-F).

Additional (vertical) managing functions within the network infrastructure consisting of:

5. Multi-connection Control Function.
    a. Multi-connection User Profile Functional Entity (MUP-FE),
    b. Multi-connection Policy control Functional Entity (MPC-FE),
    c. Multi-connection Coordination Functional Entity(MC-FE), and
    d. Multi-connection Registration Functional Entity (MR-FE).

4.2 Description of Transport Function

The Transport Function provides connectivity from the involved access networks requested by the subscriber and/or network operator to all components and functions within the NGN multi-connection architecture. The function provides support for unicast and/or multicast transfer of media, as well as the transfer control and management.

The Transport Function is composed of a number of Access Networks and Access Control Functional Entities.

4.3 Description of Access Network and Access Control Functional Entity (AC-FE)

In the context of the multi-connection architecture, the Access Networks and the Access Control Functional Entities (AC-FE) reside inside of the Transport Function, in analogy to the access networks (RAN or UTRANs) in the mobile network architecture.

4.4 Access Network Description

The Access Network provides direct connectivity to the MUE. It gathers and aggregates incoming and outgoing traffic from/to the accesses towards the multi-connection core network. Some QoS functions are also performed upon the user data by the Access Networks.

4.5 Access Control Functional Entity (AC-FE)

The AC-FE includes resource control functions, such as spectrum, channel, and access point control. It also contains admission control functions, network attachment control functions, as well as mobility management, and other control functions within the NGN [2].

4.6 Description of Multi-connection Media Function (MMF)

The Multi-connection Media Function is conceptually placed between the Transport Function and the Service Control Function. Its main task is to enforce multiple access policies, load assignment

and QoS to meet the requirement of the multi-connection quality of service experience. Some of the MMF managed functions to provide specific network resources include:

1) Identification of flows to manipulate the mapping between a specific multi-connection service to one or more connections across heterogeneous accesses.

2) Enforcement of specific policies in each access according to dynamic information in them, such as handover activity across different accesses, network utilization, addition or removal of one or more accesses into a multi-connection service.

3) Report of dynamic traffic load information to the MC-FE, and

4) Maintaining the mapping of resource identifiers among flow IDs, access network IDs, and interface IDs, among others.

Other functions might be needed, and are for further study, as the multi-connection architecture evolves and matures in the ITU-T next study period, in conjunction with efforts from other forums.

4.7 Description of Service Control Function (SCF)

The Service Control Function performs resource control for multi-connection sessions, registration, authentication, and authorization at the service level for mediated and non-mediated services. It also supports service initiation, service release, authentication, authorization, and routing of service messages.

More specific presently, the SCF supports the:

1) Sending of service control messages to the Multi-connection Application Support Function (MAS-F) to support specific services and third-party applications.

2) Receiving and processing service control messages, and

3) Providing authentication and authorization in the service control layer, thus ensuring that the subscriber has valid access permissions to use the requested service.

Other functions might be added to the SCF, these are for further study, as the multi-connection architecture evolves and matures in conjunction with other forum efforts.

4.8 Description of Multi-connection Application Support Function (MAS-F)

The Multi-connection Application Support Function provides support to the application or applications on top of it. It also interfaces the application or applications with the Service Control Function, behaving as an API to easy an open access of the multi-connection architecture. One of the main reasons to include MAS-F in the multi-connection architecture was to encourage application designers to experiment and incorporate novel applications running on top of platforms like iPhone and other smartphones capable of providing parallel accesses for new user services.

In some languages like Java, and API refers to classes, interfaces, constructs, members, and serialized forms by which a programmer accesses a class, interface, or package. A programmer who writes a program that uses an API is referred to as a user of the API. A class whose implementation uses an API is a client of the API [3]: Effective Java, Joshua Bloch, Second edition].

The Multi-connection Application Support Function provides also control capability for those services interacting with the Multi-connection User Profile Functional Entity (MUP-FE) in the Multi-connection Control Function. It includes functions at the application level such as the service gateway (including open API), registration, and AAA required by applications.

Interacting with MAS-F, the applications may invoke multi-connection capabilities, such as bandwidth converge, low time delay, increased security, efficient utilization of network resources, load balancing, connection reliability, and service continuity. Other QoS and QoE features provided by the multi-connection network might be added in future multi-connection architecture platforms.

More precisely, the functions performed by MAS-F are categorized as follows [1]:

1) Provide multi-connection application support functionality, such as the execution of service procedures comprising service composition and service decomposition based on the subscriber's profile and/or presently available network capabilities,

2) Support of legacy applications; i.e., single-connection applications. It is advisable that in these cases, the existence of the multi-connection capability, provided by the network, is hidden from the single-connection application, and

3) Support interactions between multi-connection applications and legacy applications.

4) As encouraged above, provide open interfaces for applications to lay emphasis on the new capabilities and resources of the multi-connection architecture.

4.9 Description of Multi-connection Control Function

The Multi-connection Control Function acts as a managing and control function, which interacts with all strata of the multi-connection architecture network. Thus, it has direct interfaces to the MUE, Transport Function, Multi-connection Media Function, and Service Control Function. Interaction among these multi-connection architectural elements and the Multi-connection Control Function is via the Rt, Cm, Cm, and Pa reference points.

Currently, indirect managing and coordinating processes from the Multi-connection Control Function to the Application, and Multi-connection Application Support Function are for further study.

The Multi-connection Control Function provides main coordination communication control among all active heterogeneous accesses to the subscriber; such as 2G, 3G, LTE, WLAN, and others [1].

The Functional Entities composing the Multi-connection Control Function are depicted in Figure 2. They are:

1) Multi-connection User Profile Functional Entity (MUP-FE).

2) Multi-connection Policy control Functional Entity (MPC-FE).

3) Multi-connection Coordination Functional Entity(MC-FE), and

4) Multi-connection Registration Functional Entity (MR-FE).

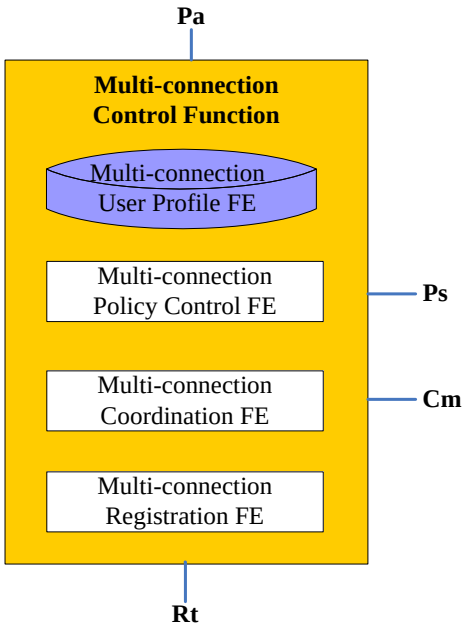

Figure 2 Multi-connection Control Function [1]

4.10 Multi-connection Functional Entities

In the following, we describe the six Functional Entities of the multi-connection functional architecture, see Ref. [1].

These are:

1. Multi-connection Terminal Control Functional Entity (MTC-FE).
2. The Access Control Functional Entity (AC-FE).
3. Multi-connection Registration Functional Entity (MR-FE).
4. Multi-connection Coordination Functional Entity (MC-FE).
5. Multi-connection Policy Control Functional Entity (MPC-FE), and
6. Multi-connection User Profile Functional Entity (MUP-FE).

A schematic of these Functional Entities is shown in Figure 3, see Ref. [1]. Where the MPC-FE, MC-FE, MR-FE, and MUP-FE reside in the Multi-connection Control Function. The AC-FE resides in the Transport Function, and the MTC-FE in the multi-connection UE.

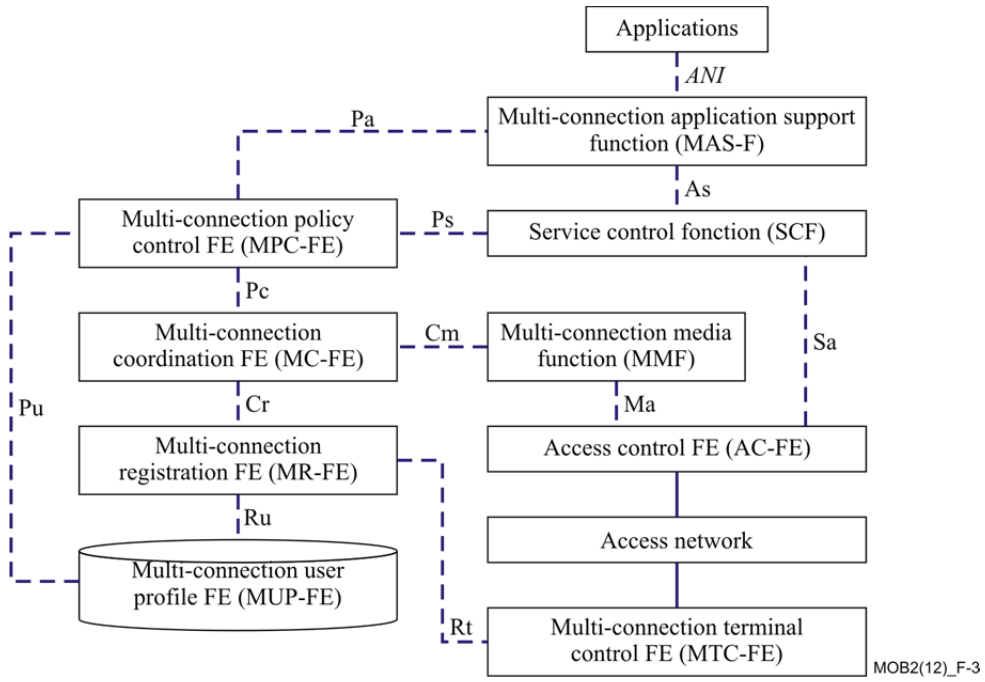

Figure 3 Multi-connection Architecture Functional Entities [1]

In the following clauses, a detailed description of these six Functional Entities is provided. The first FE to be described is a new function or practically speaking, a stack, within the multi-connection UE (MUE).

4.11 Multi-connection Terminal Control Functional Entity (MTC-FE)

The Multi-connection Terminal Control Functional Entity resides in the multi-connection UE (MUE). See Figure 3. It is a new function within the "currently" or presently market-deployed UE, since it allows the MUE to exchange multi-connection related information with the network through the reference point Rt.

MTC-FE communicates with MR-FE to support multi-connection user traffic and pertaining signalling. For instance, multiple registrations and their management, discovery and selection of available and permissible access networks, and other functionality related to policy control, authentication, authorization, and roaming.

Specifically, the functions carried by MTC- FE are as follows, see Ref. [1]:

1) Identification and maintenance of available network access information in MUE.

2) Removal of invalid access network information in MUE, following policy compliance.

3) Receipt and enforcement of access network selection information following the policies implemented in the multi-connection network, for instance provided by the operator in a static form or in a dynamic form, and transported by the reference point Rt.

Currently, the optionality of implementation is considered for services provided prior to setting up the multi-connection session; i.e., before allowing initial access to the multi-connection network. Services such as:

- Authentication types
- Home/roaming operator lists
- Location
- 3GPP information
- Record authentication, and authorization of credentials in the MUE

Other functionality to be implemented within the MTC-FE is for further study and most likely will be developed in concert with the 3GPP and IETF standardization progress.

4.12 Access Control Functional Entity (AC-FE) and further LTE - PCC Enhancements

The Access Control Functional Entity (AC-FE) is responsible for coordinating and controlling user plane tunnels established by the MUE [1]. The AC-FE interacts with the Multi-connection Coordination (MC-FE), Multi-connection Registration (MR-FE), and Multi-connection Policy Control Functional Entity (MPC-FE) at initiation, addition, removal, composition, and decomposition of connections for each access network active in the multi-connection session.

A number of tasks are performed by the AC-FE, these are:

1) Interaction with the MR-FE for authorisation of connection establishment.
2) Interaction with the MC-FE to report access network resources and their availability.
3) Lawful Interception.
4) IP address allocation (for IPv4 or IPv6).
5) QoS enforcement (gating and bandwidth control in accordance to a QoS policy).
6) Charging rules enforcement (both online and offline).
7) DHCPv4 or DHCPv6 services.
8) Mobility anchoring within a single access, and
9) Optionally support of deep packet inspection functionality.

In addition interactions between the AC-FE and MC-FE report enhancement of network performance via multiple access retransmission optimization.

LTE develops the Policy and Charging Control (PCC) architecture, see Ref. [4]. The multi-connection architecture shall align its QoS enforcement scheme to the architecture to reach compatibility between the two systems, thus diminishing implementation effort and obtain interoperability for mobile operators' benefit.

Figure 4 shows the 3GPP PCC Rel.11 architecture. The Figure includes the robust case where the Policy and Charging Enforcement Function (PCEF) resides in the mobile visited network, and supports local breakout – as explained in more detail below, in this case the Subscription Profile Repository (SPR) network element is used.

The multi-connection requirements, see Ref. [15] "Recommendation ITU-T Y.2251, Multi-connection Requirements" call for specific items to be fulfilled under the umbrella of identification of multiple connections and map them to specific IP flows; Among these requirements are a binding mechanism.

The following is required when facing the problem of supporting multiple connections in the IP network; i.e., identifying IP flows and binding them to different access network connections:

1) Classification of IP flows. All packets belonging to a particular flow are required to have a set of properties. These are:

    - One or more packet header fields; e.g., destination IP address, transport header field (e.g., destination port number), or application header field (e.g., RTP header fields)
    - One or more characteristics of the packet; e.g., number of MPLS labels
    - One or more fields derived from packet treatment; e.g., next hop IP address or the output interface. A packet is defined to belong to a flow if it completely satisfies all the defined properties of the flow.

2) Identification of IP flows. In the multi-connections environment, the MUE and network

need to distinguish IP flows. It is required to classify all kinds of current identifiers of the UE: service data and user, such as IP address, and choose a proper one or create a new one to identify the IP flows in the multi-connection environment

3) Binding of IP flows. The connections are used to carry certain IP flows, so IP flows marked by their identifiers are required to be bound to proper connections.

Likewise, in the PCC model when accessing a visited network, the Visited Policy and Charging Rules Function PCRF (V-PCRF) performs 11 policy and charging functions including, see Ref. [4]:

1. Enforcing visited operator policies supporting QoS authorization requested by the home operator; for instance on a per QoS Class Identifier (QCI), or on a per service basis following roaming agreements. The V-PCRF informs the Home PCRF (H-PCRF) if a request has been denied and it may provide the acceptable QoS Information for the service.
2. If the interaction of the Gxx reference point is terminated locally at the V-PCRF, the linkage of the reference point Gx to the Gateway Control Session. (The Gxx reference point resides between the PCRF and the Bearer Binding and Event reporting Function (BBERF)). This reference point enables a PCRF to have dynamic control over the BBERF behaviour. Finally, the Gxx reference point also enables the signalling of QoS control decisions.
3. If the interaction of the Gxx reference point is terminated locally at the V-PCRF, the extraction of QoS rules from the PCC rules provided by the H-PCRF over the S9 reference point (between the V-PCRF and the HPCRF). Additionally, the V-PCRF provides updated PCC rules to the PCEF and QoS rules to the BBERF, if appropriate.
4. Before this functionality is explained, consider that the LTE Application Function (AF) is an element offering applications that require dynamic policy and/or charging control over the IP-CAN user plane. The AF communicates with the PCRF to transfer dynamic session information. This information is required for the decisions taken by the PCRF, as well as to receive IP-CAN specific information and notifications about the IP-CAN bearer level events. For instance, an AF may be the P-CSCF of the IMS. The AF may receive an indication that the service information is not accepted by the PCRF in conjunction with service information that the PCRF would accept; in such case, the AF rejects the service establishment towards the MUE – or in one of the accesses handled by the MUE. If possible the AF forwards the service information to the MUE that the PCRF would accept. Thus, if the AF resides in the VPLMN:
   - Proxy Rx authorizations over the S9 reference point to the H-PCRF
   - Relay event subscriptions and notifications between the H-PCRF and the visited AF

If the Gx reference point interactions are proxied between the PCEF and the H-PCRF, the V-PCRF proxies:

5. Providing indication of IP-CAN Session Establishment and Termination.
6. Provisioning of Policy and Charging Rule.
7. Provisioning of Application Detection and Control Rules.
8. Requesting Policy and Charging Rules.

In other scenario, if a Gateway Control Session is used and if during the IP-CAN Session Establishment the Gateway Control Session Establishment procedure was proxied to the H-PCRF, then the V-PCRF shall also proxy all other Gateway Control Session procedures to the H-PCRF.

But, if the Gateway Control Session was not proxied to the H-PCRF then the V-PCRF shall handle all Gateway Control Session procedures locally and not proxy them to the H-PCRF. The following implications then arise:

9. An IP-CAN Session modification may trigger the V-PCRF to update the Gateway Control Session if required, in order to maintain the alignment of PCC and QoS Rules.

10. An IP-CAN Session termination procedure may trigger the V-PCRF to terminate the Gateway Control Session if the Gateway Control Session was established for the purpose of a single IP-CAN session. Otherwise, a Gateway Control and QoS Rules Provision procedure may be initiated to remove the QoS Rules associated with the IP-CAN session.

11. The V-PCRF performs certain event reporting procedures for the PCEF in the visited network and locally terminated Gxx interaction when receiving a Gateway Control message and QoS Rules Request message from the BBERF.

When Rx components are proxied between an AF, in the VPLMN, and the H-PCRF, the V-PCRF shall proxy service session information between the AF and the H-PCRF.

The V-PCRF shall provide Application Detection Control (ADC) rules control as instructed by the H-PCRF over the S9 reference point. The V-PCRF shall provide updated ADC rules to the PCEF or Traffic Detection Function (TDF), depending on the VPLMN configuration.

In aligning the multi-connection architecture and the LTE PCC system, for a more mature multi-connection system, the SPR might be proposed to be an independent function, or Functional Entity, contained in the Multi-connection User Profile Functional Entity (MUP-FE); i.e., essentially a part of the Multi-connection Control Function.

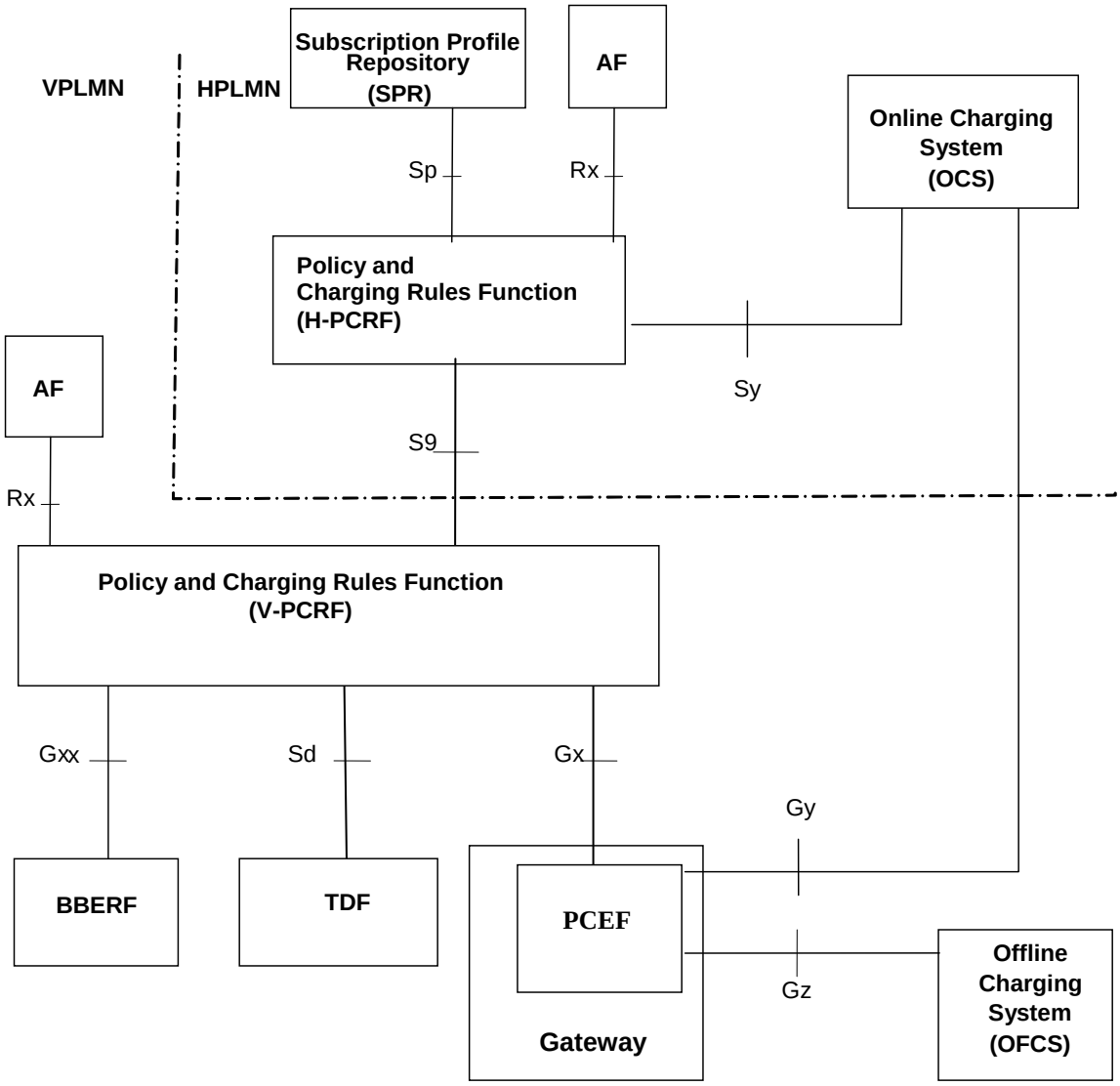

Figure 4 Overall PCC Architecture for Roaming with PCEF in Visited Network (Local Breakout) When SPR is Used [4]

4.13 Multi-connection Registration Functional Entity (MR-FE) and further LTE/Evolved Packet Core (EPC) Enhancements

The Multi-connection Registration Functional Entity (MR-FE) manages active MUEs. It monitors their status of connectivity to the available access networks. The connectivity provides the MUEs with multi-connection sessions. The MR-FE takes part in the initial phase to establish those sessions; i.e., their registration and interactions to the corresponding multi-connection FEs.

The MR-FE accepts the registration requests from every MUE to all valid network accesses. It is responsible for binding each MUE with all available network access IDs, utilizing for instance IP addresses and MSISDNs.

The MR-FE shares most recent network access information to the MUE and provides information to optimize multi-connection MUE pre-configuration.

It also exchanges multi-connection signalling information to the MUE via the reference point Rt; to the Multi-connection User Profile Functional Entity (MUP-FE) via the reference point Ru; and to the Multi-connection Coordination Functional Entity (MC-FE) via the reference point Cr.

At least six functions are performed by the MR-FE, these are [1]:

1) Identification and maintenance of binding information among different multiple accesses for each MUE.
2) Removal of invalid access network information to the MUE.
3) Push and selection of access network to the MUE according to recommended operator's policies with provisioned access information before initiating the actual network access. The information relates to authentication types, home/roaming operator lists, location, 3GPP information, and other.
4) Update the available access network information to MUEs.
5) Provide available multi-connection information of MUEs to the MC-FE for making multi-connection policy decisions, and
6) Optionally, provide multi-connection authentication and authorization, and allocation and maintenance of MUE identifiers.

To align the multi-connection architecture to the LTE/Evolved Packet Core (EPC), alignment and enhancements are suggested to enhance the functions above under the scheme of trusted and untrusted non-3GPP networks, see Ref. [5].

For alignment purposes towards the EPC architecture, consideration shall be done on the MUE to perform during initial attach, or handover-attach, the discovery of the trust relationship; whether it is a Trusted or Untrusted Non-3GPP Access Network, of the non-3GPP access network in order to know which non-3GPP IP access procedure to initiate. The trust relationship of a non-3GPP access network would be then known to the MUE with one of the following two options:

1) If the non-3GPP access supports 3GPP-based access authentication, the MUE discovers the trust relationship during the 3GPP-based access authentication, or if
2) The MUE operates on the basis of pre-configured policy in the MUE.

There exists an important use case in the multi-connection scenarios, Load Balance [6] case. Similarly, although optional, there exists the capability of WLAN offload; or more precisely Non-seamless WLAN offload. This capability applies to the MUE supporting WLAN radio access in addition to radio access.

A MUE supporting non-seamless WLAN offload may, while connected to WLAN access, route specific IP flows via the WLAN access without traversing the EPC. These IP flows are identified

via user preferences, the Local Operating Environment Information where, in addition to operator policy and user preferences, the MUE may take into account the Local Operating Environment Information [7] when deciding which access to use for an IP flow. The actual Local Operating Environment Information is implementation dependent and may comprise such items as, radio environment information, quality of IP connection, application specific requirements, and power considerations, among other items. The IP flows are also identified via policies that may be statically pre-configured by the operator on the UE, or dynamically set by the operator via the Access Network Discovery and Selection Function (ANDSF). For such IP flows, the MUE uses the local IP-address allocated by the WLAN access network and no IP address preservation is provided between WLAN and 3GPP accesses.

In order to perform the non-seamless WLAN offload, the MUE needs to acquire a local IP-address on WLAN access, and it is not required to connect to an evolved Packet Data Gateway (ePDG).

Also, in case the WLAN access is EPC connected it is possible for a MUE supporting seamless WLAN offload to perform seamless WLAN offload for some IP flows, and non-seamless WLAN offload for some other IP flows simultaneously.

Specially helpful, for future enhancements towards a tightly coupled system to the 3GPP developments in Releases 10 and 11, is the addition of an access to a PDN connection. In the following the additions of a:

1) WLAN access, and
2) 3GPP Access

are examined, following the 3GPP Release 10, see Ref. [7] guidelines.

The following procedures and signalling flows assume that the MUE supports IP flow mobility and that the MUE has performed a PDN Connection establishment procedure through one network access. Subsequently, the MUE attaches to a second access and starts using both accesses for the same PDN connection. *As a result the MUE is simultaneously connected via both accesses* (which is one of the goals of the multi-connection architecture) and a set of traffic flows are routed through one access while the remaining traffic flows are routed through the other access.
Non-roaming, home routed roaming and Local Breakout cases are also supported by this procedure. The Authentication, Authorization and Accounting (AAA) proxy and visited Policy and Charging Rules Function (vPCRF) are only used in the case of home routed roaming and Local Breakout. In non-roaming scenarios, the AAA proxy and vPCRF are not involved.

The optional interaction steps between the gateways and the PCRF in the procedures only occur if dynamic policy provisioning is deployed in the Evolved Packet Core (EPC). These steps are never present when the solution is applied to the I-WLAN mobility architecture [8].

4.13.1 Addition of WLAN Access

After successfully attachment to a 3GPP access, the MUE has established a PDN connection over 3GPP access. Subsequently the MUE performs the WLAN attachment, and requests to establish a PDN connection using the same Access Point Name (APN), and attempts to use both accesses for the same PDN connection simultaneously. The WLAN access may be considered as the UE's foreign link from DSMIPv6 perspective.

The signalling flow in Figure 5 below depicts the particular case *where the MUE is firstly connected to a 3GPP access and then it requests the addition of a WLAN access.*

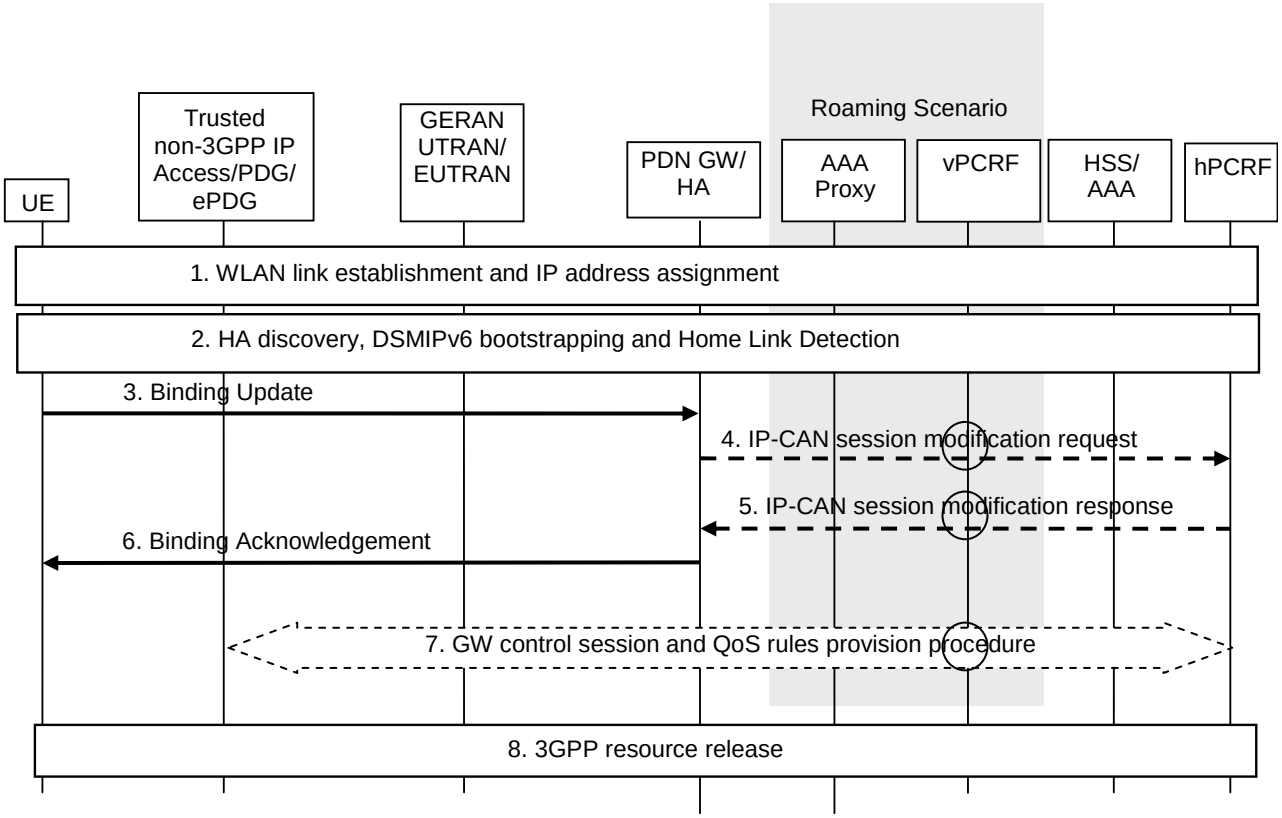

Figure 5 Addition of WLAN Access to the PDN Connection [7]

In the flow:

1. The MUE discovers a WLAN and connects to it and configures an IPv4 address and/or an IPv6 address/prefix according to TS 23.402 [5] or TS 23.327 [8], depending whether the WLAN access is used in the context of EPC or I-WLAN mobility architecture.

2. The MUE performs Home Agent (HA) discovery, DSMIPv6 bootstrapping and DSMIPv6 home link detection procedure according to TS 23.402 [5] unless already performed in the 3GPP access.

3. The MUE sends a DSMIPv6 Binding Update (Home Address (HoA), Care-of Address (CoA), Lifetime, Binding ID (BID), Flow Identification (FID), flow description) message to the Home Agent (HA) over the WLAN access. The MUE may include the requested routing rules via the FID mobility option with both the routing filters and the BID - which includes the routing address, as specified in IETF RFC 5555 [9], IETF RFC 5648 [10] and RFC 6089 [11]. The MUE can include more than one routing rule by including multiple FID mobility options in the Binding Update. The DSMIPv6 Binding Update also contains an indication which indicates that the home link; i.e., the 3GPP access, is still connected and also the BID mobility options which identify that one binding is associated with the home address; i.e., the 3GPP access, and the other with the Care-of-Address from the WLAN access. The MUE also indicates in the Binding Update which is the default binding where the Home Agent (HA) should route packets not matching any FID as specified in RFC 6089 [11].

4. In case the HA function is located in the PDN GW and dynamic PCC is deployed, the PDN GW sends an IP-CAN session modification request to the PCRF. In this request, the PDN GW provides the updated routing rules to the PCRF. The PCRF stores the mapping between each Service Description Framework (SDF) and its routing address.

5. If the HA function is located in the PDN GW, based on the successful establishment of resources at the Bearer Binding and Event Reporting Function (BBERF), the PCRF sends an acknowledgement to the PDN GW, including updated PCC rules if appropriate.

6. The HA creates a DSMIPv6 binding, installs the IP flow routing rules and sends a Binding Acknowledgment (Lifetime, HoA, CoA, BID, FID) as specified in RFC 5555 [9], RFC 5648 [10] and RFC 6089 [11], to indicate which routing rules requested by the MUE are accepted.

   The PDN GW may send message 6 before receiving the reply from PCRF in message 5.

7. Based on the IP-CAN session modification request (if step 4 was performed), the PCRF ensures that the relevant QoS rules for the SDFs are installed in the target BBERF. This is done by a GW control session and QoS rules provision procedure as specified in TS 23.203 [4].

8. In case the HA function is located in the PDN GW, appropriate resource release procedures are executed for the resources associated with the flows that were moved away from the 3GPP source access. This procedure may be triggered by the PCRF via a GW control session and QoS rules provision procedure if Proxy Mobile IPv6 (PMIPv6) is used on S5 and it may be triggered by the PDN GW in case GTP is used on S5.

   If the HA function is implemented in I-WLAN mobility, the MUE may initiate GPRS resource release procedures for those resources that were moved away from the 3GPP source access, as specified in TS 23.060 [12].

4.13.2 Addition of 3GPP Access

After successfully attachment to WLAN access, the MUE has established a PDN connection over WLAN. As the MUE detects that the WLAN access is not the home link from DSMIPv6 perspective, DSMIPv6 signalling is triggered over the WLAN access.

Subsequently, as described below, the MUE performs the initial attachment procedure or PDN Connection establishment procedure over a 3GPP access and establishes a PDN connection using the same APN, as described in TS 23.060 [12], TS 23.401 [13] or TS 23.402 [5]. As the MUE has indicated IP flow mobility during the initial attachment over WLAN, the 3GPP access attachment completion shall not trigger the DSMIPv6 binding deregistration.

The signalling flow in Figure 6 below depicts the particular case where the M*UE is firstly connected to a WLAN access and then it requests addition of a 3GPP access.*

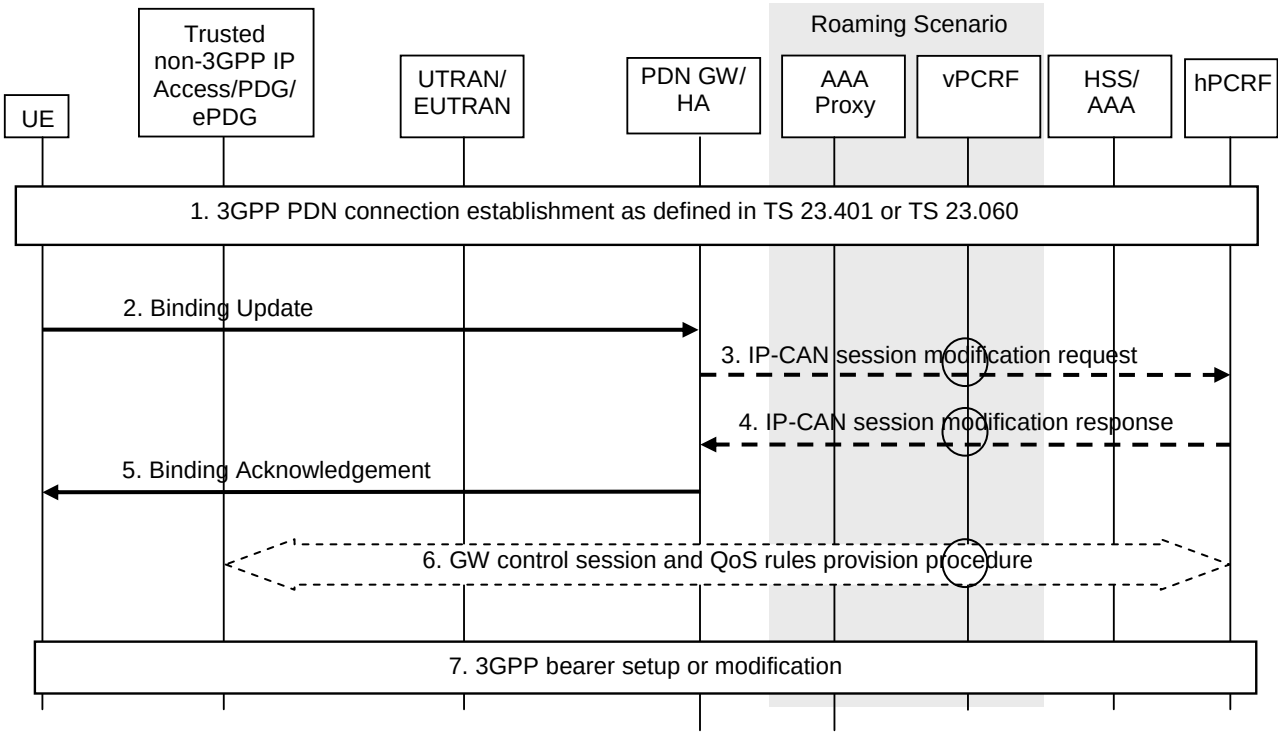

Figure 6 Addition of 3GPP Access to the PDN Connection [7]

In the flow:

1. The MUE discovers a 3GPP access and performs the Attach or PDN Connection establishment procedure according to TS 23.401 [13] or TS 23.060 [12]. Specifically, the MUE sets the Request Type to Handover to facilitate that the MME selects the same PDN GW/HA as the MUE uses to connect to the WLAN Access. Since the MUE has indicated IP flow mobility support during the initial attachment over WLAN, the HA shall not deregister the DSMIPv6 binding by sending a Binding Revocation Indication towards the WLAN access.

2. The MUE sends a DSMIPv6 Binding Update (HoA, CoA, Lifetime, BID, FID, flow description) message to the HA over the 3GPP access. The MUE may include the requested routing rules via the FID mobility option with both the routing filters and the BID; which includes the routing address, as specified in RFC 5555 [9], RFC 5648 [10] and RFC 6089 [11]. If the 3GPP access is the home link, the MUE sets the 'H' flag in the respective BID mobility option, as specified in RFC 6089 [11]. The MUE can include more than one routing rule by including multiple FID mobility options in the Binding Update. The MUE also indicates in the Binding Update which is the default binding where the HA should route packets not matching any FID as specified in RFC 6089 [11].

3. In case the HA function is located in the PDN GW and dynamic PCC is deployed, the PDN GW sends an IP-CAN session modification request to the PCRF. In this request, the PDN GW provides the updated routing rules to the PCRF. The PCRF stores the mapping between each Service Description Framework (SDF) and its routing address.

4. If the HA function is located in the PDN GW, based on the successful establishment of resources at the BBERF, the PCRF sends an acknowledgement to the PDN GW, including updated PCC rules if appropriate.

5. The HA sends a Binding Acknowledgment (Lifetime, HoA, CoA, BID, FID) as specified in RFC 5555 [9], RFC 5648 [10] and RFC 6089 [11], to indicate which routing rules requested by the MUE are accepted.

The PDN GW/HA may send message 5 before receiving the reply from PCRF in message 4.

6. Based on the IP-CAN session modification request (if step 3 was performed), the PCRF ensures that the relevant QoS rules for the SDFs are installed in the target BBERF. This is done by a GW control session and QoS rules provision procedure as specified in TS 23.203 [4].

7. In case the HA function is located in the PDN GW, appropriate bearer setup or modification procedures are executed for the resources associated with the flows that were moved onto the 3GPP access. This procedure may be triggered by the PCRF via a GW control session and QoS rules provision procedure; if PMIPv6 is used on S5; and it may be triggered by the PDN GW in case GTP is used on S5.

If the HA function is implemented in I-WLAN mobility, the MUE may initiate GPRS bearer setup or modification procedures for those resources that were moved onto the 3GPP access, as specified in TS 23.060 [12].

4.14 Multi-connection Coordination Functional Entity (MC-FE)

The Multi-connection Coordination Function Entity manages both, the IP-based and flow-based mobility management mechanisms. This is done based on the dynamic behavior of the status of the different active accesses connected to the multi-connection network.

The MC-FE connects directly to the Multi-connection Policy Control FE (MPC-FE) through the PC reference point; to the Multi-connection Registration FE (MR-FE) through the Cr reference point; and to the Multi-connection Media Function (MMF) through the Cm reference point.

The MC-FE is a composition of multi-connection coordinating control functions.

Among others, these functions are:

1) Set up and update specific traffic loads and QoS policy for each access network and consequently assignment to the Multi-media Media Function of such load to the Multi-connection Media Function (MMF).

2) Dynamically collect and maintain traffic load information in active accesses.

3) Report abnormal status in the active accesses.

4) Optionally obtain user’s preferences on network selection.

4.15 Multi-connection Policy Control Functional Entity (MPC-FE) Enhancements and Alignment towards the PCC Architecture

The Multi-connection Policy Control Functional Entity provides policies for every multi-connection session and guarantees the QoS of the session by sending the policies to the Multi-connection Coordination Functional Entity (MC-FE) and Access Control Functional Entity (AC-FE). The MC-FE and AC-FE subsequently assign specific policies to each access network based on the policies received from the MPC-FE, such as control routing paths, or bit rates for the active IP flows.

The MPC-FE has direct connectivity to the:

1) Multi-connection Application Support Function (MAS-F) through the Pa reference point.

2) Service Control Function (SCF) through the Ps reference point.

3) Multi-connection Coordination Functional Entity (MC-FE) through the Pc reference point.

4) Multi-connection User Profile FE (MUP-FE) through the Pu reference point.

Other reference points may be created following the PCC architecture to align the multi-connection architecture for compatibility purposes.

The six functions of MPC-FE in the multi-connection functional architecture are as follows [1]:

1) Acquire service information from the Service Control Function (SCF).

2) Receive and authorize the QoS resource request from the SCF.

3) Store and maintain the rules to make policies defined by the network operator.

4) Obtain subscription profile from the MUP-FE.

5) Make policy decisions based on the above information and provide the decisions to the MC-FE.

6) And optionally, support and provide policy mapping between different networks for the AC-FEs.

At least functions (1) and (2) above might be enhanced by the PCC architecture, specially with features as described in the following clauses after TS 23.203 [4] for service information and QoS compatibility.

4.15.1 PCC Rule Authorization and QoS Rule Generation

Policy and Charging Control (PCC) Rule authorization is the selection of the QoS parameters (QoS Class Identifier (QCI), Address Resolution Protocol (ARP), Guaranteed bitrate (GBR), Maximum bitrate (MBR), and others) for the PCC rules.

The Policy and Charging Rules Function (PCRF) shall perform the PCC rule authorization for complete dynamic PCC rules belonging to Application Function (AF) sessions, as well as for PCC rules without corresponding AF sessions. Based on AF instructions dynamic PCC rules can be authorized even if they are not complete; e.g., due to missing service information regarding QoS or traffic filter parameters.

The PCC rule authorization depends on the IP-CAN bearer establishment mode of the IP-CAN session and the mode (UE or Network (NW)) of the PCC rule:

- In UE/NW bearer establishment mode, the PCRF shall perform the authorization for all PCC rules that are to be handled in NW mode

- Otherwise, if PCC rules are to be handled in MUE mode or when in UE-only bearer establishment mode, the PCRF shall first identify the PCC rules that correspond to a MUE resource request and authorize only these

  The PCRF shall compare the traffic mapping information of the MUE resource request with the service data flow filter information of the services that are allowed for the user. Each part of the traffic mapping information shall be evaluated separately in the order of their related precedence. Any matching service data flow filter leads to an authorization of the corresponding PCC rule for the MUE resource request unless the PCC rule is already authorized for a more specific traffic mapping information or the PCC rule cannot be authorized for the QCI that is related to the MUE resource request (details are described in the next paragraph). Since a PCC rule can contain multiple service data flow filters it shall be ensured by the PCRF that a service data flow is only authorized for a single MUE resource request.

  NOTE 1: For example, a PCC rule containing multiple service data flow filters that match traffic mapping information of different MUE resource requests could be segmented by the PCRF according to the different matching traffic mapping information. Afterwards, the PCRF can authorize the different PCC rules individually.
  The PCRF knows whether a PCC rule can be authorized for a single QCI only or a set of QCIs; based on Subscription Profile Repository (SPR) information or local configuration). If the processing of the traffic mapping information would lead to an authorization of a PCC

rule, the PCRF shall also check whether the PCC rule can be authorized for the QCI that is related to the MUE resource request containing the traffic mapping information. If the PCC rule cannot be authorized for this QCI, the PCRF shall reject the traffic mapping information unless otherwise stated in [4].

If there is any traffic mapping information not matching to any service data flow filter known to the PCRF and the MUE is allowed to request for enhanced QoS for traffic not belonging to operator-controlled services, the PCRF shall authorize this traffic mapping information by adding the respective service data flow filter to a new or existing PCC. If the PCRF received a Service Description Framework (SDF) filter identifier together with this traffic mapping information, the PCRF shall modify the existing PCC rule if the PCC rule is authorized for a GBR QCI.

NOTE 2: If the PCC rule is authorized for a non-GBR QCI, the PCRF may either create a new PCC rule or modify the existing PCC rule.

The PCC rule that needs to be modified can be identified by the service data flow filter the SDF filter identifier refers to. The requested QoS shall be checked against the subscription limitations for traffic not belonging to operator-controlled services.

If the PCRF needs to perform the authorization based on incomplete service information and thus cannot associate a PCC rule with a single IP-CAN bearer, then the PCRF shall generate for the affected service data flow an individual PCC rule per IP-CAN bearer that could carry that service data flow. Once the PCRF receives the complete service information, the PCC rule on the IP-CAN bearer with the matching traffic mapping information shall be updated according to the service information. Any other PCC rule(s) previously generated for the same service data flow shall be removed by the PCRF.

NOTE 3: This is required to enable the successful activation or modification of IP-CAN bearers before knowing the intended use of the IP-CAN bearers to carry the service data flow(s).

For an IP-CAN, where the PCRF gains no information about the uplink IP flows; i.e., the MUE provided traffic mapping information contains no information about the uplink IP flows, the binding mechanism shall assume that, for bi-directional service data flows, both downlink and uplink packets travel on the same IP-CAN bearer.

Whenever the service data flow template or the MUE provided traffic mapping information change, the existing authorizations shall be re-evaluated; i.e. the authorization procedure herein specified is performed. The re-evaluation may, for a service data flow, require a new authorization for a different MUE provided mapping information.

Based on PCRF configuration or AF instructions, dynamic PCC rules may have to be first authorized for the default QCI/default bearer; i.e., bearer without MUE provided traffic mapping information, until a corresponding MUE resource request occurs.

NOTE 4: This is required to enable services that start before dedicated resources are allocated.

A PCC rule for a service data flow that is a candidate for visited Single Radio Voice Call Continuity (vSRVCC) according to TS 23.216 [14] shall have the packet switched (PS) to circuit switched (CS) session continuity indicator set.

For the authorization of a PCC rule the PCRF shall take into account the IP-CAN specific restrictions and other information available to the PCRF. Each PCC rule receives a set of QoS parameters that can be supported by the IP-CAN. The authorization of a PCC rule associated with an emergency service shall be supported without subscription information; i.e., information stored in the Subscription Profile Repository (SPR). The PCRF shall apply policies configured for the emergency service.

When both a Gx and associated Gxx interface(s) exist for an IP-CAN session, the PCRF shall generate QoS rules for all the authorized PCC rules at this stage. The PCRF shall ensure consistency between the QoS rules and PCC rules authorized for the same service data flow when QoS rules are derived from corresponding PCC rules.

When flow mobility applies for the IP-CAN Session, one IP-CAN session may be associated to multiple Gateway Control Sessions with separate Bearer Binding and Event Reporting Functions (BBRFs). In this case, the PCRF shall provision QoS rules only to the appropriate BBERF based on IP flow mobility routing rules received from the PCEF.

4.15.2 Policy Control

The Multi-connection Policy Control Functional Element (MPC-FE) requires to make parallel alignment to the PCC model. This effort shall match to the following functionality, see Ref. [4]:

- Binding; i.e., the generation of an association between a service data flow and the IP-CAN bearer transporting that service data flow
- Gating control; i.e., the blocking or allowing of packets, belonging to a service data flow or specified by an Application Identifier, to pass through to the desired endpoint
- Event reporting; i.e., the notification of and reaction to application events to trigger new behaviour in the user plane as well as the reporting of events related to the resources in the GW (PCEF)
- QoS control; i.e., the authorisation and enforcement of the maximum QoS that is authorised for a service data flow, an Application identified by Application Identifier, or an IP-CAN bearer
- Redirection; i.e., the steering of packets, belonging to an application defined by the Application Identifier to the specified redirection address
- IP-CAN bearer establishment for IP-CANs that support network initiated procedures for IP-CAN bearer establishment

An important use case, covered in the multi-connection Scenarios, see Ref. [6] is Bandwidth Aggregation, in this case, after PCC, the aggregation of multiple service data flows; e.g., for GPRS a PDP context, the combination of the authorised QoS information of the individual service data flows is provided as the authorised QoS for this aggregate, see Ref. [4].

The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the GW (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorised QoS may, depending on operator policy and network capabilities, lead to network initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules shall firstly take place.

QoS authorization information may be dynamically provisioned by the PCRF or, it can be a pre-defined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorised QoS information for the IP-CAN bearer, combined QoS, may be provided. For predefined PCC rules within the PCEF the authorized QoS information shall take affect when the PCC rule is activated. The PCEF shall combine the different sets of authorized QoS information; i.e., the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF shall know the authorized QoS information of the predefined PCC rules and shall take this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription

and operator policies regardless of whether these PCC rules are dynamically provided, predefined or both.

For policy control, the Application Function (AF) interacts with the PCRF and the PCRF interacts with the PCEF as instructed by the AF. For certain events related to policy control, the AF shall be able to provide instructions to the PCRF to act on its own; i.e., based on the service information currently available.

The following events are subject to instructions from the AF:

- The authorization of the service based on incomplete service information

  NOTE 1: The QoS authorization based on incomplete service information is required for instance by IMS session setup scenarios with available resources on the originating side and a need for resource reservation on the terminating side.
- The immediate authorization of the service
- The gate control; i.e., whether there is a common gate handling per AF session or an individual gate handling per AF session component required
- The forwarding of IP-CAN bearer level information, or the following events happen:
  - Type of IP-CAN; e.g., GPRS and I-WLAN
  - Transmission resource status: established, released, or lost
  - Access Network Charging Correlation Information
  - Credit denied

    NOTE 2: The credit denied information is only relevant for AFs not performing service charging.

To enable the binding functionality, the MUE and the AF shall provide all available flow description information; e.g., source and destination IP address, port numbers, and the protocol information. The MUE shall use the traffic mapping information to indicate downlink and uplink IP flows.

4.15.3 Service (data flow) Prioritization and Conflict Handling

Service pre-emption priority enables the PCRF to resolve conflicts where the activation of all requested active PCC rules for services result in a cumulative authorized QoS which exceeds the Subscribed Guaranteed bandwidth QoS, see Ref. [4].

For example, when supporting network controlled QoS, the PCRF may use the pre-emption priority of a service, the activation of which causes that the subscriber's authorized QoS is exceeded. If this pre-emption priority is greater than that of any one or more active PCC rules, the PCRF can determine whether the deactivation of any one or more such rules would allow the higher pre-emption priority PCC rule to be activated whilst ensuring the resulting cumulative QoS does not exceed a subscriber's Subscribed Guaranteed Bandwidth QoS.

If such a determination can be made, the PCRF may resolve the conflict by deactivating those selected PCC rules with lower pre-emption priorities and accepting the higher priority service information from the AF. If such a determination cannot be made, the PCRF may reject the service information from the AF.

NOTE: Normative PCRF requirements for conflict handling are not defined. Alternative procedures may use a combination of pre-emption priority and Application Function (AF) provided priority indicator.

4.15.4 Policy Control and Charging Rules Function (PCRF)

The PCRF encompasses policy control decision and flow based charging control functionalities, see TS 23.203 Ref. [4].

The PCRF provides network control regarding the service data flow detection, gating, QoS, and flow based charging (except credit management) towards the PCEF.

The PCRF shall apply the security procedures, as required by the operator, before accepting service information from the Application Function (AF).

The PCRF shall decide whether application traffic detection is applicable, as per operator policies, based on user profile configuration, received within subscription information.

The PCRF shall decide how certain service data flow/detected application traffic shall be treated in the PCEF and in the TDF, if applicable, and ensure that the PCEF user plane traffic mapping and treatment is in accordance with the user's subscription profile.

If Gxx applies, the PCRF shall provide QoS rules with identical service data flow templates as provided to the PCEF in the PCC rules. If the service data flow is tunneled at the Bearer Binding and Event Reporting Function (BBERF), then the PCRF shall provide the BBERF with information received from the PCEF to enable the service data flow detection in the mobility tunnel at the BBERF. In some cases, the PCRF may also provide to the BBERF the charging ID information received from the PCEF. If IP flow mobility, as specified in TS 23.261 [7] applies, the PCRF shall, based on IP flow mobility routing rules received from the PCEF, and provide the authorized QoS rules to the applicable BBERF.

The PCRF should derive for an IP-CAN session, from IP-CAN specific restrictions, operator policy and SPR data, the list of permitted QoS class identifiers and associated GBR and MBR limits for the IP-CAN session.

The PCRF may check that the service information provided by the AF is consistent with both, the operator defined policy rules, and the related subscription information as received from the SPR during IP-CAN session establishment, before storing the service information. The service information shall be used to derive the QoS for the service. The PCRF may reject the request received from the AF when the service information is not consistent with either the related subscription information or the operator defined policy rules and as a result the PCRF shall indicate that this service information is not covered by the subscription information, or by operator defined policy rules and may indicate, in the response to the AF, the service information that can be accepted by the PCRF; e.g., the acceptable bandwidth. In the absence of other policy control mechanisms outside the scope of PCC, it is recommended that the PCRF include this information in the response.

In the current Release, the PCRF supports only a single Rx reference point (between H-PCRF and P-CSCF); i.e., there is one AF for each AF session.

The PCRF authorizes QoS resources. It uses the service information received from the AF; e.g., SDP information or other available application information, and/or the subscription information received from the SPR to calculate the proper QoS authorization (QoS class identifier, bitrates). The PCRF may also take into account the requested QoS received from the PCEF via the Gx interface.

NOTE 1: The PCRF provides always the maximum values for the authorized QoS even if the requested QoS is lower than what can be authorized.

The Authorization of QoS resources shall be based on complete service information unless the PCRF is required to perform the authorization of QoS resources based on incomplete service information. The PCRF shall, after receiving the complete service information, update the affected PCC rules accordingly.

The PCRF may use the subscription information as basis for policy and charging control decisions. The subscription information may apply for both session based and non-session based services.

The PCRF determines whether a Gx session from the PCEF is to be linked with a Gateway Control Session from the BBERF by matching the IPv4 address and/or IPv6 network prefix and

conditionally the MUE Identity, PDN Connection ID, and PDN ID towards open Gateway Control Sessions. When IP flow mobility as specified in TS 23.261, see Ref. [7] applies, one Gx session may be linked with multiple Gateway Control Sessions.

If the BBERF does not provide any PDN ID at the Gateway Control Session Establishment, then the PCRF maintains Gateway Control Session to Gx session linking to the Gx sessions where the assigned Care of Address) CoA and MUE Identity, if available over the Gxx reference point are equal. The PCRF and BBERF shall be capable of separating information for each IP-CAN session within the common Gateway Control Session.

If the BBERF provides a PDN ID at the Gateway Control Session Establishment, then the PCRF maintains Gateway Control Session to Gx session linking where the MUE identity and PDN ID are equal. If the BBERF provides a PDN ID at Gateway Control Session establishment, it may also indicate in the Gateway Control Session establishment that the PCRF shall not attempt linking the new Gateway Control Session with an existing Gx session immediately. If the PCRF receives such an indication, it keeps the new Gateway Control Session pending and defers linking until an IP-CAN session establishment or an IP-CAN session modification with matching MUE Identity, PDN ID and IP-CAN type arrives via Gx.

If the BBERF provides a PDN ID and a PDN Connection ID at the Gateway Control Session establishment, then the PCRF maintains Gateway Control Session to Gx session linking where the MUE identity, PDN Connection ID and PDN ID are equal.

When a BBERF establishes multiple Gateway Control Sessions for the same PDN ID and the IP-CAN type changes, the PCRF assumes that this constitutes inter-system BBERF relocations of existing Gateway Control Sessions. The BBERF may supply MUE IPv4 address and/or IPv6 network prefix, if known, which can be used for linking the new Gateway Control Session to the existing Gx session. If the MUE IPv4 address and/or IPv6 network prefix is/are not provided in the new Gateway Control Session establishment, the PCRF shall defer the linking with existing Gx session until receiving an IP-CAN Session modification with matching MUE Identity, IP-CAN type, PDN Connection ID, and PDN ID.

The PCRF determines which case applies.

If an AF requests the PCRF to report on the signalling path status, for the AF session, the PCRF shall, upon indication of loss of resources from the PCEF, for PCC rules corresponding to the signalling traffic notify the AF on changes to the signalling path status. The PCRF needs to have the knowledge of which PCC rules identify signalling traffic.

Negotiation of IP-CAN bearer establishment mode takes place via Gx for IP-CANs. For non-3GPP IP-CANs specified in TS 23.402 [5] negotiation of bearer establishment mode takes place via Gx when GPRS Tunneling Protocol (GTP) is used and via Gxx for the rest of the cases. For other accesses supporting multiple IP-CAN bearer establishment modes, if Gxx applies, the negotiation takes place via Gxx, otherwise via Gx. To support the different IP-CAN bearer establishment modes (UE-only or UE/NW) the PCRF shall:

- set the IP-CAN bearer establishment mode for the IP-CAN session based on operator configuration, network and MUE capabilities
- if the bearer establishment mode is UE/NW, decide what mode (UE or NW) shall apply for a PCC rule and resolve race conditions between UE-initiated requests and NW-initiated requests

  NOTE 2: For an operator-controlled service, the MUE and the PCRF may be provisioned with information indicating which mode is to be used.

- may reject a MUE request that is already served by a NW-initiated procedure in progress. When rejecting a MUE-initiated request by sending a reject indication, the PCRF shall use an appropriate cause value which shall be delivered to the MUE

  NOTE 3: This situation may occur if the PCRF has already triggered a NW-initiated procedure that corresponds to the MUE request.
- guarantee the precedence of dynamic PCC rules for network controlled services in the service data flow detection process at the PCEF by setting the PCC rule precedence information to appropriate values

If an AF requests the PCRF to report on the change of type of IP-CAN, the PCRF shall provide to the AF the information about the IP-CAN type that the user is currently using and upon indication of change of IP-CAN type, notify the AF on changes of the type of IP-CAN. In the case of 3GPP IP-CAN, the information of the Radio Access Technology Type; e.g., UTRAN, shall be also reported to the AF. If IP flow mobility as specified in TS 23.261 [7] applies, the PCRF shall provide to the AF the IP-CAN type information about the IP-CAN type that the service data flow currently transports within and upon indication of change of IP-CAN type, notify the AF on changes of the type of IP-CAN. In the case of 3GPP IP-CAN, the information of the Radio Access Technology Type; e.g., UTRAN, shall be also reported to the AF. When IP flow mobility is allowed within the same IP-CAN session, the PCRF shall only report the IP-CAN type change when the IP flow mobility applies to the service information provided by the AF.

If an AF requests the PCRF to report Access Network Information, the PCRF shall set the Access Network Information report parameters in the corresponding PCC rules or QoS rules and provision them together with the corresponding event trigger to the PCEF or BBERF. The PCRF shall, upon receiving an Access Network Information report corresponding to the AF session from the PCEF or BBERF, forward the Access Network Information as requested by the AF.

If an AF requests the PCRF to report Access Network Charging Correlation Information, the PCRF shall provide to the AF the Access Network Charging Correlation Information, which will identify the usage reports that include measurement for the flows, once the Access Network Charging Correlation Information is known at the PCRF. If not known in advance, the PCRF subscribes for the Access Network Charging Correlation Information event for the applicable PCC rule(s).

If Gxx applies together with the PCEF provided information about the required event triggers, the PCRF shall provide these event triggers to the BBERF and notify the PCEF of the outcome of the provisioning procedure by using the PCRF initiated IP-CAN Session Modification procedure. The PCRF shall include the parameter values received in the response from the BBERF in the notification to the PCEF. When multiple BBERFs exist; e.g., in IP flow mobility case, the PCEF may subscribe to different or common set of event triggers at different BBERFs; when the PCRF receives event notification from any BBERF, the PCRF shall include both the parameters values received from the BBERF and also the information for identifying the BBERF in the notification to the PCEF.

If Sd (reference point between the PCRF and the TDF) applies and the Traffic Detection Function (TDF) provided information about required event triggers, the PCRF shall provide these event triggers to the PCEF or BBERF; if Gxx applies, and notify the TDF of the outcome of the provisioning procedure within the PCEF initiated IP-CAN Session Modification procedure. The PCRF shall include the parameter values, received in the response from the PCEF/BBERF, in the notification to the TDF.

The relevant Event Triggers are: PLMN change, Location change, Change in type of IP-CAN, RAT type change, SGSN change, and Serving GW change.

NOTE 4: For IP flow mobility feature enabled, the TDF does not have accurate information about the location and the type of RAT where the user is to be attached.

When the PCRF gets an event report from the BBERF that is required by the PCEF, the PCRF shall forward this event report to the PCEF.

When the PCRF gets an Event Report from the PCEF/BBERF that is required by the TDF, the PCRF shall forward this Event Report to the TDF.

The PCRF may support usage monitoring control. The Usage is defined as volume of traffic in the user plane.

The PCRF may receive information about total allowed usage per PDN and MUE from the SPR; i.e., the overall amount of allowed resources, traffic volume, that are to be monitored for the PDN connections of a user. In addition, information about total allowed usage for Monitoring key(s) per PDN and MUE may also be received from the SPR.

The PCRF may authorise an application service provider to request specific PCC decisions; e.g., authorisation to request sponsored IP flows, or authorisation to request QoS resources.

For the purpose of usage monitoring control, the PCRF shall request the Usage report trigger and provide the necessary usage threshold(s) upon which the requested node (PCEF or TDF) shall report to the PCRF. The PCRF shall decide if and when to activate usage monitoring to the PCEF and TDF.

The PCRF may provide a Monitoring time to the PCEF/TDF for the Monitoring keys(s). When the Monitoring time occurs, the accumulated volume usage shall be recorded by the PCEF/TDF and the usage threshold shall be re-applied. The PCEF/TDF can send the report at a later time as triggered by the events. This report shall be split by the PCEF/TDF to indicate the volume usage up to the Monitoring time and volume usage after the Monitoring time.

It shall be possible for the PCRF to request a usage report from the requested node (PCEF or TDF) containing the accumulated volume usage since the time of the last usage report.

NOTE 5: The PCRF ensures that the number of requests and subsequent policy decisions provided over Gx/Sd reference points do not cause excessive signalling load, for instance, by assigning the same time for the report only for a preconfigured number of IP-CAN/TDF sessions.

Once the PCRF receives a usage report from the requested node (PCEF or TDF) the PCRF shall deduct the value of the usage report from the totally allowed usage for that PDN and MUE (in case usage per IP-CAN session is reported). If usage is reported from the TDF or the PCEF, the PCRF shall deduct the value of the usage report from the totally allowed usage for individual Monitoring key(s) for that PDN and MUE (in case the usage for one or several Monitoring keys is reported).

NOTE 6: The PCRF maintains usage thresholds for each Monitoring key and IP-CAN session that is active for a certain PDN and UE. Updating the total allowanced usage after the PCEF reporting, minimizes the risk of exceeding the usage allowance.

If the PCEF or TDF reports usage for a certain Monitoring key and if monitoring shall continue for that Monitoring key, then the PCRF shall provide new threshold values in the response to the PCEF or TDF respectively.

If monitoring shall no longer continue for that Monitoring key, then the PCRF shall not provide a new threshold in the response to the PCEF or TDF.

NOTE 7: If the PCRF decides to deactivate all PCC rules or ADC rules associated with a certain Monitoring key, then the conditions for continued Monitoring will no longer be fulfilled for that Monitoring key.

If all IP-CAN session of a user to the same APN is terminated, the PCRF shall store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the SPR.

For sponsored data connectivity, the PCRF may receive a usage threshold from the AF.

If the AF specifies a usage threshold, the PCRF shall use the Sponsor Identity to construct a Monitoring key for monitoring the volume of user plane traffic, and invoke usage monitoring on the

PCEF. The PCRF shall notify the AF when the PCEF reports that a usage threshold for the Monitoring key is reached, provided that the AF requests to be notified for this event. If the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold to the PCRF. Alternatively, the AF may allow the session to continue without specifying a usage threshold. If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the PCEF shall be discontinued for that monitoring key by the PCRF, unless there are other reasons for continuing the monitoring.

If the AF revokes the service information and the AF has notified previously a usage threshold to the PCRF, the PCRF shall report the usage up to the time of the revocation of service authorization.

If the IP-CAN session terminates and the AF has specified a usage threshold then the PCRF shall notify the AF of the consumed volume of user plane traffic since the last usage report.

The PCRF performs authorizations based on sponsored data connectivity profiles stored in the SPR. If the AF is in the operator's network and is based on the OSA/Parlay-X GW, the PCRF is not required to verify that a trust relationship exists between the operator and the sponsors.

If the H-PCRF detects that the MUE is accessing the sponsored data connectivity in the roaming scenario with home routed access, it may allow the sponsored data connectivity in the service authorization request, reject the service authorization request, or initiate the AF session termination based on home operator policy.

NOTE 8: Sponsored data connectivity is not supported in the roaming with visited access scenario in 3GPP Release 11.

For the solicited application reporting, it is PCRF's responsibility to coordinate the PCC rules and QoS rules, if applicable, with ADC rules in order to ensure consistent service delivery.

The PCRF uses the information relating to subscriber spending available in the Online Charging System (OCS) as input for policy decisions related to for instance QoS control, gating, or charging conditions.

4.15.4 Application Function (AF)

The Application Function (AF) is an element offering applications that require dynamic policy and/or charging control over the IP Connectivity Access Network (IP-CAN) user plane behavior, see Ref. [4]. The AF shall communicate with the Policy and Charging Rules Function (PCRF) to transfer dynamic session information, required for PCRF decisions as well as to receive IP-CAN specific information and notifications about IP-CAN bearer level events. One example of an AF is the Proxy-Call Session Control Function (P-CSCF) of IMS.

The AF may receive an indication that the service information is not accepted by the PCRF together with service information that the PCRF would accept. In that case, the AF rejects the service establishment towards the UE. If possible the AF forwards the service information to the MUE that the PCRF would accept. In the multi-connection architecture this feature has an extended value since decisions could be taken to choose the best access network available.

An AF may communicate with multiple PCRFs. The AF shall contact the appropriate PCRF based on either:

- the end user IP Address, and/or
- a MUE identity that the AF is aware of

NOTE 1: By using the end user IP address, an AF is not required to acquire any MUE identity in order to provide information to the PCRF for a specific user.

In case of private IP address being used for the end user, the AF may send additional PDN information; e.g., PDN ID over the Rx interface. This PDN information is used by the PCRF for session binding, and it is also used to help selecting the correct PCRF.

For certain events related to policy control, the AF shall be able to give instructions to the PCRF to act on its own; i.e., based on the service information currently available.

The AF may use the IP-CAN bearer level information in the AF session signalling or to adjust the IP-CAN bearer level event reporting.

The AF may request the PCRF to report on IP-CAN bearer level events; e.g., the signalling path status for the AF session. The AF shall cancel the request when the AF ceases communication with the user.

NOTE 2: The QoS authorization based on incomplete service information is required for instance at IMS session setup scenarios with available resources on the originating side and requirements for resource reservation at the terminating side.

The AF may request the PCRF to report on the change of type of IP-CAN. In the case of 3GPP IP-CAN, the information of the Radio Access Technology Type; e.g., UTRAN and the change thereof shall be also reported to the AF, even if the IP-CAN type is unchanged.

The AF may request the PCRF to report any combination of the user location and/or MUE Timezone at AF session establishment, modification, or termination.

NOTE 3: The H-PCRF informs the AF of event triggers that cannot be reported.

To support sponsored data connectivity, the AF may provide to the PCRF with the sponsored data connectivity information, including optionally a usage threshold. The AF may request the PCRF to report events related to sponsored data connectivity.

If the user plane traffic traverses the AF, the AF may handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCRF as part of the sponsored data connectivity information.

4.15.5 IP-CAN Session Modification – GW (PCEF) Initiated

In the following, a description of the signalling flow for the IP-CAN Session modification initiated by the GW(PCEF) is provided, see Ref. [4]. These modifications include IP-CAN bearer establishment and termination as well as modification if the triggering conditions given to the PCEF are fulfilled.

For the PCEF enhanced with Application Detection and Control (ADC), the reason for such a modification may be that a start or stop of application traffic that matches with one of the activated ADC Rules is detected.

The AF may be involved. For instance in the scenario where authorization of a session-based service for which an IP-CAN Session is also modified.

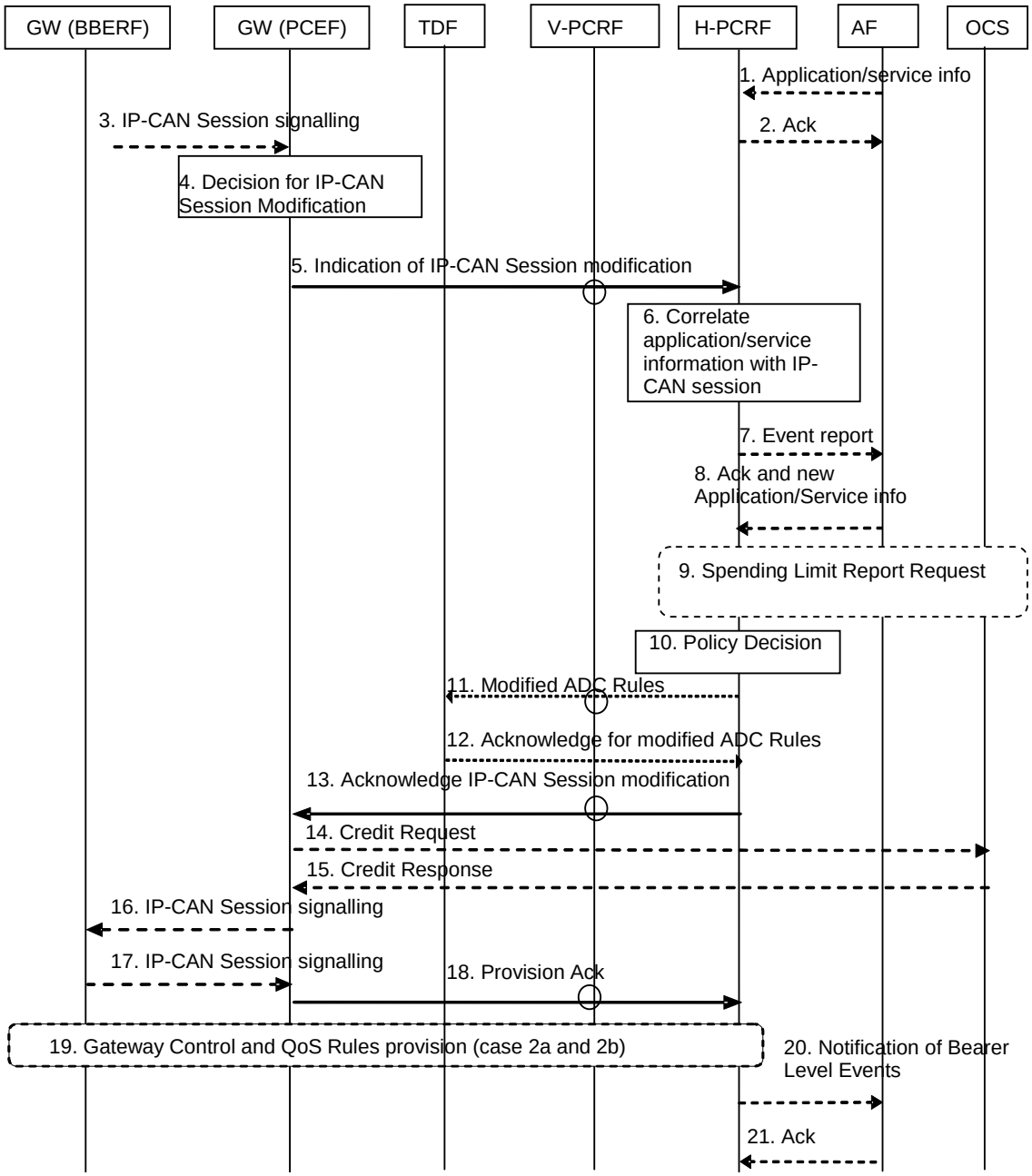

Figure 7 IP-CAN Session Modification – GW (PCEF) Initiated [4]

This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access applies or if case for Local Breakout applies, when a Gateway Control Session is used, the H-PCRF may initiate a Gateway Control and QoS Rules Provisioning procedure towards the BBERF and proxy the information through the V-PCRF over reference point S9.

For the Local Breakout scenario and if the Gateway Control Session is terminated locally at the V-PCRF, the V-PCRF shall initiate the Gateway Control and QoS Rules Provisioning procedure locally without notifying the H-PCRF. For this case the V-PCRF shall proxy the Indication and Acknowledge of IP-CAN Session Modification over S9 between the PCEF in the VPLMN and the H-PCRF. If the AF is located in the VPLMN for this scenario, the V-PCRF shall proxy AF session signalling over S9 between the AF and the H-PCRF.

NOTE 1: The case when the AF resides in the VPLMN is not shown in the Figure.

In the non-roaming case, the V-PCRF is not involved at all.

1. Optionally, the AF provides/revokes service information to the PCRF due to AF session signalling. The AF may subscribe at this point to notification of bearer level events related to the service information.

NOTE 2: For the PCRF to generate the applicable events, the PCRF instructs the PCEF to report events related to the corresponding PCC rules. Such events are not shown in this sequence diagram.

2. The PCRF stores the service information and responds with the Acknowledgement to the AF.

3. The GW (PCEF) may receive IP-CAN session signalling for IP-CAN Session modification. PDN Connection Identifier may be included in the IP-CAN session signalling.

4. The GW (PCEF) makes a decision to trigger IP-CAN Session modification either caused by the previous step or based on an internal decision or, for instance if the GW (PCEF) enhanced with ADC, has detected the start/stop of application traffic, requested by one of the activated ADC Rules.

5. The GW (PCEF) determines that the PCC interaction is required and sends an Indication of IP-CAN Session modification (Event Report, affected PCC Rules, if available, the PDN Connection Identifier) to the PCRF and, if changed, the new IP-CAN bearer establishment modes supported. If there is a limitation or termination of the transmission resources for a PCC Rule, the GW (PCEF) reports this to the PCRF. If flow mobility applies, the GW (PCEF) may include updated IP flow mobility routing information for any IP flows; the GW (PCEF) also provides an indication if default route for the IP-CAN session is changed.

6. The PCRF correlates the request for PCC Rules with the IP-CAN session and service information available at the GW (PCEF).

7. The PCRF may need to report to the AF an event related to the transmission resources, if the AF requested it at initial authorisation.

8. The AF acknowledges the event report and/or responds with the requested information.

9. If the PCRF determines a change to policy counter status reporting is required, it may alter the subscribed list of policy counters using the Initial, Intermediate or Final Spending Limit Report Request procedures.

10. The PCRF makes the authorization and policy decision.

11. For the TDF solicited application reporting, the steps 11-12 take place. The PCRF provides all new ADC decisions to the TDF. This may include ADC Rules activation, deactivation and modification. This may also include the list of Event triggers and also Event Report for the Event triggers, if reported by the PCEF/BBERF to the PCRF, if the TDF has previously subscribed for such an Event Report. In case of local breakout, the V-PCRF shall provide ADC rules as instructed by the H-PCRF over the S9 reference point.

12. The TDF sends an Ack (accept or reject of the ADC rule operation(s)) to inform the PCRF about the outcome of the actions related to the decision(s) received in step 11. The Ack may also include the list of Event Triggers to report. The Event Triggers indicate to the PCRF what events to be forwarded from the PCRF to the TDF, once PCRF gets the corresponding Event Report from the PCEF/BBERF.

13. The PCRF sends an Acknowledge of IP-CAN Session modification (PCC Rules, Event Triggers and, if changed, the chosen IP-CAN bearer establishment mode) to the GW (PCEF). The GW (PCEF) enforces the decision. The PCRF may also provide all new ADC decisions to the PCEF, enhanced with ADC. If the TDF provided a list of Event Triggers to the PCRF in the previous step, the PCRF shall also provide those Event Triggers to the PCEF.

14. If online charging is applicable, the GW (PCEF) may request credit for new charging keys from and/or shall issue final reports and return remaining credit for charging keys no longer active to the OCS.

15. If OCS was contacted, the OCS provides the credit information to the GW (PCEF), and/or acknowledges the credit report.

16. The GW (PCEF) acknowledges or rejects any IP-CAN Session signalling received in step 3.

    An IP-CAN bearer establishment is accepted if at least one PCC rule is active for the IP-CAN bearer and in case that: online charging credit was not denied by the OCS. Otherwise, the IP-CAN bearer establishment is rejected.

    An IP-CAN bearer termination is always acknowledged by the GW (PCEF).

    An IP-CAN bearer modification not upgrading the QoS and not providing traffic mapping information is always acknowledged by the GW (PCEF). An IP-CAN bearer modification is accepted if the provided traffic mapping information is accepted by the PCRF. Otherwise, the IP-CAN bearer modification is rejected.

    In case of a GW (PCEF) internal decision the GW (PCEF) initiates any additional IP-CAN Session signalling required for completion of the IP-CAN Session modification.

    In case the IP-CAN session modification is due to the BBF transitioning from a BBERF in the source access-network to the PCEF, the PCEF initiates IP-CAN bearer signalling to activate bearers in the target access network.

17. The GW (PCEF) receives the response for the IP-CAN Session signalling request.

18. The GW (PCEF) sends a Provision Ack (accept or reject of the PCC rule operation(s)) to inform the PCRF about the outcome of the GW (PCEF) actions related to the decision(s) received in step 13.

19. Based on the result of PCC rule operations, the PCRF decides whether to initiate a Gateway Control and QoS Rules provision procedure, if required to keep the PCC and QoS rules aligned.

    If there are multiple BBERFs associated with the IP-CAN session, this step is performed with all the affected BBERFs.

20. If the AF requested it, the PCRF notifies the AF of related bearer level events; e.g., transmission resources are established/released/lost.

NOTE 4: Based on the outcome reported in this step the AF performs the appropriate action; e.g., starting charging or terminating the AF session.

21. The AF acknowledges the notification from the PCRF.

4.15.6 IP-CAN Session Modification - PCRF Initiated

In the following, a description of the signalling flow for the IP Connectivity Access Network (IP-CAN) Session modification initiated by the Policy and Charging Rules Function (PCRF) is treated, see Ref. [4]. The Application Function (AF), or Traffic Detection Function (TDF), or the OCS may be involved. An example of PCRF inputs that may trigger the procedure include:

- Initiation and authorization of a session-based service for which an IP-CAN Session is modified

- A change in the status of a policy counter

IP-CAN Session handling and handling of Policy and Charging Control (PCC) rules for non-session based services, and also general handling of PCC rules that are not subject to AF-interaction or TDF-interaction is also applicable here.

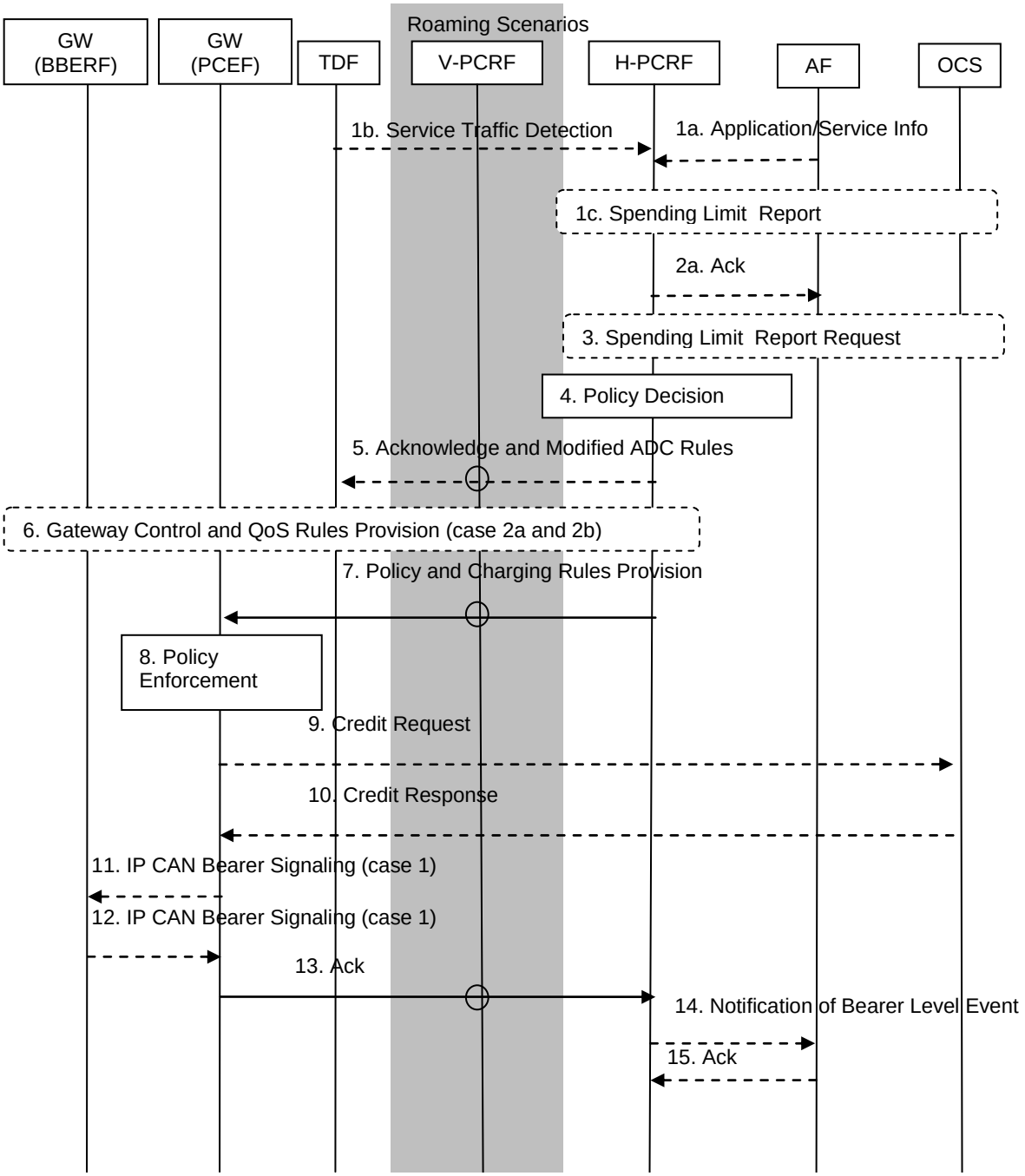

Figure 8 IP-CAN Session Modification; PCRF Initiated [4]

This procedure concerns both roaming and non-roaming scenarios. In the roaming case when home routed access applies or if case Local Breakout, when a Gateway Control Session is used, the Visited-PCRF (V-PCRF) shall proxy Gateway Control and QoS Rules Request between the Bearer Binding and Event Reporting Function (BBERF) in the VPLMN and the Home-PCRF (H-PCRF) over the S9 reference point. For this case the H-PCRF may also initiate a Gateway Control and QoS Rules Provisioning procedure towards the BBERF in the VPLMN and proxy the information via the V-PCRF over the S9 reference point.

For the Local Breakout scenario and if the Gateway Control Session is terminated locally at the V-PCRF, the V-PCRF shall reply to/initiate Gateway Control Session and QoS Rules

Request/Provisioning procedures locally without notifying the H-PCRF. For this case the V-PCRF shall proxy the Policy and Charging Rules Provisioning and Acknowledge over the S9 reference point between the PCEF in the VPLMN and the H-PCRF. If the AF is located in the VPLMN for this scenario, the V-PCRF shall proxy AF session signalling over the S9 reference point between the AF and the H-PCRF.

NOTE 1: The case when the AF resides in the VPLMN is not showed in the Figure.

In the non-roaming case the V-PCRF is not involved at all.

1a. Optionally, the AF provides/revokes service information to the PCRF due to AF session signalling. The AF may subscribe at this point to notification of bearer level events related to the service information.

NOTE 2: For the PCRF to generate the applicable events, the PCRF instructs the PCEF to report events related to the corresponding PCC rules. Such events are not shown in this sequence diagram.

1b. Alternatively, optionally, for TDF, e.g. the TDF detects the start/stop of an application traffic that matches with one of the activated ADC Rules. Then, in case of solicited application reporting, for the start of traffic detection, in case the enforcement actions were provided as a part of ADC rules, the TDF shall enforce those actions.

For the solicited application reporting, if the start/stop of application traffic detection Event Trigger was received from PCRF, the TDF shall provide application information to the PCRF, including the Application Identifier, start or stop of application traffic detection event trigger and, for the start of application's traffic detection, the service flow data descriptions, if deducible. Additionally, the application instance identifier should be included in the report both for Start and for Stop of application traffic detection, when the service data flow descriptions are provided.

For the unsolicited application reporting, the TDF shall provide application information to the PCRF, including the Application Identifier and the service data flow descriptions, if deducible.

1c. Alternatively, optionally, the OCS provides a Spending Limit Report to the PCRF.

2a. The PCRF stores the service information if available and responds with the Acknowledgement to the AF. This is applicable to case (1a).

NOTE 3: Without AF interaction, a trigger event in the PCRF may cause the PCRF to determine that the PCC rules require updating at the PCEF; e.g., change to configured policy.

NOTE 4: This procedure could also be triggered by the Gateway Control and QoS Rules Request procedure.

3. If the PCRF determines a change to policy counter status reporting is required, it may alter the subscribed list of policy counters using the Initial, Intermediate or Final Spending Limit Report Request procedures.

4. The PCRF makes the authorization and policy decision.

5. The PCRF may store the application information if available and responds with the Acknowledgement to the TDF (applicable for solicited service reporting as described in case 1b). For the TDF solicited application reporting, the PCRF may provide a new ADC decisions to the TDF within this acknowledge. This may include ADC Rules activation, deactivation and modification. This may also include the list of relevant Event Triggers, according to Table 1, Event Triggers [4], below. If the last ADC rule is deactivated, the PCRF requests the TDF to terminate the TDF session toward the PCRF. If there is no active TDF session between the TDF and the PCRF, the PCRF requests the TDF to establish the TDF session towards PCRF and provides Application Detection and Control Rules and Event Triggers to

the TDF. In case of local breakout, the V-PCRF shall provide ADC rules as instructed by the H-PCRF over the S9 reference point.

5a. If requested by PCRF, the TDF sends a Provision Ack (accept or reject of the ADC Rule operation(s)) to inform the PCRF about the outcome of the actions related to the decision(s) received in step 5. The Provision Ack may also include the list of Event Triggers to report. The Event Triggers indicate to the PCRF what events to be forwarded from the PCRF to the TDF, once PCRF gets the corresponding Event Report from the PCEF/BBERF.

6. If there is no Gateway Control and QoS Rules Reply pending and there is a need to provision QoS rules, the PCRF initiates a Gateway Control and QoS Rules Provision Procedure; applicable for cases 2a and 2b.

   If there are multiple BBERFs associated with the IP-CAN session, Step 5 is performed with the BBERFs that support UE/NW bearer establishment mode.

NOTE 5: If there is a Gateway Control and QoS Rules Reply pending, e.g. this procedure was invoked from the Gateway Control and QoS Rules Request procedure, the PCRF shall use that opportunity for provisioning the applicable QoS rules. If there are multiple BBERFs associated with the IP-CAN session, and the procedure was invoked by a Gateway Control and QoS Rules Request procedure from the primary BBERF, the PCRF may receive a Gateway Control and QoS Rules Request from the non-primary BBERFs.

7. The PCRF sends the Policy and Charging Rules Provision (PCC Rules, Event Trigger, Event Report) to the PCEF. The PCRF may also provide all new ADC decisions to the PCEF, enhanced with ADC. If the TDF provided a list of Event Triggers to the PCRF in the previous step, the PCRF shall also provide those Event Triggers to the PCEF.

8. The PCEF enforces the decision.

9. If online charging is applicable, the PCEF may request credit for new charging keys from and/or shall return the remaining credit for charging keys no longer active to the OCS.

10. If OCS was involved, the OCS provides the credit information to the PCEF, and/or acknowledges the credit report.

11. The GW (PCEF) may send an IP-CAN Bearer establishment, modification or termination request (applicable for case 1).

    An IP-CAN bearer modification is sent by the GW (PCEF) if the QoS of the IP-CAN bearer exceeds the authorized QoS provided by the PCRF in step 4.

    An IP-CAN bearer termination request is sent by the GW (PCEF) if all PCC rules for an IP-CAN bearer have been removed.

12. The GW (PCEF) receives the response for the IP-CAN Bearer modification or termination request (applicable for case 1).

13. The PCEF sends Acknowledge Policy and Charging Rules Provisioning (accept or reject of the PCC rule operation(s)) to the PCRF.

14. If the AF requested it, the PCRF notifies the AF related bearer level events; e.g., transmission resources are established, released, or lost.

15. The AF acknowledges the notification from the PCRF.

Table 1 Event triggers [4]

Event trigger	Description	Reported from	Condition for reporting
PLMN change	The UE has moved to another operators' domain.	PCEF	PCRF
QoS change	The QoS of the IP-CAN bearer has changed (note 3).	PCEF, BBERF	PCRF
QoS change exceeding authorization	The QoS of the IP-CAN bearer has changed and exceeds the authorized QoS (note 3).	PCEF	PCRF
Traffic mapping information change	The traffic mapping information of the IP-CAN bearer has changed (note 3).	PCEF	Always set
Resource modification request	A request for resource modification has been received by the BBERF/PCEF (note 6).	PCEF, BBERF	Always set
Routing information change	The IP flow mobility routing information has changed	PCEF	Always set if IP flow mobility is supported
Change in type of IP-CAN (see note 1)	The access type of the IP-CAN bearer has changed.	PCEF	PCRF
Loss/recovery of transmission resources	The IP-CAN transmission resources are no longer usable/again usable.	PCEF, BBERF	PCRF
Location change (serving cell) (see note 10)	The serving cell of the UE has changed.	PCEF, BBERF	PCRF
Location change (serving area) (see notes 4 and 10)	The serving area of the UE has changed.	PCEF, BBERF	PCRF
Location change (serving CN node) (see notes 5 and 10)	The serving core network node of the UE has changed.	PCEF, BBERF	PCRF
Out of credit	Credit is no longer available.	PCEF	PCRF
Enforced PCC rule request	PCEF is performing a PCC rules request as instructed by the PCRF.	PCEF	PCRF
Enforced ADC rule request	PCEF/TDF is performing an ADC rules request as instructed by the PCRF.	PCEF, TDF	PCRF
UE IP address change (see note 9)	A UE IP address has been allocated/released	PCEF	Always set
Access Network Charging Correlation Information	Access Network Charging Correlation Information has been assigned.	PCEF	PCRF
Usage report (see note 7)	The IP-CAN session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	PCEF, TDF	PCRF
Start of application traffic detection and Stop of application traffic detection (see note 8)	The start or the stop of application traffic has been detected.	PCEF, TDF	PCRF
SRVCC CS to PS handover	A CS to PS handover has been detected	PCEF	PCRF
Access Network Information report	Access information as specified in the Access Network Information Reporting part of a PCC rule.	PCEF, BBERF	PCRF

NOTE 1: This list is not exhaustive. Events specific for each IP-CAN are specified in clause A.
NOTE 2: A change in the type of IP-CAN may also result in a change in the PLMN.
NOTE 3: Available only when the bearer binding mechanism is allocated to the PCRF.
NOTE 4: A change in the serving area may also result in a change in the serving cell, and a change in the serving CN node.
NOTE 5: A change in the serving CN node may also result in a change in the serving cell, and possibly a change in the serving area.
NOTE 6: Available only when the IP-CAN supports corresponding procedures for bearer independent resource requests.
NOTE 7: Usage is defined as volume of user plane traffic.
NOTE 8: The start and stop of application traffic detection are separate event triggers, but received under the same subscription from PCRF.
NOTE 9: If TDF for solicited application reporting is applicable, upon receiving this event report from PCEF, PCRF always updates the TDF.
NOTE 10: Due to the potential increase in signalling load, it is recommended that such event trigger subscription is only applied for a limited number of subscribers.
NOTE 11: In this Table the term UE is used as opposed to MUE to keep compatibility with its original Reference [1].

4.16 Multi-connection User Profile Functional Entity (MUP-FE) - Enhancements and Alignment towards the Policy and Charging Control (PCC) Architecture

The Multi-connection User Profile Functional Entity contains and maintains all MUE subscription related information. It provides as well information to the Multi-connection Policy Control Functional Entity (MPC-FE) to further be able to make policy decisions. Likewise, it provides information to the Multi-connection Registration Functional Entity (MR-FE), so it can perform registration management.

In summary, MUP-FE communicates directly with the MR-FE through the Ru reference point, and the MPC-FE through the Pu reference point.

It is also responsible to provide responses to queries on users' profiles, which can be stored in one or more databases.

The MUP-FE provides at least the following items related to the subscribers:

1) User information, for instance subscriber's identifiers.
2) Allowed services.
3) Allowed QoS, such as bandwidth, priority, and others
4) Subscription and charging information.
5) Authentication and authorization information.
6) Location information.
7) Presence; e.g., online/offline status.
8) IP address.

The HSS in mobile networks, after Release 5, has a number of subscription information synchronized for consistency purposes with the PCC information elements. After the PCC model, MUP-FE shall pursue alignment to the following parameter input and usage behavior into other functions for decision purposes:

4.16.1 Input for PCC decisions

The Policy and Charging Rules Function (PCRF) shall accept input for PCC decision-making from the Policy and Charging Control Enforcement Function (PCEF), the Bearer Binding and Event Reporting Function (BBERF) if present, the Traffic Detection Function (TDF) if present, the Subscription Profile Repository (SPR) and if the Application Function (AF) is involved, from the AF, as well as the PCRF may use its own pre-defined information, see Ref. [4]. These different nodes should provide as much information as possible to the PCRF. At the same time, the information below describes examples of the information provided. Depending on the particular scenario all the information may not be available or is already provided to the PCRF.

The PCEF and/or BBERF may provide the following information:

- Subscriber Identifier
- IPv4 address of the UE
- IPv6 network prefix assigned to the UE
- IP flow routing information, if IP flow mobility is used

  NOTE 1: This information is provided only by the PCEF.
- IP-CAN bearer attributes
- Request type; i.e., initial, modification, and others

- Type of IP-CAN; e.g., GPRS, I-WLAN, and others

  NOTE 2: The Type of IP-CAN parameter should allow extension to include new types of accesses.
- Location of the subscriber

  NOTE 3: Alignment to 23.203 [4] for location information
- A PDN ID
- A PLMN identifier
- IP-CAN bearer establishment mode

The PCEF enhanced with Application Detection and Control (ADC) or the Traffic Detection Function (TDF) may provide the following information:

- Detected Application Identifier
- Allocated Application Instance Identifier
- Detected service data flow descriptions

  NOTE 4: Depending on the type of IP-CAN, the limited update rate for the location information at the PCEF may lead to a MUE moving outside the area indicated in the detailed location information without notifying the PCEF.

The SPR may provide the following information for a subscriber, connecting to a specific PDN:

- Subscriber's allowed services; i.e., list of Service IDs
- For each allowed service, a pre-emption priority
- Information on subscriber's allowed QoS, including:
  - the Subscribed Guaranteed Bandwidth QoS
  - a list of QoS class identifiers together with the Maximum Bitrate (MBR) limit and, for real-time QoS class identifiers, the Guaranteed Bitrate (GBR) limit
- Subscriber's charging related information
- Spending limits profile containing an indication that policy decisions depend on policy counters available at the Online Charging System (OCS) that has a spending limit associated with it and optionally the list of relevant policy counters
- Subscriber category
- Subscriber's usage monitoring related information
- Subscriber's profile configuration
- Sponsored data connectivity profiles
- Multimedia Priority Service (MPS) Evolved Packet System (EPS) Priority, MPS Priority Level, see TS 23.401 [13] for more detail on MPS Subscription
- IMS Signalling Priority

  NOTE 5: The MPS Priority Level represents user priority.

  NOTE 6: The MPS Priority Level is one among other input data such as operator policy for the PCRF to set the Address Resolution Protocol (ARP) value. The MPS EPS Priority, and MPS Priority Level are consistent with the corresponding parameters defined in the HSS.

The AF, if involved, may provide the following application session related information; e.g., based on SIP and Session Description Protocol (SDP):

- Subscriber Identifier
- IP address of the UE
- Media Type
- Media Format; e.g., media format sub-field of the media announcement and all other parameter information (a= lines) associated with the media format
- Bandwidth
- Sponsored data connectivity information, see TS 23.203 [4]
- Flow description; e.g., source and destination IP address and port numbers and the protocol
- AF Application Identifier
- AF Communication Service Identifier; e.g., IMS Communication Service Identifier and MUE identifier provided via AF
- AF Application Event Identifier
- AF Record Information
- Flow status, for gating decision
- Priority indicator, which may be used by the PCRF to guarantee service for an application session of a higher relative priority

  NOTE 7: The AF Priority information represents session/application priority and is separate from the MPS EPS Priority indicator.
- Emergency indicator
- Application service provider

  NOTE 8: The application service provider may be identified in numerous forms; e.g., the AF Application Identifier, or the host realm at Diameter level.

The OCS, if involved, may provide the following information for a subscriber:

- Policy counter status for each relevant policy counter

In addition, the pre-defined information in the PCRF may contain additional rules based on charging policies in the network, whether the subscriber is in its home network or roaming, depending on the IP-CAN bearer attributes.

The QoS Class Identifier, see TS 23.203 [4], in the PCC rule is derived by the PCRF from AF or SPR interaction if available. The input can be SDP information or other available application information, in line with operator policy.

The Allocation/Retention Priority in the PCC Rule is derived by the PCRF from AF or SPR interaction if available, in line with operator policy.

Additionally – in case of GPRS connectivity, the PCRF shall accept any of the following data provided by the PCEF, as a basis for decisions on PCC rule operations:

- Subscriber Identifier in the form of IMSI or MSISDN

- A Public data network (PDN) identifier in the form of an Access Point Name (APN)
- A PLMN identifier in the form of SGSN Mobile Country Code and Mobile Network Code
- Type of IP-CAN set to GPRS
- IP-CAN bearer attributes in the form of:
  - Requested QoS, for a PDP context
  - Traffic Flow Template (TFT), to enable the identification of the corresponding PDP Context
- Location of the subscriber in the form of Cell Global Identification (CGI)/Service Area Identity (SAI) or Routeing Area Identity (RAI)

As well as the *following parameters:*

- RAT type
- Subscribed APN- Aggregate Maximum Bit Rate (AMBR)
- Maximum Bit rate (MBR)/APN-AMBR

The Subscription Profile Repository (SPR) may provide the following information for a subscriber connecting to a specific PDN:

- Authorized APN-AMBR

The Authorized APN-AMBR is derived by the PCRF from SPR interaction, according to operator policy.

4.1.2 Subscription Information Management in the PCRF

The Policy and Charging Rules Function (PCRF) may request subscription information from the SPR for an IP-CAN session at establishment, or a gateway control session at establishment, see Ref. TS 23.203 [4]. The subscription information may include user profile configuration indicating whether application detection and control should be enabled. The PCRF should specify the subscriber ID and, if available, the PDN identifier in the request. The PCRF should retain the subscription information that is relevant for Policy and Charging Control (PCC) decisions until the IP-CAN session termination and the gateway control session termination.

The PCRF may request notifications from the SPR on changes in the subscription information. Upon reception of a notification, the PCRF shall make the PCC decisions necessary to accommodate the change in the subscription and update the PCEF, the BBERF, and the TDF by providing the new PCC/Application Detection and Control (ADC) decisions if needed. The PCRF shall send a cancellation notification request to the SPR when the related subscription information has been deleted.

4.16.3 Subscription Profile Repository (SPR)

The SPR logical entity contains all subscriber/subscription related information needed for subscription-based policies and IP-CAN bearer level PCC rules by the PCRF, see TS 23.203 [4].

NOTE 1: The SPR's relation to existing subscriber databases is not specified in this Release.

The SPR may provide the following subscription profile information; per PDN, identified by the PDN identifier:

- Subscriber's allowed services

- For each allowed service, a pre-emption priority
- Information on subscriber's allowed QoS, including the Subscribed Guaranteed Bandwidth QoS
- Subscriber's charging related information; e.g., location information relevant for charging
- Subscriber's User Closed Subscriber Group (CSG) Information reporting rules
- Subscriber category
- Subscriber's usage monitoring related information
- Multimedia Priority Service (MPS) Evolved Packet System (EPS) Priority and MPS Priority Level
- IMS Signalling Priority
- Subscriber's profile configuration indicating whether application detection and control should be enabled
- Spending limits profile containing an indication that policy decisions are based on policy counters available at Online Charging System (OCS) that has a spending limit associated with it and optionally the list of policy counters

The SPR may provide the following sponsored data connectivity profile information:

- A list of Application Service Providers and their applications per sponsor identity

NOTE 2: The sponsored data connectivity profile may be locally configured at the PCRF.

If the IMS Signalling Priority is set, it indicates that the IMS Signalling Bearer and the Default Bearer are assigned Address Resolution Protocol (ARP) appropriate for MPS at the time of the establishment of the PDN connection for IMS; i.e., EPS Attach or PDN Connectivity Request.

4.16.4 V-PCRF Functional Element in PCC

Likewise, in the visited network, the Visited-Policy and Charging Rules Function (V-PCRF) connected to the Home Policy and Charging Rules Function (H-PCRF) via the S9 reference point is a functional element that encompasses policy and charging control decision functionalities in the V-PLMN. In the multi-connection architecture a similar network element is required to be added into the functional architecture in order to cover roaming cases as well, following the PCC architecture.

The V-PCRF includes functionality for both home routed access and visited access - local breakout, see Figure 4 and TS 23.203 [4].

The V-PCRF determines based on the subscriber identity if a request is for a roaming user.

A Gateway Control Session request received over the Gxx reference point may trigger a request over the S9 reference point from the V-PCRF to the H-PCRF.

If a Gateway Control Session establishment request is received that can not be bound to an existing Gx session then the associated IP-CAN session is either home routed or it is visited access but the IP-CAN session establishment request has not yet been received over Gx.

For this case the V-PCRF may determine based on PDN-Id carried in the GW control session and roaming agreements if the request shall be proxied to the H-PCRF over S9 or not. The V-PCRF may choose not to proxy the Gateway Control Session Establishment only if the PDN-Id indicates the request is for visited access.

The Gateway Control Session Establishment request should only be proxied to the H-PCRF over S9 in case the V-PCRF is configured to do so, for instance based on roaming agreement.

NOTE: Proxying the Gateway Control Session Establishment makes the H-PCRF aware of the Gateway Control Session and enables binding in case a subsequent IP-CAN Session is established with home routed access or visited access.

If the V-PCRF determines that a Gateway Control Session Establishment shall be proxied to the H-PCRF over S9 then the reply from the H-PCRF shall also be communicated back to the GW (BBERF) over Gxx.

In case the V-PCRF determines that a Gateway Control Session Establishment request shall not be proxied, then the V-PCRF shall respond to the request made by the GW (BBERF) without notifying the H-PCRF.

If an IP-CAN session establishment request is received for a roaming user over the Gx reference point, then the V-PCRF shall conclude that the IP-CAN session use visited access, see TS 23.203 [4].

If a Gateway Control and QoS rules provision is received by the V-PCRF over the S9 reference point for a Gateway Control session which is not associated, at the V-PCRF, with an existing Gx session, the V-PCRF shall conclude that the IP-CAN session associated with the Gateway Control session is home routed, see TS 23.203 [4].

4.16.4 V-PCRF and Home Routed Access

Another case that may be considered for inclusion in the multi-connection functional architecture is the home routed access, after the PCC model.

The V-PCRF provides functions to proxy Gxx interactions between the BBERF and the H-PCRF as follows, see TS 23.203 [4]:

- Gateway Control Session establishment and termination
- Gateway Control and QoS Policy Rules Provision
- Gateway Control and QoS Rule Request

The V-PCRF provides functions to enforce visited operator policies regarding QoS authorization requested by the home operator as indicated by the roaming agreements. The V-PCRF informs the H-PCRF when a request has been denied and may provide the acceptable QoS Information.

Within an IP-CAN session, a different V-PCRF may be selected when a new Gateway Control Session is established.

4.16.5 V-PCRF and Visited Access (local breakout)

The Visited-Policy and Charging Rules Function (V-PCRF) needs also in principle a counterpart functional entity in the multi-connection architecture to provide for the following functions, see TS 23.203 [4]:

- Enforce visited operator policies regarding QoS authorization requested by the home operator; e.g., on a per QoS Class Identifier (QCI) or service basis as indicated by the roaming agreements. The V-PCRF informs the H-PCRF when a request has been denied and may provide the acceptable QoS Information for the service
- When Gxx interaction is terminated locally at the V-PCRF, perform Gx to Gateway Control Session linking
- When Gxx interaction is terminated locally at the V-PCRF, extract QoS rules [4] from PCC rules provided by the H-PCRF over the S9 reference point. The V-PCRF provides updated PCC rules to the PCEF and QoS rules to the BBERF, if appropriate
- For the case in which the Application Function (AF) is in the VPLMN:

- Proxy the Rx (by the P-CSCF) authorizations over the S9 reference point to the H-PCRF
- Relay event subscriptions and notifications between the H-PCRF and Visited Application Function (V-AF)

When Gx interactions are proxied between the PCEF and the H-PCRF, the V-PCRF proxies:

- Indication of IP-CAN Session Establishment and Termination
- Policy and Charging Rule Provisioning
- Application Detection and Control rules provisioning
- Request Policy and Charging Rules

If a Gateway Control Session is used, and if during the IP-CAN Session Establishment the Gateway Control Session Establishment procedure was proxied to the H-PCRF, see TS 23.203 [4], then the V-PCRF shall also proxy all other Gateway Control Session procedures to the H-PCRF.

If the Gateway Control Session was not proxied to the H-PCRF, then the V-PCRF shall handle all Gateway Control Session procedures locally and not proxy them to the H-PCRF. This has the following implications:

- An IP-CAN Session modification may trigger the V-PCRF to update the Gateway Control Session if required in order to maintain the alignment of PCC and QoS Rules
- An IP-CAN Session termination procedure may trigger the V-PCRF to terminate the Gateway Control Session if the Gateway Control Session was established for the purpose of a single IP-CAN session. Otherwise, a Gateway Control and QoS Rules Provision procedure may be initiated to remove the QoS Rules associated with the IP-CAN session
- On receiving a Gateway Control and QoS Rules Request message from the BBERF, the V-PCRF performs the procedure described in TS 23.203 [4] for the event reporting for PCEF in visited network and locally terminated Gxx interaction

  NOTE 1: The V-PCRF has to set the event triggers at the PCEF in a way that the PCEF triggers a PCEF initiated IP-CAN Session Modification Procedure if an interaction with the H-PCRF is required.

When Rx components are proxied between an AF in the VPLMN and the H-PCRF, the V-PCRF shall proxy service session information between the AF and the H-PCRF.

The V-PCRF shall provide Application Detection and Control (ADC) rules control as instructed by the H-PCRF over the S9 reference point. The V-PCRF shall provide updated ADC rules to the PCEF or Traffic Detection Function (TDF), as appropriate in the VPLMN configuration.

NOTE 2: There may be situations where the TDF is not able to detect the traffic requested by the H-PCRF. Prior agreements could be arranged to ensure that there is a common understanding of the meaning of Application Identifiers transferred between PLMNs.

The V-PCRF shall install the event triggers in the PCEF, in the TDF and in the Bearer Binding and Event Reporting Function (BBERF) previously provided for the IP-CAN session and install additional event triggers in the BBERF relevant only to the PCEF, such event triggers are typically set by the OCS or the TDF. On receiving an Event report from the PCEF/BBERF, the V-PCRF forwards it to the TDF, if TDF has previously subscribed for it.

NOTE 3: Event reports over Gxx relevant only to the PCEF will not trigger a PCEF initiated IP-CAN session modification procedure.

Within an IP-CAN session the same V-PCRF remains for the whole lifetime of the IP-CAN session.

4.16.6 H-PCRF Functional Element in PCC

In the home PLMN, the Home-Policy and Charging Rules Function (H-PCRF) connected to the:

1. Visited Policy and Charging Rules Function (V-PCRF), via the S9 reference point,
2. P-CSCF, in the IMS infrastructure, via the Rx reference point, and
3. P-GW (PCEF), via the Gx reference point

is a functional element that encompasses policy and charging control decision functionalities in the H-PLMN, see TS 23.203 [4]. In the multi-connection architecture a similar network element, is required to provide aligned functionality and capabilities following the PCC architecture.

The H-PCRF (Home-Policy and Charging Rules Function) is a functional element that encompasses policy and charging control decision functionalities in the H-PLMN and in the VPLMN. The H-PCRF includes functionality for both home routed access and visited access (local breakout).

If a Gateway Control Session is used and a Gateway Control Session Establishment is indicated over the S9 reference point, then one or more of the following cases applies:

1. One, or several, home routed IP-CAN sessions are known to the H-PCRF that can be bound to the Gateway Control session. For such IP-CAN sessions, the H-PCRF behaves as described in TS 23.203 [4].

2. No IP-CAN session is known to the H-PCRF that can be bound to the Gateway Control session. This is the case when an IP-CAN session establishment process has not yet been initiated over Gx or S9 reference points.

If an IP-CAN Session Establishment is received over the Gx reference point, then the H-PCRF shall conclude that the IP-CAN session is home routed and act as described in TS 23.203 [4].

If an IP-CAN Session Establishment is received over the S9 reference point, then the H-PCRF shall conclude that the IP-CAN session use visited access and act as described in TS 23.203 [4].

4.16.7 H-PCRF and Home Routed Access

The H-PCRF shall use the S9 reference point to proxy information to the Bearer Binding and Event Reporting Function (BBERF) via the V-PCRF for the following related Gxx procedures, see TS 23.203 [4]:

- Gateway Control Session establishment and termination

- Gateway Control and QoS Policy Rules Provision

- Gateway Control and QoS Rule Request

If an IP-CAN session termination is received over the Gx reference point, then the H-PCRF shall initiate a Gateway Control Session Termination procedure over the S9 reference point, if the Gateway Control Session was established for the purpose of a single IP-CAN session. Otherwise, a Gateway Control and QoS Rules Provision procedure may be initiated over the S9 reference point to remove the QoS Rules in the BBERF associated with the IP-CAN session.

4.16.8 H-PCRF and Visited Access (Local Breakout)

The H-PCRF shall use the S9 reference point to proxy information to the PCEF, and indirectly also to the BBERF when the Gateway Control Session is not proxied to the H-PCRF, and indirectly also to the TDF via the V-PCRF for the following related Gx procedures, see TS 23.203 [4]:

- Indication of IP-CAN Session Establishment and Termination messages

- Policy and Charging Rule Provisioning messages

- Application Detection and Control rules provisioning messages

- Request Policy and Charging Rules messages

When the Gateway Control Session is proxied to the H-PCRF, the H-PCRF shall use the S9 reference point to proxy information to the BBERF via the V PCRF for the following related Gxx procedures:

- Indication of Gateway Control Session Establishment and Termination messages
- QoS Rules Provisioning messages
- Request QoS Rules messages

For the application traffic detection, the H-PCRF shall provide Application Detection and Control (ADC) rule operations.

The H-PCRF should generate PCC rules for both cases when the AF is located in the VPLMN and when the AF is located in the HPLMN. The H-PCRF provides the PCC and ADC rules to the V-PCRF over the S9 reference point.

Additionally, recent enhancement, see Ref. [4], deal with the policy and charging control rule operations; and application detection and control rule operations as specified in the next two clauses.

4.16.9 Policy and Charging Control Rule Operations

Policy and charging control rule operations consist of activation, modification and de-activation of PCC rules.

Activation of a dynamic PCC rule provides the PCC rule information to the PCEF via the Gx reference point.

Activation of a predefined PCC rule provides an identifier of the relevant PCC rule to the PCEF via the Gx reference point.

Activation of a predefined PCC rule, not known in the PCRF, may be done by the PCEF based on operator policy. The PCEF may only activate such predefined PCC rule if there are no MUE provided traffic mapping information related to the IP-CAN bearer.

An active PCC rule means that:

- The service data flow template shall be used for service data flow detection
- The service data flow template shall be used for mapping of downlink packets to the IP-CAN bearer determined by the bearer binding
- The service data flow template shall be used for service data flow detection of uplink packets on the IP-CAN bearer determined by the bearer binding
- Usage data for the service data flow shall be recorded, further details can be found in topics for Reporting and Credit Management in Ref. [4]
- Policies associated with the PCC rule, if any, shall be invoked.

A predefined PCC rule is known at least, within the scope of one access point.

NOTE 1: The same predefined PCC rule can be activated for multiple IP-CAN bearers in multiple IP-CAN sessions.

A predefined PCC rule that contains downlink service data flow filters can only be activated once per IP-CAN session. A predefined PCC rule that contains only uplink service data flow filters can be activated for multiple IP-CAN bearers of the same IP-CAN session (deactivation of such a predefined PCC rule would remove this PCC rule from every IP-CAN bearer).

The PCRF may, at any time, modify an active/dynamic PCC rule.

The PCRF may, at any time, deactivate an active PCC rule in the PCEF via the Gx reference point. At IP-CAN bearer termination all active PCC rules on that bearer are deactivated without explicit instructions from the PCRF to do so.

Policy and charging control rule operations can be also performed in a deferred mode. A PCC rule may have either a single deferred activation time, or a single deferred deactivation time or both.

A PCC rule with only a deferred activation time shall be inactive until that time. A PCC rule with only a deferred deactivation time shall be active until that time. When the rule activation time occurs prior to the rule deactivation time, the rule is inactive until the activation and remains active until the deactivation time occurs. When the rule deactivation time occurs prior to the rule activation time, the rule is initially active until the deactivation time, then remains inactive until the activation time, and then becomes active again. An inactive PCC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCRF.

The PCRF may modify a currently installed PCC rule, including setting, modifying or clearing its deferred activation and/or deactivation time, see Ref. [4]. When modifying a dynamic PCC rule with a prior and/or new deferred activation and/or deactivation time, the PCRF shall provide all attributes of that rule, including attributes that have not changed.

NOTE 2: In this case, the PCRF omission of an attribute that has a prior value will erase that attribute from the rule.

Deferred activation and deactivation of PCC rules can only be used for PCC rules that belong to the IP-CAN bearer without traffic mapping information.

NOTE 3: This limitation prevents dependencies on the signalling of changed traffic mapping information towards the UE.

Deferred modification of PCC rules shall not be applied for changes of the QoS or service data flow filter information of PCC rules.

4.16.10 Application Detection and Control Rule Operations

Application Detection and Control rule operations apply for solicited reporting and consist of activation, modification and deactivation of ADC rules.

Activation: The PCRF provides the ADC Rule identifier to the PCEF enhanced with ADC or TDF. The PCRF may provide data for usage monitoring and enforcement control for a dynamic ADC rule.

An active ADC rule means that:

- The application traffic, matching the corresponding application, is detected, and
- Start or stop of application traffic is reported to the PCRF, if applicable and requested by the PCRF; the notification for Start may include service data flow filters, if possible to provide; and the application instance identifier associated with the service data flow filter, and
- Monitoring and enforcement, as specified within the rule, is applied

The PCRF may, at any time, modify an active, dynamic ADC rule.

The PCRF may, at any time, deactivate an active ADC rule. The IP-CAN session termination shall deactivate all ADC rules for that IP-CAN session.

Application Detection and Control rule activation/deactivation operations can also be performed in a deferred mode. For this case, the PCRF shall indicate a time at which the relevant ADC rule operation shall be performed by the PCEF or the TDF.

If a deferred ADC rule operation is received by the PCEF or the TDF and there is already a stored ADC rule operation with the same ADC Rule Identifier, this newly received ADC rule operation shall replace the stored ADC rule operation. If an ADC rule operation (non-deferred) is received for an ADC rule, which has a pending deferred ADC rule operation, the deferred ADC rule operation shall no longer be valid. When modifying a dynamic ADC rule with a prior and/or new deferred activation and/or deactivation time, the PCRF shall provide all attributes of that rule, including attributes that have not changed.

NOTE: In this case, the PCRF omission of an attribute that has a prior value will erase that attribute from the rule.

5 Security in the multi-connection architecture

The multi-connection functional architecture draws an initial set of requirements to support:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

Across all connections, see "ITU-T multi-connection Requirements" [15], including as well:

1) Protection against unauthorized use of multi-connection capability,

2) Mechanisms for data confidentiality among multiple accesses when necessary. The data contains user's profile in each connection, for instance:

- Preferences
- Profiles
- Presence
- Availability and location information

3) Mechanisms for data integrity in the case that the data of an application is delivered through several connections,

4) Mechanisms of non-repudiation for preventing one, or more, of the connections in a communication from falsely denying having participated in multi-connection communication,

5) Protection to minimize faked connection registration, and the hostile attack by one of the connections,

6) Mechanisms for protecting the data transferred in one connection from the attack of another connection when each connection has different security level,

7) Protection against unauthorized updates to operator's and user's multi-connection policies on the UE,

8) Secure storage, handling and enforcement of operator's and user's multi-connection policies on the UE, and

9) A security coordination function is required to coordinate each and all involved accesses according to multi-connection operator's predefined security policies and that of the user.

Architecturally however, the current "ITU-T Y.2027 (2012) Draft Recommendation Y.MC-ARCH Functional Architecture of multi-connection" [1] suggests two different paths, as alternatives to take, but so far lacking details on the Security Functions and/or Functional Elements and their interconnection with defined reference points. The following excerpts reflect the current multi-connection architectural issues. See Ref. [1].

Different access networks, with trusted access and untrusted access have different security policies, controlled by separated providers or the mobile network itself. For example, some airports normally provide free Wi-Fi to the public, while the operators provide chargeable GSM/UMTS/LTE accesses

for their service subscribers. Based on various security requirements, for different networks, there are two routes of action to take in the multi-connection architecture and its security aspects:

On the one hand an alternative is that the multi-connection architecture do not tackle directly the security issues on a any given single access scenario, such as unauthorized utilization of connections and/or faked connection registrations.

The second alternative being that the multi-connection architecture might include new security mechanisms affecting the various parallel accesses offered by the network. For instance, when data is transmitted in one connection others connections shall be protected from attacks coming from that connection. Specially, when each connection requests from the multi-connection network an independent level of security protection.

A number of security issues and updated mechanisms associated and developed within different fora, like IETF, and IEEE need to be followed to aligned to. Principally, the interactions of the different security mechanisms serving concurrently each individual network access need to be coordinated by a *"Coordinating Security Function"*, its residency might be embedded within the Multi-connection Control Function.

6 Reference Points

Currently, the reference points defined in the multi-connection functional architecture are defined in Ref. [1]. The Functions and Functional Entities interconnected are shown in Table 2 below.

Table 2 Reference Points in the multi-connection Functional Architecture

Ref. Points	MPC-FE	MC-FE	MR-FE	MUP-FE	Appli-cations	MAS-F	SCF	MMF	AC-FE	MTC-FE
MPC-FE		Pc		Pu		Pa	Ps			
MC-FE	Pc		Cr					Cm		
MR-FE		Cr		Ru						Rt
MUP-FE	Pu		Ru							
Appli-cations						ANI				
MAS-F	Pa				ANI		As			
SCF	Ps					As			Sa	
MMF		Cm							Ma	
AC-FE							Sa	Ma		
MTC-FE			Rt							

These reference points are defined currently in the multi-connection architecture as follows:

Reference Point ANI

It interfaces the Applications and the MAS-F. The Applications and MAS-F exchange signalling messages for application support, such as SIP messages.

Reference Point As

It interfaces the MAS-F and the SCF. SCF and MAS-F exchange signalling messages for service control, such as SIP messages.

Reference Point Pa

It interfaces the MAS-F and the MPC-FE. MPC-FE sends policies to MAS-F through this reference point. The reference point is provided only to the trusted MAS-F.

Reference Point Ps

It interfaces the SCF and the MPC-FE. It allows QoS resource request information needed for QoS resource authorization and reservation to be exchanged between the SCF and MPC-FE.

Reference Point Ru

It interfaces the MR-FE and the MUP-FE. The MR-FE and the MUP-FE exchange registration messages, such as user profile, authentication and authorization information, presence; e.g., online/offline status through this reference point.

Reference Point Pu

It interfaces the MPC-FE and the MUP-FE. It supports the MPC-FE to interact with the MUP-FE to check on the MUE subscription information.

Reference Point Pc

It interfaces the MPC-FE and the MC-FE. It supports the MPC-FE to interact with the MC-FE in order to coordinate traffic over multiple accesses. MC-FE reports the status of the access network resource to the MPC-FE. The MC-FE also obtains service information from the MPC-FE through this reference point.

Reference Point Cr

It interfaces the MC-FE and the MR-EF. It supports the MC-FE to interact with the MR-FE to check on the MUE's available connection information. The MC-FE reports abnormal status in the access network to the MR-FE in order to update available access network information. The MR-FE updates the connection information of the MUE towards the MC-FE via the Rt and Cr reference points.

Reference Point Cm

It interfaces the MC-FE and the MMF. It supports the MC-FE to push policy decisions to the MMF for enforcement purposes. The MC-FE sends specific load and/or QoS policy to the MMF via this reference point. The MMF updates real-time connection information to MC-FE in order to re-authorize multi-connection policies.

Reference Point Ma

It interfaces the MMF and the AC-FE. It supports the MMF to facilitate that the AC-FE enforces specific policy decisions thus assigning traffic loads among the active access networks.

Reference Point Rt

It interfaces the MR-FE and MUE. The MUE reports its available access information and/or location information to the MR-FE via the Rt reference point. The MR-FE might also record user's preferences or ISP's network selection policies and push them to the MUE via by Rt reference point.

7 QoS in a multi-connection network environment – Enhancements for GPRS and E-UTRAN

QoS in a multi-connection network calls for a multiplicity of QoS profiles, or sets used simultaneously by the MUE, and the combination and interactions among the active network accesses that the subscriber requests or are given to her by the network.

The sets of QoS provided to the subscriber per network access is supported by the functionality, the combined interactions of Functional Entities, and the signalling through specific reference points in the multi-connection network, see Ref. [1]:

1. The Multi-connection Media Function is responsible to enforce multiple access policies including load assignment and/or QoS to meet the requirement of multi-connection service experience.
2. The Access Control FE is responsible for QoS enforcement; e.g., gating and bandwidth control in accordance to the QoS policy.
3. The Multi-connection Coordination Function Entity manages and updates specific loads after QoS policies for each access network conveying them to the MMF.
4. The Multi-connection Policy Control Functional Entity (MPC-FE) provides policies for every session, as well as guarantees the QoS of the session by sending those policies to the MC-FE and AC-FE. Afterwards, the MC-FE and AC-FE assign specific policies to each access based on the policies received from the MPC-FE, such as control routing paths, or rate of the IP flows. It also receives and authorizes the QoS resource request from the SCF.
5. The Multi-connection User Profile Functional Entity provides subscribers' allowed QoS, such as bandwidth and priority.
6. The Reference Point Ps, connecting the SCF and the MPC-FE, transports QoS resource request information needed for QoS resource authorization and reservation to be exchanged between the SCF and MPC-FE.
7. The Reference Point Cm, connecting the MC-FE and the MMF, allowing the MC-FE to push policy decisions to the MMF for enforcement. The MC-FE sends pecific load and/or QoS policy to the MMF using this reference point. Then the MMF updates real-time connection information to the MC-FE to re-authorize multi-connection policies.
8. On Adding a New Connection, the flows in the multi-connection functional architecture suggest that: the MPC-FE selects a set of QoS rules for the new connection, based on operator's policies and the information of the new connection. Afterwards, the MPC-FE selects the policy to be applied to the MUE based on those policies and forwards it to the MC-FE.
9. On Updating a Connection, the flows in the multi-connection functional architecture suggest that: the MPC-FE shall control the resources for the transport layer based on the Transport Resource Modification Request, and subsequently send a QoS Policy Rules Delete/Update message to the MC-FE.
10. Also that on Updating a Connection, the flows in the multi-connection functional architecture suggest that: MC-FE receives the QoS Policy Rules Delete/Update message and afterwards returns an ACK message to MPC-FE.
11. When the MUE initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the MPC-FE selects new QoS policy rules for the connection based on operator's policies and the updated connection information. Afterwards, it returns a Transport Resource Modification Response message to the MC-FE.
12. Also, when the MUE initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the MMF sends the new QoS rules to AC-FE.

13. And finally when the MUE initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the AC-FE updates the QoS policy rules of the connection. And subsequently, it returns an ACK message to the MMF.
14. When the multi-connection network initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the MPC-FE selects new QoS policy rules for the connection based on operator's policies and the updated connection information. Subsequently, it returns a Transport Resource Modification Response message to MC-FE.
15. Also, when the multi-connection network initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the MMF sends the new QoS rules to AC-FE.
16. And finally when the multi-connection network initiates the IP Flow Mobility, the flows in the multi-connection functional architecture suggest that: the AC-FE updates the QoS policy rules of the connection, and then it returns an ACK message to MMF.
17. Upon the service decomposition the multi-connection functional architecture suggest that: the MPC-FE selects policy rules based on QoS resource requirements, and other dynamic events. Afterwards, it sends a request to install the rules in the MMF under the appropriate connection.
18. And finally upon service decomposition the multi-connection functional architecture suggest that: the MPC-FE makes policy rules based on QoS resource requirements, and other dynamic events. Afterwards, it sends a request to install the rules in the MMF.

In order to minimize service degradation among multi-connections, the QoS classes may require mapping among same or similar QoS classes. According to the QoS parameters specified in each standard; e.g., IEEE 802.16e, 802.11e, GPRS, UMTS, and LTE, traffic flows are required to be allocated both, for the service flows and the packet queues. The bandwidth is required to be constrained by classes and parameter mapping by a QoS management functional entity. Table 3 below, see Ref. [15], shows an example of the multi-connection QoS mapping.

After the mapping process, scheduling policy may be required to be performed, such as strict priority (SP), weighted round robin (WRR), or weighted fair queue (WFQ).

Congestion control policy is also required in the multi-connection architecture, such policies include tail-drop, random early detection (RED). Additional queue related mechanisms for the accesses combination or traffic mix are also a consideration, for instance the Buffer Size.

Table 3 Case Example of QoS Mapping Among Different Access Networks [15]

Priority	802.16e	802.11e	GSM/GPRS	UMTS/LTE	Services
0	BE	AC_BK	Delay class 4	Background (QCI=9)	E-mail
1	BE	AC_BK	Delay class 1-3	Interactive (QCI=8)	Web
2	nrtPS	AC_BE	Delay class 1-3	Interactive (QCI=7)	FTP (low quality)
3	nrtPS	AC_BE	Delay class 1-3	Interactive (QCI=5, 6)	FTP (high quality)
4	rtPS	AC_VI	Delay class 1	Streaming (QCI=4)	VoD
5	ertPS	AC_VI	Delay class 1	Streaming (QCI=4)	Realtime streaming
6	UGS	AC_VO	Delay class 1	Conversational (QCI=2, 3)	VoIP (low quality)
7	UGS	AC_VO	Delay class 1	Conversational (QCI=1)	VoIP (high quality)

7.1 The QoS concept in GPRS, LTE, and Evolved Packet System

The QoS model in the Evolved Packet System (EPS) is currently followed to a certain extent in the multi-connection network. In the following clauses, its concept is analyzed, it is encouraged to continue the close alignment in a deeper technical detail by the multi-connection functional architecture. Including at least the following topics, see Ref. TS 23.401 [13]:

- PDP connectivity service
- EPS bearer
    - EPS bearer with GTP-based S5/S8
    - The EPS bearer with PMIP-based S5/S8
- Bearer level QoS parameters
- Session Management
- QoS and interaction with the Policy and Charging Control (PCC) functionality
    - Dedicated Bearer Activation
    - Bearer Modification with Bearer QoS Update
        - PDN GW Initiated Bearer Modification with Bearer QoS Update
        - HSS Initiated Subscribed QoS Modification
- QoS Parameter Mapping between EPS and other 3GPP Releases

7.1.1 PDN Connectivity Service

After TS 23.401 [13], the Evolved Packet System (EPS) provides IP connectivity between a UE and a PLMN external packet data network. This is referred to as PDN Connectivity Service.

The PDN Connectivity Service supports the transport of traffic flow aggregate(s), consisting of one or more Service Data Flows (SDFs). Note that the concept of SDF is defined in the context of PCC, see Ref. TS 23.203 [4], and is not explicitly visible in the NAS signalling.

7.1.2 The EPS bearer

For E-UTRAN, access to the Evolved Packet Core (EPC) the PDN connectivity service is provided by an Evolved Packet System (EPS) bearer for GPRS Tunneling Protocol (GTP)-based Reference Point between the Serving Gateway (S-GW) and the PDN Gateway (P-GW) (PCEF) in visited network (S5)/Reference Point between S-GW and P-GW (PCEF) in home network (S8), and by an EPS bearer concatenated with IP connectivity between the S-GW and P-GW for Proxy Mobile IPv6 (PMIP)-based S5/S8, see TS 23.401 [13].

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a MUE and a PDN GW for GTP-based S5/S8, and between MUE and Serving GW for PMIP-based S5/S8. The packet filters signalled in the NAS procedures are associated with a unique packet filter identifier on per-PDN connection basis.

NOTE 1: The EPS Bearer Identity together with the packet filter identifier is used to reference which packet filter the MUE intends to modify or delete, i.e. it is used to implement the unique packet filter identifier.

The EPS bearer Traffic Flow Template (TFT) is the set of all packet filters associated with that EPS bearer.

An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. That is, all traffic mapped to the same EPS bearer receives the same bearer level packet forwarding treatment; e.g., scheduling policy, queue management policy, rate shaping policy, Radio Link Control (RLC) configuration, and others.

Providing different bearer level packet forwarding treatment requires separate EPS bearers.

NOTE 2: In addition but independent to bearer level QoS control, the PCC framework allows an optional enforcement of service level QoS control on the granularity of Service Data Flows (SDFs), independent of the mapping of SDFs to EPS bearers.

One EPS bearer is established when the MUE connects to a PDN. The EPS bearer remains established throughout the lifetime of the PDN connection to provide to the MUE always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. Any additional EPS bearer that is established for the same PDN connection is referred to as a dedicated bearer.

An Up Link Traffic Flow Template (UL TFT) is the set of uplink packet filters in a TFT. A Down Link Traffic Flow Template (DL TFT) is the set of downlink packet filters in a TFT. Every dedicated EPS bearer is associated with a TFT. The MUE uses the UL TFT for mapping traffic to an EPS bearer in the uplink direction. The Policy and Charging Control Enforcement Function (PCEF) (for GTP-based S5/S8) or the Bearer Binding and Event Reporting Function (BBERF) (for PMIP-based S5/S8) uses the DL TFT for mapping traffic to an EPS bearer in the downlink direction. The MUE may use the UL TFT and DL TFT to associate EPS Bearer Activation or Modification procedures to an application and to traffic flow aggregates of the application. Therefore, the PDN GW shall, in the “Create Dedicated Bearer Request” and the “Update Bearer Request” messages, provide all available traffic flow description information; e.g., source and destination IP address, port numbers, and the protocol information.

For the UE, the evaluation precedence order of the packet filters making up the UL TFTs is signalled from the P-GW to the MUE as part of any appropriate TFT operations.

NOTE 3: The evaluation precedence index of the packet filters associated with the default bearer, in relation to those associated with the dedicated bearers, is operator configuration dependant. It is possible to "force" certain traffic onto the default bearer by setting the evaluation precedence index of the corresponding filters to a value that is lower than the values used for filters associated with the dedicated bearers. It is also possible to use the default bearer for traffic that does not match any of the filters associated with the dedicated bearers. In this case, the evaluation precedence index of the corresponding filter(s); e.g., a "match all filter" need to be set to a value that is higher than the values used for filters associated with dedicated bearers.

A TFT of a unidirectional EPS bearer is either associated with UL packet filter(s) or DL packet filter(s) that matches the unidirectional traffic flow(s) and a DL packet filter or a UL packet filter that effectively disallows any useful packet flows, see clause 15.3.3.4 in TS 23.060 [12] for an example of such packet filter.

The initial bearer level QoS parameter values of the default bearer are assigned by the network based on subscription data, in E-UTRAN the Mobility Management Entity (MME) sets those initial values based on subscription data retrieved from Home Subscriber Server (HSS).

In a non-roaming scenario, the PCEF may change the QoS parameter value received from the MME based on interaction with the Policy and Charging Rules Function (PCRF) or based on local configuration. When the PCEF changes those values, the MME shall use the bearer level QoS parameter values received on the Reference Point between the Serving Gateway (S-GW) and the MME (S11) during establishment or modification of the default bearer.

In a roaming scenario, based on local configuration, the MME may downgrade the Address Resolution Protocol (ARP) or Access Point Name (APN)-Aggregate Maximum Bit Rate (AMBR) and/or remap QoS Class Identifier (QCI) parameter values received from the HSS to the value locally configured in MME; e.g., when the values received from HSS do not comply with services provided by the visited PLMN. The PCEF may change the QoS parameter values received from the MME based on interaction with the PCRF or based on local configuration. Alternatively, the PCEF may reject the bearer establishment.

NOTE 4: For certain APNs; e.g., in the IMS APN defined by GSMA, the QCI value is strictly defined and therefore remapping of QCI is not permitted.

NOTE 5: In roaming scenarios, the ARP/APN-AMBR/QCI values provided by the MME for a default bearer may deviate from the subscribed values depending on the roaming agreement. If the PCC/PCEF rejects the establishment of the default bearer, this would imply that Attach via E-UTRAN fails. Similarly, if the PCEF, based on interaction with the PCRF or based on local configuration, upgrades the ARP/APN-AMBR/QCI

parameter values received from the MME, the default bearer establishment and attach may be rejected by the MME.

NOTE 6: Subscription data related to bearer level QoS parameter values retrieved from the HSS are not applicable for dedicated bearers.

For E-UTRAN, the decision to establish or modify a dedicated bearer can only be taken by the EPC, and the bearer level QoS parameter values are always assigned by the EPC.

The MME shall not modify the bearer level QoS parameter values received on the S11 reference point during establishment or modification of a default or dedicated bearer. Instead, the MME shall only transparently forwards those values to the E-UTRAN. Consequently, "QoS negotiation" between the E-UTRAN and the EPC during default or dedicated bearer establishment or modification is not supported. The MME may, however, reject the establishment or modification of a default or dedicated bearer; e.g., if the bearer level QoS parameter values sent by the PCEF over a GTP based S8 roaming interface do not comply with a roaming agreement.

The distinction between default and dedicated bearers should be transparent to the access network; e.g., E-UTRAN.

An EPS bearer is referred to as a GBR bearer if dedicated network resources related to a Guaranteed Bit Rate (GBR) value that is associated with the EPS bearer are permanently allocated; e.g., by an admission control function in the eNodeB, at bearer establishment or modification. Otherwise, an EPS bearer is referred to as a Non-GBR bearer.

NOTE 7: Admission control can be performed at establishment or modification of a Non-GBR bearer even though a Non-GBR bearer is not associated with a GBR value.

A dedicated bearer can either be a GBR or a Non-GBR bearer. A default bearer shall be a Non-GBR bearer.

NOTE 8: A default bearer provides the MUE with IP connectivity throughout the lifetime of the PDN connection. That motivates the restriction of a default bearer to a Non-GBR bearer type.

The MUE routes uplink packets to the different EPS bearers based on uplink packet filters in the TFTs assigned to these EPS bearers. The MUE evaluates a matching, firstly the uplink packet filter amongst all TFTs that have the lowest evaluation precedence index and, if no match is found, proceeds with the evaluation of uplink packet filters in increasing order of their evaluation precedence index. This procedure shall be executed until a match is found or all uplink packet filters have been evaluated. If a match is found, the uplink data packet is transmitted on the EPS bearer that is associated with the TFT of the matching uplink packet filter. If no match is found, the uplink data packet shall be sent via the EPS bearer that has not been assigned any uplink packet filter. If all EPS bearers, including the default EPS bearer for that PDN, have been assigned one or more uplink packet filters, the MUE shall discard the uplink data packet.

NOTE 9: The above algorithm implies that there is at most one EPS bearer without any uplink packet filter; i.e., either EPS bearer without any TFT or an EPS bearer with only DL packet filter(s). Therefore, some UEs may expect that during the lifetime of a PDN connection, where only the network has provided TFT packet filters, at most one EPS bearer exist without a TFT or with a TFT without any uplink packet filter.

To ensure that at most one EPS bearer exist without a TFT or with a TFT without any uplink packet filter, the PCEF, for GTP-based S5/S8, and the BBERF, for PMIP-based S5/S8, applies the Session Management restrictions as described in clause 9.2.0 of TS 23.060 [12].

7.1.3 The EPS Bearer with GTP-based S5/S8 Reference Points

Figure 9 depicts two Evolved Packet System (EPS) bearers using the GTP protocol through the S5 or S8 reference points. Uplink and Downlink traffic flow aggregates feed and receive information to and from an application. IP packets are transmitted from the MUE through the X2, S1, S5/S8 reference points to the PDN Gateway (P-GW). They are transmitted at different layers through the radio, S1, and S5/S8 bearers.

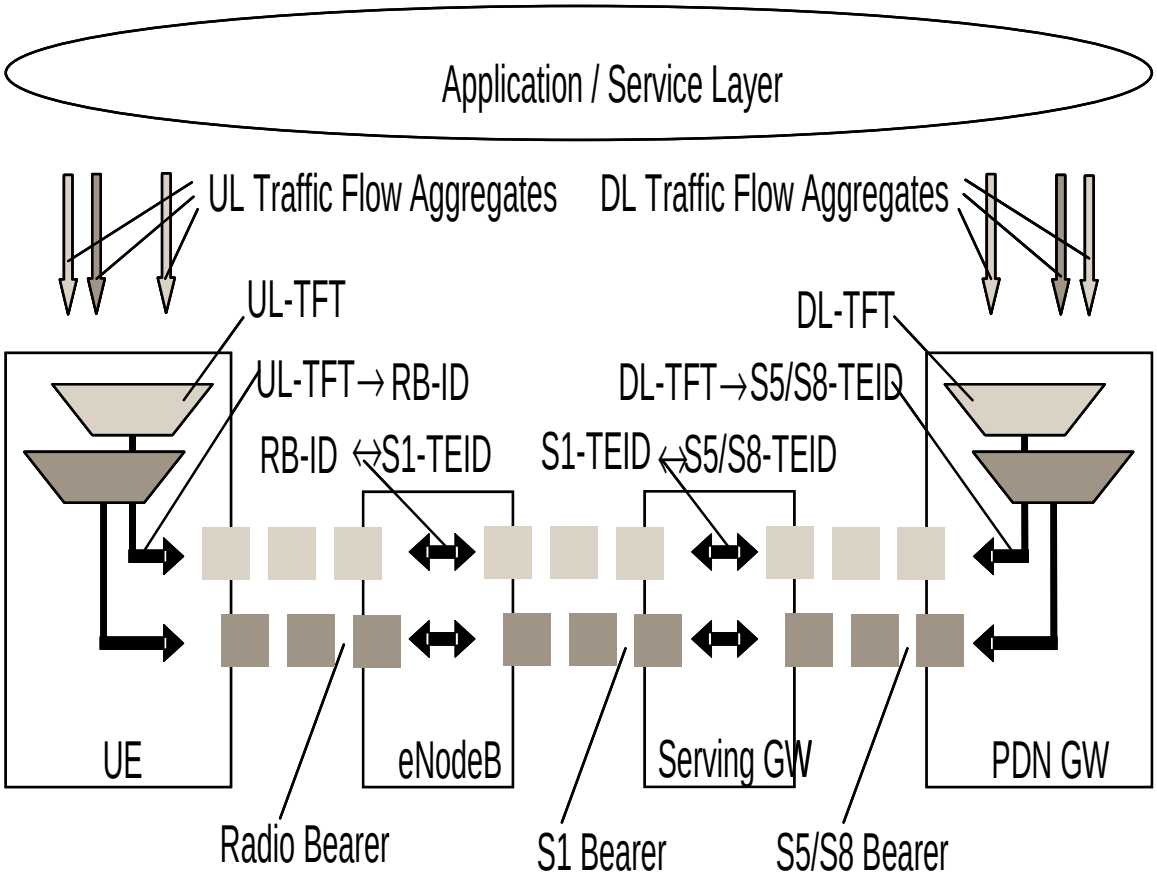

Figure 9 Two Unicast EPS Bearers – GPRS Tunneling Protocol (GTP)-Based S5/S8 [13]

More in detail, an EPS bearer is created by the MUE and network in the following steps and network elements, see TS 23.401 [13]:

- In the UE, the Uplink (UL) Traffic Flow Template (TFT) maps a traffic flow aggregate to an Evolved Packet System (EPS) bearer in the uplink direction
- In the PDN GW, the Downlink (DL) TFT maps a traffic flow aggregate to an EPS bearer in the downlink direction
- A radio bearer (defined in TS 36.300 [17]) transports the packets of an EPS bearer between a MUE and an eNodeB. If a radio bearer exists, there is a one-to-one mapping between an EPS bearer and this radio bearer
- An S1 bearer transports the packets of an EPS bearer between an eNodeB and a Serving GW
- An E-RAB (E-UTRAN Radio Access Bearer) refers to the concatenation of an S1 bearer and the corresponding radio bearer, as defined in TS 36.300 [17]
- An S5/S8 bearer transports the packets of an EPS bearer between a Serving GW and a PDN GW
- A MUE stores a mapping between an uplink packet filter and a radio bearer to create the mapping between a traffic flow aggregate and a radio bearer in the uplink
- A PDN GW stores a mapping between a downlink packet filter and an S5/S8 bearer to create the mapping between a traffic flow aggregate and an S5/S8 bearer in the downlink

- An eNodeB stores a one-to-one mapping between a radio bearer and an S1 Bearer to create the mapping between a radio bearer and an S1 bearer in both the uplink and downlink directions

- A Serving GW stores a one-to-one mapping between an S1 Bearer and an S5/S8 bearer to create the mapping between an S1 bearer and an S5/S8 bearer, in both the uplink and downlink directions

The PDN GW routes downlink packets to the different EPS bearers based on the downlink packet filters in the TFTs assigned to the EPS bearers in the PDN connection. Upon reception of a downlink data packet, the PDN GW tries to find a match, firstly against the downlink packet filter that has the lowest evaluation precedence index and, if no match is found, proceeds with the evaluation of downlink packet filters in increasing order of their evaluation precedence index. This procedure shall be executed until a match is found, in which case the downlink data packet is tunneled to the Serving GW on the EPS bearer that is associated with the TFT of the matching downlink packet filter.

If no match is found, the downlink data packet shall be sent via the EPS bearer that does not have any downlink packet filter assigned. If all EPS bearers, including the default EPS bearer for that PDN, have been assigned a downlink packet filter, the PDN GW shall discard the downlink data packet.

7.1.4 The EPS Bearer with PMIP-based S5/S8 and E-UTRAN access

Figure 10 depicts two EPS bearers using the PMIP-based S5/S8 reference points and E-UTRAN access.

In detail, see TS 23.402 [5], for PMIP-based S5/S8 and E-UTRAN access, an EPS bearer consists of the concatenation of one Radio Bearer and one S1 bearer. The PDN Connectivity Service between a MUE and an external packet data network is supported through a concatenation of an EPS Bearer and IP connectivity between Serving GW and PDN GW. QoS control between a Serving GW and a PDN GW is provided at the Transport Network Layer (TNL).

The EPS bearer is created by the following actions and network elements:

- In the UE, the Uplink (UL) Traffic Flow Template (TFT) maps a traffic flow aggregate to an EPS bearer in the uplink direction

- In the Serving GW, the Downlink (DL) TFT maps a traffic flow aggregate to an EPS bearer in the downlink direction

- A radio bearer transports the packets of an EPS bearer between a MUE and an eNodeB. There is a one-to-one mapping between an EPS bearer and a radio bearer

- An S1 bearer transports the packets of an EPS bearer between an eNodeB and a Serving GW. There is a one-to-one mapping between an EPS bearer and a S1 bearer

- A per MUE per PDN tunnel transports the packets of an EPS bearer between a Serving GW and a PDN GW. There is a many-to-one mapping between an EPS bearer and this per UE, per PDN tunnel

- A MUE stores a mapping between an uplink packet filter and a radio bearer to create the mapping between a traffic flow aggregate and a radio bearer in the uplink

- An eNodeB stores a one-to-one mapping between a radio bearer and an S1 bearer to create the binding between a radio bearer and an S1 bearer in both the uplink and the downlink direction

- A Serving GW stores a one-to-one mapping between a downlink packet filter and an S1 bearer to create the mapping between a traffic flow aggregate and an S1 bearer in the downlink

- A PDN GW enforces Access Point Name (APN)- Aggregate Maximum Bit Rate (AMBR) across all SDFs of the same APN that is associated with Non- Guaranteed Bitrate (GBR) QoS Class Identifier (QCIs)

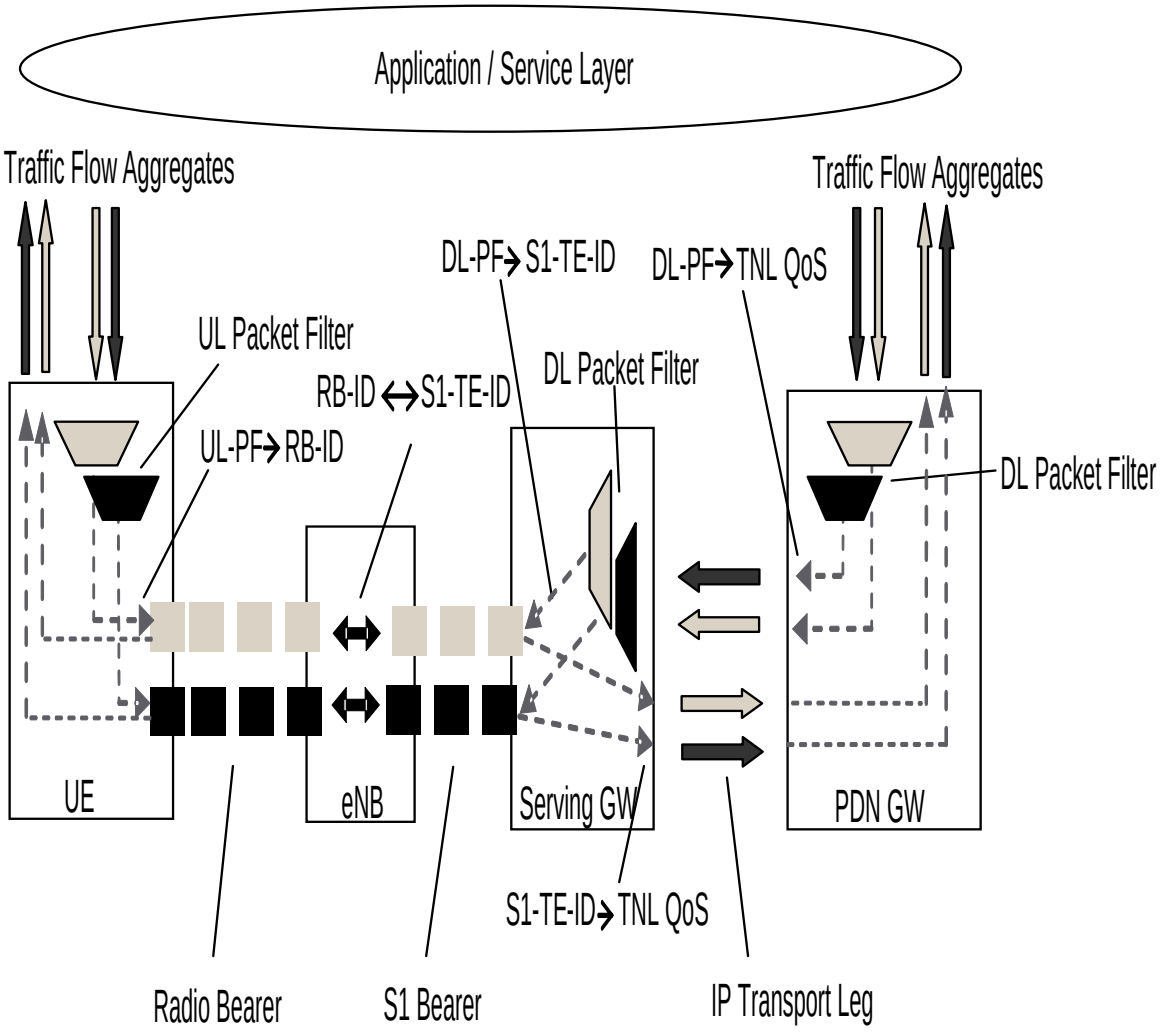

Figure 10 Two Unicast EPS Bearers - PMIP-Based S5/S8 and E-UTRAN Access [13]

7.2 Bearer Level QoS Parameters

The EPS bearer QoS profile includes the parameters QoS Class Identifier (QCI), Address Resolution Protocol (ARP), Guaranteed Bitrate (GBR) and Maximum Bitrate (MBR), described in TS 23.401 [13]. In the following, the QoS parameters are described. They apply to an aggregated set of EPS Bearers: Access Point Name (APN)- Aggregate Maximum Bit Rate (AMBR) and UE-AMBR.

Each EPS bearer, Guaranteed Bitrate (GBR) and Non-GBR, is associated with the following bearer level QoS parameters:

- QoS Class Identifier (QCI)
- Allocation and Retention Priority (ARP)

A QCI is a scalar, is used as a reference to access node-specific parameters that control bearer level packet forwarding treatment; e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others, and that have been pre-configured by the operator owning the access node; e.g., the eNodeB. A one-to-one mapping of standardized QCI values to standardized characteristics is captured in TS 23.203 [4].

Note 1: On the radio interface and on S1, each Protocol Data Unit (PDU); e.g. Radio Link Control (RLC) PDU or GPRS Tunnelling Protocol (GTP)-U PDU, is indirectly associated with one QCI via the bearer identifier carried in the PDU header. The same applies to the S5 and S8 interfaces if they are based on GTP.

The ARP shall contain information about the priority level (a scalar), the pre-emption capability (a flag) and the pre-emption vulnerability (flag). The primary purpose of ARP is to decide whether a bearer establishment or modification request can be accepted or needs to be rejected due to resource limitations, a typically reason is available radio capacity, for GBR bearers. The priority level information of the ARP is used for this decision to ensure that the request of the bearer with the higher priority level is preferred.

In addition, the ARP can be used; e.g., by the eNodeB, to decide which bearer(s) to drop during exceptional resource limitations; e.g., at handover. The pre-emption capability information of the ARP defines whether a bearer with a lower ARP priority level should be dropped to free up the required resources. The pre-emption vulnerability information of the ARP defines whether a bearer is applicable for such dropping by a pre-emption capable bearer with a higher ARP priority value. Once successfully established, a bearer's ARP shall not have any impact on the bearer level packet forwarding treatment; e.g., scheduling and rate control. Such packet forwarding treatment should be solely determined by the other EPS bearer QoS parameters: QCI, GBR and MBR, and by the AMBR parameters. The ARP is not included within the EPS QoS Profile sent to the MUE.

Note 2: The ARP should be understood as "Priority of Allocation and Retention"; not as "Allocation, Retention, and Priority".

Note 3: Video telephony is one use case where it may be beneficial to use EPS bearers with different ARP values for the same MUE. In this use case, an operator could map voice to one bearer with a higher ARP, and video to another bearer with a lower ARP. In a congestion situation; e.g., cell edge, the eNodeB can then drop the "video bearer" without affecting the "voice bearer", improving service continuity.

Note 4: The ARP may also be used to free up capacity in exceptional situations; e.g., a disaster situation. In such a case, the eNodeB may drop bearers with a lower ARP priority level to free up capacity if the pre-emption vulnerability information allows this.

Each GBR bearer is additionally associated with the following bearer level QoS parameters:

- Guaranteed Bit Rate (GBR)
- Maximum Bit Rate (MBR)

The GBR denotes the bit rate, expected to be provided by a GBR bearer. The MBR limits the bit rate that can be expected to be provided by a GBR bearer; e.g., excess traffic may get discarded by a rate shaping function. See TS 23.401 [13] for further details on GBR and MBR.

Each APN access, by a UE, is associated with the following QoS parameter:

- per APN Aggregate Maximum Bit Rate (APN-AMBR)

The APN-AMBR is a subscription parameter stored per APN in the Home Subscriber Server (HSS). It limits the aggregate bit rate that can be expected to be provided across all Non-GBR bearers and across all PDN connections of the same APN; i.e., excess traffic may get discarded by a rate shaping function. Each of those Non-GBR bearers could potentially utilize the entire APN-AMBR; e.g., when the other Non-GBR bearers do not carry any traffic.

GBR bearers are outside the scope of the APN-AMBR. The P-GW enforces the APN-AMBR in downlink. Enforcement of APN-AMBR in uplink is done in the MUE and additionally in the P-GW.

Note 5: All simultaneous active PDN connections of a MUE that are associated with the same APN shall be provided by the same PDN GW, see TS 23.401 [13].

APN-AMBR applies to all PDN connections of an APN. For the case of multiple PDN connections of an APN, if a change of APN-AMBR occurs due to local policy or the PGW is provided the updated APN-AMBR for each PDN connection from the MME or PCRF, the PGW initiates explicit signaling for each PDN connection to update the APN-AMBR value.

Each MUE in state EMM-REGISTERED (see Note * below) is associated with the following bearer aggregate level QoS parameter:

- per MUE Aggregate Maximum Bit Rate (MUE-AMBR)

Note* After 23.401 [13], the MUE enters the EMM-REGISTERED state by a successful registration with an Attach procedure to either E-UTRAN or GERAN/UTRAN. The MME enters the EMM-REGISTERED state by a successful Tracking Area Update procedure for a MUE selecting an E-UTRAN cell from GERAN/UTRAN or by an Attach procedure via E-UTRAN. In the EMM-REGISTERED state, the MUE can receive services that require registration in the EPS.

NOTE: The MUE employs a single combined state machine for EMM and GMM states.

The MUE location is known in the Mobility Management Entity (MME) to at least an accuracy of the tracking area list allocated to that UE, excluding some abnormal cases.

In the EMM-REGISTERED state, the MUE shall:

- always have at least one active PDN connection
- setup the EPS security context

After performing the Detach procedure, the state is changed to EMM-DEREGISTERED in the MUE and in the MME. Upon receiving the Tracking Area Update (TAU) Reject and Attach Reject messages the actions of the MUE and MME depend upon the 'cause value' in the reject message, but, in many cases the state is changed to EMM-DEREGISTERED in the MUE and in the MME.

If all the bearers belonging to a MUE are released; e.g., after handover from E-UTRAN to non-3GPP access, the MME shall change the MM state of the MUE to EMM-DEREGISTERED.

If the MUE camps on E-UTRAN and the MUE detects that all of its bearers are released, the MUE shall change the MM state to EMM-DEREGISTERED. If all the bearers (PDP contexts) belonging to a MUE are released while the MUE camps on GERAN/UTRAN, the MUE shall deactivate Idle-mode Signalling Reduction (ISR) by setting its TIN to "P-TMSI" as specified in TS 23.060 [12]. This ensures that the MUE performs Tracking Area Update when it re-selects E-UTRAN. If the MUE switches off its E-UTRAN interface when performing handover to non-3GPP access, the MUE shall automatically change its MM state to EMM-DEREGISTERED.

The MME may perform an implicit detach any time after the Implicit Detach timer expires. The state is changed to EMM-DEREGISTERED in the MME after performing the implicit detach – End of Note *.

The UE-AMBR is limited by a subscription parameter stored in the HSS. The MME shall set the UE-AMBR to:

> "The *sum* of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR."

The UE-AMBR limits the aggregate bit rate expected to be provided across all Non-GBR bearers of a UE; e.g., excess traffic may get discarded by a rate shaping function.

Each of those Non-GBR bearers could potentially utilize the entire UE-AMBR; e.g., when the other Non-GBR bearers do not carry any traffic. Again, GBR bearers are outside the scope of MUE AMBR. The E-UTRAN enforces the UE-AMBR in uplink and downlink.

The GBR and MBR denote bit rates of traffic per bearer, while MUE-AMBR and APN-AMBR denote bit rates of traffic per group of bearers. Each of those QoS parameters has an uplink and a downlink component.

On S1_MME the values of the GBR, MBR, and AMBR refer to the bit stream excluding the GTP-U/IP header overhead of the tunnel on S1_U.

The HSS defines, for each PDN subscription context, the 'EPS subscribed QoS profile' which contains the bearer level QoS parameter values for the default bearer (QCI and ARP) and the subscribed APN-AMBR value.

The subscribed ARP shall be used to set the priority level of the EPS bearer parameter ARP for the default bearer while the pre-emption capability and the pre-emption vulnerability information for the default bearer are set based on MME operator policy. In addition, the subscribed ARP shall be applied by the P-GW for setting the ARP priority level of all dedicated EPS bearers of the same PDN connection unless a specific ARP priority level setting is required; due to P-GW configuration or interaction with the Policy and Charging Rules Function (PCRF).

Note 6: The ARP parameter of the EPS bearer can be modified by the P-GW; e.g., based on interaction with the PCRF, to assign the appropriate pre-emption capability and the pre-emption vulnerability setting.

The ARP pre-emption vulnerability of the default bearer should be set appropriately to minimize the risk of unnecessary release of the default bearer.

7.3 PDN GW Selection Function in 3GPP Accesses

The PDN GW selection function allocates a PDN GW that shall provide the PDN connectivity for the 3GPP access, Refer to TS 23.401 [13]. The function uses subscriber information provided by the HSS and possibly additional criteria such as Selective IP Traffic Offloading (SIPTO) and Local IP Access (LIPA) support per Access Point Name (APN) configured in the Serving GPRS Support Node (SGSN) and Mobility Management Entity (MME). The criteria for PDN GW selection may include load balancing between PDN GWs. When the PDN GW IP addresses returned from the Domain Name System (DNS) server include Weight Factors, the MME should use it if load balancing is required. The Weight Factor is typically set according to the capacity of a PDN GW node relative to other PDN GW nodes serving the same APN.

The PDN subscription contexts provided by the HSS contain:

- the identity of a PDN GW and an APN (PDN subscription contexts with subscribed PDN GW address are not used when there is interoperation with pre Rel-8 2G/3G SGSN), or
- an APN and an indication for this APN whether the allocation of a PDN GW from the visited PLMN is allowed or whether a PDN GW from the home PLMN shall be allocated. Optionally an identity of a PDN GW may be contained for handover with non-3GPP accesses

- optionally, for an APN, an indication of whether SIPTO is allowed or prohibited for this APN
- optionally, for an APN, an indication of whether LIPA is conditional, prohibited, or only LIPA is supported for this APN

In the case of static address allocation, a static PDN GW is selected by either having the APN configured to map to a given PDN GW, or the PDN GW identity provided by the HSS indicates the static PDN GW.

The HSS also indicates which of the PDN subscription contexts is the Default one for the UE.

To establish connectivity with a PDN when the MUE is already connected to one or more PDNs, the MUE provides the requested APN for the PDN GW selection function.

If one of the PDN subscription contexts provided by the HSS contains a wild card APN, see TS 23.003 [18], a PDN connection with dynamic address allocation may be established towards any APN requested by the UE. An indication that SIPTO is allowed or prohibited for the wild card APN allows or prohibits SIPTO for any APN that is not present in the subscription data.

If the HSS provides the identity of a statically allocated PDN GW, or the HSS provides the identity of a dynamically allocated PDN GW and the Request Type indicates "Handover", no further PDN GW selection functionality is performed. If the HSS provides the identity of a dynamically allocated PDN GW, the HSS also provides information that identifies the PLMN in which the PDN GW is located.

NOTE 1: The MME uses this information to determine an appropriate APN-Operator Identifier (OI) and S8 protocol type (PMIP or GTP) when the MME and PDN GW are located in different PLMNs.

If the HSS provides the identity of a dynamically allocated PDN GW and the Request Type indicates "Initial Request", either the provided PDN GW is used or a new PDN GW is selected. When a PDN connection for an APN with SIPTO-allowed is requested, the PDN GW selection function shall ensure the selection of a PDN GW that is appropriate for the UE's location. The PDN GW identity refers to a specific PDN GW. If the PDN GW identity includes the IP address of the PDN GW, that IP address shall be used as the PDN GW IP address; otherwise the PDN GW identity includes a Fully Qualified Domain Name (FQDN) which is used to derive the PDN GW IP address by using the Domain Name Service function, taking into account the protocol type on S5/S8 (PMIP or GTP).

NOTE 2: Provision of a PDN GW identity of a PDN GW as part of the subscriber information allows also for a PDN GW allocation by the HSS.

If the HSS provides a PDN subscription context that allows for allocation of a PDN GW from the visited PLMN for this APN and, optionally, the MME is configured to know that the visited VPLMN has a suitable roaming agreement with the HPLMN of the UE, the PDN GW selection function derives a PDN GW identity from the visited PLMN. If a visited PDN GW identity cannot be derived, or if the subscription does not allow for allocation of a PDN GW from the visited PLMN, then the APN is used to derive a PDN GW identity from the HPLMN. The PDN GW identity is derived from the APN, subscription data and additional information by using the Domain Name Service function.

If the PDN GW identity is a logical name, instead of an IP address, the PDN GW address is derived from the PDN GW identity protocol type on S5/S8 (PMIP or GTP) by using the Domain Name Service function. The S8 protocol type (PMIP or GTP) is configured per HPLMN in the MME/SGSN.

In order to select the appropriate PDN GW for SIPTO service, the PDN GW selection function uses the TAI (Tracking Area Identity), the serving eNodeB identifier, or TAI together with serving eNodeB identifier depending on the operator's deployment during the DNS interrogation to find the PDN GW identity. In the roaming scenario PDN GW selection for SIPTO is only possible when a

PDN GW in the visited PLMN is selected. Therefore, in a roaming scenario with home routed traffic, PDN GW selection for SIPTO is not performed.

In order to select the appropriate Local GateWay (L-GW) for Local IP Access (LIPA) service, if permitted by the Closed Subscriber Group (CSG) subscription data and if the MUE is roaming, the VPLMN LIPA is allowed, the PDN GW selection function uses the L-GW address proposed by HeNB in the S1-AP message, instead of DNS interrogation. If no L-GW address is proposed by the HeNB, and the MUE requested an APN with LIPA permissions set to "LIPA-only", the request shall be rejected. If no L-GW address is proposed by the HeNB and the MUE requested an APN with LIPA permissions set to "LIPA-conditional", the MME uses DNS interrogation for PGW selection to establish a non-LIPA PDN connection. The PDN subscription context for an APN with LIPA permissions set to "LIPA-only" shall not contain a statically configured PDN address or a statically allocated PDN GW. A static PDN address or a static PDN GW address, if configured by HSS for an APN with LIPA permissions set to "LIPA-conditional", is ignored by MME when the APN is established as a LIPA PDN connection. When establishing a PDN connection for a LIPA APN, the VPLMN Address Allowed flag is not considered.

The PDN GW domain name shall be constructed and resolved by the method described in TS 29.303 [19], which takes into account any value received in the APN-OI Replacement field for home routed traffic. Otherwise, or when the resolution of the above PDN GW domain name fails, the PDN GW domain name shall be constructed by the serving node using the method specified in TS 23.060 [12] and TS 23.003 [18].

If the Domain Name Service function provides a list of PDN GW addresses, one PDN GW address is selected from this list. If the selected PDN GW cannot be used; e.g., due to an error, then another PDN GW is selected from the list. The specific interaction between the MME/SGSN and the Domain Name Service function may include functionality to allow for the retrieval or provision of additional information regarding the PDN GW capabilities; e.g., whether the PDN GW supports PMIP-based or GTP-based S5/S8, or both.

Note 3: The APN as constructed by the MME/SGSN for PDN GW resolution takes into account the APN-Operator Identifer (OI) Replacement field. This differs from the APN that is provided in charging data to another SGSN and MME over the S3 (reference point between SGSN Rel. 8 and MME), S10 (reference point between MME and MME) and S16 (reference point between SGSN and SGSN) interfaces as well as to Serving GW and PDN GW over the S11 (reference point between MME and S-GW), S4 (reference point between S-GW and SGSN Rel.8) and S5 (reference point between S-GW and P-GW) and S8 (reference point between S-GW and P-GW) interfaces, in that the APN-OI Replacement field is not applied. See clause TS 23.401 [13] for more details.

If the MUE provides an APN for a PDN, this APN is then used to derive the PDN GW identity, as specified for the case of HSS provided APN, if one of the subscription contexts allows for this APN.

If there is an existing PDN connection to the same APN used to derive the PDN GW address, the same PDN GW shall be selected.

As part of PDN GW selection, an IP address of the assigned PDN GW may be provided to the MUE for use with host based mobility as defined in TS 23.402 [5], if the PDN GW supports host-based mobility for inter-access mobility towards accesses where host-based mobility can be used. If a MUE explicitly requests the address of the PDN GW and the PDN GW supports host based mobility then the PDN GW address shall be returned to the MUE.

7.4 Support for Application / Service Layer Rate Adaptation

The E-UTRAN/UTRAN and the MUE support RFC 3168 [20] Explicit Congestion Notification (ECN), as described in TS 36.300 "Evolved Universal Terrestrial Radio Access (E-UTRA) and Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Overall

Description; Stage 2 [17], ETSI TS 25.401 UTRAN Overall Description [21], and ETSI TS 26.114 IMS; Multimedia Telephony; Media Handling and Interaction [22].

The IP level ECN scheme enables the E-UTRAN/UTRAN to trigger a rate adaptation scheme at the application / service / transport layer. To make sufficient time available for end-to-end codec rate adaptation the E-UTRAN/UTRAN should attempt to not drop any packets on a bearer for a default grace period of at least 500 ms after it has indicated congestion with ECN on the bearer for packets within the packet delay budget. During this ECN grace period the E-UTRAN/UTRAN should also attempt to meet the QoS Class Identifier (QCI) characteristics / QoS class associated with the bearer.

NOTE 1: Note that the receiving end-point should interpret all ECN-CE signals received within one end-to-end round-trip time as one "congestion event" (see IETF RFC 3168 [20] and TS 26.114 [22]).

The MBR of a particular GBR bearer may be set larger than the GBR.

Note 2: Enforcement of APN-AMBR / UE-AMBR is independent of whether the MBR of a particular GBR bearer has been set larger than the GBR (see TS 23.401 [13].

The EPC does not support E-UTRAN/UTRAN-initiated "QoS re-negotiation". That is, the EPC does not support an eNodeB/RNC initiated bearer modification procedure. If an eNodeB/RNC can no longer sustain the GBR of an active GBR bearer then the eNodeB/RNC should simply trigger a deactivation of that bearer.

7.5 Session Management – QoS and interaction with PCC Functionality

The interaction between QoS management and Policy and Charging Control is a key issue when coordinating multiple connections and network accesses. It is suggested that the multi-connection architecture aligns closely to the PCC model. In the following, the network access activation (dedicated bearer activation) is shown as explicit actions.

7.5.1 Dedicated Bearer Activation

The dedicated bearer activation procedure for a GPRS Tunneling Protocol (GTP) based on S5 and S8 reference points is depicted in Figure 11, see Ref. [13].

Note 1: Steps 3-10 are common for architecture variants with GPRS Tunnelling Protocol (GTP) based S5 and S8 reference points and Proxy Mobile IP (PMIP)-based S5 and S8 reference points. For a PMIP-based S5 and S8, procedure steps (A) and (B) are defined in TS 23.402 [5]. Steps 1, 2, 11 and 12 concern GTP based S5 and S8 reference points.

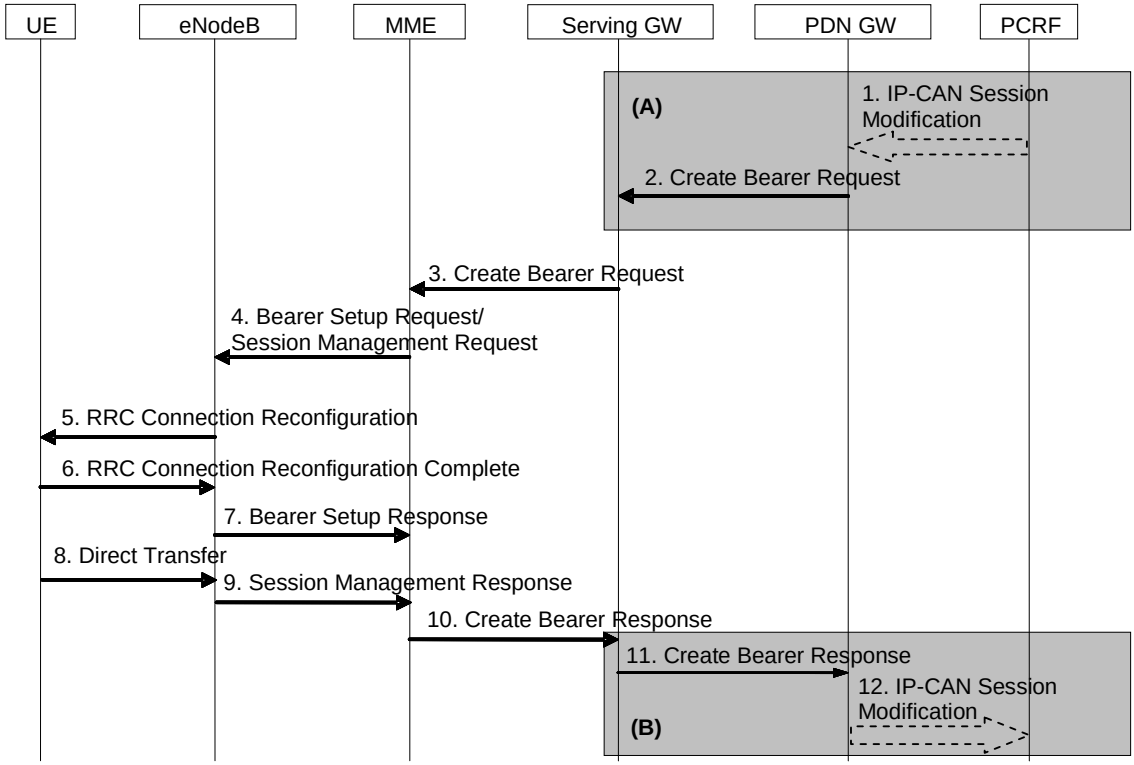

Figure 11 Dedicated Bearer Activation Procedure [13]

1. If dynamic PCC is deployed, the Policy and Charging Rules Function (PCRF) sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP-CAN Session Modification procedure or to the PCRF response in the Policy and Charging Control Enforcement Function (PCEF) initiated IP-CAN Session Modification procedure as defined in TS 23.203 [6], up to the point that the PDN GW requests IP-CAN Bearer Signalling. The PCC decision provision message may indicate that User Location Information and/or MUE Time Zone and/or User CSG Information is to be provided to the PCRF as defined in TS 23.203 [4]. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

2. The PDN GW uses this QoS policy to assign the EPS Bearer QoS; i.e., it assigns the values to the bearer level QoS parameters QCI, ARP, GBR and MBR; see TS 23.401 [13]. The PGW generates a Charging Id for the dedicated bearer. The PDN GW sends a Create Bearer Request message (IMSI, Procedure Transaction Id (PTI), EPS Bearer QoS, Traffic Flow Template (TFT), S5/S8 Tunnel Endpoint Identifier (TEID), Charging Id, Linked EPS Bearer Identity (LBI), Protocol Configuration Options) to the Serving GW, the LBI is the EPS Bearer Identity of the default bearer. The PTI parameter is only used when the procedure was initiated by a MUE Requested Bearer Resource Modification Procedure. Protocol Configuration Options may be used to transfer application level parameters between the MUE and the PDN GW, see TS 23.228 [23], and are sent transparently through the Mobility Management Entity (MME) and the Serving GW.

   Note 2: The Protocol Configuration Options (PCO) is sent in the dedicated bearer activation procedure either in response to a PCO received from the UE, or without the need to send a response to a MUE provided PCO; e.g., when the network wants the bearer to be dedicated for IMS signalling.

3. The Serving GW sends the Create Bearer Request (IMSI, PTI, EPS Bearer QoS, TFT, S1-TEID, PDN GW TEID (GTP-based S5/S8), LBI, Protocol Configuration Options) message to the MME. If the MUE is in ECM-IDLE state the MME will trigger the Network Triggered Service Request from step 3. In that case the following steps 4-7 may be combined into Network Triggered Service Request procedure or be performed standalone.

Note 3: If Idle-mode Signalling Reduction (ISR) is activated and the Serving GW does not have a downlink S1-U and the SGSN has notified the Serving GW that the MUE has moved to PMM-IDLE or STANDBY state, the Serving GW sends Downlink Data Notification to trigger MME and SGSN to page the MUE before sending the Create Bearer Request message.

4. The MME selects an EPS Bearer Identity, which has not yet been assigned to the UE. The MME then builds a Session Management Request including the PTI, TFT, EPS Bearer QoS parameters (excluding ARP), Protocol Configuration Options, the EPS Bearer Identity and the Linked EPS Bearer Identity (LBI). If the MUE has UTRAN or GERAN capabilities and the network supports mobility to UTRAN or GERAN, the MME uses the EPS bearer QoS parameters to derive the corresponding PDP context parameters QoS Negotiated (R99 QoS profile), Radio Priority, Packet Flow Id and TI and includes them in the Session Management Request. If the MUE indicated in the MUE Network Capability it does not support BSS packet flow procedures, then the MME shall not include the Packet Flow Id. The MME then signals the Bearer Setup Request (EPS Bearer Identity, EPS Bearer QoS, Session Management Request, S1-TEID) message to the eNodeB.

5. The eNodeB maps the EPS Bearer QoS to the Radio Bearer QoS. It then signals a RRC Connection Reconfiguration (Radio Bearer QoS, Session Management Request, EPS RB Identity) message to the UE. The MUE shall store the QoS Negotiated, Radio Priority, Packet Flow Id and TI, which it received in the Session Management Request, for use when accessing via GERAN or UTRAN. The MUE Non-Access Stratum (NAS) stores the EPS Bearer Identity and links the dedicated bearer to the default bearer indicated by the Linked EPS Bearer Identity (LBI). The MUE uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the radio bearer. The MUE may provide the EPS Bearer QoS parameters to the application handling the traffic flow. The application usage of the EPS Bearer QoS is implementation dependent. The MUE shall not reject the RRC Connection Reconfiguration on the basis of the EPS Bearer QoS parameters contained in the Session Management Request.

   Note: The details of the Radio Bearer QoS are specified in TS 36.300 [17].

6. The MUE acknowledges the radio bearer activation to the eNodeB with a RRC Connection Reconfiguration Complete message.

7. The eNodeB acknowledges the bearer activation to the MME with a Bearer Setup Response (EPS Bearer Identity, S1-TEID) message. The eNodeB indicates whether the requested EPS Bearer QoS could be allocated or not.

   The MME shall be prepared to receive this message either before or after the Session Management Response message, sent in step 9.

8. The MUE NAS layer builds a Session Management Response including EPS Bearer Identity. The MUE then sends a Direct Transfer (Session Management Response) message to the eNodeB.

9. The eNodeB sends an Uplink NAS Transport (Session Management Response) message to the MME.

10. Upon reception of the Bearer Setup Response message in step 7 and the Session Management Response message in step 9, the MME acknowledges the bearer activation to the Serving GW by sending a Create Bearer Response (EPS Bearer Identity, S1-TEID, User Location Information (ECGI), User CSG Information) message.

11. The Serving GW acknowledges the bearer activation to the PDN GW by sending a Create Bearer Response (EPS Bearer Identity, S5 and S8 reference points - Tunnel Endpoint Identifier (TEID), User Location Information (ECGI), User CSG Information) message.

12. If the dedicated bearer activation procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not, allowing the completion of the PCRF-Initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], after the completion of IP-CAN bearer signalling. If requested by the PCRF the PDN GW indicates User Location Information and/or MUE Time Zone and/or User CSG Information to the PCRF as defined in TS 23.203 [4].

Note 4: The exact signalling of step 1 and 12; e.g., for local break-out, is outside the scope of this specification. This signalling and its interaction with the dedicated bearer activation procedure are to be specified in TS 23.203 [4].

7.5.2 Bearer Modification with Bearer QoS update

In the following, similarly to the previous clause, the PDN GW initiated bearer modification with bearer QoS update is shown as explicit actions. In the Aggregation scenario of the multi-connection functional architecture if the service data flows are changed or if a service data flow is aggregated to or removed from an active bearer the architecture should mimic the 3GPP model.

7.5.3 PDN GW Initiated Bearer Modification with Bearer QoS Update

The PDN GW initiated bearer modification procedure (including EPS Bearer QoS update) for a GTP based S5 and S8 reference points is depicted in figure 12, see TS 23.401 [13]. This procedure is used in cases when one or several of the EPS Bearer QoS parameters QCI, GBR, MBR or ARP are modified including the QCI or the ARP of the default EPS bearer; e.g., due to the HSS Initiated Subscribed QoS Modification procedure or to modify the APN-AMBR. Modification from a QCI of resource type non-GBR to a QCI of resource type GBR and vice versa is not supported by this procedure.

NOTE 1: The QCI of an existing dedicated bearer should only be modified if no additional bearer can be established with the desired QCI.

NOTE 2: Steps 3-10 are common for architecture variants with GTP based S5 and S8 reference points and PMIP-based S5 and S8 reference points. For a PMIP-based S5 and S8 reference points, procedure steps (A) and (B) are defined in TS 23.402 [5]. Steps 1, 2, 11 and 12 concern GTP based S5 and S8 reference points.

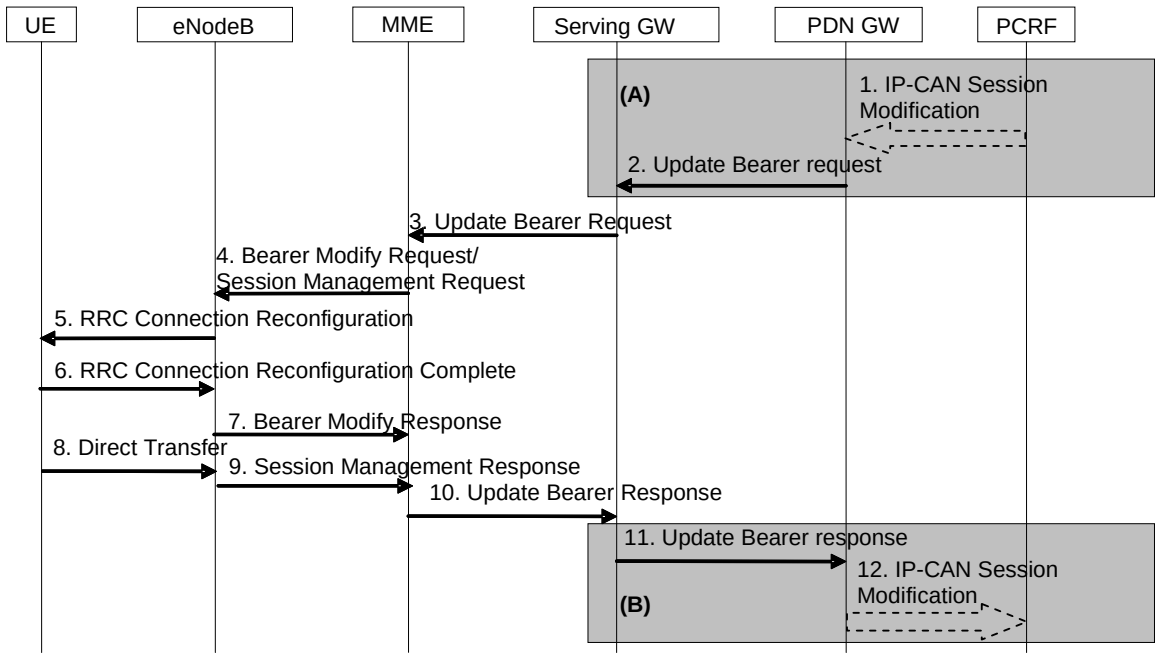

Figure 12 Dedicated Bearer Activation Procedure [13]

1. If dynamic PCC is deployed, the PCRF sends a PCC decision provision (QoS policy) message to the PDN GW. This corresponds to the initial steps of the PCRF-Initiated IP-CAN Session Modification procedure or to the PCRF response in the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], up to the point that the PDN GW requests IP-CAN Bearer Signalling. The PCC decision provision message may indicate that User Location Information and/or MUE Time Zone and/or User CSG Information is to be provided to the PCRF as defined in TS 23.203 [4]. If dynamic PCC is not deployed, the PDN GW may apply local QoS policy.

2. The PDN GW uses this QoS policy to determine that the authorized QoS of a service data flow has changed or that a service data flow shall be aggregated to or removed from an active bearer. The PDN GW generates the TFT and updates the EPS Bearer QoS to match the traffic flow aggregate. The PDN GW then sends the Update Bearer Request (PTI, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, TFT) message to the Serving GW. The Procedure Transaction Id (PTI) parameter is used when the procedure was initiated by a MUE Requested Bearer Resource Modification Procedure. For APN-AMBR, the EPS bearer identity must refer to a non-GBR bearer.

3. The Serving GW sends the Update Bearer Request (PTI, EPS Bearer Identity, EPS Bearer QoS, TFT, APN-AMBR) message to the MME. If the MUE is in ECM-IDLE state the MME will trigger the Network Triggered Service Request from step 3. In that case the following steps 4-7 may be combined into Network Triggered Service Request procedure or be performed standalone. If only the QoS parameter ARP is modified and if the MUE is in ECM IDLE state the MME shall skip the Network Triggered Service Request. In that case the following steps 4-9 are also skipped.

   NOTE 3: If ISR is activated and the Serving GW does not have a downlink S1-U and the SGSN has notified the Serving GW that the MUE has moved to PMM-IDLE or STANDBY state, the Serving GW sends Downlink Data Notification to trigger MME and SGSN to page the MUE before sending the Update Bearer Request message.

4. The MME builds a Session Management Request including the PTI, EPS Bearer QoS parameters (excluding ARP), TFT, APN-AMBR and EPS Bearer Identity. If the MUE has UTRAN or GERAN capabilities and the network supports mobility to UTRAN or GERAN, the MME uses the EPS Bearer QoS parameters to derive the corresponding PDP context parameters QoS Negotiated (R99 QoS profile), Radio Priority and Packet Flow Id and includes them in the Session Management Request. If the MUE indicated in the MUE Network Capability it does not support BSS packet flow procedures, then the MME shall not include the Packet Flow Id. If the APN-AMBR has changed the MME may update the UE-AMBR if appropriate. The MME then sends the Bearer Modify Request (EPS Bearer Identity, EPS Bearer QoS, Session Management Request, UE-AMBR) message to the eNodeB.

5. The eNodeB maps the modified EPS Bearer QoS to the Radio Bearer QoS. It then signals a RRC Connection Reconfiguration (Radio Bearer QoS, Session Management Request, EPS RB Identity) message to the MUE. The MUE shall store the QoS Negotiated, Radio Priority, Packet Flow Id, which it received in the Session Management Request, for use when accessing via GERAN or UTRAN. If the APN-AMBR has changed, the MUE stores the modified APN-AMBR value and sets the MBR parameter of the corresponding non-GBR PDP contexts (of this PDN connection) to the new value. The MUE uses the uplink packet filter (UL TFT) to determine the mapping of traffic flows to the radio bearer. The MUE may provide EPS Bearer QoS parameters to the application handling the traffic flow(s). The application usage of the EPS Bearer QoS is implementation dependent. The MUE shall not reject the Radio Bearer Modify Request on the basis of the EPS Bearer QoS parameters

contained in the Session Management Request. The MUE shall set its Temporary Identifier used in Next update (TIN) to Globally Unique Temporary Identity ("GUTI") if the modified EPS bearer was established before ISR activation.

NOTE 4: The details of the Radio Bearer QoS are specified in TS 36.300 [17].

6. The MUE acknowledges the radio bearer modification to the eNodeB with a RRC Connection Reconfiguration Complete message.

7. The eNodeB acknowledges the bearer modification to the MME with a Bearer Modify Response (EPS Bearer Identity) message. With this message, the eNodeB indicates whether the requested EPS Bearer QoS could be allocated or not.

   The MME shall be prepared to receive this message either before or after the Session Management Response message (sent in step 9).

8. The MUE NAS layer builds a Session Management Response including EPS Bearer Identity. The MUE then sends a Direct Transfer (Session Management Response) message to the eNodeB.

9. The eNodeB sends an Uplink NAS Transport (Session Management Response) message to the MME.

10. Upon reception of the Bearer Modify Response message in step 7 and the Session Management Response message in step 9, the MME acknowledges the bearer modification to the Serving GW by sending an Update Bearer Response (EPS Bearer Identity, User Location Information (ECGI), User CSG Information) message.

11. The Serving GW acknowledges the bearer modification to the PDN GW by sending an Update Bearer Response (EPS Bearer Identity, User Location Information (ECGI), User CSG Information) message.

12. If the Bearer modification procedure was triggered by a PCC Decision Provision message from the PCRF, the PDN GW indicates to the PCRF whether the requested PCC decision (QoS policy) could be enforced or not by sending a Provision Ack message allowing the completion of the PCRF-Initiated IP-CAN Session Modification procedure or the PCEF initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4], after the completion of IP-CAN bearer signalling. If requested by the PCRF the PDN GW indicates User Location Information and/or MUE Time Zone and/or User CSG Information to the PCRF as defined in TS 23.203 [4].

    NOTE 5: The exact signalling of step 1 and 12; e.g., for local break-out and its interaction with the bearer activation procedure are specified in TS 23.203 [4].

7.5.4 HSS Initiated Subscribed QoS Modification

In the multi-connection functional architecture the (MUP-FE) and (MR-FE) in charge of storing functionality data related to: subscription information, allowed QoS, location information, presence, available access information authentication types, home roaming operator lists, multi-connection policy decisions, and others, has homologous functionality as the information stored in the HSS. It is therefore encouraged the alignment and compartmentalization of the multi-connection architecture and functionality of its functional entities to that of the LTE PCC model.

As in previous clauses on QoS coverage, the following example on HSS initiated subscribed QoS modification analyses. The HSS Initiated Subscribed QoS Modification for a GTP-based S5 and S8 reference points is depicted in Figure 13, see TS 23.401 [13].

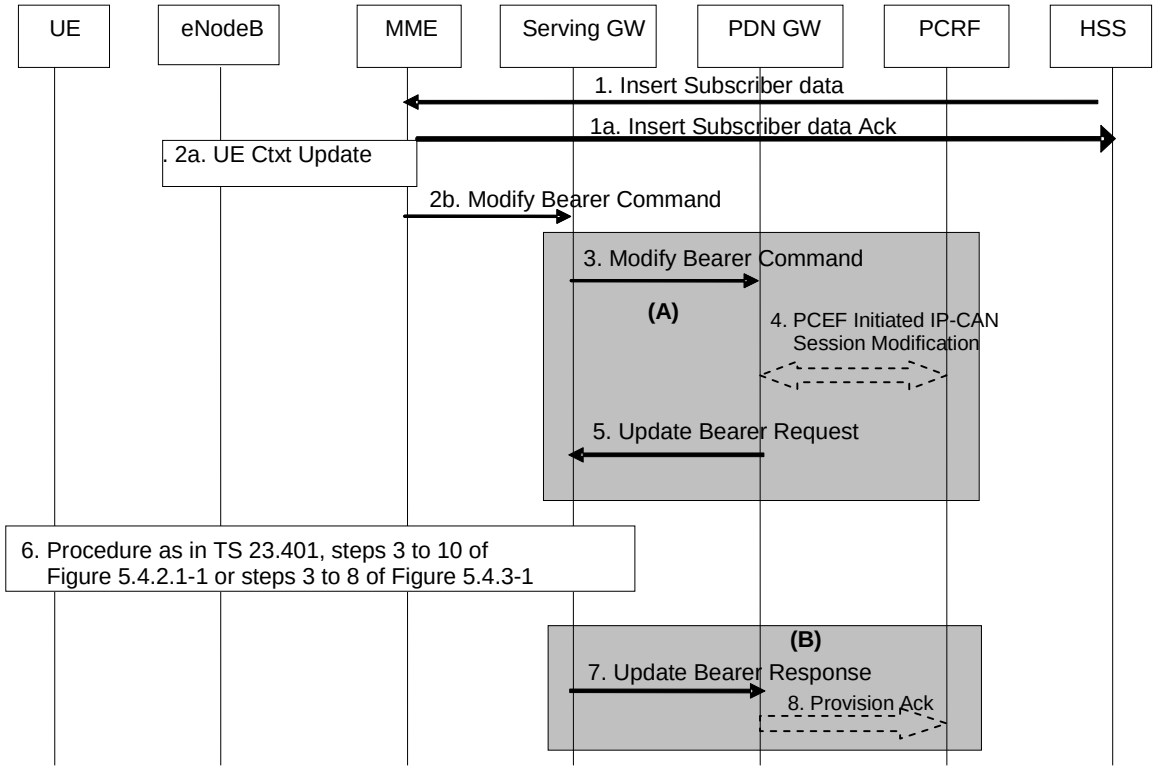

Figure 13 HSS Initiated Subscribed QoS Modification [13]

NOTE 1: For a PMIP-based S5/S8, procedure steps (A) and steps (B) are defined in TS 23.402 [5]. Steps 3, 4, 5, 7 and 8 concern GTP based S5 and S8 reference points.

1. The HSS sends an Insert Subscriber Data (IMSI, Subscription Data) message to the Mobility Management Entity (MME). The Subscription Data includes EPS subscribed QoS (QCI, ARP) and the subscribed UE-AMBR and APN-AMBR.

1a. The MME updates the stored Subscription Data and acknowledges the Insert Subscriber Data message by returning an Insert Subscriber Data Ack (IMSI) message to the HSS.

2a. If only the subscribed UE-AMBR has been modified, the MME calculates a new UE-AMBR value and may then signal a modified UE-AMBR value to the eNodeB by using S1-AP MUE Context Modification Procedure. The HSS Initiated Subscribed QoS Modification Procedure ends after completion of the MUE Context Modification Procedure.

2b. If the QCI and/or ARP and/or subscribed APN-AMBR has been modified and there is related active PDN connection with the modified QoS Profile the MME sends the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN-AMBR) message to the Serving GW. The EPS Bearer Identity identifies the default bearer of the affected PDN connection. The EPS Bearer QoS contains the EPS subscribed QoS profile to be updated.

3. The Serving GW sends the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN-AMBR) message to the PDN GW.

4. If PCC infrastructure is deployed, the PDN GW informs the PCRF about the updated EPS Bearer QoS and APN-AMBR. The PCRF sends new updated PCC decision to the PDN GW. This corresponds to the PCEF-initiated IP-CAN Session Modification procedure as defined in TS 23.203 [4].

   The PCRF may modify the APN-AMBR and the QoS parameters (QCI and ARP) associated with the default bearer in the response to the PDN GW as defined in TS 23.203 [4].

5. The PDN GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the PDN GW shall also modify all dedicated EPS bearers having the previously subscribed ARP value unless superseded by PCRF decision. The PDN GW then sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS, TFT, APN-AMBR) message to the Serving GW.

   NOTE 2: As no PTI is included the MME use protocol specific details, as described in TS 29.274 [24], to determine if the Update Bearer Request was triggered by this procedure or not.

6. If the QCI and/or ARP parameter(s) have been modified, steps 3 to 10, as described in Figure 13, are invoked. If neither the QCI nor the ARP have been modified, but instead only the APN-AMBR was updated, steps 3 to 8, as described in TS 23.401 [13] are invoked.

7. The Serving GW acknowledges the bearer modification to the PDN GW by sending an Update Bearer Response (EPS Bearer Identity, User Location Information (ECGI), User CSG Information) message. If the bearer modification fails the PDN GW deletes the concerned EPS Bearer.

8. The PDN GW indicates to the PCRF whether the requested PCC decision was enforced or not by sending a Provision Ack message.

7.6 Mapping between EPS and Release 99 QoS Parameters

Following the mapping example of Table 3 “Case Example of QoS Mapping Among Different Access Networks”, a more descriptive mapping regarding only QoS parameters is given below. It shows examples of radio access technologies mapping sets, these are helpful to follow for each component access network in the multi-connection architecture.

Specifically, it is shown how the QoS parameter values of an EPS bearer are mapped to/from the Release 99 QoS parameter values of a PDP context in PDN GW, S4-SGSN and MME, see TS 23.401 [13].

Within this clause and within the RAT, different names are used for the QoS parameters of a PDP context; e.g., "R99 QoS profile" and "R99 QoS parameters", but nevertheless the whole QoS IE as described in TS 24.008 [25] is referred to including the R99 and R97/98 QoS attributes. This means that the MME performs QoS mapping, populates and forwards both R99 and R97/98 QoS attributes towards the MUE in S1 mode, if the MUE supports A/Gb mode or Iu mode or both. The MME also performs QoS mapping, populates and forwards both R99 and R97/98 QoS attributes also on Interface between SGSN and GGSN (Gn) when deployed in the interoperation scenarios. The Reference Point between S-GW and SGSN Rel.8 (S4)-SGSN performs QoS mapping, populates and forwards either both R99 and R97/98 QoS attributes or only R97/98 QoS attributes towards the MUE in Iu mode and A/Gb mode. The P-GW performs QoS mapping, populates and forwards both R99 and R97/98 QoS attributes over Gn/Gp when deployed in the interoperation scenarios.

The following mapping rules hold:

- There is a one-to-one mapping between an EPS bearer and a PDP context
- When EPS bearer QoS parameters are mapped to Release 99 QoS parameters the pre-emption capability and the pre-emption vulnerability information of the EPS bearer ARP are ignored and the priority of the EPS bearer parameter ARP is mapped to the Release 99 bearer parameter ARP

Table 4 Mapping of EPS Bearer ARP to Release 99 Bearer Parameter ARP [13]

EPS Bearer ARP Priority Value	Release 99 bearer parameter ARP Value
1 to H	1
H+1 to M	2
M+1 to 15	3

When Release 99 QoS parameters are mapped to EPS bearer QoS parameters the pre-emption capability and the pre-emption vulnerability information of the EPS bearer ARP are set based on operator policy in the entity that performs the mapping. The Release 99 bearer parameter ARP is mapped to the priority level information of the EPS bearer parameter ARP as described in Table 5 below.

The values of H (high priority) and M (medium priority) can be set according to operator requirements to ensure proper treatment of users with higher priority level information. The minimum value of H is 1. The minimum value of M is H+1.

From Release 9 onwards, the priority of the EPS bearer parameter ARP is mapped one-to-one to/from the Evolved ARP parameter of a PDP context, if the network supports this parameter.

Table 5 Mapping of Release 99 bearer parameter ARP to EPS bearer ARP [13]

Release 99 bearer parameter ARP Value	EPS Bearer ARP Priority Value
1	1
2	H+1
3	M+1

NOTE 1: The setting of the values for H and M may be based on the SGSN mapping from the Release 99 bearer parameter ARP to the ARP parameter that is used for UTRAN/GERAN.

NOTE 2: After a handover from UTRAN/GERAN to E-UTRAN the ARP parameter of the EPS bearer can be modified by the P-GW to re-assign the appropriate priority level, pre-emption capability and pre-emption vulnerability setting.

NOTE 3: A mapping from the EPS bearer parameter ARP to the Release 99 bearer parameter ARP is not required for a P-GW when connected to an SGSN via the Gn/Gp interfaces, since any change of the bearer ARP parameter may get overwritten by the SGSN due to subscription enforcement. However, the P-GW should not combine services with different EPS bearer ARP values onto the same PDP context to enable a modification of the bearer ARP without impacting the assignment of services to bearers after a handover to E-UTRAN.

- The EPS bearer parameters GBR and MBR of a GBR EPS bearer are mapped one-to-one to/from the Release 99 bearer parameters GBR and MBR of a PDP context associated with Traffic class 'conversational' or 'streaming'

- When EPS bearer QoS parameters are mapped to Release 99 QoS parameters the Release 99 bearer parameter MBR of PDP contexts associated with Traffic Class 'interactive' or 'background' is set equal to the value of the authorized APN-AMBR. If the APN-AMBR is modified while the MUE accesses the EPS through E-UTRAN, the MUE shall also set the Release 99 bearer parameter MBR to the new APN-AMBR value for all non-GBR PDP contexts of this PDN connection. The P-GW shall enforce the APN-AMBR across all PDP contexts with Traffic Class 'interactive' and 'background' for that APN. The MME or S4-SGSN may attempt to transfer APN-AMBR and UE-AMBR to a Gn/Gp SGSN

- When Release 99 QoS parameters are mapped to EPS bearer QoS parameters the AMBR for the corresponding APN shall be set equal to the MBR value of the subscribed QoS profile. At handover from a Gn/Gp SGSN the MME or S4-SGSN shall provide this APN-AMBR value, if not explicitly received from the Gn/Gp SGSN, to the Serving GW and the PDN GW for each PDN connection. It is required that the subscribed MBR in the HLR/HSS is set to the desired APN-AMBR value for all subscribed APNs which may lead to a selection of a P-GW. The MUE derives the APN-AMBR from the value of the MBR of a PDP context created by the PDP Context Activation Procedure as described in TS 23.060 [12]

  NOTE 5: If the pre-Rel-8 MUE with the updated subscribed MBR is connected to a GGSN, the GGSN can downgrade the MBR of the PDP contexts based on either local policy or PCC (where the MBR per QCI information is provided to the PCEF). It is assumed here that a MUE was implemented before and after Release 8.

  NOTE 6: From Release 9 onwards, the APN-AMBR is available on Gn/Gp.

- For handover from a Gn/Gp SGSN and if the MME does not receive AMBR values from the Gn/Gp SGSN, the MME provides a local UE-AMBR to the eNodeB until MME gets the EPS subscribed UE-AMBR. When the MME gets the subscribed UE-AMBR value from the HSS, it calculates the UE-AMBR (UE-AMBR=MIN (subscribed UE-AMBR, sum APN-AMBR of all active APNs)). Then it compares this value with the local UE-AMBR and if the local UE-

AMBR is different from the corresponding derived UE-AMBR, the MME initiates HSS Initiated Subscribed QoS Modification procedure to notify the derived UE-AMBR to the eNodeB

NOTE 7: The local UE-AMBR may be for example based on the sum of the APN-AMBR values of all active APNs of the MUE or on internal configuration.

- A standardized value of the EPS bearer parameter QCI is mapped one-to-one to/from values of the Release 99 parameters Traffic Class, Traffic Handling Priority, Signalling Indication, and Source Statistics Descriptor as shown in Table 7

NOTE 8: When mapping to QCI=2 or QCI=3, the Release 99 parameter Transfer Delay is used in addition to the four Release 99 parameters mentioned above.

- When EPS bearer QoS parameters are mapped to Release 99 QoS parameters the setting of the values of the Release 99 parameters Transfer Delay and SDU Error Ratio is derived from the corresponding QCI's Packet Delay Budget and Packet Loss Rate, respectively. When Packet Loss Rate parameter is further mapped to Release 99 QoS parameter Reliability Class (Ref. TS 23.107 [26], see Table 6 below), the Residual BER is considered <= $2*10^{-4}$. Also when Release 99 QoS parameters are mapped to EPS bearer QoS parameters the values of the Release 99 parameter SDU Error Ratio are ignored

Table 6 Rules for determining R97/98 attributes from R99 attributes [26]

Resulting R97/98 Attribute		Derived from R99 Attribute	
Name	**Value**	**Value**	**Name**
Delay class	1	conversational	Traffic class
	1	streaming	Traffic class
	1	Interactive	Traffic class
		1	Traffic handling priority
	2	Interactive	Traffic class
		2	Traffic handling priority
	3	Interactive	Traffic class
		3	Traffic handling priority
	4	Background	Traffic class
Reliability class	3	<= 10^{-5}	SDU error ratio (NOTE 4)
	3	10^{-5} < x <= $5*10^{-4}$	SDU error ratio
	4	> $5*10^{-4}$	SDU error ratio
		<= $2*10^{-4}$	Residual bit error ratio
	5	> $5*10^{-4}$	SDU error ratio
		> $2*10^{-4}$	Residual bit error ratio
Peak throughput class	1	< 16	Maximum bitrate [kbps]
	2	16 <= x < 32	
	3	32 <= x < 64	
	4	64 <= x < 128	
	5	128 <= x < 256	
	6	256 <= x < 512	
	7	512 <= x < 1024	
	8	1024 <= x < 2048	
	9	>= 2048	
Precedence class	1	1	Allocation/retention priority
	2	2	
	3	3	
Mean throughput class	Always set to 31	-	
Reordering Required (Information in the SGSN and the GGSN PDP Contexts)	yes'	yes'	Delivery order
	'no'	'no'	
Precedence class	1	1	Priority Level of the Evolved Allocation/retention priority
	2	H+1	
	3	M+1	

- The setting of the values of all other Release 99 QoS is based on operator policy pre-configured in the MME and S4-SGSN

- In networks that support mobility from E-UTRAN to UTRAN/GERAN, if the MUE has indicated support of UTRAN or GERAN, the EPS network shall provide the MUE with the Release 99 QoS parameters in addition to the EPS bearer QoS parameters within EPS bearer signalling

Table 7 Mapping between Standardized QCIs and Release 99 QoS Parameter Values [13]

QCI	Traffic Class	Traffic Handling Priority	Signalling Indication	Source Statistics Descriptor
1	Conversational	N/A	N/A	Speech
2	Conversational	N/A	N/A	Unknown (NOTE 1)
3	Conversational	N/A	N/A	Unknown (NOTE 2)
4	Streaming	N/A	N/A	Unknown (NOTE 3)
5	Interactive	1	Yes	N/A
6	Interactive	1	No	N/A
7	Interactive	2	No	N/A
8	Interactive	3	No	N/A
9	Background	N/A	N/A	N/A

NOTE 1: When QCI 2 is mapped to Release 99 QoS parameter values, the Transfer Delay parameter is set to 150 ms. When Release 99 QoS parameter values are mapped to a QCI, QCI 2 is used for conversational/unknown if the Transfer Delay parameter is greater or equal to 150 ms.

NOTE 2: When QCI 3 is mapped to Release 99 QoS parameter values, the Transfer Delay parameter is set to 80 ms as the lowest possible value, according to TS 23.107 [26]. When Release 99 QoS parameter values are mapped to a QCI, QCI 3 is used for conversational/unknown if the Transfer Delay parameter is lower than 150 ms.

NOTE 3: When QCI 4 is mapped to Release 99 QoS parameter values, it is mapped to Streaming/Unknown. When Release 99 QoS parameter values are mapped to a QCI, Streaming/Unknown and Streaming/Speech are both mapped to QCI 4.

7.7 Standardized QoS characteristics in the Context of Policy and Charging Control Architecture

Furthermore, in the context of the Policy and Charging Control (PCC) model of the Evolved Packet System (EPS)/LTE, some special handling of the QoS parameters and functions within present and to be deployed EPS/LTE mobile networks need to be followed by the multi-connection architecture, its functions and functional elements.

As previously mentioned the QoS model in the Evolved Packet System (EPS) is followed to a certain extent in the multi-connection network. The following clauses look in detail the:

- Service level and associated individual and aggregated SDFs
- QoS parameters, as QCI, ARP, GBR, and MBR
- QoS Classes and treatments on SDFs edge-to-edge between MUE and PCEF in aggregation scenarios
- Parameters controling packet forwarding treatment
- Queue management thresholds
- Link layer protocol configuration
- Pre-configured nodes, like eNodeB
- Standardized QCI values
- Allocation and Retention Priority characteristics

after the PCC model of TS 23.203 [4]. Again, further improvements and completeness for the multi-connection architecture shall follow the instantiations in the following clauses.

The service level; i.e., per Service Data Flow (SDF) or per SDF aggregate. The QoS parameters are QCI, ARP, GBR, and MBR.

Each Service Data Flow (SDF) is associated with one and only one QoS Class Identifier (QCI). For the same IP-CAN session multiple SDFs with the same QCI and ARP can be treated as a single traffic aggregate, which is referred to as an SDF aggregate. An SDF is a special case of an SDF aggregate. The QCI is scalar that is used as a reference to node specific parameters that control packet forwarding treatment; e.g., scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, and others. These parameters have been pre-configured by the operator owning the node, for instance an eNodeB.

7.8 Standardized QCI characteristics

This Clause specifies standardized characteristics associated with standardized QCI values, see TS 23.203 [4]. The characteristics describe the packet forwarding treatment that an SDF aggregate receives edge-to-edge between the MUE and the PCEF, see Figure 14 below, in terms of the following performance characteristics:

1 Resource Type (GBR or Non-GBR).

2 Priority.

3 Packet Delay Budget.

4 Packet Error Loss Rate.

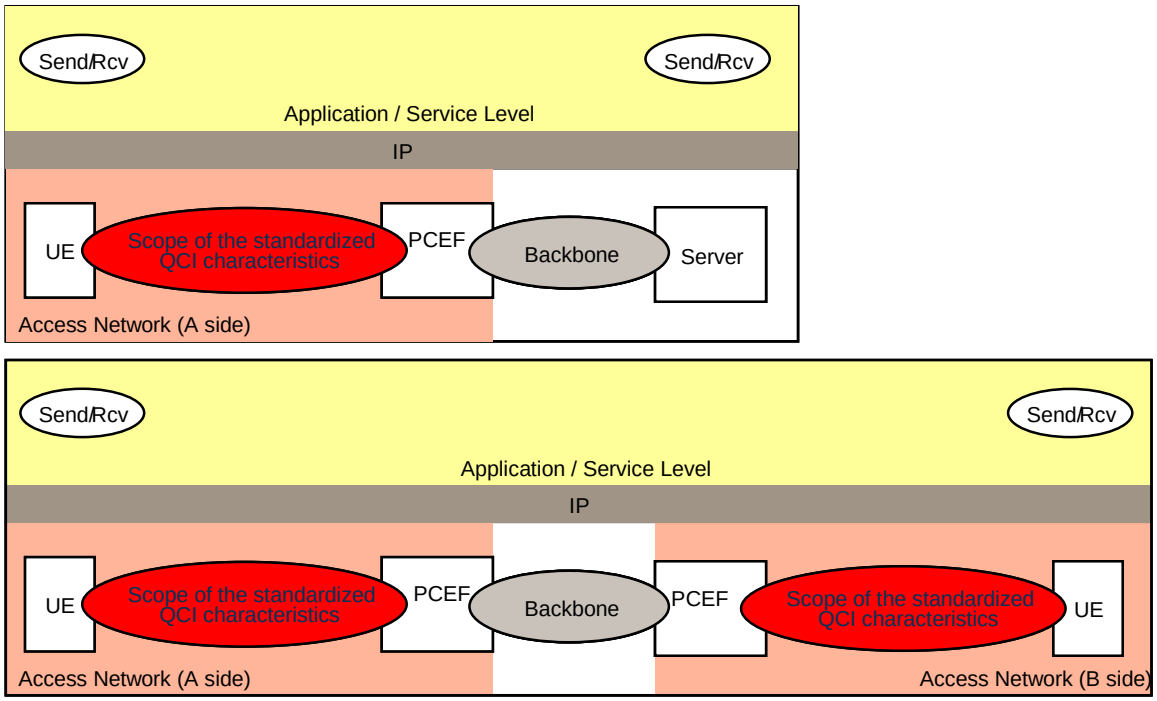

Figure 14 Scope of the Standardized QCI Characteristics for Client/Server (upper Figure) and Peer to Peer (lower Figure) Communication [4]

The standardized characteristics are not signalled on any interface. They should be understood as guidelines for the pre-configuration of node specific parameters for each QCI. The goal of standardizing a QCI with corresponding characteristics is to ensure that applications and services mapped to that QCI receive the same minimum level of QoS in multi-vendor network deployments and in case of roaming. A standardized QCI and corresponding characteristics is independent of the UE's current access (3GPP or Non-3GPP).

The one-to-one mapping of standardized QCI values to standardized characteristics is captured in Table 8 below.

Table 8 Standardized QCI characteristics [4]

QCI	Resource Type	Priority	Packet Delay Budget (NOTE 1)	Packet Error Loss Rate (NOTE 2)	Example Services
1		2	100 ms	10^{-2}	Conversational Voice

(NOTE 3)	GBR				
2 (NOTE 3)		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3)		3	50 ms	10^{-3}	Real Time Gaming
4 (NOTE 3)		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5 (NOTE 3)	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9 (NOTE 6)		9			

NOTE 1: A delay of 20 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. This delay is the average between the case where the PCEF is located "close" to the radio base station (roughly 10 ms) and the case where the PCEF is located "far" from the radio base station, e.g. in case of roaming with home routed traffic (the one-way packet delay between Europe and the US west coast is roughly 50 ms). The average takes into account that roaming is a less typical scenario. It is expected that subtracting this average delay of 20 ms from a given PDB will lead to desired end-to-end performance in most typical cases. Also, note that the PDB defines an upper bound. Actual packet delays - in particular for GBR traffic - should typically be lower than the PDB specified for a QCI as long as the UE has sufficient radio channel quality.

NOTE 2: The rate of non congestion related packet losses that may occur between a radio base station and a PCEF should be regarded to be negligible. A PELR value specified for a standardized QCI therefore applies completely to the radio interface between a UE and radio base station.

NOTE 3: This QCI is typically associated with an operator controlled service, i.e., a service where the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. In case of E-UTRAN this is the point in time when a corresponding dedicated EPS bearer is established / modified.

NOTE 4: If the network supports Multimedia Priority Services (MPS) then this QCI could be used for the prioritization of non real-time data (i.e. most typically TCP-based services/applications) of MPS subscribers.

NOTE 5: This QCI could be used for a dedicated "premium bearer" (e.g. associated with premium content) for any subscriber / subscriber group. Also in this case, the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. Alternatively, this QCI could be used for the default bearer of a UE/PDN for "premium subscribers".

NOTE 6: This QCI is typically used for the default bearer of a UE/PDN for non privileged subscribers. Note that AMBR can be used as a "tool" to provide subscriber differentiation between subscriber groups connected to the same PDN with the same QCI on the default bearer.

NOTE 7: In this Table the term UE is used as opposed to MUE to keep compatibility with its original Reference [4].

The Resource Type determines if dedicated network resources related to a service or bearer level Guaranteed Bit Rate (GBR) value are permanently allocated; e.g., by an admission control function in a radio base station. GBR SDF aggregates are therefore typically authorized "on demand" which requires dynamic policy and charging control. A Non GBR SDF aggregate may be pre-authorized through static policy and charging control.

The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the MUE and the PCEF. For a certain QCI the value of the PDB is the same in uplink and

downlink. The purpose of the PDB is to support the configuration of scheduling and link layer functions (e.g. the setting of scheduling priority weights and HARQ target operating points). The PDB shall be interpreted as a maximum delay with a confidence level of 98 percent.

NOTE 1: The PDB denotes a "soft upper bound" in the sense that an "expired" packet; e.g., a link layer SDU that has exceeded the PDB, does not need to be discarded (for instance by the Radio Link Control sub-layer (RLC) in E-UTRAN). The discarding (dropping) of packets is expected to be controlled by a queue management function; e.g., based on pre-configured dropping thresholds.

The support for Single Radio Voice Call Continuity (SRVCC) requires QCI=1 only be used for IMS speech sessions in accordance to TS 23.216 [14].

NOTE 2: Triggering SRVCC will cause service interruption and/or inconsistent service experience when using QCI=1 for non-IMS services.

Services using a Non-GBR QCI should be prepared to experience congestion related packet drops, and 98 percent of the packets that have not been dropped due to congestion should not experience a delay exceeding the QCI's PDB. This may for example occur during traffic load peaks or when the MUE becomes coverage limited.

Packets that have not been dropped due to congestion may still be subject to non congestion related packet losses (see PELR below).

Services using a GBR QCI and sending at a rate smaller than or equal to GBR can in general assume that congestion related packet drops will not occur, and 98 percent of the packets shall not experience a delay exceeding the QCI's PDB. Exceptions; e.g., transient link outages, can always occur in a radio access system which may then lead to congestion related packet drops even for services using a GBR QCI and sending at a rate smaller than or equal to GBR. Packets that have not been dropped due to congestion may still be subject to non congestion related packet losses (see PELR below).

Every QCI (GBR and Non-GBR) is associated with a Priority level. Priority level 1 is the highest Priority level. The Priority levels shall be used to differentiate between SDF aggregates of the same UE, and it shall also be used to differentiate between SDF aggregates from different UEs. Via its QCI an SDF aggregate is associated with a Priority level and a PDB. Scheduling between different SDF aggregates shall primarily be based on the PDB. If the target set by the PDB can no longer be met for one or more SDF aggregate(s) across all UEs that have sufficient radio channel quality then Priority shall be used as follows: in this case a scheduler shall meet the PDB of an SDF aggregate on Priority level N in preference to meeting the PDB of SDF aggregates on Priority level N+1 until the priority N SDF aggregate's GBR (in case of a GBR SDF aggregate) has been satisfied. Other aspects related to the treatment of traffic exceeding an SDF aggregate's GBR are out of scope of this specification.

NOTE 3: The definition (or quantification) of "sufficient radio channel quality" is out of the scope of ETSI specifications.

NOTE 4: In case of E-UTRAN a QCI's Priority level may be used as the basis for assigning the uplink priority per Radio Bearer, see TS 36.300 [17] for details.

The Packet Error Loss Rate (PELR) defines an upper bound for the rate of Service Data Units (SDUs); e.g., IP packets, that have been processed by the sender of a link layer protocol; e.g. Radio Link Control sub-layer (RLC) in E-UTRAN, but that are not successfully delivered by the corresponding receiver to the upper layer; e.g. Packet Data Convergence Protocol (PDCP) in E-UTRAN. Thus, the PELR defines an upper bound for a rate of non congestion related packet losses. The purpose of the PELR is to allow for appropriate link layer protocol configurations; e.g., RLC and Hybrid Automatic Repeat reQuest (HARQ) in E-UTRAN. For a certain QCI the value of the PELR is the same in uplink and downlink.

NOTE 5: The characteristics PDB and PELR are specified only based on application and service level requirements; i.e., those characteristics should be regarded as being access agnostic,

independent from the roaming scenario (roaming or non-roaming), and independent from operator policies.

7.9 Allocation and Retention Priority Characteristics

The QoS parameter ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The priority level defines the relative importance of a resource request. This allows deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). It can also be used to decide which existing bearers to pre-empt during resource limitations.

The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority. The pre-emption capability information defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. The pre-emption vulnerability information defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. The pre-emption capability and the pre-emption vulnerability can be either set to 'yes' or 'no'.

The ARP priority levels 1-8 should only be assigned to resources for services that are authorized to receive prioritized treatment within an operator domain; i.e. they are authorized by the serving network. The ARP priority levels 9-15 may be assigned to resources that are authorized by the home network and thus applicable when a MUE is roaming.

NOTE: This ensures that future releases may use ARP priority level 1-8 to indicate for instance emergency and other priority services within an operator domain in a backward compatible manner. This does not prevent the use of ARP priority level 1-8 in roaming situation in case appropriate roaming agreements exist that ensure a compatible use of these priority levels.

8 The multi-connection user equipment

The multi-connection architecture requires a new breed of User Equipment (UE). Figure 15 shows in a simple way how the multi-connection functional architecture discerns between a terminal having multi-connection characteristics; i.e., a multi-connection UE (MUE) and a normal UE, or Single User Equipment (SUE), see Ref. [1].

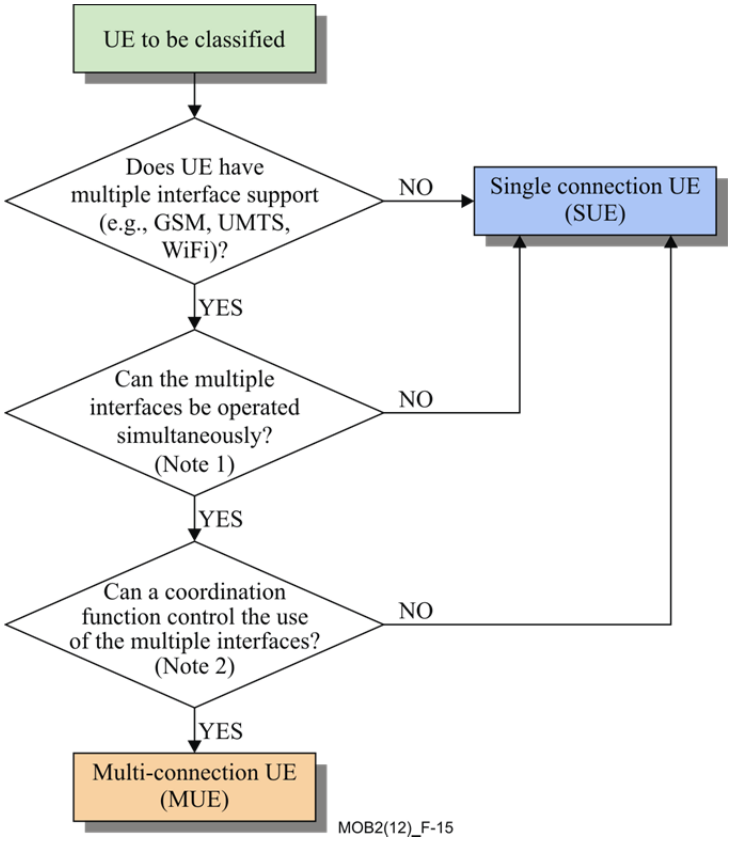

Figure 15 Discerning between SUE and MUE [1]

Note 1: The MUE is capable to run not only a number of RAT stacks, but the stacks are able to run simultaneously. A multi-connection network is capable to take advantage and offer the multi-connection features to the MUE.

Note 2: The existence of a coordinating function in the network infrastructure with its counterpart functionality embedded in the MUE makes the MUE a proper MUE.

The MUE functionality requires the support of internal management functionality, see Ref. [1], among different radio access networks, as well as coordination with the multi-connection network. This is shown in Figure 16, below.

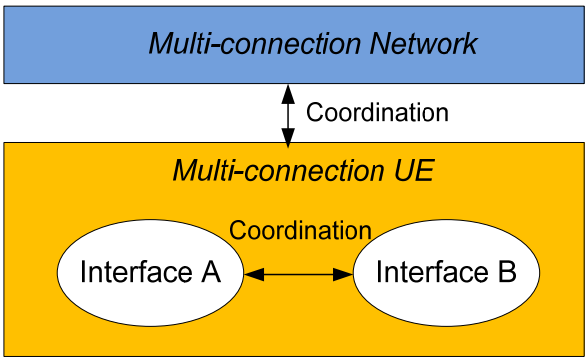

Figure 16 Characteristics of the MUE [1]

9 Resource IDs and multi-connection functional entities

Recommendation ITU-T Y.2252 (2012), "Identification and configuration of resources for Multi-Connection", see Ref. [28] describes the identification of resources and attributes given by different types of connections simultaneously at the MUE.

Ref. [28] Sets forward a description of the relationship between the multi-connection resource identifiers (IDs) at the MUE and the multi-connection Functional Entities in the network.

Figure 17 depicts the alignment between the multi-connection resource IDs in the MUE and the multi-connection FEs at network side.

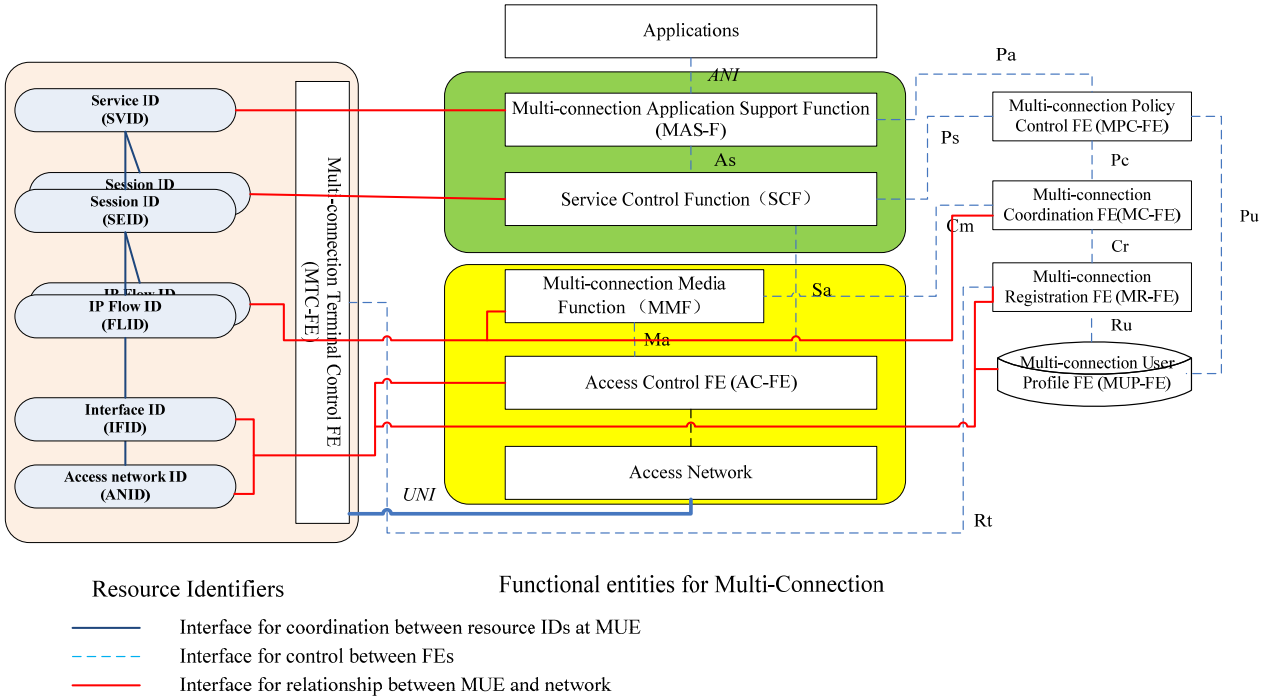

Figure 17 Resource IDs in the MUE and multi-connection FEs [28]

A MUE may exchange its multi-connection configuration information with the network through the MTC-FE via the reference point Rt. The MR-FE is responsible for managing the status of the current active MUEs, so that available resources in MUE, such as the IFID and the ANID are maintained in the MR-FE. Moreover these IDs are to be registered in the MUP-FE in order to select appropriate policies in the MUE, following subscriber's and network operator's agreements.

The Access Control Functional Entity is responsible to connect the MUE to the core network. The FE manages the current location information in the MUE, such as IFID and ANID.

The Multi-connection Media Function (MMF) is responsible to apply multiple access policies. Thus, information for configuration in the MUE is maintained and managed together with the FLID (element of transport stratum resources), the IFID, the ANID, and the subscriber's policy. These resource IDs can be obtained from the MR-FE and the MUP-FE. The FLID is also maintained in the MC-FE.

The Service Control Function (SCF) maintains the multi-connection capability at the session layer and is responsible for session continuity when the service is transferred among active connections. Therefore, the SEID is maintained in the SCF which manages the multi-connection session layer.

Finally, the SVID is maintained in the Multi-connection Application Support Function (MAS-F).

10 Analogy between the multi-connection functional architecture and that of the EPC/IMS

An initial analogy has been made in the multi-connection functional architecture to equate functionality and Functional Entities to the EPC/IMS. The comparison is depicted in Figure 18, see Ref. [1]. The Figure compares the current multi-connection functional architecture vs. the EPC and IMS models. Further comparative enhancements to the multi-connection functional architecture may take this assessment as a start point.

The architecture on top Figure is the multi-connection functional architecture, the one below is the evolved EPC and IMS architecture. The functions marked with a star "*" hint to enhancements suggested to be made to the IMS/EPC network to evolve into the multi-connection functional architecture.

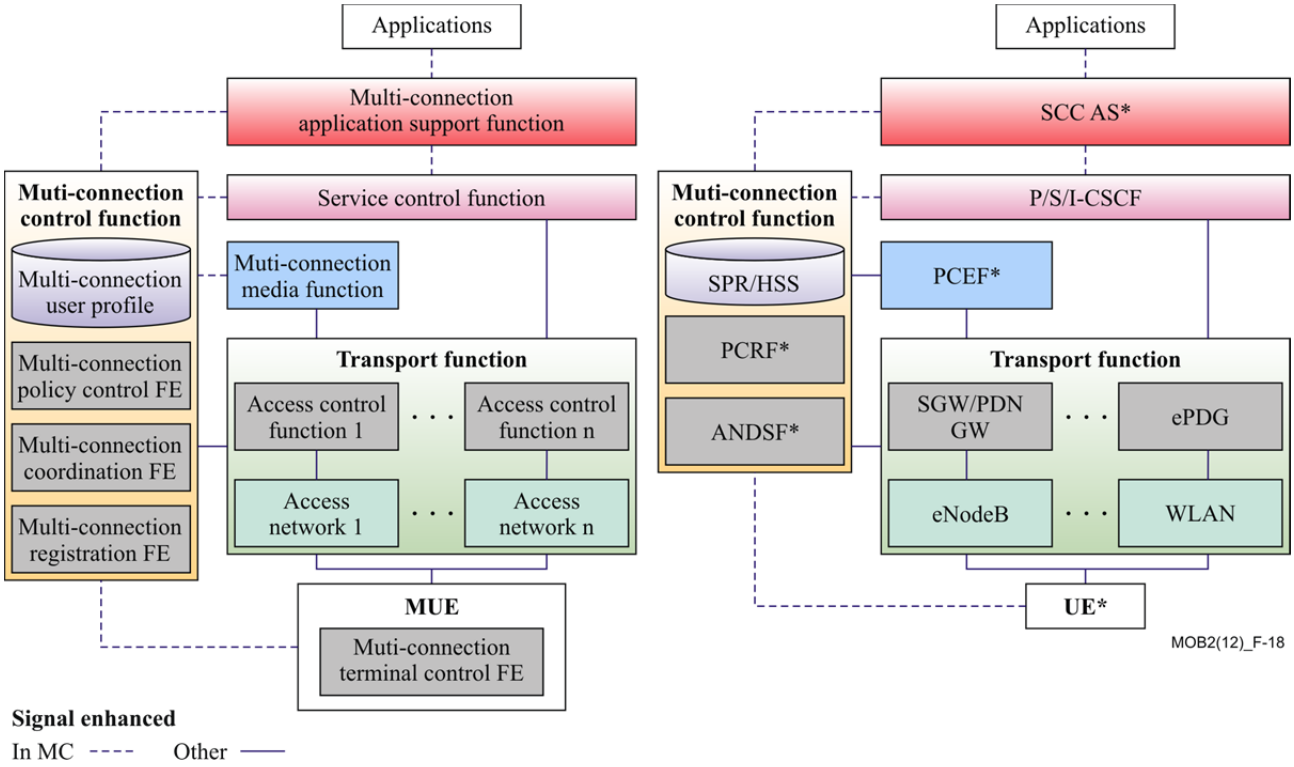

Figure 18 Comparison of the multi-connection functional architecture and the EPC/IMS model [1]

11 Analogy between the multi-connection functional architecture and that of the next generation-hotspot (NGH)/IMS

Additional interesting functional architecture analogies can be made, for instance the comparison to the Next Generation Hotspot (NGH)/IMS architecture; e.g., the architecture based on Wi-Fi Alliance (WFA)/Wireless Broadband Alliance (WBA) Hotspot2.0 and IMS. Figure 19 shows how some of the functionality of the multi-connection functional architecture maps to the NGH/IMS model, see Ref. [1].

The functions marked with a star "*" refer to a minimum functionality enhancement required as a start point to evolve the NGH/IMS architecture into the multi-connection functional architecture.

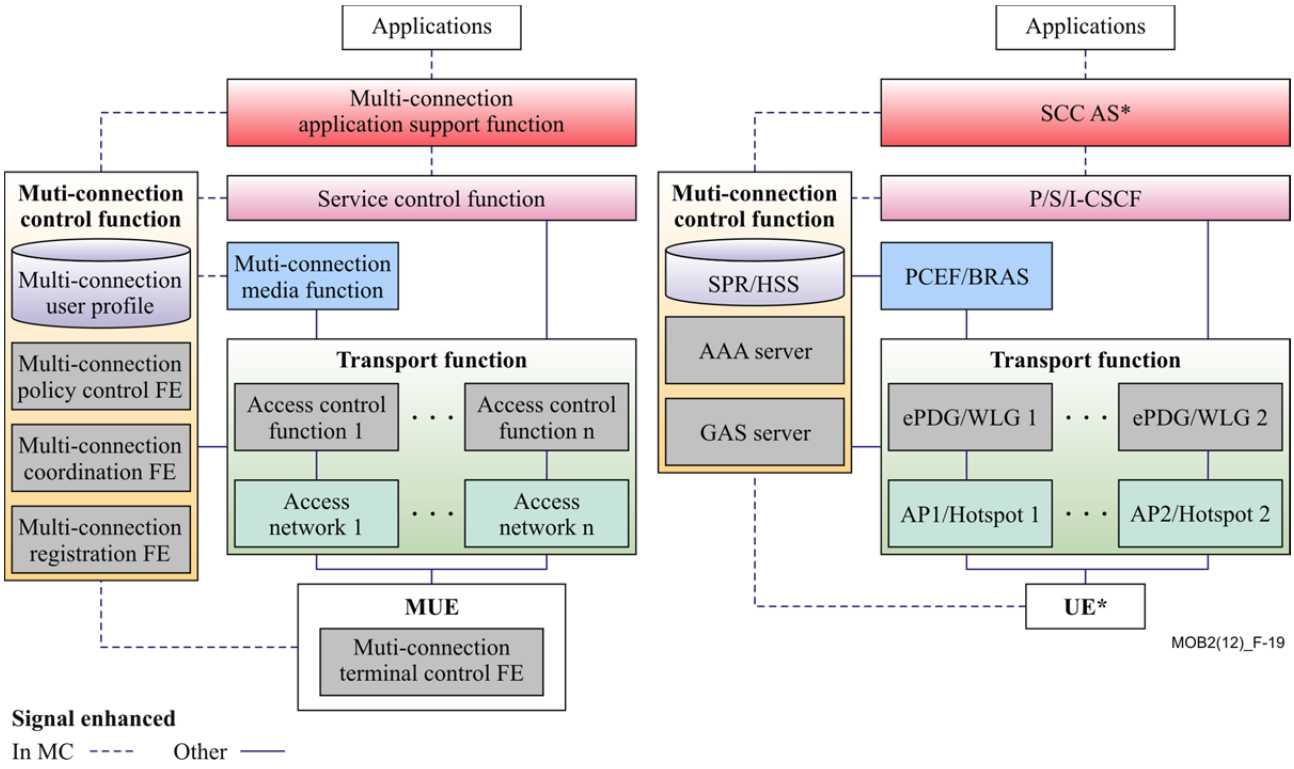

Figure 19 Analogy between the multi-connection Functional Architecture vs. NGH/IMS Model [1]

12 Conclusions

Mobile and NGN networks are currently world-wide deployed, however they lack the capability to connect subscribers' terminals and network infrastructures with more than one connection or network access actively transmitting data in parallel; of course an exception happens in the transient effect when handover takes place. Since the mid-2000's this topic started to attract attention of network designers and standards forum activities.

Because the multi-connection architecture supports a number of Use Cases, see Ref. [6], it is suggested to pursue a thorough analysis in ITU-T's Next Study Period (NSP) regarding service mechanisms to choose from in order to support each of those individual Use Cases. The service mechanisms presently offered include for instance, the dual stack, PMIP, GTP tunneling, and others, developed with the dynamic output from IETF.

Such Use Cases and applications in today's mobile smart terminals, as shown in this technical paper, portray the necessity to be supported by a multi-connection heterogeneous access network.

In a form of gap analysis, and since some of the scenarios are not yet fully supported by the multi-connection architecture functionality, an attempt is made in this technical paper to provide a positive perspective on the available technologies and techniques to provide compatibility with present mobile network techniques.

Currently, the uses cases included in the "Multi-connection Supplement in multi-connection Scenarios", see ref. [6], encompass: Multimedia Division, Load Balance, Reliability, MUE Initiated Network Selection, Network-Initiated Network Selection, Service Continuity, Bandwidth Aggregation, Service Transfer, Service Flow Duplication, and Data Transmission Rate Adjustment.

It is natural then that the multi-connection work in ITU-T shall bond efforts from standards like IETF, and IEEE to functionally couple global standards' resulting recommendations and specifications in order to offer compatibility for present and future mobile operators, both in their infrastructures and corresponding multi-connection terminals (MUEs).

The multi-connection network opens doors for a series of access technologies to interact concurrently, thus serving a single running application or multiple applications in the multi-connection terminal (MUE). These accesses vary from 2G, 3G, and LTE, to technologies like Wi-Fi and WiMAX.

In order to control and manage the diversity of access network technologies, additional techniques from LTE Policy and Charging Control (PCC), IP flow mobility, QoS, and others mechanisms are used to organize and optimize previous 2nd and 3rd generation mobile networks – including naturally LTE network nodes and corresponding reference points. These techniques take effect on the radio and core network alike. Emphasis was attempted herein to endure on the current state of the multi-connection architecture's maturity and further enhance it with such recent technological developments in IETF, and IEEE.

One way in which this was endeavoured is by suggesting the inclusion of counterpart network elements from the network and IETF complementary techniques, filling up gaps in the multi-connection network functions and Function Entities to support some desired use cases; as well as in the behaviour of its interfaces and reference points' functionality. Ref. [1] also provides analogies between the multi-connection architecture and the Evolved Packet Core (EPC)/IMS and NGH/IMS to map functionality among such networks and offers a starting point for continuing the design of the multi-connection network.

It is hoped that the suggestions herein are guidance leading to further steps to achieve a more matured ITU-T multi-connection functional architecture in the next recommendation development phase, namely NSP.

Besides the enhancements shown in previous sections, the next clauses present very recent PCC trends on Service Awareness and Privacy Policies (SAPP) and other topics. These are only used as examples.

12.1 Next Steps: an Instance – Service Awareness and Privacy Policies

As one example of current developments in the Policy and Charging Control Architecture, see Ref. [4], updates in the area of Service Awareness and Privacy Policies (SAPP) are made in 3GPP Release 11. These enhancements find its way to the multi-connection Functional Entities mapping in the multi-connection architecture to cater for additional new Use Cases in the scenarios set forward by the multi-connection services. Including the Application Detection and Control (ADC) decision, consisting of ADC rules and Traffic Detection Function (TDF) session attributes, which are provided by the Policy and Charging Rules Function (PCRF) to the TDF/ Policy and Charging Control Enforcement Function (PCEF) enhanced with ADC for application detection and control.

Among other functionality, the next clauses provide an example of SAPP development.

12.1.1 Usage Monitoring Control

Advantageous is to apply usage monitoring for the accumulated usage of network resources on a per IP-CAN session and user basis. This capability is required for enforcing dynamic policy decisions based on the total network usage in real-time.

The Policy and Charging Rules Function (PCRF) that uses usage monitoring for making dynamic policy decisions shall set and send the applicable thresholds to the Charging Control Enforcement Function (PCEF) or Traffic Detection Function (TDF) for monitoring. The usage monitoring thresholds shall be based on volume. The PCEF or TDF shall notify the PCRF when a threshold is reached and report the accumulated usage since the last report for usage monitoring.

NOTE: There are reasons other than reaching a threshold that may cause the PCEF/TDF to report accumulated usage to the PCRF, as defined in Ref. [4].

The usage monitoring capability shall be possible to apply for an individual service data flow, a group of services data flows, or for all traffic of an IP-CAN session in the PCEF. Usage monitoring, if activated, shall be performed both for service data flows associated with predefined PCC rules and dynamic PCC rules, including rules with deferred activation and/or deactivation times while those rules are active.

The usage monitoring capability shall be possible to apply for application traffic detected by the TDF or by PCEF enhanced with ADC. Usage monitoring, if activated, shall be performed for a particular application, a group of applications, as identified by the ADC rule(s), or all detected traffic belonging to a specific TDF session.

12.1.2 Application Detection and Control

The application detection and control feature comprise the request to detect the specified application traffic, report to the PCRF on the start or stop of application traffic and to apply the specified enforcement actions.

The application detection and control shall be implemented either by the TDF or by the PCEF enhanced with ADC.

Two models may be applied, depending on operator requirements: solicited and unsolicited application reporting.

Solicited application reporting: The PCRF shall instruct the TDF, or the PCEF enhanced with ADC, on which applications to detect and report to the PCRF by activating the appropriate ADC rules. The PCRF may, in a dynamic ADC rule, instruct the TDF or PCEF enhanced with ADC, what enforcement actions to apply for the detected application traffic. The PCRF may activate application detection only if user profile configuration allows this.

Unsolicited application reporting: The TDF is pre-configured on which applications to detect and report. The enforcement is done in the PCEF. It is assumed that user profile configuration indicating whether application detection and control can be enabled is not required.

The report to the PCRF shall include the same information for solicited and unsolicited application reporting that is whether the report is for start or stop, the detected Application Identifier and, if deducible, the service data flow descriptions for the application user plane traffic.

For the application types, where service data flow descriptions are deducible, the Start of the application may be indicated multiple times, including the application instance identifier to inform the PCRF about the service data flow descriptions belonging to that application instance. The application instance identifier is dynamically assigned by TDF or PCEF enhanced with ADC rules in order to allow correlation of application Start and Stop events to the specific service data flow description.

For the solicited application reporting model:

- For those cases, where service data flow description for the detected applications is not possible to be provided by the TDF to the PCRF, the TDF shall perform gating, redirection and bandwidth limitation for the detected applications, if required. The existing PCEF/Bearer Binding and Event Reporting Function (BBERF) functionality remains unchanged.

  NOTE: Redirection may not be possible for all types of detected application traffic; e.g., this may only be performed on specific HTTP based flows.
- For those cases, where service data flow description is provided by the TDF to the PCRF, the actions resulting of application detection may be performed by the PCEF, as part of the charging and policy enforcement per service data flow and by the BBERF for bearer binding as defined in this document, or may be performed by the TDF as described above.

For the solicited application reporting, it is PCRF's responsibility to coordinate the PCC rules with ADC rules in order to ensure consistent service delivery.

Usage monitoring, as described in Ref. [4] may be activated in conjunction with application detection and control. The usage monitoring functionality is only applicable to solicited application reporting model.

12.1.3 Gx reference point

As previously analysed in the enhancements between the PCEF and PCRF, the Gx reference point resides between the PCEF and the PCRF.

The Gx reference point enables a PCRF to have dynamic control over the PCC/ADC behaviour at a PCEF.

The Gx reference point enables the signalling of PCC/ADC decision, which governs the PCC/ADC behaviour, and it supports the following functions:

- Establishment of Gx session, corresponding to an IP-CAN session, by the PCEF
- Request for PCC/ADC decision from the PCEF to the PCRF
- Provision of IP flow mobility routing information from PCEF to PCRF; this applies only when IP flow mobility as defined in TS 23.261 [7] is supported
- Provision of PCC/ADC decision from the PCRF to the PCEF

- Reporting of the start and the stop of a detected applications and transfer of service data flow descriptions and application instance identifiers for detected applications from the PCEF to the PCRF
- Reporting of the accumulated usage of network resources on a per IP-CAN session basis from the PCEF to the PCRF
- Delivery of IP-CAN session specific parameters from the PCEF to the PCRF or, in case Gxx is deployed, from the PCRF to the PCEF per corresponding request
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/network)
- Termination of Gx session (corresponding to an IP-CAN session) by the PCEF or the PCRF

  NOTE: The PCRF decision to terminate an Gx session is based on operator policies. It should only occur in rare situations; e.g., the removal of a MUE subscription to avoid service interruption due to the termination of the IP-CAN session.

The information contained in a PCC rule and in an ADC rule is defined in Ref. [4].

12.1.4 Sd reference point

The Sd reference point resides between the PCRF and the TDF. The Sd reference point enables a PCRF to have dynamic control over the application detection and control behaviour at a TDF.

The Sd reference point enables the signalling of ADC decision, which governs the ADC behaviour, and it supports the following functions:

1. Establishment of TDF session between the PCRF and the TDF.
2. Termination of TDF session between the PCRF and the TDF.
3. Provision of ADC decision from the PCRF for the purpose of application's traffic detection and enforcement at the TDF.
4. Request for ADC decision from the TDF to the PCRF.
5. Reporting of the start and the stop of a detected applications and transfer of service data flow descriptions and application instance identifiers for detected applications from the TDF to the PCRF.
6. Reporting of the accumulated usage of network resources on a per TDF session basis from the TDF to the PCRF.
7. Request and delivery of IP-CAN session specific parameters between the PCRF and the TDF.

While 1-7 are relevant for solicited application reporting; only 1, 2 and 5 are relevant for unsolicited application reporting.

The information contained in an ADC rule is defined in Ref. [4].

12.1.5 ADC rule authorization

ADC Rule authorization is the selection of the parameters (Application Identifier, enforcement actions, and others) for the ADC rules used in order to define the application traffic, required for detection, as well as enforcement action to be applied once the traffic is detected, if applicable.

In case of solicited application reporting, user profile configuration, received within subscription information, indicating whether application detection and control can be enabled, shall be taken into account by PCRF, when deciding on ADC rule authorization.

The enforcement actions are applicable in case of solicited application reporting.

In case of solicited application reporting, the ADC rules shall be authorized on IP-CAN session basis.

In case of unsolicited application reporting, the ADC rules are pre-provisioned at TDF.

12.1.6 Redirection

Redirection is an option applicable in the TDF or the PCEF enhanced with ADC.

Redirect address within the ADC rule allows the PCEF or TDF to decide whether to perform redirection or not towards a specific destination. The redirection is enforced by the PCEF enhanced with ADC/TDF on application's traffic matching the ADC rule for which the redirection is enabled.

PCRF redirection control is achieved by provisioning dynamic ADC rules with the redirect information provided over Gx interface or Sd interface. The redirection address may be locally configured in the PCEF or TDF or dynamically provisioned over Sd or Gx reference points. In the absence of the redirection address in the dynamic ADC Rule, the redirection information address configured in the PCEF or the TDF applies for application's traffic matching the ADC Rule, if detected.

12.1.7 Traffic Detection Function (TDF)

The TDF is a functional entity that performs application detection and reporting of detected application and its service data flow description to the PCRF.

For those cases where service data flow description is not possible to be provided by the TDF to the PCRF, the TDF performs:

- Gating
- Redirection
- Bandwidth limitation

for the detected applications.

For those cases where service data flow description is provided by the TDF to the PCRF the actions resulting of application detection may be performed by the PCEF as part of the charging and policy enforcement per service data flow and by the BBERF for bearer binding as defined in this document or may be performed by the TDF.

The PCEF can be enhanced with application detection and control feature as specified in Ref. [4].

For the solicited application reporting, the TDF shall support usage monitoring as specified in Ref. [4].

If usage monitoring is supported, the TDF shall support the usage reporting functions as specified in Ref. [4] assigned to the PCEF.

If there are required events, which cannot be monitored in the TDF; e.g., related to the location changes, the TDF shall provide the information about these Event Triggers to the PCRF using either:

- the IP-CAN Session Establishment procedure, or
- the PCEF initiated IP-CAN Session Modification procedure, or
- in the response to a PCRF initiated IP-CAN Session Modification, or
- within the Update of the subscription information in the PCRF procedure

as defined in Ref. [4].

Annex A – Multi-connection signalling flows

To support the "Use multi-connection Cases", example signalling flow diagrams were crafted for the multi-connection architecture, see Ref. [1]. These flows provide an initial guidance for designers. However, it is suggested that the flow diagrams and functional entities' behavior are further paired to their counterparts in the LTE models, such as Policy and Charging Control (PCC), IP flow mobility, and QoS mechanisms among others. Specially, for the implementation of the Aggregation use case, which is one of the first cases investigated by 3GPP, the following signalling flow procedures show the steps for:

1. Initiating and adding new connections.
2. Updating a connection.
3. Executing IP flow mobility, initiated by the MUE.
4. Executing IP flow mobility, initiated by the network.
5. Service Composition During Call Establishing.
6. Service Decomposition During Call Establishing.
7. Service decomposition with QoS policy control.
8. Subscriber attaching to the access network.
9. Policy control procedure.

A.1 Initiating and Adding a New Connection

If the MUE is using multiple connections to receive and to send flows, the IP flows routing paths are affected when adding new connections. This clause describes the high-level information flows triggered by the changes of multiple available connections in the MUE.

When the MUE moves into the coverage of a new access network and successfully pass authentication, the MUE can use the access network to send and receive packets. Before the MUE uses the new connection, it is required to register the new connection in the MR-FE. Figure 20 shows a possible signalling flow when adding a new connection.

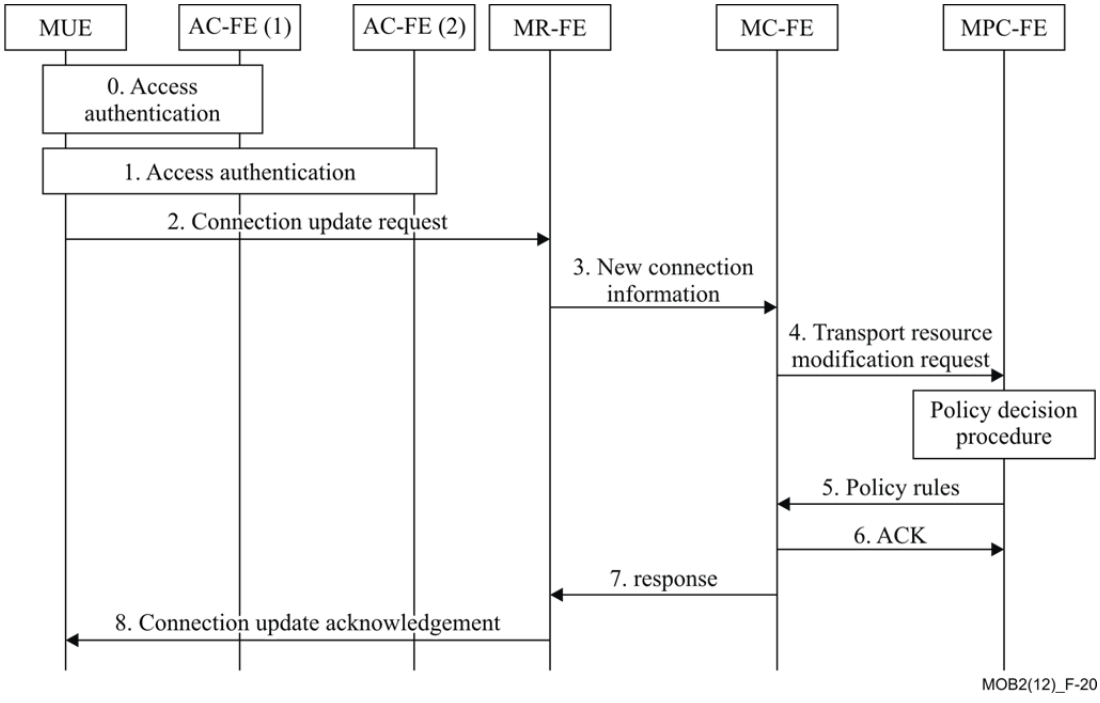

Figure 20 Adding a New Connection [1]

0) A MUE accesses an access network via AC-FE (1) through the access authentication process. After the successful access authentication, the MUE obtains an IP address for the interface connecting the access network;

1) After detecting a new available access network, the MUE starts the authentication process via AC-FE (2) and obtains a new IP address for it;

2) The MUE sends a Connection Update Request message with the new IP address to the MR-FE to register a new connection;

3) The MR-FE updates the available connections of the MUE and sends a New Connection Information message which contains the available connections of the MUE to the MC-FE;

4) The MC-FE sends a Transport Resource Modification Request message to the MPC-FE;

5) The MPC-FE selects a set of QoS rules for the new connection based on the operator policy and the information of the new connection. Afterwards, the MPC-FE sets the policy for the MUE's ongoing IP flows, based on the multi-connection policies and sends it to the MC-FE;

6) The MC-FE sends an ACK message to the MPC-FE after receiving the policy rules;

7) The MC-FE sends a Response message to MR-FE;

8) The MR-FE binds between the MUE and the new connections and sends a Connection Update Acknowledgement message to the MUE.

A.2 Updating a Connection

When a MUE moves out of the coverage of an access network, it is required to moves all IP flows associated with that access and detach from it. Figure 21 shows an example of a signalling flow diagram to update the involved connection.

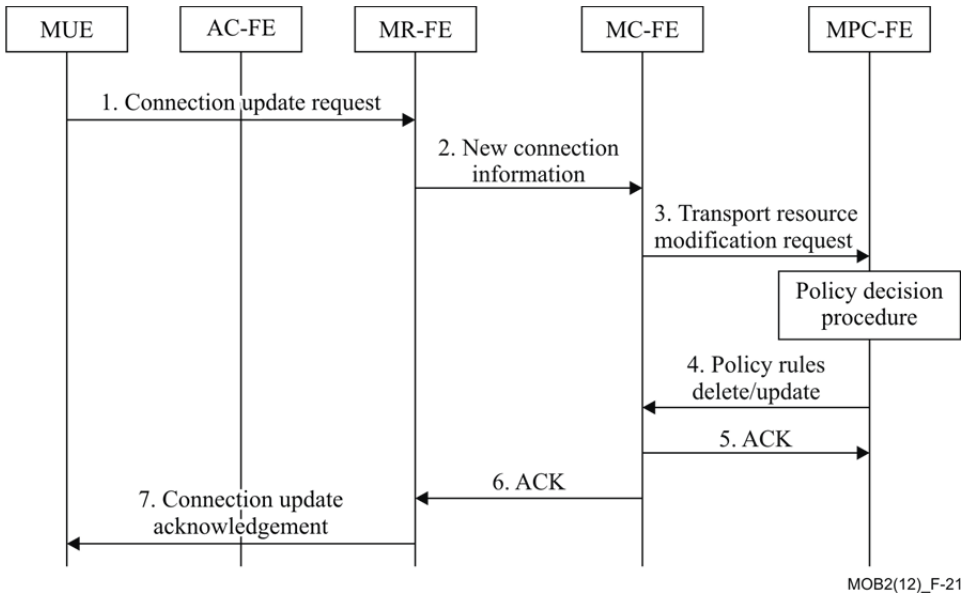

Figure 21 Updating a Connection [1]

1) The MUE sends a Connection Update Request message to the MR-FE. The message contains the identifier of the connection to be updated;

2) The MR-FE deletes the associate connection information based on the Connection Update Request message. And then the MR-FE sends a New Connection Information message which contains the available connections of the MUE to the MC-FE;

3) The MC-FE sends a Transport Resource Modification Request message to the MPC-FE;

4) The MPC-FE controls transport resource based on the Transport Resource Modification Request, and then sends a QoS Policy Rules Delete/Update message to the MC-FE;

5) The MC-FE receives the QoS Policy Rules Delete/Update message and then returns an ACK message to the MPC-FE;

6) The MC-FE returns an ACK message to the MR-FE;

7) The MR-FE binds between the MUE and new connections and returns a Connection Update Acknowledgement message to the MUE.

A.3 MUE Initiated IP Flow Mobility

When the MUE is connected simultaneously to multiple access networks, the MUE may use multiple connections to send and receive IP flows. Because of changes in the access network sometimes the MUE needs to move one IP flow from one access network to another access network. In that case, the MUE is required to modify the parameters of the available connections. Figure 22 and corresponding steps portray the required actions to be taken by the multi-connection network.

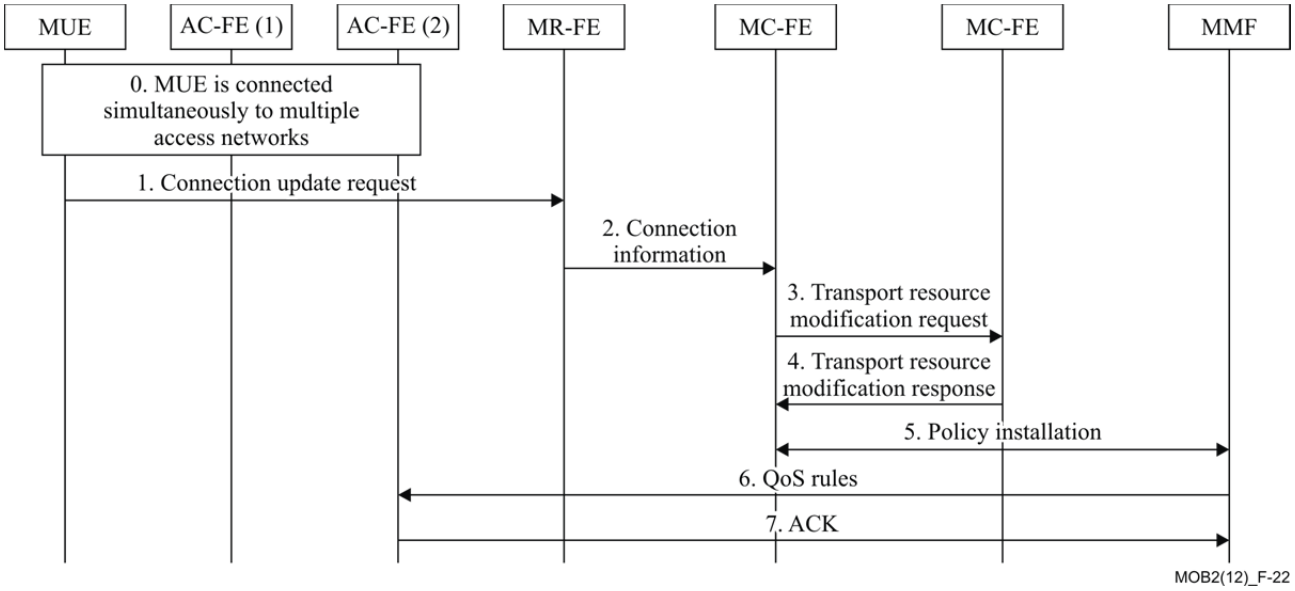

Figure 22 MUE Initated IP Flow Mobility [1]

0) The MUE is connected simultaneously to multiple access networks and utilizes multiple connections to send and receive IP flows;

1) The MUE sends a Connection Update Request message to the MR-FE. The message contains the identifier and new information of the connection that the network wants to modify;

2) The MR-FE updates the information of the connection based on the Connection Update Request message. Then MR-FE sends a Connection Information message to the MC-FE;

3) The MC-FE sends a Transport Resource Modification Request message containing the updated information of the connections to the MPC-FE;

4) The MPC-FE selects new QoS policy rules for the connection based on the operator policy and the updated connection information. Then it returns a Transport Resource Modification Response message to the MC-FE.

5) The MC-FE makes and assigns related rules for the access network to the MMF. The MMF installs the policy rules;

6) The MMF sends the new QoS rules to the AC-FE(2);

7) The AC-FE(2) updates the QoS policy rules of the connection. Then, it returns an ACK message to the MMF.

A.4 Network Initiated IP Flow Mobility

Based on the current status of access network, the network decides to move one IP flow from one access network to another access network. In this case, the network is required to initiate the IP flow mobility procedure thus interacting with the related function entities directly. Figure 23 and corresponding next steps portray the required actions to be taken by the multi-connection network.

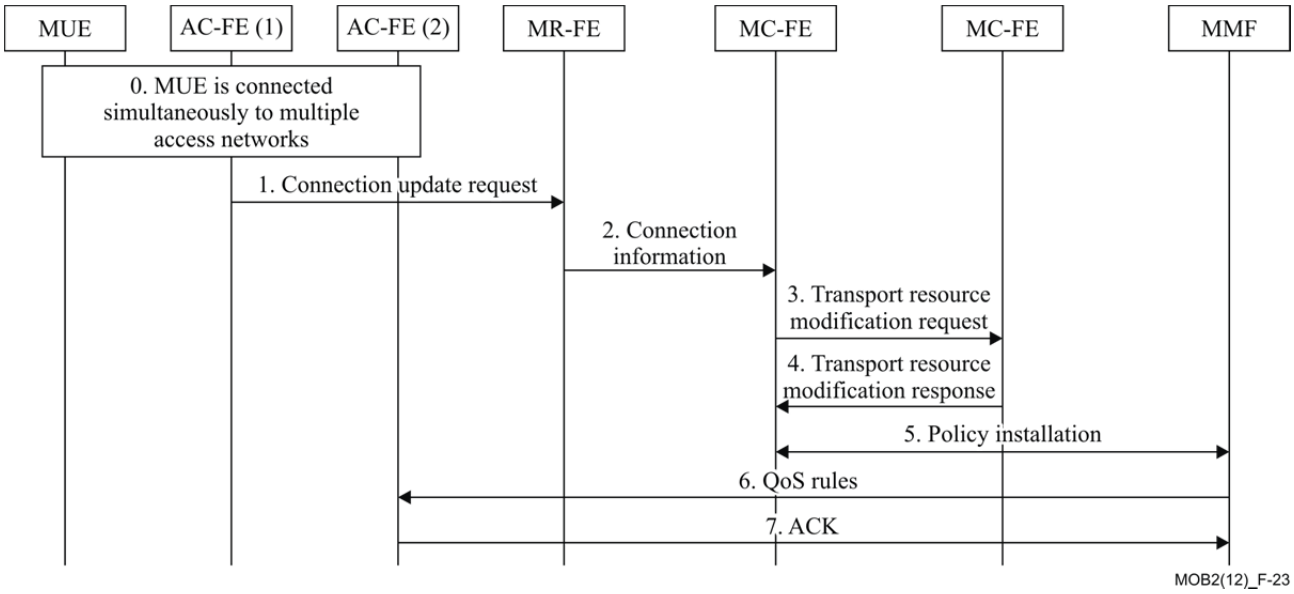

Figure 23 Network Initated IP Flow Mobility [1]

0) The MUE is connected to multiple access networks simultaneously and utilizes multiple connections to send and receive IP flows;

1) The AC-FE(1) sends a Connection Update Request message to the MR-FE. The message contains the identifier and new information of the connection that the network wants to modify;

2) The MR-FE updates the information of the connection based on the Connection Update Request message. Afterwards, the MR-FE sends a Connection Information message to the MC-FE;

3) The MC-FE sends a Transport Resource Modification Request message which contains the updated information of the connections to the MPC-FE;

4) The MPC-FE selects new QoS policy rules for the connection based on operator's policy and the updated connection information. Then, it returns a Transport Resource Modification Response message to the MC-FE;

5) The MC-FE creates and assigns related rules, for the access network, and sends them to the MMF. The MMF installs the rules;

6) The MMF sends the new QoS rules to AC-FE(2);

7) The AC-FE(2) updates the QoS policy rules of the connection. Then, it returns an ACK message to the MMF.

A.5 Service Composition During Call Establishment

When the MUE creates several service components through multiple network interfaces, the service components can be composed into one service component to serve the application and the remote MUE. Figure 24 depicts the process. The procedure below happens during call establishing. This procedure supports, for instance the user case 10 in the multi-connections scenarios supplement, see Ref. [6].

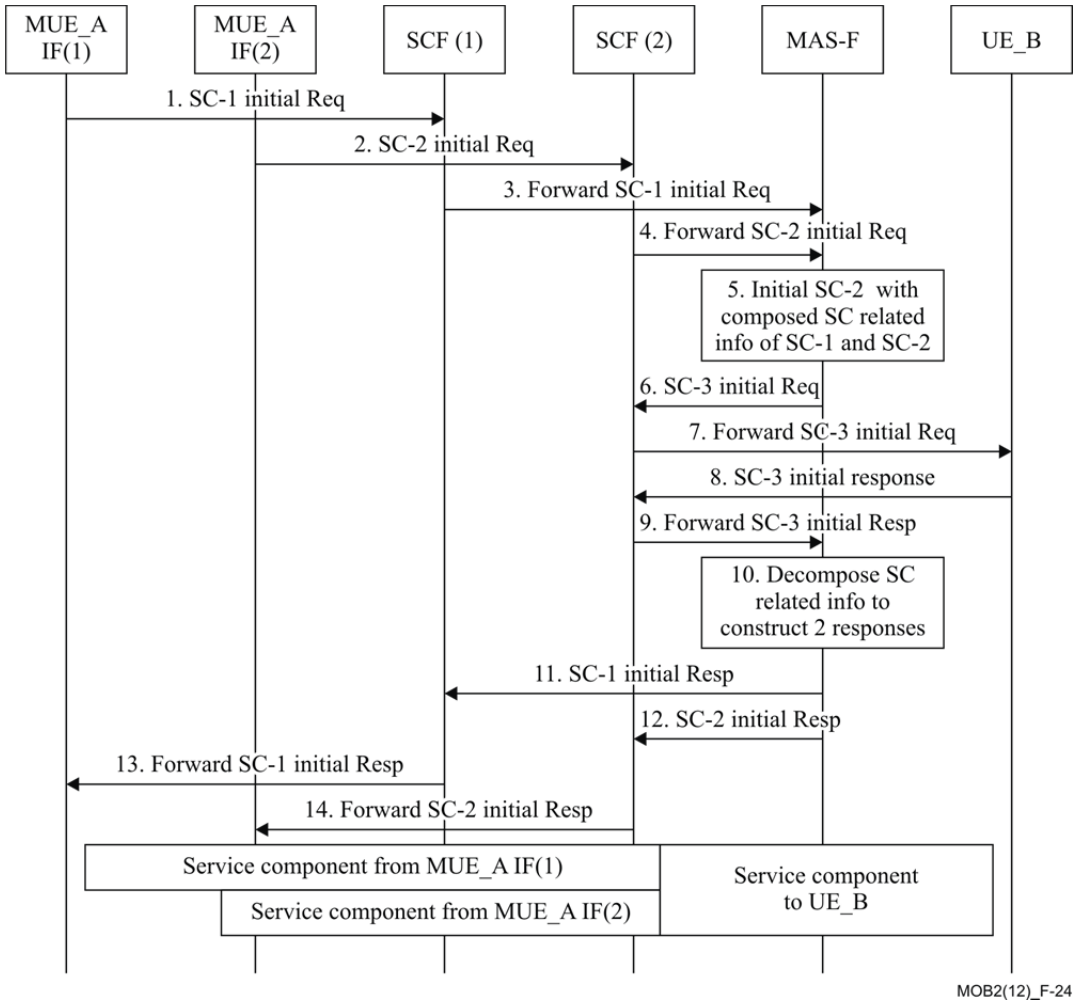

Figure 24 Service Composition During Call Establishment [1]

The next steps portray the required actions to be taken by the multi-connection network.

1) - 4) The MUE_A initiates two service components (SC-1& SC-2) from two interfaces; i.e., MUE_A IF(1) & MUE_A IF(2). The initial requests are sent to corresponding SCEs through different networks, and are forwarded to MAS-F respectively.

5) The MAS-F identifies that the requests belong to a same call and can be composed. Hence, it composes the information of SC-1 and SC-2, and initiates a new service component (SC-3) to the MUE_B, which can be a multi-connection MUE or even an ordinary UE.

6) - 7) The initial request of SC-3 is routed to a SCF, which is SCF(2) and can also be other proper one, and is forwarded to the MUE_B. The MUE_B can be a multi-connection MUE or an ordinary UE.

8) - 9) The MUE_B negotiates media parameters to establish SC-3. Then, MUE_B constructs a response for SC-3, and returns it along the transmission path. The response is then forwarded to the MAS-F.

10) The MAS-F decomposes service components related information from the response, and constructs two responses for SC-1 and SC-2.

11) - 14) The MAS-F constructs two responses for SC-1 and SC-2. The responses are routed to the MUE_A along the original paths.

After the steps above, the MUE_A and the MUE_B have established a call. Within it, there are two service components for the MUE_A, which are through different interfaces and different networks, and only one service component for the UE_B.

A.6 Service Decomposition During Call Establishment

A service that supports the multi-connection capability can be decomposed into several service components. The procedure below happens during call establishing and is depicted in Figure 25.

This procedure supports, for instance the user case 11 in the multi-connections scenarios supplement, see Ref. [6].

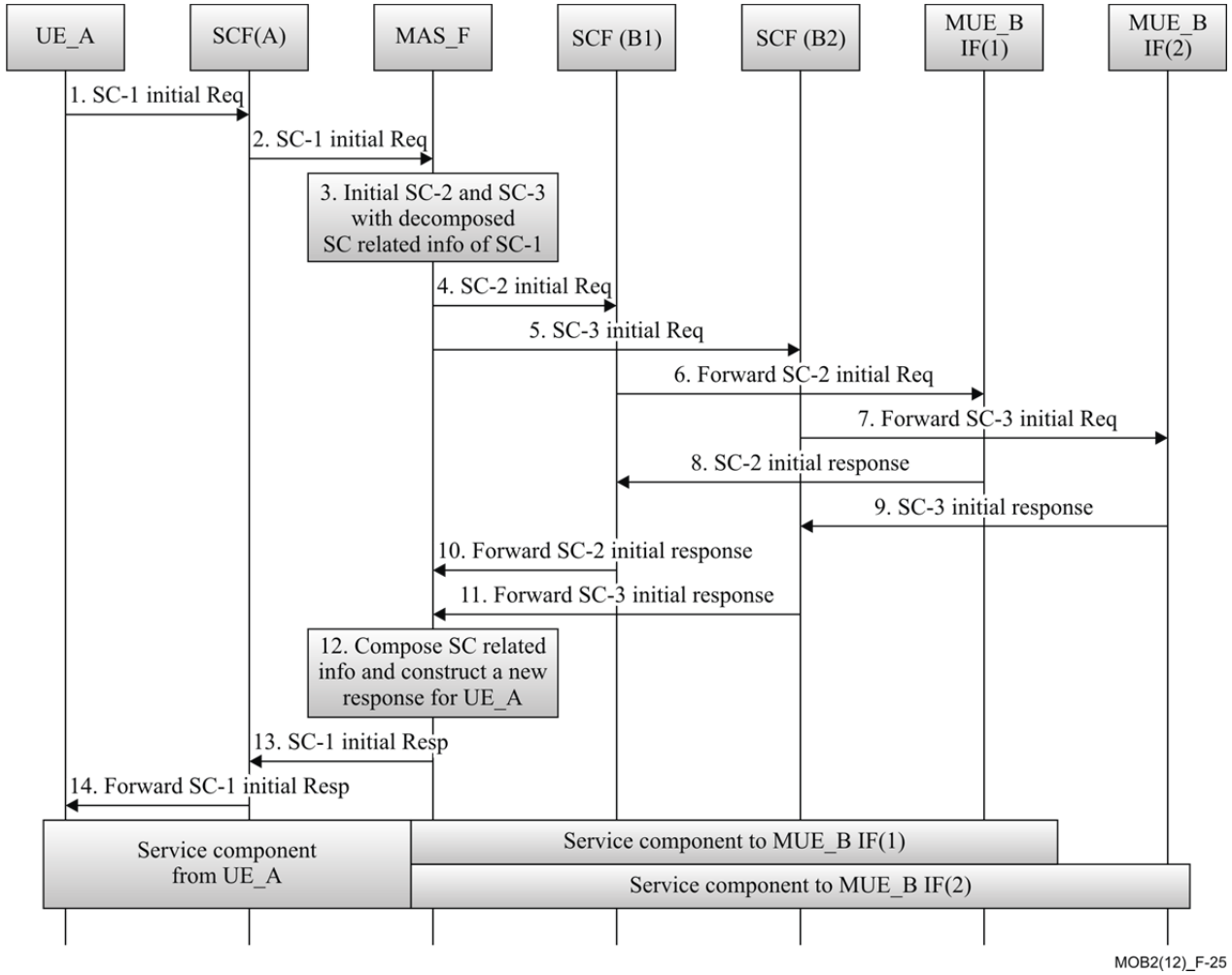

Figure 25 Service Decomposition During Call Establishment [1]

1) - 2) The MUE_A, which can be a MUE or even an ordinary UE, initiates a service (SC-1) to the MUE_B, which is a proper MUE, see Ref. [1]. The initial request is routed to SCF(A), and SCF(A) forwards it to the MAS-F.

3) The MAS-F identifies that SC-1 can be decomposed for the MUE_B, since The MUE_B is a MUE. So MAS-F splits the Session Description Protocol (SDP) descriptions extracted from the initial request of SC-1, and initiates two new service components

(SC-2 & SC-3) to two interfaces of MUE_B; i.e., the MUE_B IF(1) and the MUE_B IF(2).

4) - 7) The MAS-F sends the new initial requests the MUE_B. The requests are routed through SCF(B1) and SCF(B2), which correspond to the different interfaces of the MUE_B.

8)-11) The responses are routed to the MAS-F via the SCFs.

12) The MAS-F composes service component related information from the two responses, and constructs a new response.

13)-14) The responses are routed to the MUE_A through SCF(A).

A.7 Service Decomposition with QoS Policy Control

This procedure shows the service decomposition with QoS policy control when a call is established. Figure 26 depicts the signaling flow diagram. The steps describe the required actions to be taken by the multi-connection network.

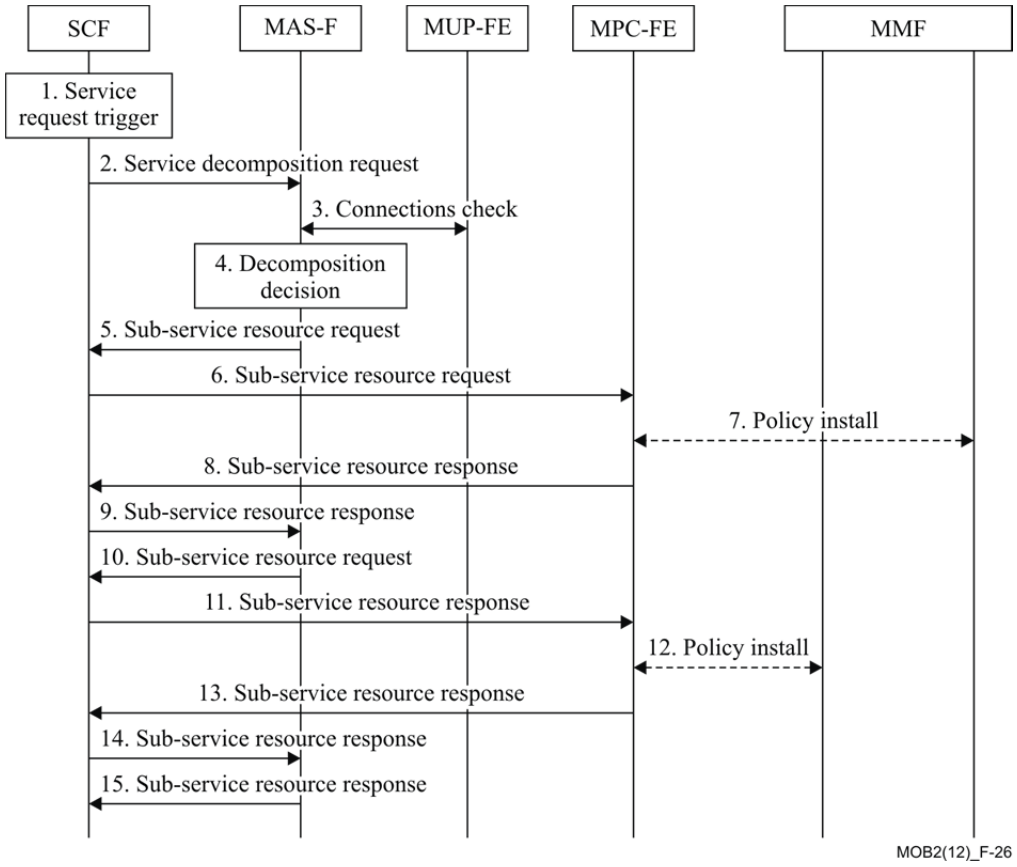

Figure 26 Service Decomposition with QoS Policy Control [1]

1) The SCF receives a service request from the remote MUE, which triggers the SCF to initiate a service request.

2) SCF further sends a service decomposition request to the MAS-F, requesting to certify if the MUE is utilizing multi-connections, and if the MUE needs service decomposition.

3) The MAS-F sends connection check request to the MUP-FE to obtain the available connections of the MUE.

4) The MAS-F makes decomposition decision based on the service decomposition request and the available connections of the MUE.

5) The MAS-F sends sub-service resource request to the SCF with service resource requirements, the service request is directed to connection one.
6) The SCF further sends the sub-service resource request to the MPC-FE.
7) The MPC-FE creates policy rules based on QoS resource requirements, and then sends a request to install the rules into the MMF for connection one.
8) The MPC-FE sends sub-service resource response to the SCF.
9) The SCF sends sub-service resource response to the MAS-F.
10) The MAS-F sends sub-service resource request to the SCF with service resource requirements, the is directed to connection two.
11) The SCF further sends the sub-service resource request to the MPC-FE.
12) The MPC-FE makes policy rules based on QoS resource requirements, and then sends a request to install the rules in the MMF.
13) The MPC-FE sends sub-service resource response to the SCF.
14) The SCF sends sub-service resource response to the MAS-F.
15) The MAS-F sends sub-service resource response to the SCF.

A.8 Subscriber Attaches to the Access Network

This clause provides a high level signalling flow defining the network attachment as well as the connection registration process. Figure 27 depicts the signalling flow diagram.

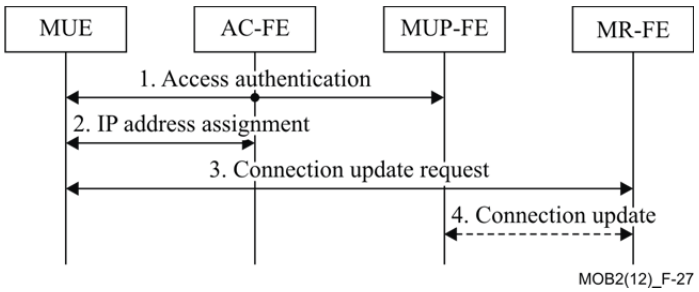

Figure 27 Subscriber Attaches to the Access Network [1]

The next steps portray the required actions to be taken by the multi-connection network.

1) The MUE attaches to an access network through the access authentication process.
2) After successful access authentication, the MUE obtains an IP address for the new interface.
3) The MUE sends a Connection Update Request message with the new IP address to the MR-FE to register a new connection.
4) The MR-FE updates the available connections of the MUE. If needed, the MR-FE further sends a Connection Update message, which contains the available connections of the MUE to the MUP-FE.

A.9 Policy Control Procedure

An example of a multi-connection policy control procedure is defined in this clause. When the MUE initiates a multi-connection service, a multi-connection control request is triggered by the SCF. Figure 28 depicts the signalling flow diagram.

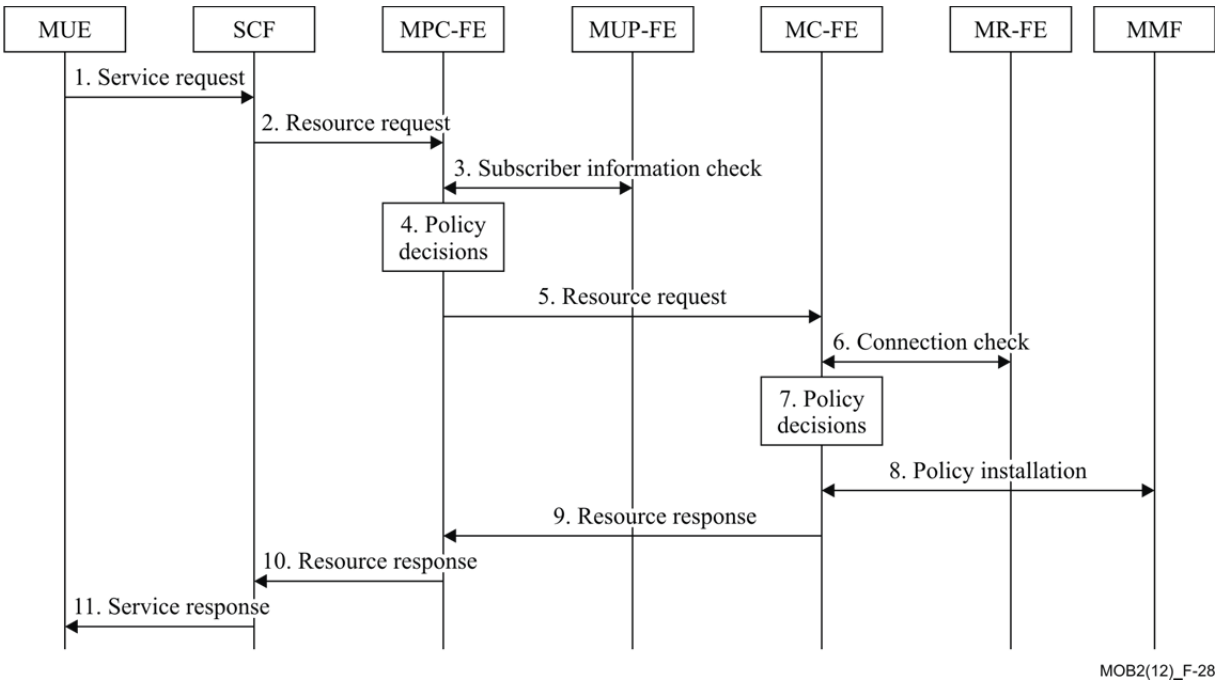

Figure 28 Policy Control Procedure [1]

The next steps portray the required actions to be taken by the multi-connection network.

1) The MUE requests a multi-connection service by sending a service request to the SCF.
2) The SCF extracts or derives the resource requirements for the requested service, and sends a resource request to the MPC-FE for resource authorization and reservation.
3) The MPC-FE sends a subscriber information check to the MUP-FE to check the subscription related information belonging to the MUE.
4) The MPC-FE creates the policy decisions based on the above information.
5) The MPC-FE sends a resource request to the MC-FE to support the application traffic over multiple accesses.
6) The MC-FE sends a connection check to the MR-FE to check the current available connections of the MUE.
7) The MC-FE makes the policy decisions based on the above information.
8) The MC-FE sends the policies to the MMF for installation.
9) The MC-FE sends a resource response to the MPC-FE.
10) The MPC-FE sends a resource response to the SCF.
11) The SCF sends a service response to the MUE.

Abbreviations and acronyms

This technical paper uses the following abbreviations and acronyms. Specific terminology used in other forums is prefixed accordingly, for context-referral:

2G	GSM Second Generation
3G	Third Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AC-FE	Access Control FE
ADC	Application Detection and Control
ADSL	Asymmetrical Digital Subscriber Line
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
AN	Access Network
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
API	Application Programming Interface
APN	Access Point Name
ARP	Address Resolution Protocol
ARP	Allocation Retention Priority
BBERF	Bearer Binding and Event Reporting Function
BSS	Base Station Subsystem
CGI	GSM Cell Global Identification
Cm	Reference Point between MC-FE and MMF
CoA	Care of Address
CS	Circuit Switched
CSG	Closed Subscriber Group
DNS	Domain Name System
DSMIPv6	Dual-Stack Mobile IPv6
ECGI	User Location Information
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
E-RAB	E-UTRAN Radio Access Bearer
E-UTRAN	Enhancements for Evolved Universal Terrestrial Radio Access Network
FE	Functional Entity
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GBR	Guaranteed Bitrate
Gn	Interface between SGSN and GGSN
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
GUTI	Globally Unique Temporary Identity
Gx	Reference Point between V-PCRF and PCEF Reference point between
Gxx	Reference Point between v-PCRF and BBERF

H-PCRF	Home PCRF
HA	Home Agent
HO	Handover
HSS	Home Subscriber Server
IETF	Internet Engineering Task Force
IF	Interface
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISP	Internet Service Provider
ISR	LTE Idle-mode Signalling Reduction
L-GW	Local GateWay
LBI	Linked Bearer Id
LTE	Long Term Evolution
MAS-F	Multi-connection Application Support Function
MBR	Maximum Bitrate
MC-ARCH	Multi-connection Architecture
MC-FE	Multi-connection Coordination FE
MME	Mobility Management Entity
MMF	Multi-connection Media Function
MPC-FE	Multi-connection Policy Control FE
MPS	Multimedia Priority Service
MR-FE	Multi-connection Registration FE
MTC-FE	Multi-connection Terminal Control FE
MUE	Multi-connection UE
MUP-FE	Multi-connection User Profile FE
NGH	Next Generation Hotspot
NGN	Next Generation Network
OCS	Online Charging System
OI	Operator Identifer
OSI	Open System Interconnect reference model
P2P	Peer to Peer
Pa	Reference Point between MPC-FE and MAS-F
PC	Personal Computer
PCC	Policy and Charging Control
PCEF	Policy and Charging Control Enforcement Function
PCO	Protocol Configuration Options
PCRF	Policy and Charging Rules Function
PDB	Packet Delay Budget
PDCP	Packet Data Convergence Protocol
PDN	Public Data Network
PDU	Protocol Data Unit
PELR	Packet Error Loss Rate
PMIPv6	Proxy Mobile IPv6
PS	Packet Switched

Ps	Reference Point between MPC-FE and SCF
PTI	Procedure Transaction Id
P-CSCF	Proxy-Call Session Control Function
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RAI	Routeing Area Identity
RAN	Radio Access Network
RED	Random Early Detection
RLC	Radio Link Control Sub-layer
Rt	Reference Point between MR-FE and MTC-FE
Rx	Reference Point between H-PCRF and P-CSCF (in the IMS)
S3	Reference Point between SGSN Rel. 8 and MME
S4	Reference Point between S-GW and SGSN Rel.8
S5	Reference Point between S-GW and P-GW (PCEF) in visited network
S8	Reference Point between S-GW and P-GW (PCEF) in home network
S9	Reference Point between H-PCRF and V-PCRF
S10	Reference point between MME and MME
S11	Reference Point between the Serving Gateway and the MME
S16	Reference Point between SGSN and SGSN
SAI	Service Area Identity
SAPP	Service Awareness and Privacy Policies
SCF	Service Control Functions
Sd	Reference Point between the PCRF and the TDF
SDF	Service Description Framework
SDF	Service Data Flow
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SP	Strict Priority
SPR	Subscription Profile Repository
SRVCC	Single Radio Voice Call Continuity
SUE	Single connection UE
TAI	Tracking Area Identity
TDF	Traffic Detection Function
TEID	Tunnel Endpoint Identifier
TFT	Traffic Flow Template
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
V-PCRF	Visited PCRF
VoIP	Voice over IP
VPN	Virtual Private Network
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance
WFQ	Weighted Fair Queue

Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRR	Weighted Round Robin

Bibliography

Note - At the time of publication, the editions indicated below were valid. All these references are subject to revision; therefore, users of this technical paper are encouraged to investigate the possibility of applying the most recent edition of the references listed below.

[1] Recommendation ITU-T Y.2027 (2012), *Functional Architecture of multi-connection*

[2] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*

[3] Bloch, Joshua, *Effective Java,* Second Edition, Addison Wesley: 2008

[4] ETSI TS 123 203, *Policy and Charging Control Architecture Rel. 11*, V11.5.0 (2012-03)

[5] ETSI TS 23.402, *Architecture Enhancements for Non-3GPP Accesses Rel. 11*, V11.2.0 (2012-03)

[6] Supplement 9 to the ITU-T Y-series Recommendations (2010), *Supplement in multi-connection Scenarios*

[7] ETSI TS 123 261, *IP Flow Mobility and Seamless WLAN Offload – Stage 2 Rel. 10,* V11.2.0 (2012-03)

[8] ETSI TS 23.327, *Mobility between 3GPP-WLAN Interworking and 3GPP Systems Rel. 11*, V11.0.0 (2012-03)

[9] IETF RFC 5555, *Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)*

[10] IETF RFC 5648, *Multiple Care-of Addresses Registration*

[11] IETF RFC 6089, *Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support*

[12] ETSI TS 23.060, *General Packet Radio Service (GPRS); Service description; Stage 2, Rel.11*,(2012-03

[13] ETSI TS 123 401, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*

[14] ETSI TS 23.216, *Single Radio Voice Call Continuity (SRVCC); Stage 2*

[15] Recommendation ITU-T Y.2251 (2011), *Multi-connection requirements*

[16] ETSI TS 23.107, *Quality of Service (QoS) concept and architecture*

[17] ETSI TS 36.300, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Overall Description; Stage 2 Rel. 11*, V11.1.0 (2012-03)

[18] ETSI TS 23.003, *Numbering, addressing and identification Rel. 11*, V11.1.0 (2012-03)

[19] ETSI TS 29.303, *Domain Name System Procedures Rel. 11*, V11.0.0 (2012-03)

[20] IETF RFC 3168, *Explicit Congestion Notification (ECN)*

[21] ETSI TS 25.401, *UTRAN Overall Description Rel. 10*, V10.2.0 (2011-06)

[22] ETSI TS 26.114, *IMS; Multimedia Telephony; Media Handling and Interaction Rel. 11*, V11.3.0 (2012-03)

[23] ETSI TS 23.228, *IMS; Stage 2 Rel. 11*, V11.4.0 (2012-03)

[24] ETSI TS 29.274, *EPS GPRS Tunnelling Protocol for Call Control Plane (GTPv2-C); Stage 3 Rel. 11,* V11.2.0 (2012-03)

[25] ETSI TS 24.008, *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 Rel. 11,* V11.2.1 (2012-03)

[26] ETSI TS 23.107, *QoS Concept and Architecture Rel. 10,* V10.2.0 (2011-12)

[27] Vasudevan, S., *Evolution to Multi-RAT Heterogeneous Networks,* presentation at CDG Technology Forum on Increasing Network Capacity and Reducing Transmission Costs through New Technological Innovations, Philadelphia, PA, September 30, 2009 http://www.cdg.org/news/events/cdmaseminar/09_TechForum_Sept/presentations/6-ALU%20Evolution%20to%20multi-RAT.pdf

[28] Recommendation ITU-T Y.2252 (2012), *Identification and configuration of resources for multi-connection*

Printed in Switzerland
Geneva, 2013