University of Piraeus
Department of Digital Systems

University Of Piraeus

Department of Digital Systems

Postgraduate Program: “Digital Systems & Services”

Postgraduate Thesis Report

“Implementation and testing of the 3GPP Policy & Charging Control architecture in a 4G-LTE lab environment”

Professor: **Tsagkaris Konstantinos**

Student: **Kornelakis Charalampos**

Student id: me13042

Piraeus, March 2016

Contents

Introduction

The main task of this dissertation was the modification of Gy interface (OCS) scripts in "C" so that it supports error codes in CCR – I (Initial) messages. Development was needed in order the error code value to be configurable by the user. The configurable error code value to be sent for a configurable percentage of CCR messages. The second task was the modification of Gx interface (PCRF) script in "Pearl" so that it supports error codes in CCR – I (Initial) message. The error code value should be configurable by the user. The configurable error code value to be sent for a configurable percentage of CCR messages. For the purpose of our tests after the modification of scripts we used the 4G lab environment of Nokia.

We modified as we mentioned above the OCS scripts that NOKIA uses for Gy interface in order to add the option for user to choose the error code that he wants to reject the new session that its state is still on-going. We also write a whole library with as much error codes as the script can support. Another task of this thesis was to do the same modification for PCRF scripts in Pearl in order the script supports the addition of a specific error code inside the CCR-I message. The final task was the participation in an inside new created team that its task was the creation of a PCRF script in C from scratch.

1. UMTS Network Architecture

The UMTS network architecture has 3 components, the first part of User Equipment is ME (Mobile Equipment) and the second one is the USIM. Furthermore the RAN (Radio Access Network) has two elements, the first one is NodeB and the other one is the RNC. On the other hand Core Network has both circuit switched and packet switched modules for its functionality. In Circuit switched (CS) module operations MSC and GMSC will be available with the following database modules: VLR and HLR. Secondly in packet switched (PS) operations SGSN and GGSN will do the necessary work. The connection for GMSC is PSTN or ISDN in circuit switched case. In packet switched case GGSN it has a direct connection with Packet data Network (PDN). Below we can see the interfaces between all these elements.

Uu interface between UE and NodeB
Iub interface between NodeB and RNC
Iur interface between RNC and RNC
Iu-CS interface between RNC and MSC
Iu-PS interface between RNC and SGSN

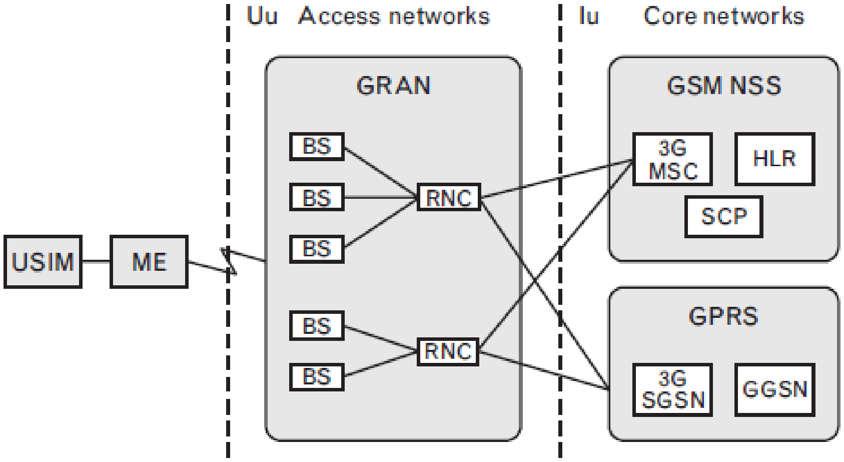
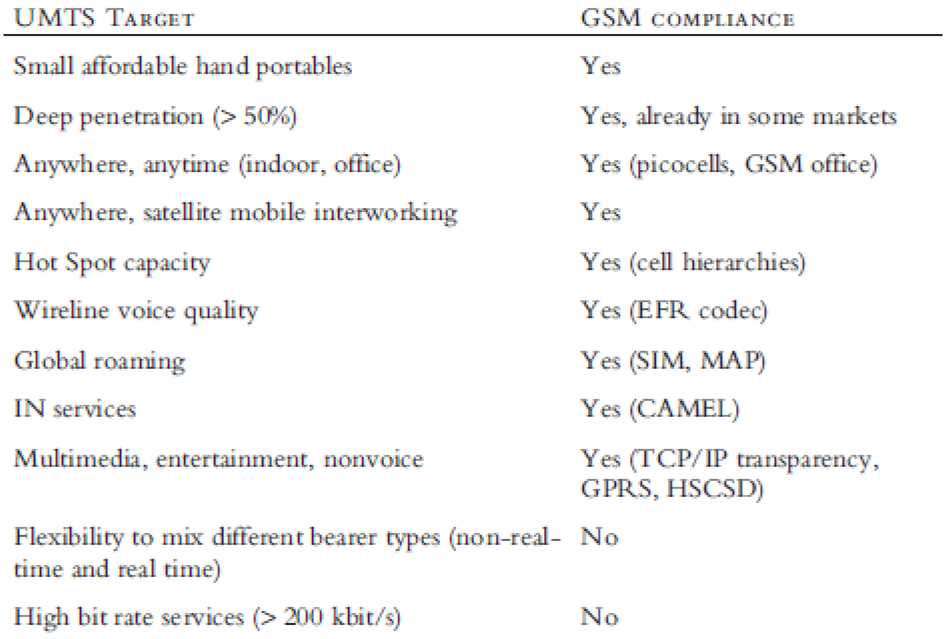


Figure 3 : UMTS Basic Architecture

1.1 UMTS Architecture

The GSM network with all the features installed is similar to a UMTS. The big advantage that UMTS network has is that itsa air interface is more capable and flexible. This advantage give to UMTS the opportunity to handle different bearer types at the same time.

Another difference is that UMTS has the ability to reach higher bit rates, but this type of differences between UMTS and GSM are not so large and observed in case that you are a simple user of mobile network. A GSM with installed all the features of 2.5GSM technology can reach data rates close to 200Kbps. According to theory and papers GSM could reach value of rates near to 384Kbps. In case that a UTRAN network wants to achieve a higher speed, it is needed to use very low spreading factors, and to allocate the resourcing power of a single base station in most to only one user. A typical WCDMA base station has only one downlink frequency carrier, and if one user provided with a downlink connection of over 2Mbps, then other users are left with nothing.



UMTS Target	GSM compliance
Small affordable hand portables	Yes
Deep penetration (> 50%)	Yes, already in some markets
Anywhere, anytime (indoor, office)	Yes (picocells, GSM office)
Anywhere, satellite mobile interworking	Yes
Hot Spot capacity	Yes (cell hierarchies)
Wireline voice quality	Yes (EFR codec)
Global roaming	Yes (SIM, MAP)
IN services	Yes (CAMEL)
Multimedia, entertainment, nonvoice	Yes (TCP/IP transparency, GPRS, HSCSD)
Flexibility to mix different bearer types (non-real-time and real time)	No
High bit rate services (> 200 kbit/s)	No

Figure 4 : GSM vs UMTS

In practice the situation is not so bad, since high – speed traffic is typically bursty and not continous, and several users can have high data rates momentarily. We can see that a GSM + GPRS combination provides a very good foundation for the UMTS core network building process. The biggest operator investment will clearly be building out the radio access network. Some of the latest GSM base stations are, however, said to be upgradeable to UTRAN standards.

1.2 UMTS Network Structure

The next figure show us the highest level of UMTS architecture. In this chapter we are going to show both the CN (Core Network) and the UTRAN.

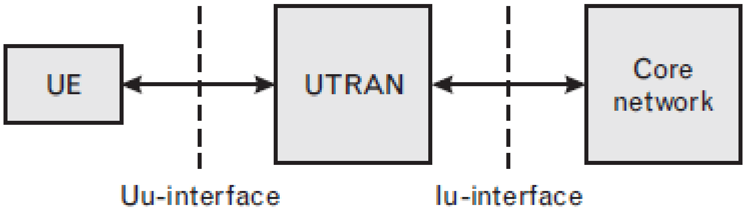


Figure 5 : High – Level UMTS Architecture

The interfaces between the UE and the UTRAN (Uu interface) and between the UTRAN and CN (Iu) are open multivendor interfaces. The next figure give us a more detailed description of the UMTS architecture. We can see that the core network is the same as in the old GSM + GPRS core network combination. The same core network entities may serve both the UTRAN and GSM radio access networks.

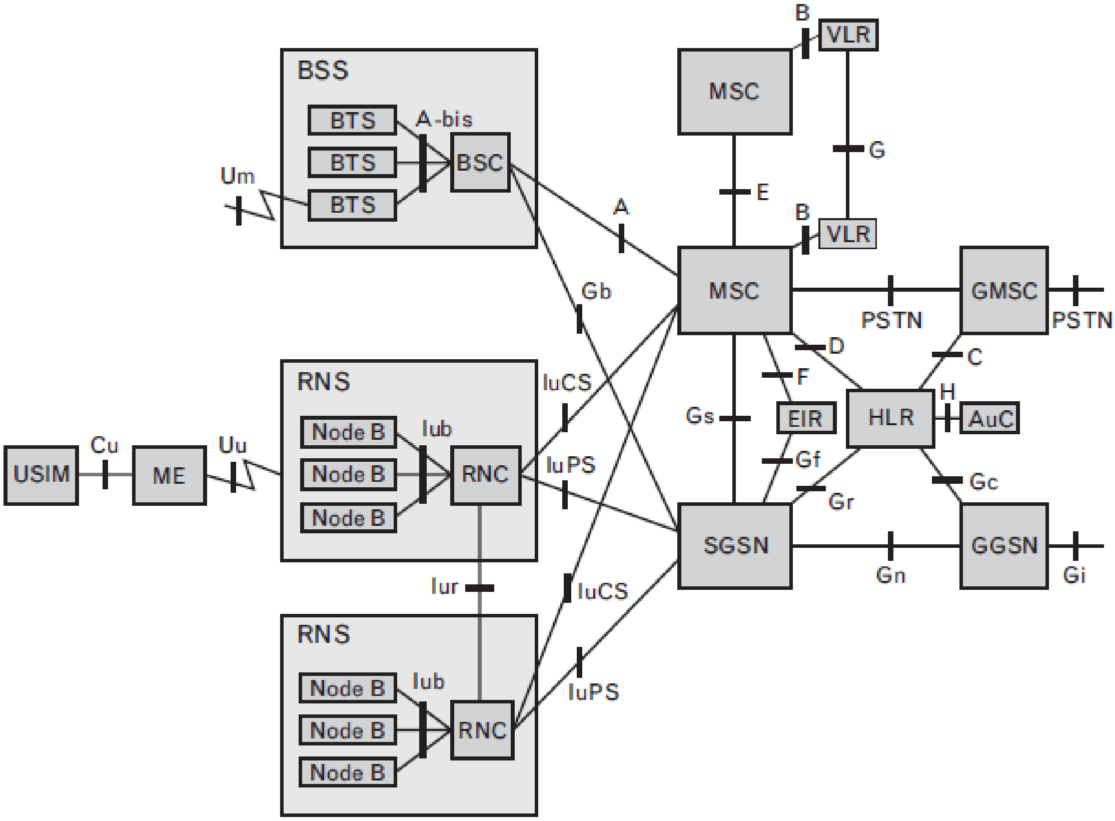


Figure 6 : UMTS network elements and interfaces.

GSM’s radio access network entities (the BSS) are included in the previous figure to clarify the relationship of these two technologies. Some of the entities of this figure will described in the next paragraphs.

1.2.1 CORE NETWORK

Mobile Switching Center (MSC)

The mobile switching center is the centerpiece of the circuit – switched core network. The same MSC can be used to serve both the GSM – BSS and the UTRAN connections. This kind of MSC must be upgraded somewhat to meet the 3G requirements, but the same MSC can be used to serve the GSM networks. In addition to the radio access networks, it has interfaces to the fixed PSTN network, other MSC’s, the packet switched network (SGSN), and various core netwotk register (HLR,EIR.AuC).

Several BSS's can be connected to an MSC. The number of MSC's also varies, a small operator may only have on e MSC, but once the number of subscribers increases, several MSCs may be needed. The functions of an MSC includes :

- Paging
- Coordination of call setup from all MSs in the MSC's jurisdiction
- Dynamic allocation of resources
- Location registartion
- Handover management
- Billing of subscribers
- Encryption parameter management
- Signaling exchange between different interfaces
- Frequency allocation management in the whole MSC area

Gateway MSC (GMSC)

The Gateway MSC (GMSC) is an MSC that is located between the PSTN and the other MSCs in the network. Its function is to route the incoming calls to the appropriate MSCs. Note that the PSTNs outside the PLMN cannot access its HLRs, and thus they cannot route the calls to the right MSC by themselves.

In practise it is also possible that all MSC's are also GMSC's in a PLMN.

Serving GPRS Support Node (SGSN)

The serving GPRS support node (SGSN) is the central element in the packet – switched network. It contains two types of information:

- Subscription information
- IMSI
- Temporary identities

- PDP addresses
- Location information
- The cell or the routing area where the MS is registered.
- VLR number
- GGSN address of each GGSN for which an active PDP context exists

The SGSN connects to the UTRAN via the IuPS interface and to the BSS via the Gb interface.

Gateway GPRS Support Node (GGSN)

The gateway GPRS support node corresponds to the GMSC in the circuit – switched network. But whereas the GMSC only routes the incoming traffic, the GGSN must also route the outgoing traffic. It has to maintain the following data:

- Subscription information
- IMSI
- PDP addresses
- Location information
- The SGSN address of the SGSN where the MS is registered.
- The GGSN receives this information from the HLR and from the SGSN.

1.2.2 UMTS Radio Access Network

Radio Network Controller (RNC)

The radio network controller controls one or more Node Bs. It may be connected via Iu interface to an MSC(IuCS) or to an SGSN (IuPS). The interface between RNCs (Iur) is a logical interface and a direct physical connection doesn't necessarily exist. An RNC is comparable to a base station controller (BSC) in GSM networks.

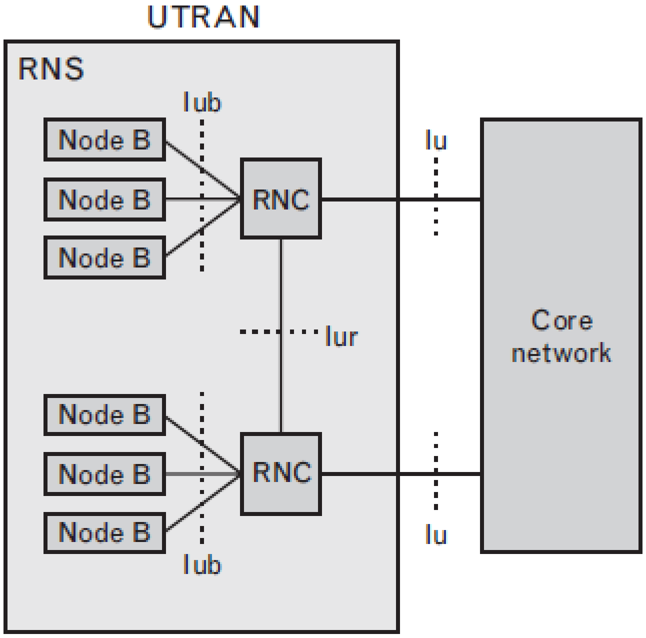


Figure 7 : UTRAN components and interfaces

Functions that are performed by the RNC include :

- Iub trasport resources managemetn
- Control of Node B logical O&M resources
- System information management and scheduling of system information
- Traffic management of common channels
- Modifications to active sets that is soft handover
- Allocation of downlink channelization codes
- Uplink outer – loop power control
- Downlink power control

- Admission control
- Reporting management
- Traffic management of shared channels

Node B

Node B is the UMTS equivalent of a base station transceiver. It may support one or more cells, although in general the specifications only talk about ine cell per Node B. The Node B term in generally used as a logical concept. When physical entities are referred to then the Base station term is often used instead. Functions that are performed by a Node B include :

- Node B logical O&M implementation
- Mapping of Node B logical resources onto hardware resources
- Transmitting of system information messages according to scheduling parameters given by the RNC
- Uplink inner – loop power control (in FDD mode)
- Reporting of uplink interference measurements and downlink power information

In addition, because Node B also contains the air interface physical layer, it has no perform the following functions related to it:

- Error detection on transport channels and indication to higher layers
- FEC encoding decoding of transport channels
- Rate matching
- Power weighting and combining of physical channels
- Modulation and spreading demodulation and dispreading of physical channels
- Frequency and time synchronization
- Radio measurements and indication to higher layers
- RF processing

2. LTE Network Architecture

2.1 Introduction

Long Term Evolution or LTE is a 3GPP defined radio access technology also known as 4G LTE. 3GPP Release 10 is the first stage of the LTE-Advanced realization. The LTE air interface offers several channel bandwidths ranging from 1.4MHz to 20MHz. In addition, LTE air interface supports both frequency division duplexing (FDD) and time division duplexing (TDD).The peak data rates can be 150 Mbps in the downlink and 50 Mbps in the uplink. The LTE is based on Orthogonal Frequency Division Multiplexing (OFDM). The peak data rates can be further increased by using advanced Multiple Input Multiple Output (MIMO) and Carrier Aggregation solutions. The Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) contains only one network element called evolved NodeB (eNodeB). Note that E-UTRAN does not include a centralized radio network controller element but is simply a network of base stations.

The 3GPP System Architecture Evolution (SAE) framework is concerned with the evolved packet core network architecture. The combined LTE/SAE framework defines the Evolved Packet System (EPS) architecture. The EPS consists of the Evolved Packet Core (EPC) and the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). The Evolved Packet Core contains a control plane entity called Mobility Management Entity (MME), and two user plane entities called Serving Gateway (S-GW) and Packet Data Network (PDN) Gateway (P-GW).

Furthermore, it is possible to implement the Serving Gateway and PDN Gateway either within a single node or as separate nodes. In either case, the solution is based on the Network Gateway that is used. Correspondingly, the MME is based Network Server software platform.

The EPC network architecture is purely IP-based. Consequently, the Evolved Packet Core is not concerned with circuit-switched technology. For instance, voice services are based on Voice-over-IP (VoIP). Alternatively, terminals - since they are multi-mode - can switch to 2G/3G access in the case of a circuit-switched call.

2.1.1 Key benefits of LTE

The combined long term evolution and system architecture evolution concept, in other words the Evolved Packet System (EPS), offers the following benefits:

- Flexible allocation and usage of frequency bands, which (for instance) allows re-farming of 2G spectrum

- Reduced cost of ownership, due to fewer nodes - and fewer types of nodes - in the network and fewer interfaces in the radio access network, as well as the unified infrastructure based on IP transport

- No packet loss - or at least reduced packet loss - during inter-eNodeB handovers. This is beneficial for TCP-based services

- Low latency due to the reduced number of nodes in the user plane. This is beneficial for real-time services.

- LTE/EPS architecture allows major improvements and updates to the network by software only.

- LTE operation can be in Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD).

- Carrier Aggregation allows further spectrum allocation flexibility and grouping of bands to increase the data rates of users.

2.2 LTE Network Reference Model

The 3GPP LTE/SAE network architecture consists of the Evolved Packet Core (EPC) and Evolved UMTS Terrestrial Radio Access Network (Evolved UTRAN), as defined by the 3GPP technical specification 23.401.

Interfaces are provided among others towards:

- the packet-switched core (PS Core) of a 3GPP non-LTE 2G/3G network
- the Home Subscriber Server (HSS) managing the user profiles
- various types of packet data networks.

In the Evolved UTRAN, there is only one type of network element, called evolved Node B (eNodeB).

The Evolved Packet Core contains a control plane entity called Mobility Management Entity (MME), and two user plane entities called Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). In some scenarios, these entities are usually integrated into a single network element.

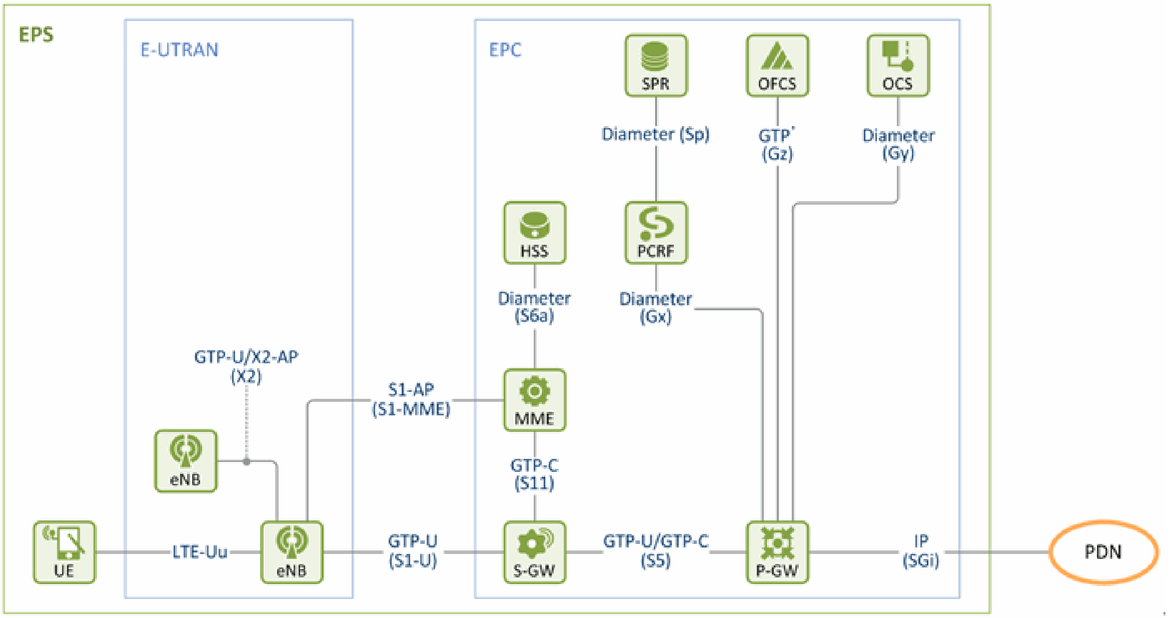


Figure 8 : LTE Network Reference Model

In the following Tables we can read a short description of LTE (Table 1) and EPC (Table 2) entities of the above figure. A detailed description for some of the EPC elements will be followed.

Entity	Description
UE	A UE connects to an eNB the LTE – Uu interface.
eNodeB (eNB)	The evolved Node B (eNodeB) supports the LTE air interface and also provides the packet-switched functionality of a traditional radio network controller (RNC). As a result, the Evolved UTRAN does not require a separate RNC network element. The eNodeB is responsible for radio transmission to and reception from the UE. This involves the following functionalities: • admission control • radio bearer control • scheduling of user data • control signaling over the air interface • IP packet header compression over the air interface. The area covered by a single eNodeB can be split into one or more cells – but typically three cells. The X2 interface between adjacent base stations supports inter-eNodeB handovers, although such handovers can also be performed in a non-optimal way without the X2 interface.

Table 1: LTE Entities

Entity	Description
MME	The Mobility Management Entity provides the control plane functionality in the Evolved Packet Core (EPC) network. This network element: • generates temporary identities and allocates them to UEs • makes sure that users in the idle state can be reached • manages the signaling during handovers • authenticates users, based on the data obtained from the Home Subscriber Server (HSS) • manages bearers in the user plane Note that no user plane traffic goes through the Mobility Management Entity.
S – GW	The Serving Gateway is responsible for packet forwarding, routing, and buffering of downlink data for UEs that are in the idle state. It also serves as a mobility anchor point during inter-eNodeB handovers,
P – GW	The PDN Gateway is the user plane gateway towards the packet data network (PDN). The PDN Gateway allocates IP addresses to mobile users, and provides policy enforcement functionality and charging support. It also serves as a mobility anchor point during inter-system mobility. The main functions support by a P-GW are: - IP routing and forwarding. - UE IP address allocation. - Mobility anchoring between 3GPP and non-3GPP. - PCRF functions. - Charging per-SDF/per-User.

HSS	HSS is an internal database where user profiles can be stored. It gives the access to user for authentication details and user profiles to the MME.
PCRF	A PCRF is the policy and charging control entity. PCRF functions: •Binding mechanism, associates a service data flow to the EPS bearer deemed to transport the service data flow. •Reporting •Credit Management •Event Trigger •Policy Control •Service (data flow) prioritization and conflict handling •Standardized QoS characteristics •Termination Action •Handling of packet filters.
OCS	An OCS give us the option for online charging to control the credit balance in real time and the opportunity to charge the user either based on volume or time.

Table 2: EPC Entities

2.3 Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

E-UTRAN is the air interface of 3GPP’s Long-Term Evolution (LTE) upgrade path for mobile networks. It is a radio access network standard meant to be a replacement of the UMTS, HSDPA, and HSUPA technologies specified in 3GPP releases 5 and beyond. LTE’s E-UTRAN is an entirely new air interface system, which provides higher data rates and lower latency and is optimized for packet data. It uses OFDMA radio access for the downlink and SC-FDMA for the uplink. The E-UTRAN in LTE architecture consists of a single node, i.e., the eNodeB that interfaces with the user equipment (UE). The aim of this simplification is to reduce the latency of all radio interface operations. eNodeBs are connected to each other via the X2 interface, and they connect to the PS core network via the S1 interface.

The **Evolved-Universal Terrestrial Radio Access Network (E-UTRAN)** contains only one network element called evolved NodeB (eNodeB). EPS the 3GPP System Architecture Evolution (SAE) framework is concerned with the evolved packet core network architecture. The combined LTE/SAE framework defines the Evolved Packet System (EPS) architecture. The EPS consists of the Evolved Packet Core (EPC) and the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).

The Evolved Packet Core contains a control plane entity called Mobility Management Entity (MME), and two user plane entities called Serving Gateway (S-GW) and Packet Data Network (PDN) Gateway (P-GW).

The EPC network architecture is purely IP-based. Consequently, the Evolved Packet Core is not concerned with circuit-switched technology.

The 3GPP LTE/SAE network architecture consists of the Evolved Packet Core (EPC) and Evolved UMTS Terrestrial Radio Access Network (Evolved UTRAN), as defined by the 3GPP technical specification 23.401.

Interfaces are provided among others towards:

the packet-switched core **(PS Core)** of a 3GPP non-LTE 2G/3G network

the Home Subscriber Server **(HSS)** managing the user profiles

various types of packet data networks.

In the Evolved UTRAN, there is only one type of network element, called evolved Node B **(eNodeB).**

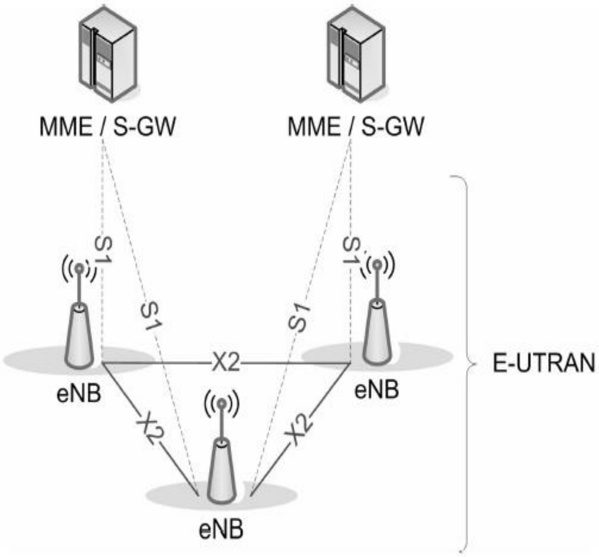


Figure 9 : E-UTRAN architecture

2.4 Evolved Packet Core (EPC) - System Architecture Evolution (SAE)

The main component of the SAE architecture is the Evolved Packet Core (EPC) which consists of the following functional elements:

2.4.1 Serving Gateway (S-GW)

The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and PDN-GW). For idle state UEs, the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, e.g., parameters of the IP bearer service and network internal routing information. It also performs replication of the user traffic in case of lawful interception.

2.4.2 Mobility Management Entity (MME)

The MME is the key control node for the LTE access network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra- LTE handover involving Core Network (CN) node relocation. It is responsible for authenticating the user. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN. Finally, the MME also terminates the S6a interface toward the home HSS for roaming UEs.

2.4.3 Packet Data Network Gateway (P-GW)

The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PDN-GW for accessing multiple packet data networks. The PDN-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the PDN-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies.

The functions of PDN-GW are as follows:

- This is the gateway to Internet. It connects to the SGW through S5-UP interface and to Internet through SGi interface. In forward direction, it takes user data packets from SGW and transfer to internet through SGi interface. In back ward direction, data packets are encapsulated into S5 GTP tunnel and forwarded it to SGW which is responsible for that intended user.
- PDN gateway is also responsible for assigning IP addresses to the mobile devices. This happens when a subscriber switched ON his/her mobile device. Mobile device sends its request to eNODEB which uses the S1-CP and forwards to MME. MME, after authentication, request the PDN gateway on a control plane protocol for IP address. If PDN gateway approves the request then it sends back an assigned IP address to MME. MME forwards it to eNODEB and eNODEB further forwards it to the subscriber. Multiple IP addresses can be assigned to a single mobile device. This is the case which happens when a subscriber is using

a multiple services provided by its network operator’s network such as IP multimedia subsystem.

- It plays an important role in case of international roaming scenarios. A roaming interface is used to connect the GSM/GPRS, UMTS/HSPA, or LTE networks of different network operators of different countries. For example, if a subscriber has moved to another country and wants to connect to an internet then a foreign network will query the user data base in the home network for authentication purposes. After authentication a bearer is established and GTP user tunnel is created between SGW of visitor’s network and PDN-GW of subscriber’s home network over an interface called S8.

2.4.4 Home subscriber server (HSS)

HSS is a data base that stores the information of each and every user in the network. It also does the authentication and authorization of the users and services provided to them. In UMTS and GSM, the database is referred to as Home location register (HLR). HSS and HLR are combined so that the seamless roaming can be made possible between different radio access networks. HSS stores the user parameters like IMSI, authentication information to authenticate the subscriber, circuit switch properties e.g. user telephone number and the services a user is allowed to use e.g. SMS, call forwarding etc.

2.4.5 PCRF (Policy and Charging Rules Function)

The PCRF server manages the service policy and sends QoS setting information for each user session and accounting rule information. The PCRF Server combines functionalities for the following two UMTS nodes:

- The Policy Decision Function (PDF)
- The Charging Rules Function (CRF)

The PDF is the network entity where the policy decisions are made. As the IMS session is being set up, SIP signaling containing media requirements are exchanged between the terminal and the P-CSCF. At some time in the session establishment process, the PDF receives those requirements from the P-CSCF and makes decisions based on network operator rules, such as:

- Allowing or rejecting the media request.
- Using new or existing PDP context for an incoming media request.
- Checking the allocation of new resources against the maximum authorized

The CRFs role is to provide operator-defined charging rules applicable to each service data flow. The CRF selects the relevant charging rules based on information provided by the P-CSCF, such as Application Identifier, Type of Stream (audio, video, etc.), Application Data Rate, etc.

The PCRF (Policy Control and Charging Rules Function) is a functional element that encompasses policy control decision and flow based charging control functionalities. These 2 functionalities are the heritage of the release 6 logical entities PDF and CRF respectively. 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 receives session and media related information from the AF and informs AF of traffic plane events.

3. Gx Reference Point

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control or both by applying AVPs relevant to the application.

3.1 Gx Reference model

The Gx reference point is defined between the PCRF and the PCEF. The relationships between the different functional entities involved are depicted in the following figure.

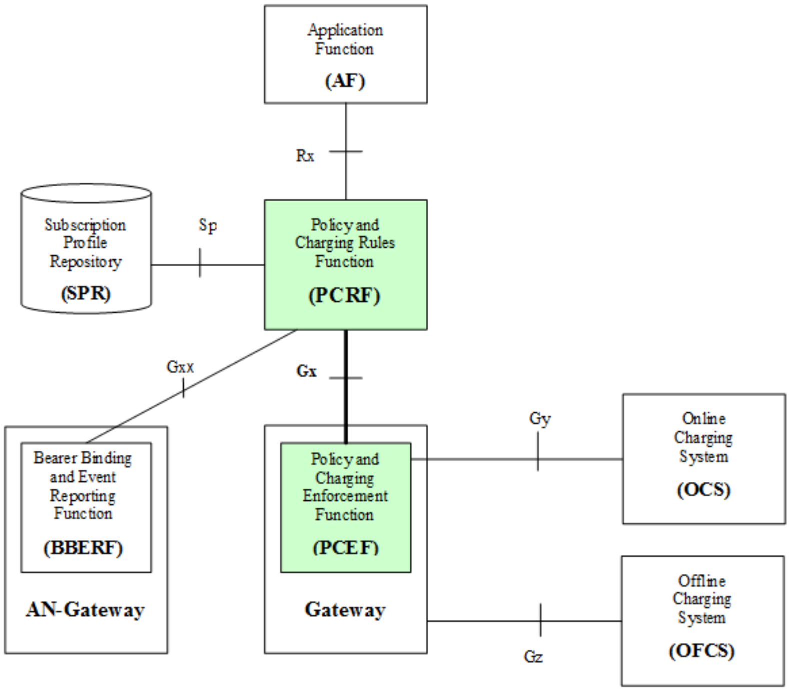

Application Function (AF)
Rx
Subscription Profile Repository (SPR)
Sp
Policy and Charging Rules Function (PCRF)
Gxx
Gx
Gy
Online Charging System (OCS)
Bearer Binding and Event Reporting Function (BBERF)
AN-Gateway
Policy and Charging Enforcement Function (PCEF)
Gateway
Offline Charging System (OFCS)
Gz

Figure 10: Gx and Gy reference point

3.2 Gx/Gxc application

3.2.1 Gx / Gxc application overview

Gateway uses the Gx/Gxc interfaces for connecting Gateway with the PCRF. The Gateway's Diameter policy control interface is compliant with the 3GPP Release 8 (September 2009), 3GPP Release 9 (December 2010) and 3GPP Release 10 (March 2012). Gx is the interface between the policy and charging enforcement function (PCEF) and the PCRF. Gxc is the interface between the bearer binding and event reporting function (BBERF) and the PCRF.

Policy enforcement can be applied to Gateway in two ways:

- Pull mode A Credit-Control-Answer (CCA) message is received from the PCRF upon a Credit-Control-Request (CCR) message sent towards the PCRF.

- Push mode A Re-Authorisation-Request (RAR) message is received from the PCRF.

These messages will be further explained later in this chapter.

3.2.2 Gx

The Gx interface is used between the P-GW or the GGSN (depending on whether Gateway is used in LTE or 3G mode) and the PCRF. Gateway supports default evolved packet system (EPS) bearer control, dedicated bearer flow control, and service data flows.

The following Diameter commands are supported with Gx:

- Credit-Control-Request/Credit-Control-Answer (CCR/CCA) commands

- Re-Auth-Request/Re-Auth-Answer (RAR/RAA) commands

3.3 Commands used in Gx

3.3.1 CCR/CCA

The Gx application in Gateway uses the CCR message to create, update, and terminate sessions towards the PCRF and to transfer sessions and bearer information. In addition, the CCR is used to report accumulated usage for a specific monitoring key when usage monitoring is enabled. The CCA message carries QoS information from the PCRF towards the PCEF (NOKIA Gateway) and it can also provide PCC rule bases that the PCEF (NOKIA Gateway) should install and/or remove. The PCRF requests for updates (CCR-U messages) from NOKIA Gateway by registering events specified in event triggers in CCA/RAR messages. When a specific event (for which the PCRF has registered) occurs, the PCEF (NOKIA Gateway) sends a CCR-U message to the PCRF. The Event-Trigger AVP contains the event type. The new value is included in the corresponding AVP of the CCR-U.

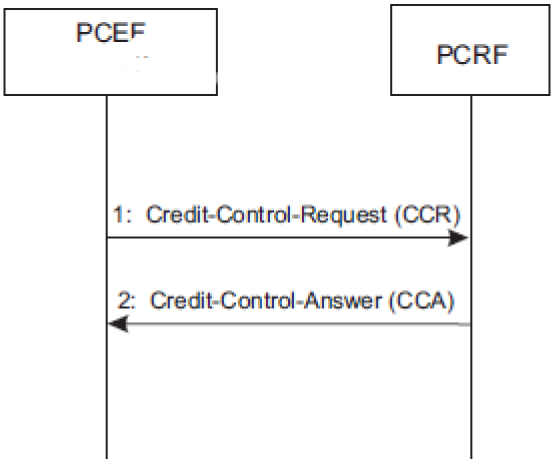

PCEF
PCRF
1: Credit-Control-Request (CCR)
2: Credit-Control-Answer (CCA)

Figure 11: CCR and CCA command flow with Gx

3.3.2 RAR/RAA

The PCRF uses the RAR message to invoke the PCEF (NOKIA Gateway) session update and termination procedures.

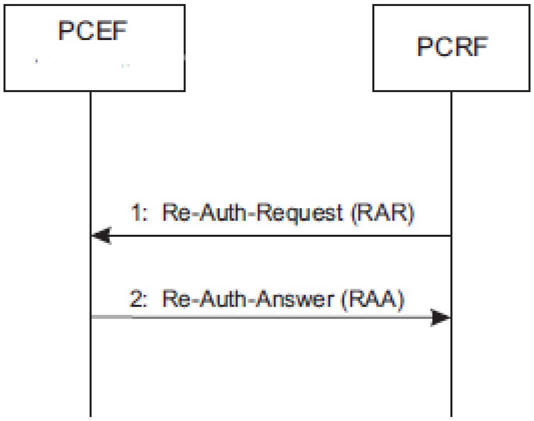


Figure 12: RAR and RAA command flow with Gx

3.4 Result codes with Gx/Gxc

By default, when any error result code (protocol, transient, permanent or unknown) appears in the received CCA-I message session establishment is not achieved. Also, when any error result code appears in the received CCA-U message only the update procedure fails while the session remains open. However, it is possible to configure the Gateway's behavior when the PCRF returns an error result code value in a CCA message which indicates an error or failure.

Configuration is made per result code or result code category. Depending on the error code the PCRF returns and the action configured for the specific error code or error code category, the session/context can be terminated, accepted to continue ignoring the received result code, or accepted to continue while terminating the Gx session. Also, assuming that a secondary PCRF is configured, a switchover can be performed. To avoid loops, if the secondary PCRF also responds with an error result code or if the secondary PCRF cannot be contacted, the session is terminated.

For configuration instructions see *Configuring the action applied to user sessions based on the received PCRF result codes and/or result code categories* in *Gateway's User Guide*. The actions configured for the result codes or result code categories are not applied on user sessions established in the S5 PMIP variant. Instead, the default handling is in effect for these sessions.

Value	Message name
2001	DIAMETER_SUCCESS
3001	DIAMETER_COMMAND_UNSUPPORTED
3007	DIAMETER_APPLICATION_UNSUPPORTED
5001	DIAMETER_AVP_UNSUPPORTED
5004	DIAMETER_INVALID_AVP_VALUE
5005	DIAMETER_MISSING_AVP
5009	DIAMETER_AVP_OCCURS_TOO_MANY_TIMES

Table 3: Result codes supported by the Diameter implementation

3.5 Handling of PCC rule bases with CCA and RAR

3.5.1 Activation of PCC rule bases through CCA-I

The following figure illustrates the activation of PCC rule bases through the CCA-I message.

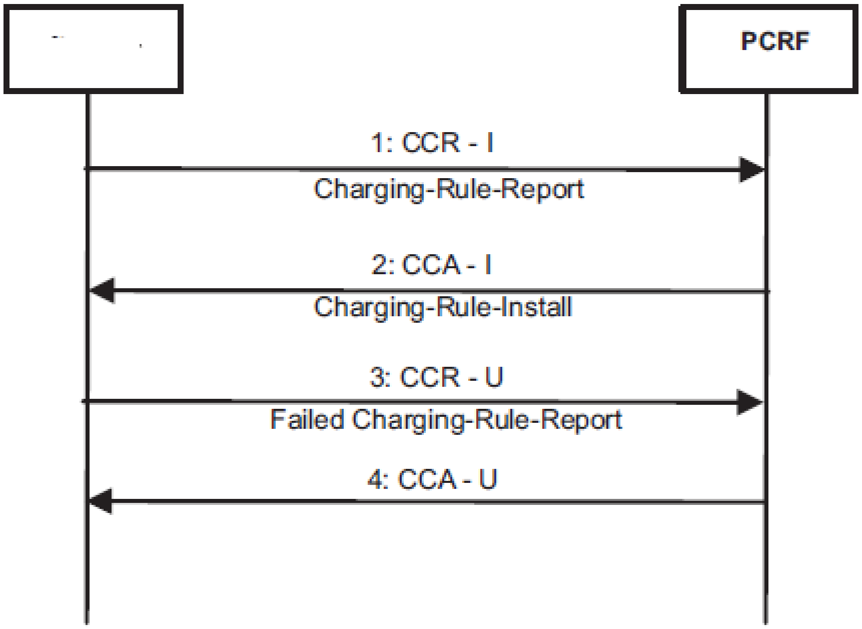


Figure 13: Activation of PCC rule bases through the CCA-I message

The procedure for activating PCC rule bases through the CCA-I message is as follows:

1. Gateway sends a CCR-I message to the PCRF. If there are PCC rule bases that are pre-installed for the specific session (for example, configured in the subscriber's session profile), then Gateway reports them in the CCR-I.

2. The PCRF responds with a CCA-I message containing a Charging-Rule-Install AVP that includes the PCC rule bases to be installed. This AVP includes the PCC rule base names which are used for referencing a PCC rule in the communication between Gateway and the PCRF. Then, Gateway installs the PCC rule bases.

- The next steps are followed only if the PCC rule base installation fails.

3. If the PCC rule base installation fails, then Gateway sends a CCR-U message with failed PCC rule bases along with the PCC-Rule-Status AVP value set to INACTIVE in the Charging-Rule-Report.

4. The PCRF responds with a CCA-U message, which includes the Success or Failure result codes. If Gateway receives a Failure result code, the session is terminated, while if it receives a Success result code, the procedure from step 2 onwards is repeated.

3.5.2 Activation of PCC rule bases through CCA-U

The following figure illustrates the activation of PCC rule bases through CCA-U.

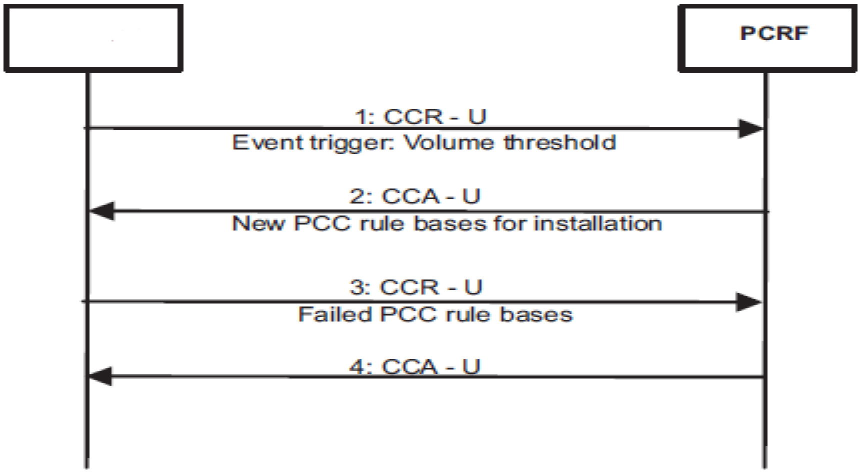

PCRF
1: CCR - U
Event trigger: Volume threshold
2: CCA - U
New PCC rule bases for installation
3: CCR - U
Failed PCC rule bases
4: CCA - U

Figure 14: Activation of PCC rule bases through CCA-U

The procedure for activating PCC rule bases through CCA-U is as follows:

1. For any internal event trigger, Gateway sends a CCR-U message to the PCRF (for example, Volume-threshold, Revalidation-timeout).

2. The PCRF responds with a CCA-U message, which includes PCC rule bases for installation. Then, Gateway installs the PCC rule bases.

3. If the PCC rule base installation fails, then Gateway sends a CCR-U message with the failed PCC rule bases along with the PCC-Rule-Status AVP value set to INACTIVE in the Charging-Rule-Report.

4. The PCRF responds with a CCA-U message, which includes the Success or Failure result codes. If Gateway receives a Failure result code, the session will be terminated, while if it receives a Success result code, and new PCC rule bases are available in the CCA-U message, the procedure from step 2 onwards will be repeated.

3.5.3 Deactivation of PCC rule bases through CCA

The following figure illustrates the deactivation of PCC rule bases with the CCA message.

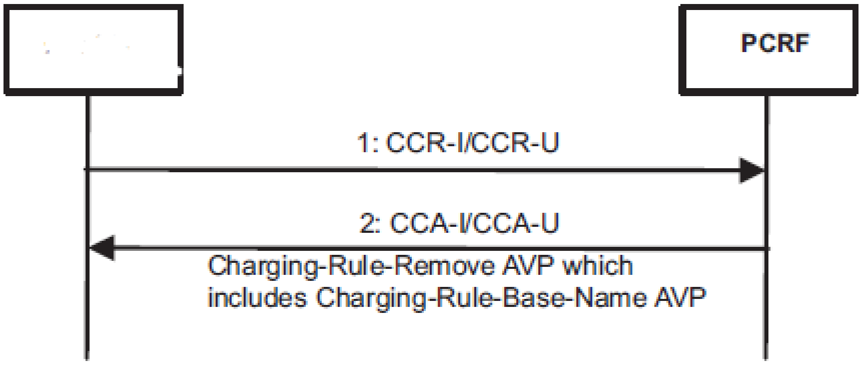

PCRF
1: CCR-I/CCR-U
2: CCA-I/CCA-U
Charging-Rule-Remove AVP which
includes Charging-Rule-Base-Name AVP

Figure 15: Deactivation of PCC rule bases with CCA-I or CCA-U message

The procedure for deactivating PCC rule bases with the CCA-I or CCA-U message is as follows:

1. Gateway sends a CCR-I or CCR-U message to the PCRF.

2. The PCRF responds with a CCA-I/ CCA-U message containing a Charging-Rule-Remove AVP that includes the PCC rule bases to be deactivated for the session. Each PCC rule base name to be deactivated is included in a Charging-Rule-Base- Name AVP under Charging-Rule-Remove AVP.

3.5.4 Activation of predefined PCC rules with CCA

The following figure illustrates the activation of predefined PCC rules with the CCA message.

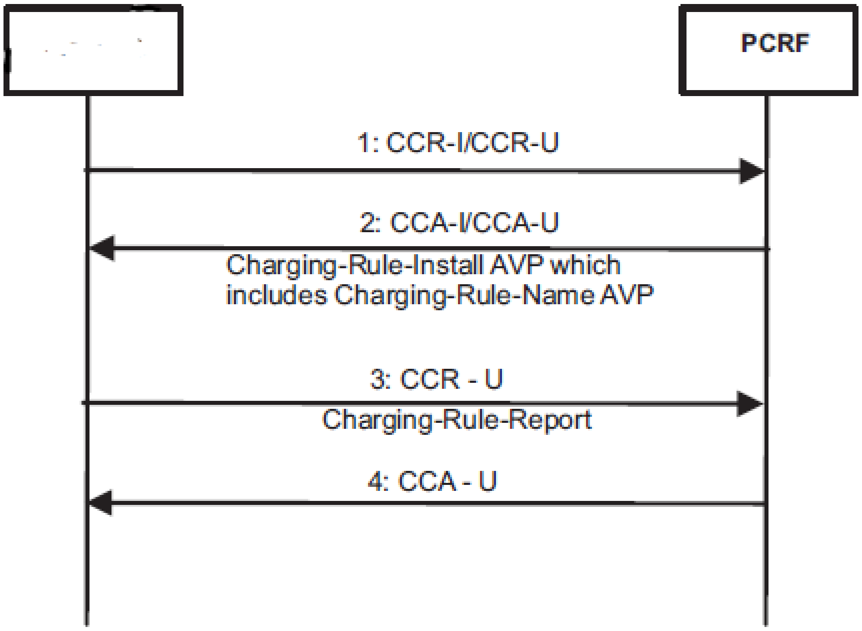


Figure 16: Activation of predefined PCC rules with the CCA-I/CCA-U message

1. Gateway sends a CCR-I or CCR-U message to the PCRF.

2. The PCRF responds to the CCR-I/ CCR-U message with a CCA-I/CCA-U message and the Charging-Rule-Install AVP that includes the predefined PCC rules to be activated for the session. Each predefined PCC rule name to be activated is included in

a Charging-Rule-Name AVP under Charging-Rule-Install AVP. The predefined PCC rule names should be configured in Gateway according to the instructions provided in chapter *Defining which PCC rules can be activated/deactivated by PCRF* in *Gateway's User Guide*. Note that Gateway can accept up to 200 predefined PCC rule names in a single message.

3. Gateway sends a CCR-U message to the PCRF to report the result of the operation. If there are PCC rules that were successfully activated, these will be reported only if the event trigger SUCCESSFUL_RESOURCE_ALLOCATION has been received from the PCRF and additionally if the Charging-Rule-Install AVP that triggered the activation of these rules contained the Resource-Allocation-Notification AVP with the value ENABLE_NOTIFICATION (0). The successful rule(s) are included inside the Charging-Rule-Report AVP, where their names are indicated in the Charging-Rule- Name AVP and their status is set to ACTIVE in the PCC-Rule-Status AVP. If there are PCC rules that failed to be activated, these will always be reported to PCRF. The failed rule(s) are included inside the Charging-Rule-Report AVP, where their names are indicated in the Charging-Rule-Name AVP, the failure reason is indicated in the Rule-Failure-Code AVP and their status is set to INACTIVE in the PCC-Rule-Status AVP.

In case it is required to report different PCC-Rule-Status or Rule-Failure-Code values for different groups of rules within the same message, Gateway reports the information for different groups using separate Charging-Rule-Report AVPs.

4. The PCRF responds with a CCA-U message.

4. Gy interface

The Gy interface is used between an external OCS and Gateway.

The following Diameter commands are supported with Gy:

- CCR/CCA commands.
- RAR/RAA commands.

4.1 Commands with Gy

4.1.1 CCR/CCA

The Gy application in Gateway uses the CCR message to create, update, and terminate sessions towards the OCS and to transfer information about the sessions.

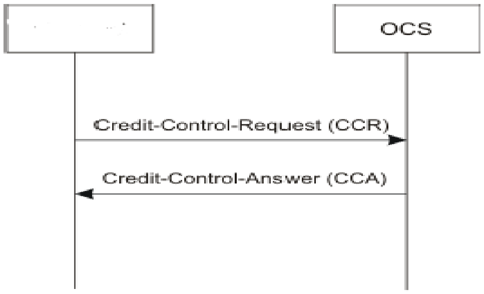


Figure 17: CCR and CCA command flow with Gy

4.1.2 RAR/RAA

The OCS can use a Re-Auth-Request (RAR) in order Gateway to send a CCR message. The AVPs in the request define the scope of re-authorization: DCCA session, rating group, or a combination of rating group and service identifier. If no rating group is provided, reauthorization is performed for all active rating groups. During the time between a CCR and a CCA message traffic is allowed to pass and the local default quota is used. If the OCS grants a valid quota, previous traffic is deducted.

4.2 Result codes with Gy

4.2.1 Result codes sent by Gateway

All Diameter answers sent by Gateway contain one of the result codes listed in Table *Result codes sent by Gateway*. Gateway does not send other codes.

Value (Code)	Meaning
SUCCESS (2001)	Gateway successfully fulfilled an OCS request.
LIMITED_SUCCESS (2002)	In RAA messages only: a CCR message is sent because of the RAR message.
COMMAND_UNSUPPORTED (3001)	An unsupported command is received.
APPLICATION_UNSUPPORTED (3007)	A command contained an unsupported application identifier.
AVP_UNSUPPORTED (5001)	An unsupported mandatory AVP is encountered. The Failed-AVP contains the offending AVP.

Table 4: Result codes supported by the Diameter implementation in Gy interface

5. Result-Code AVP

AVP code is a number in Unsigned32 type and show us that:

1) We have a successful complete request from user side

2) An error was found.

The messages that diameter answer to the requested messages need to include at least on AVP (Called result-code).

An AVP that is not successful (one containing a non-2xxx value other than DIAMETER_REDIRECT_INDICATION) it is needed to have the error-report-hosting AVP in case that the value of host that it is inserted in the result-code AVP is different from the value presented in the Origin-Host AVP. The dimeter protocol are supporting the types of errors that are shown below, all of them can be recognized from the first digit (show the thousands) in the decimal notation:

- 1xxx (Informational)
- 2xxx (Success)
- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

A type of error that it isn’t represented in the above list can be considered as unknown and needs to take it as a fail error case.

5.1 Informational

Errors that fall within this category are used to inform the requester that a request could not be satisfied, and additional action is required on its part before access is granted.

- ➢ DIAMETER_MULTI_ROUND_AUTH 1001:

This informational error is returned by a Diameter server to inform the access device that the authentication mechanism being used requires multiple round trips, and a subsequent request needs to be issued in order for access to be granted.

5.2 Success

Errors that fall within the Success category are used to inform a peer that a request has been successfully completed.

- ➢ DIAMETER_SUCCESS 2001

The request was successfully completed.

- ➢ DIAMETER_LIMITED_SUCCESS 2002

When returned, the request was successfully completed, but additional processing is required by the application in order to provide service to the user.

5.3 Protocol Errors

Errors that fall within the Protocol Error category SHOULD be treated on a per-hop basis, and Diameter proxies MAY attempt to correct the error, if it is possible. Note that these errors MUST only be used in answer messages whose ’E’ bit is set.

- DIAMETER_COMMAND_UNSUPPORTED 3001

This error code is used when a Diameter entity receives a message with a Command Code that it does not support.

- DIAMETER_UNABLE_TO_DELIVER 3002

This error is given when Diameter cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request or because the Destination-Host AVP was given without the associated Destination-Realm AVP.

- DIAMETER_REALM_NOT_SERVED 3003

The intended realm of the request is not recognized.

- DIAMETER_TOO_BUSY 3004

When returned, a Diameter node SHOULD attempt to send the message to an alternate peer. This error MUST only be used when a specific server is requested, and it cannot provide the requested service.

- DIAMETER_LOOP_DETECTED 3005

An agent detected a loop while trying to get the message to the intended recipient. The message MAY be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.

- DIAMETER_REDIRECT_INDICATION 3006

A redirect agent has determined that the request could not be satisfied locally, and the initiator of the request SHOULD direct the request directly to the server, whose contact information has been added to the response. When set, the Redirect-Host AVP MUST be present.

- DIAMETER_APPLICATION_UNSUPPORTED 3007

A request was sent for an application that is not supported.

- DIAMETER_INVALID_HDR_BITS 3008

A request was received whose bits in the Diameter header were set either to an invalid combination or to a value that is inconsistent with the Command Code's definition.

- DIAMETER_INVALID_AVP_BITS 3009

A request was received that included an AVP whose flag bits are set to an unrecognized value or that is inconsistent with the AVP's definition.

- DIAMETER_UNKNOWN_PEER 3010

A CER was received from an unknown peer.

6. Implementation and testing of PCRF and OCS scripts

The main task of this thesis was the modification of Gy interface (OCS) scripts in "C" so that it supports error codes in CCR – I (Initial) messages. Development was needed in order the error code value to be configurable by the user. The configurable error code value to be sent for a configurable percentage of CCR messages. Another task was the modification of Gx interface (PCRF) script in "Pearl" so that it supports error codes in CCR – I (Initial) message. The error code value should be configurable by the user. The configurable error code value to be sent for a configurable percentage of CCR messages.

The following screenshots show the result code in the appropriate AVP (result – code) as the user configured the script for OCS and PCRF respectively. Details and configuration of the script cannot be presented as it is confidential NOKIA material. All the tests and runs executed in NOKIA Technology Center of Athens Lab.

6.1 NOKIA TC Athens Lab Environment

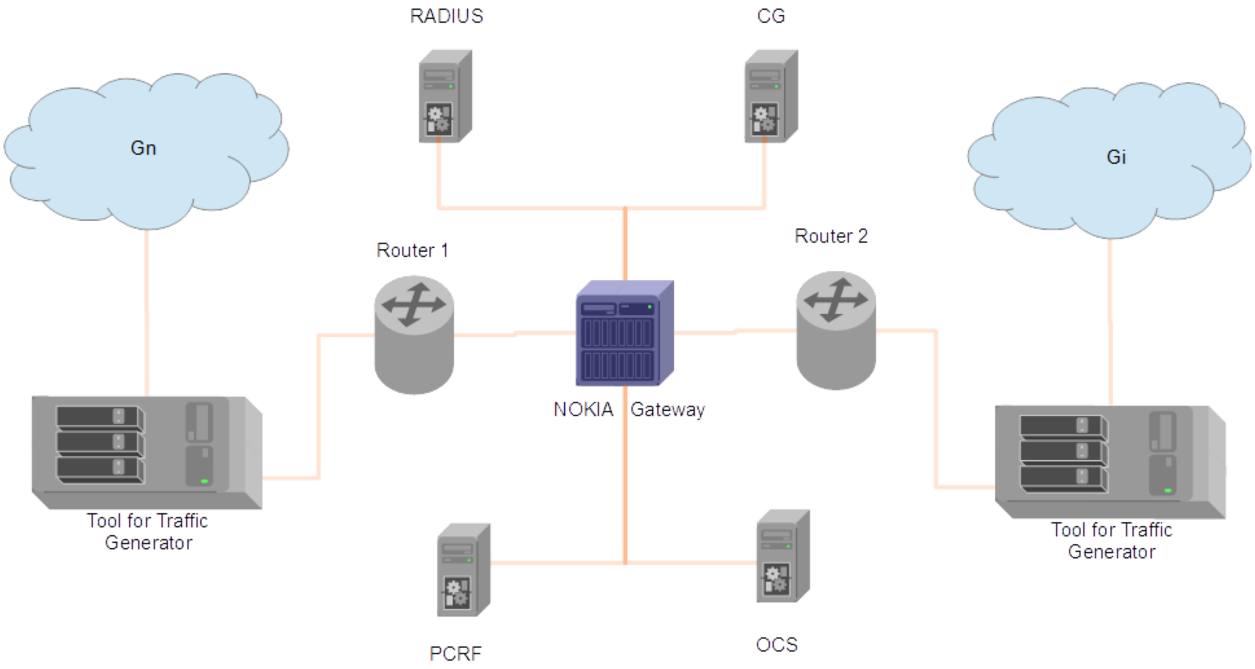


Figure 18: NOKIA’s Lab Environment

The above figure show us a short description of the Lab environment in NOKIA TC Athens where all of our test executed. Our first task was the configuration of the Traffic Generation Tool in order to simulate the traffic on Gn and Gi side of our simulated network.

Router 1 and Router 2 are responsible for the routing connections through our network in order all elements to be connected. This wasn’t our responsibility but on the other hand the configuration of Gateway element it was necessary and very useful for our test. All the other elements like (PCRF, OCS, Radius and CG) called peripheral servers and are emulated. They run a simulation script in C or Pearl programming language. For the purpose of this thesis as we have mentioned above we modified the scripts for OCS and PCRF. The other two elements are necessary for our test environment in order to make it as much real as we can.

6.2 Tests Description and Test Results for OCS

The first part of this thesis was the modification of the simulated script for OCS in C in order the user choose his the error code that he wants. The purpose of this modification has two options:

1) Change the charging from Online to Offline using a specific error code in CCR-I message.
2) Reject the session for several reasons using the appropriate error code in every case.

The most important step was to create a library with all supported error codes in order the user can pick the right error code for his test scenario.

The script was running with the below command:

./errorfastocs count=10000000000 time=104 address=xx.xx.xx.xx error=4011

where errorfastocs is the name of scripts, count is the maximum number of CCR/CCA messages that Gateway and OCS can send/receive, time is the value of time that OCS has to send a request to Gateway for providing quota for the user, address is the IP address of peripheral server and the parameter error is the extra option that we add in this script for choosing by the user the error code that the session will be rejected.

6.2.1 Error codes in OCS Responses 1

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce OCS error response 4011

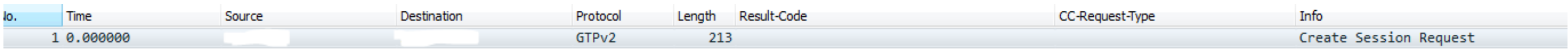
Expected Results:

Verify that signaling and traffic for users without OCS is not affected. The affected user connections are established but online charging is turned to offline if offline charging is enabled.

Comments:

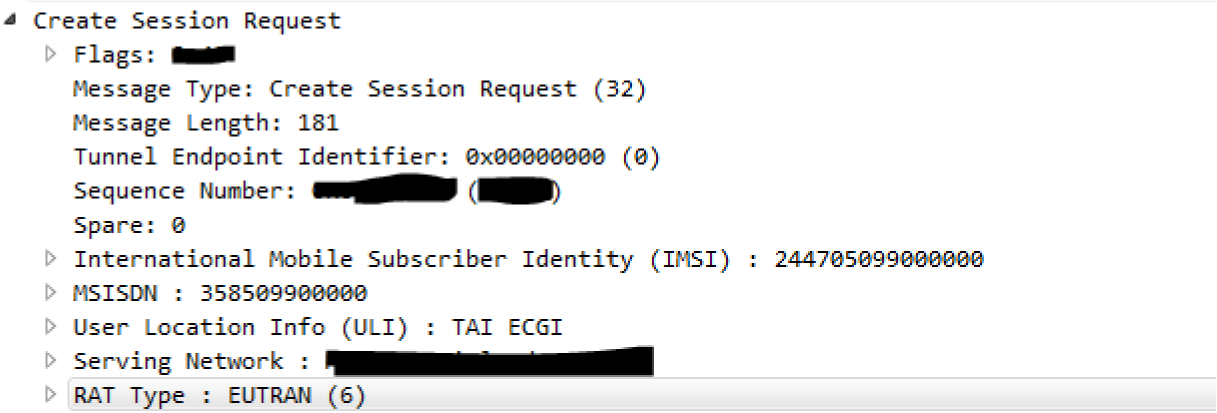
- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to OCS as shown below.



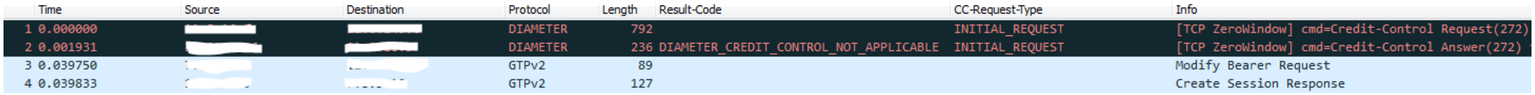
lo.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	213			Create Session Request

Figure 19 : Create Session Request message



```
◢ Create Session Request
  ▷ Flags: [redacted]
    Message Type: Create Session Request (32)
    Message Length: 181
    Tunnel Endpoint Identifier: 0x00000000 (0)
    Sequence Number: [redacted] ([redacted])
    Spare: 0
  ▷ International Mobile Subscriber Identity (IMSI) : 244705099000000
  ▷ MSISDN : 358509900000
  ▷ User Location Info (ULI) : TAI ECGI
  ▷ Serving Network : [redacted]
  ▷ RAT Type : EUTRAN (6)
```

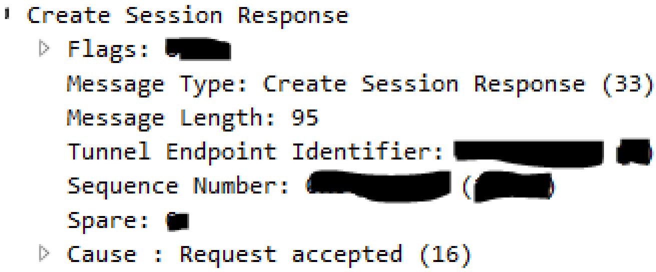
Figure 20 : Detailed avp of Create Session Request



	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	DIAMETER	792		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
2	0.001931	[redacted]	[redacted]	DIAMETER	236	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
3	0.039750	[redacted]	[redacted]	GTPv2	89			Modify Bearer Request
4	0.039833	[redacted]	[redacted]	GTPv2	127			Create Session Response

Figure 21 : CCR/CCA messages and Result Code 4011

As we can see in figure above the CCR and CCA messages was send and received between Gateway and OCS. In CCA message we can see clearly the result code from the error code we choose when we start run the script (4011 = Diameter_Credit_Control_Not_Applicable). The next step for this scenario is to check the Create Session Response message. In case that this is success the session will turn from online charging mode to offline charging mode. The output of this message is shown in the below figure (Cause : Request Accepted).



```
Create Session Response
  ▷ Flags: [redacted]
    Message Type: Create Session Response (33)
    Message Length: 95
    Tunnel Endpoint Identifier: [redacted]
    Sequence Number: [redacted]
    Spare: [redacted]
  ▷ Cause : Request accepted (16)
```

6.2.2 Error codes in OCS Responses 2

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce OCS error response 4012

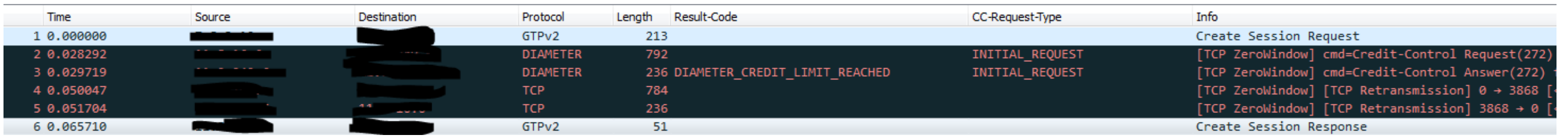
Expected Results:

Verify that signaling and traffic for users without OCS is not affected. The Gateway rejects the affected procedures and sessions.

Comments:

- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

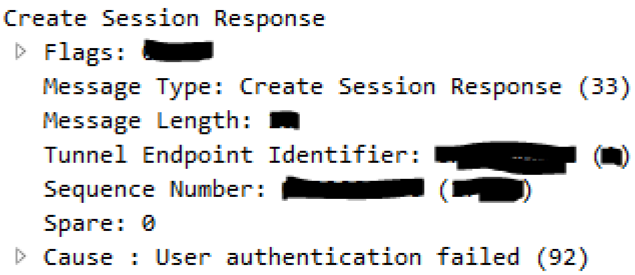
The first message is a Create Session Request from Gateway to OCS as shown below.



	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	213			Create Session Request
2	0.028292	[redacted]	[redacted]	DIAMETER	792		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
3	0.029719	[redacted]	[redacted]	DIAMETER	236	DIAMETER_CREDIT_LIMIT_REACHED	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
4	0.050047	[redacted]	[redacted]	TCP	784			[TCP ZeroWindow] [TCP Retransmission] 0 → 3868 [
5	0.051704	[redacted]	[redacted]	TCP	236			[TCP ZeroWindow] [TCP Retransmission] 3868 → 0 [
6	0.065710	[redacted]	[redacted]	GTPv2	51			Create Session Response

Figure 22 : Create Session Request/Response and CCR/CCA messages for Result Code 4012

As we can see in figure 23 the CCR and CCA messages was send and received between Gateway and OCS. In CCA message we can see clearly the result code from the error code we choose when we start run the script (4012 = Diameter_Credit_Limit_Reached). The next step for this scenario is to check the Create Session Response message. In case that this is reject, the session will be failed and the user authentication will be failed.



```
Create Session Response
▷ Flags: [redacted]
  Message Type: Create Session Response (33)
  Message Length: [redacted]
  Tunnel Endpoint Identifier: [redacted] ([redacted])
  Sequence Number: [redacted] ([redacted])
  Spare: 0
▷ Cause : User authentication failed (92)
```

6.2.3 Error codes in OCS Responses 3

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce OCS error response 5003

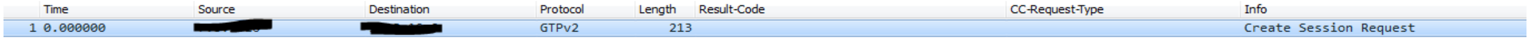
Expected Results:

Verify that signaling and traffic for users without OCS is not affected. The Gateway rejects the affected procedures and sessions.

Comments:

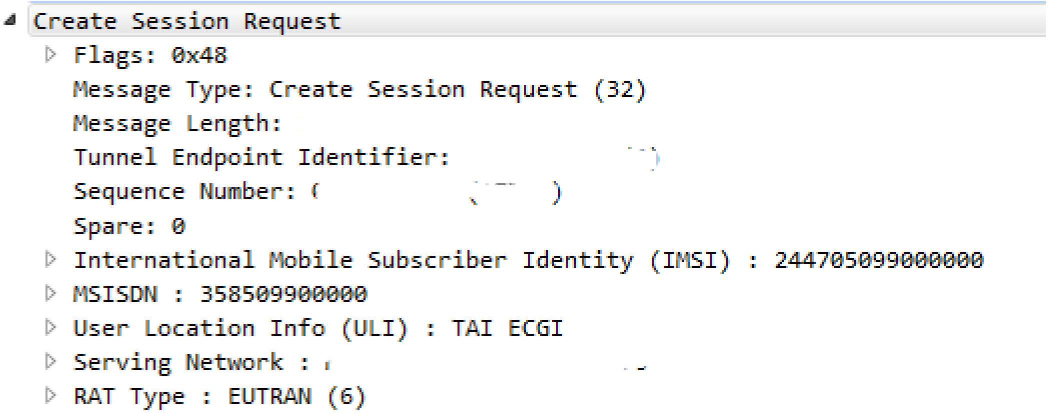
- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to OCS as shown below.



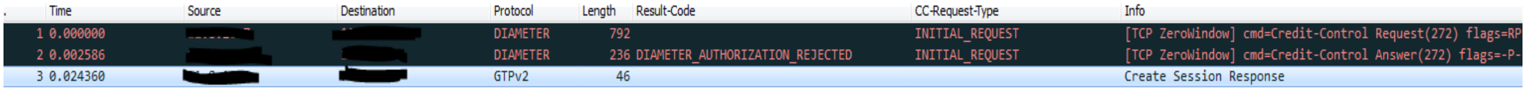
	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	213			Create Session Request

Figure 23 : Create Session Request message



```
◢ Create Session Request
  ▷ Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length:
    Tunnel Endpoint Identifier:
    Sequence Number: (                )
    Spare: 0
  ▷ International Mobile Subscriber Identity (IMSI) : 244705099000000
  ▷ MSISDN : 358509900000
  ▷ User Location Info (ULI) : TAI ECGI
  ▷ Serving Network :
  ▷ RAT Type : EUTRAN (6)
```

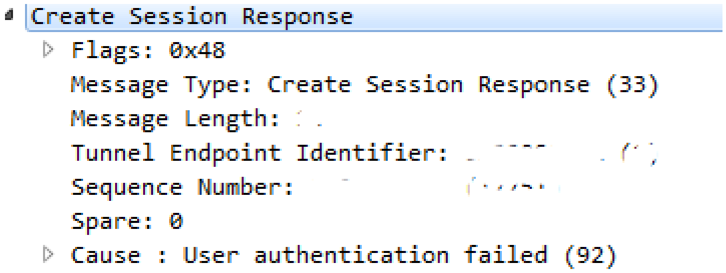
Figure 24 : Detailed avp of Create Session Request



	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	DIAMETER	792		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272) flags=RP
2	0.002586	[redacted]	[redacted]	DIAMETER	236	DIAMETER_AUTHORIZATION_REJECTED	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272) flags=-P-
3	0.024360	[redacted]	[redacted]	GTPv2	46			Create Session Response

Figure 25 : CCR/CCA messages and Result Code 5003

As we can see in figure 26 the CCR and CCA messages was send and received between Gateway and OCS. In CCA message we can see clearly the result code from the error code we choose when we start run the script (5003 = Diameter_Authorization_Rejected). The next step for this scenario is to check the Create Session Response message. . In case that this is reject, the session will be failed and the user authentication will be failed.



```
◢ Create Session Response
  ▷ Flags: 0x48
    Message Type: Create Session Response (33)
    Message Length:
    Tunnel Endpoint Identifier:
    Sequence Number:
    Spare: 0
  ▷ Cause : User authentication failed (92)
```

6.2.4 Error codes in OCS Responses 4

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce OCS error response 5030

Expected Results:

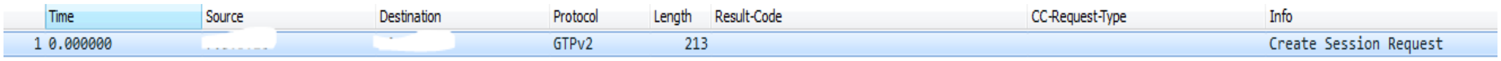
Verify that signaling and traffic for users without OCS is not affected. The Gateway rejects the affected procedures and sessions.

Comments:

- no unexpected files generated during the test.
- alarms generated to be cleared.

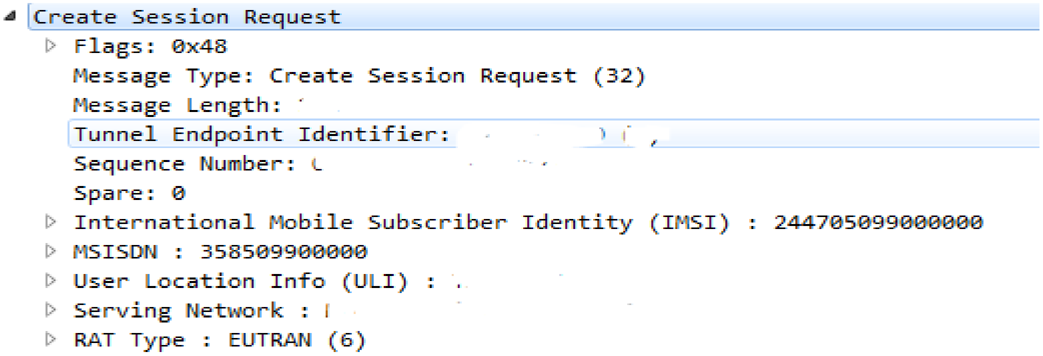
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to OCS as shown below.



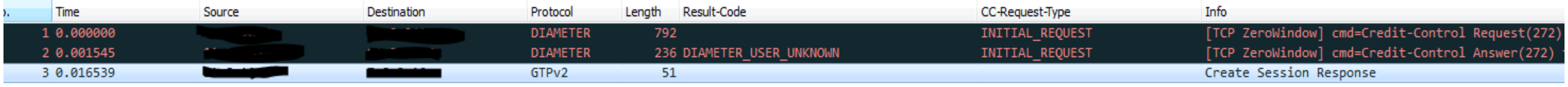
```
  Time        Source      Destination  Protocol  Length  Result-Code  CC-Request-Type  Info
1 0.000000    [redacted]  [redacted]   GTPv2     213                                   Create Session Request
```

Figure 26 : Create Session Request message



```
◢ Create Session Request
  ▷ Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length: [redacted]
    Tunnel Endpoint Identifier: [redacted]
    Sequence Number: [redacted]
    Spare: 0
  ▷ International Mobile Subscriber Identity (IMSI) : 244705099000000
  ▷ MSISDN : 358509900000
  ▷ User Location Info (ULI) : [redacted]
  ▷ Serving Network : [redacted]
  ▷ RAT Type : EUTRAN (6)
```

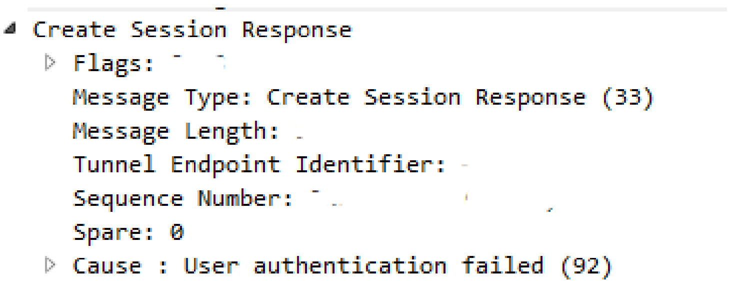
Figure 27 : Detailed avp of Create Session Request



```
  Time        Source      Destination  Protocol  Length  Result-Code            CC-Request-Type  Info
1 0.000000    [redacted]  [redacted]   DIAMETER  792                            INITIAL_REQUEST  [TCP ZeroWindow] cmd=Credit-Control Request(272)
2 0.001545    [redacted]  [redacted]   DIAMETER  236     DIAMETER_USER_UNKNOWN  INITIAL_REQUEST  [TCP ZeroWindow] cmd=Credit-Control Answer(272)
3 0.016539    [redacted]  [redacted]   GTPv2     51                                              Create Session Response
```

Figure 28: CCR/CCA messages and Result Code 5030

As we can see in figure 29 the CCR and CCA messages was send and received between Gateway and OCS. In CCA message we can see clearly the result code from the error code we choose when we start run the script (5030 = Diameter_User_Unknown). The next step for this scenario is to check the Create Session Response message. In case that this is reject, the session will be failed and the user authentication will be failed.



```
◢ Create Session Response
   ▷ Flags:
     Message Type: Create Session Response (33)
     Message Length:
     Tunnel Endpoint Identifier:
     Sequence Number:
     Spare: 0
   ▷ Cause : User authentication failed (92)
```

6.3 Tests Description and Test Results for PCRF

The second part of this thesis was the modification of the simulated script for PCRF in Pearl in order the user choose his the error code that he wants. The purpose of this modification was given to user the option to reject the session for several reasons using the appropriate error code in every case . That could happen by changing the right function in Pearl script by choosing the error code that you wanted to be presented into the specific AVP. The most important step was to create a library with all supported error codes in order the user can pick the right error code for his test scenario.

The script was running with the below command :

./PCS_Qos_VoLTE_DEDI_BEAR_ROBU_Error5030_NoRAR.pl ip: XX.X.XXX.X port:xxxx

where PCS_Qos_VoLTE_DEDI_BEAR_ROBU_Error5030_NoRAR.pl is the name of scripts, ip is the IP address of peripheral server and the parameter port is the port number of the peripheral script.

6.3.1 Error codes in PCRF Responses 1

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce PCRF error response 4011

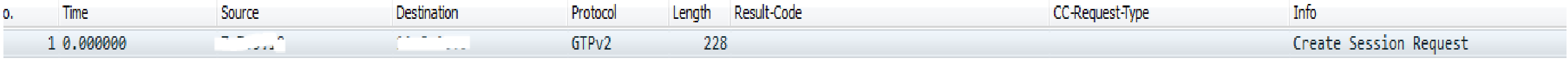
Expected Results:

Verify that signalling and traffic for users without PCRF is not affected. The NG rejects the affected procedures.

Comments:

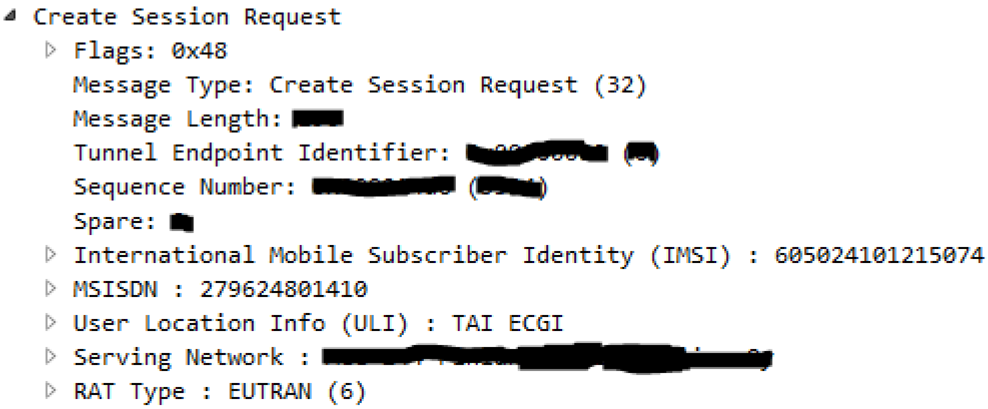
- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to PCRF as shown below.



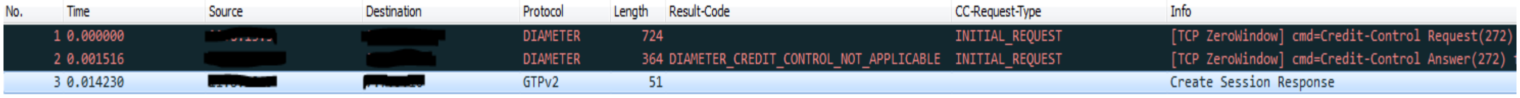
o.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	228			Create Session Request

Figure 29 : Create Session Request message



```
◢ Create Session Request
  ▷ Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length: [redacted]
    Tunnel Endpoint Identifier: [redacted] [redacted]
    Sequence Number: [redacted] [redacted]
    Spare: [redacted]
  ▷ International Mobile Subscriber Identity (IMSI) : 605024101215074
  ▷ MSISDN : 279624801410
  ▷ User Location Info (ULI) : TAI ECGI
  ▷ Serving Network : [redacted]
  ▷ RAT Type : EUTRAN (6)
```

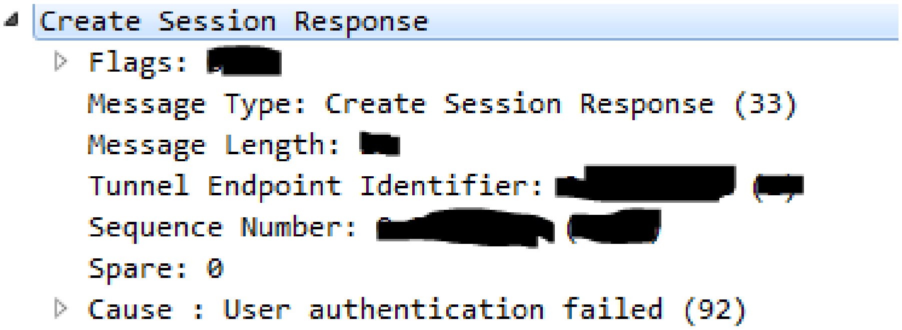
Figure 30 : Detailed avp of Create Session Request



No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	DIAMETER	724		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
2	0.001516	[redacted]	[redacted]	DIAMETER	364	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
3	0.014230	[redacted]	[redacted]	GTPv2	51			Create Session Response

Figure 31 : CCR/CCA messages and Result Code 4011

As we can see in figure above the CCR and CCA messages was send and received between Gateway and PCRF. In CCA message we can see clearly the result code from the error code we choose in the script (4011 = Diameter_Credit_Control_Not_Applicable). The next step for this scenario is to check the Create Session Response message. In case that this is reject, the session will be failed and the user authentication will be failed.



```
◢ Create Session Response
  ▷ Flags: [redacted]
    Message Type: Create Session Response (33)
    Message Length: [redacted]
    Tunnel Endpoint Identifier: [redacted] [redacted]
    Sequence Number: [redacted] [redacted]
    Spare: 0
  ▷ Cause : User authentication failed (92)
```

6.3.2 Error codes in PCRF Responses 2

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce PCRF error response 4012

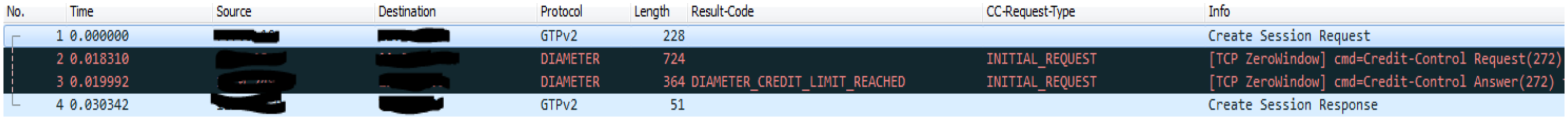
Expected Results:

Verify that signaling and traffic for users without PCRF is not affected. The NG rejects the affected procedures

Comments:

- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

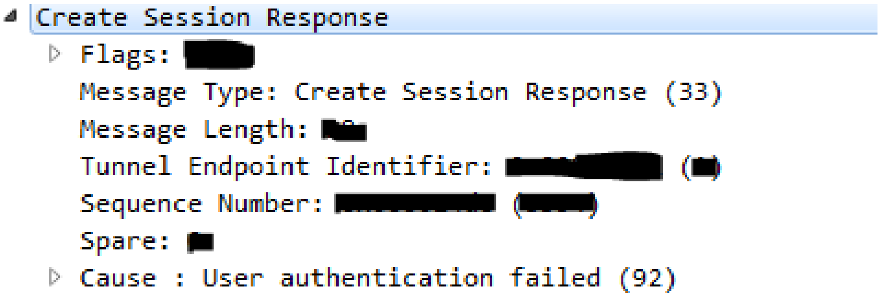
The first message is a Create Session Request from Gateway to PCRF as shown below.



No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	228			Create Session Request
2	0.018310	[redacted]	[redacted]	DIAMETER	724		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
3	0.019992	[redacted]	[redacted]	DIAMETER	364	DIAMETER_CREDIT_LIMIT_REACHED	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
4	0.030342	[redacted]	[redacted]	GTPv2	51			Create Session Response

Figure 32 : Create Session Request/Response and CCR/CCA messages for Result Code 4012

As we can see in figure 33 the CCR and CCA messages was send and received between Gateway and PCRF. In CCA message we can see clearly the result code from the error code we choose when we start run the script (4012 = Diameter_Credit_Limit_Reached). The next step for this scenario is to check the Create Session Response message. In case that this is reject, the session will be failed and the user authentication will be failed.



```
◢ Create Session Response
  ▷ Flags: [redacted]
    Message Type: Create Session Response (33)
    Message Length: [redacted]
    Tunnel Endpoint Identifier: [redacted] ([redacted])
    Sequence Number: [redacted] ([redacted])
    Spare: [redacted]
  ▷ Cause : User authentication failed (92)
```

6.3.3 Error codes in PCRF Responses 3

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce PCRF error response 5003

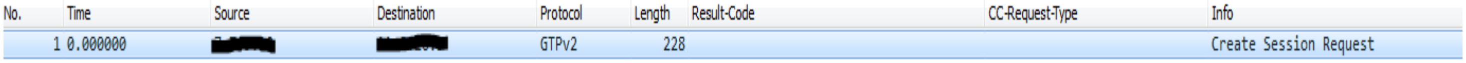
Expected Results:

Verify that signaling and traffic for users without PCRF is not affected. The Gateway rejects the affected procedures and sessions.

Comments:

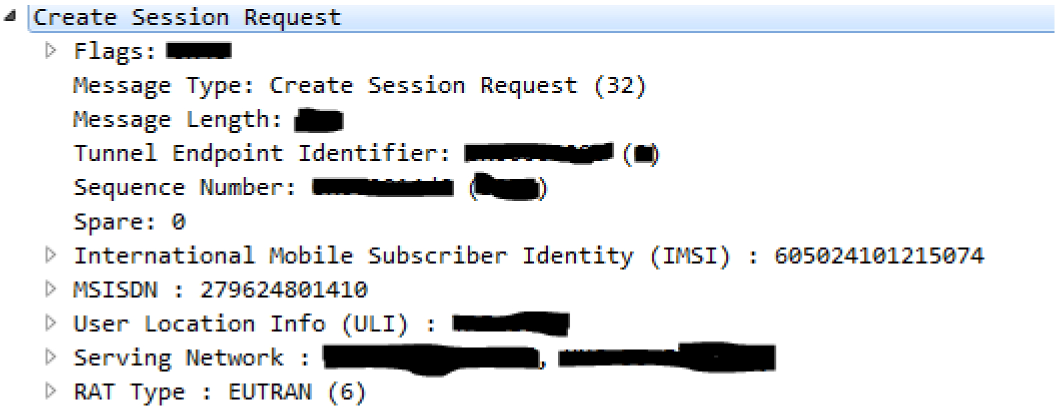
- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to PCRF as shown below.



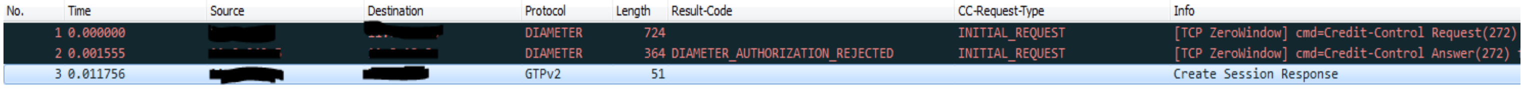
No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	228			Create Session Request

Figure 33 : Create Session Request message



```
◢ Create Session Request
    ▷ Flags: [redacted]
      Message Type: Create Session Request (32)
      Message Length: [redacted]
      Tunnel Endpoint Identifier: [redacted] ([redacted])
      Sequence Number: [redacted] ([redacted])
      Spare: 0
    ▷ International Mobile Subscriber Identity (IMSI) : 605024101215074
    ▷ MSISDN : 279624801410
    ▷ User Location Info (ULI) : [redacted]
    ▷ Serving Network : [redacted], [redacted]
    ▷ RAT Type : EUTRAN (6)
```

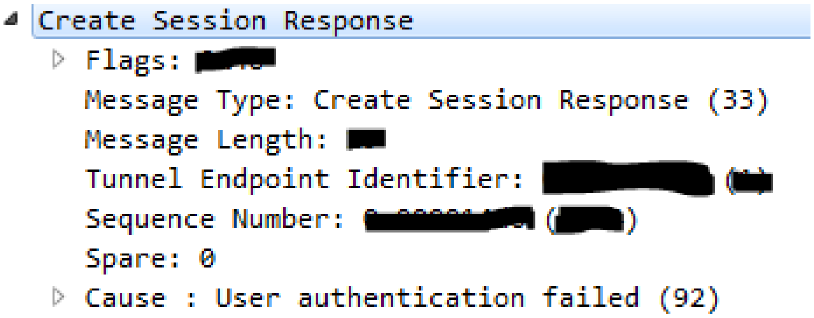
Figure 34 : Detailed avp of Create Session Request



No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	DIAMETER	724		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
2	0.001555	[redacted]	[redacted]	DIAMETER	364	DIAMETER_AUTHORIZATION_REJECTED	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
3	0.011756	[redacted]	[redacted]	GTPv2	51			Create Session Response

Figure 35 : CCR/CCA messages and Result Code 5003

As we can see in figure 36 the CCR and CCA messages was send and received between Gateway and PCRF. In CCA message we can see clearly the result code from the error code we choose when we start run the script (5003 = Diameter_Authorization_Rejected). The next step for this scenario is to check the Create Session Response message. . In case that this is reject, the session will be failed and the user authentication will be failed.



```
◢ Create Session Response
   ▷ Flags: [redacted]
     Message Type: Create Session Response (33)
     Message Length: [redacted]
     Tunnel Endpoint Identifier: [redacted] ([redacted])
     Sequence Number: [redacted] ([redacted])
     Spare: 0
   ▷ Cause : User authentication failed (92)
```

6.3.4 Error codes in PCRF Responses 4

Description:

This Test Scenario verifies Gateway after peripheral server error response

Required test environment:

Environment as described in Figure 19

Setup:

- Setup Gateway with full DB installed.

- Use proposed traffic profile.

Execution steps:

Introduce PCRF error response 5030

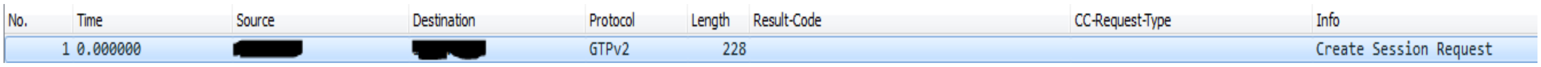
Expected Results:

Verify that signaling and traffic for users without PCRF is not affected. The Gateway rejects the affected procedures and sessions.

Comments:

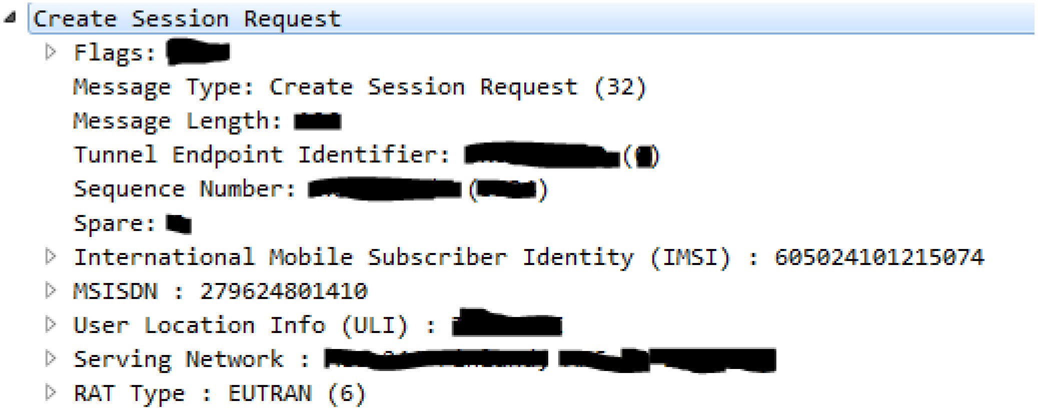
- no unexpected files generated during the test.
- alarms generated to be cleared.
- no process restarts in the remaining nodes.
- check that cdrs are created and sent to CG peripheral server.

The first message is a Create Session Request from Gateway to PCRF as shown below.



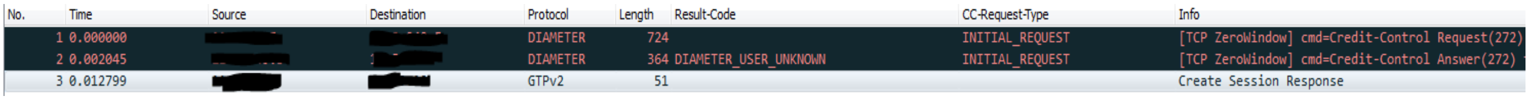
No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	GTPv2	228			Create Session Request

Figure 36 : Create Session Request message



```
◢ Create Session Request
  ▷ Flags: [redacted]
    Message Type: Create Session Request (32)
    Message Length: [redacted]
    Tunnel Endpoint Identifier: [redacted] ([redacted])
    Sequence Number: [redacted] ([redacted])
    Spare: [redacted]
  ▷ International Mobile Subscriber Identity (IMSI) : 605024101215074
  ▷ MSISDN : 279624801410
  ▷ User Location Info (ULI) : [redacted]
  ▷ Serving Network : [redacted] [redacted]
  ▷ RAT Type : EUTRAN (6)
```

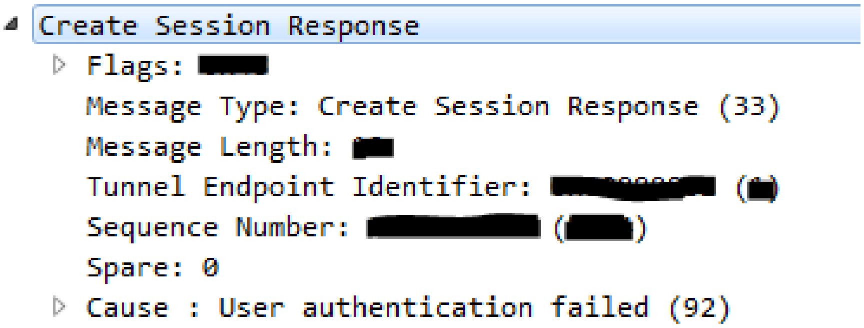
Figure 37 : Detailed avp of Create Session Request



No.	Time	Source	Destination	Protocol	Length	Result-Code	CC-Request-Type	Info
1	0.000000	[redacted]	[redacted]	DIAMETER	724		INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Request(272)
2	0.002045	[redacted]	[redacted]	DIAMETER	364	DIAMETER_USER_UNKNOWN	INITIAL_REQUEST	[TCP ZeroWindow] cmd=Credit-Control Answer(272)
3	0.012799	[redacted]	[redacted]	GTPv2	51			Create Session Response

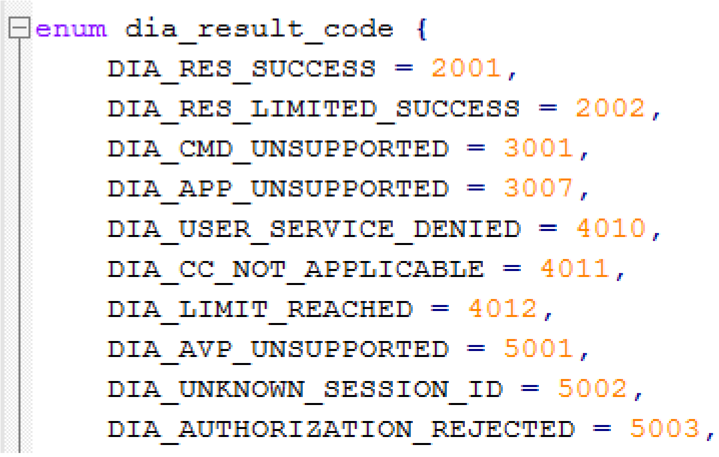
Figure 38: CCR/CCA messages and Result Code 5030

As we can see in figure 39 the CCR and CCA messages was send and received between Gateway and PCRF. In CCA message we can see clearly the result code from the error code we choose when we start run the script (5030 = Diameter_User_Unknown). The next step for this scenario is to check the Create Session Response message. In case that this is reject, the session will be failed and the user authentication will be failed.



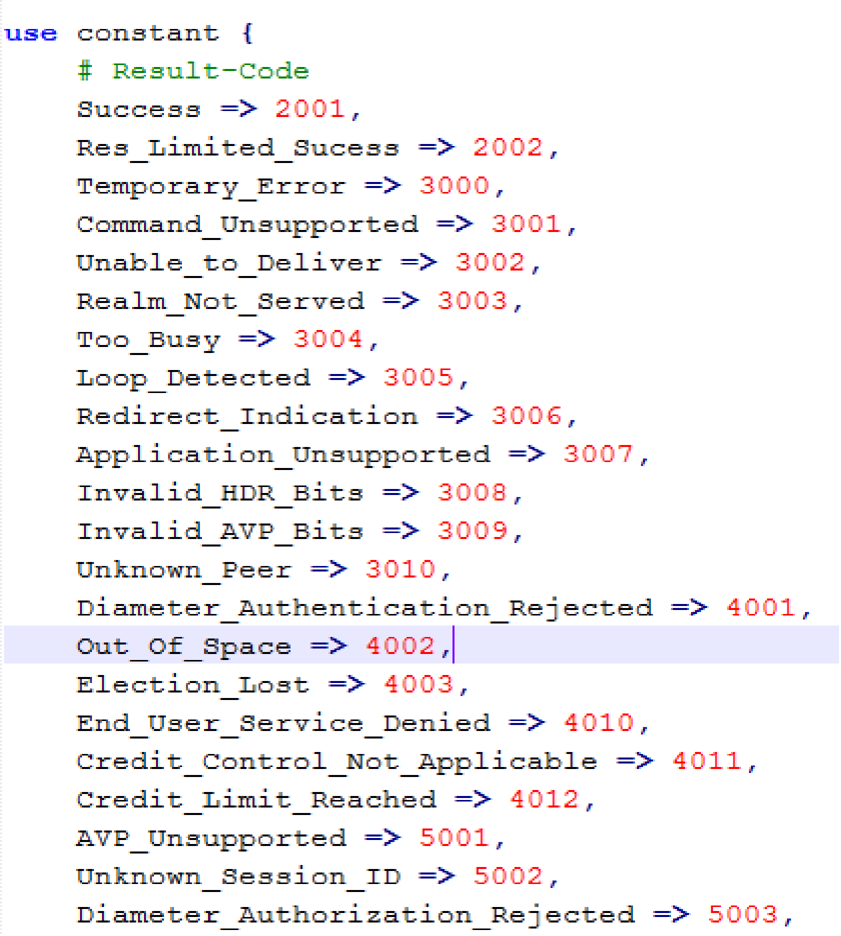
```
◢ Create Session Response
   ▷ Flags: [redacted]
     Message Type: Create Session Response (33)
     Message Length: [redacted]
     Tunnel Endpoint Identifier: [redacted] ([redacted])
     Sequence Number: [redacted] ([redacted])
     Spare: 0
   ▷ Cause : User authentication failed (92)
```

6.4 Created Libraries for OCS & PCRF



```
enum dia_result_code {
        DIA_RES_SUCCESS = 2001,
        DIA_RES_LIMITED_SUCCESS = 2002,
        DIA_CMD_UNSUPPORTED = 3001,
        DIA_APP_UNSUPPORTED = 3007,
        DIA_USER_SERVICE_DENIED = 4010,
        DIA_CC_NOT_APPLICABLE = 4011,
        DIA_LIMIT_REACHED = 4012,
        DIA_AVP_UNSUPPORTED = 5001,
        DIA_UNKNOWN_SESSION_ID = 5002,
        DIA_AUTHORIZATION_REJECTED = 5003,
```

Figure 39 : A part of the created library for OCS in order to support all error codes



```
use constant {
    # Result-Code
    Success => 2001,
    Res_Limited_Sucess => 2002,
    Temporary_Error => 3000,
    Command_Unsupported => 3001,
    Unable_to_Deliver => 3002,
    Realm_Not_Served => 3003,
    Too_Busy => 3004,
    Loop_Detected => 3005,
    Redirect_Indication => 3006,
    Application_Unsupported => 3007,
    Invalid_HDR_Bits => 3008,
    Invalid_AVP_Bits => 3009,
    Unknown_Peer => 3010,
    Diameter_Authentication_Rejected => 4001,
    Out_Of_Space => 4002,
    Election_Lost => 4003,
    End_User_Service_Denied => 4010,
    Credit_Control_Not_Applicable => 4011,
    Credit_Limit_Reached => 4012,
    AVP_Unsupported => 5001,
    Unknown_Session_ID => 5002,
    Diameter_Authorization_Rejected => 5003,
```

Figure 40 : A part of the created library for PCRF in order to support all error code

6.5 Support the Implementation of PCRF script in C

6.5.1 Introduction

“Peripheral emulator scripts” are very common in everyday testing, especially in Performance and Provocative testing phases. Though they can be very helpful in simulating different scenarios, they often become the blocking point in testing, because of their slow performance, code hangs, very limited scalability and restricted amount of configurable options. These testing requirements have lead to the idea of creating a new script from scratch that would:

- ➢ Emulate most of the widely used Gateway external interfaces (Gx, Gxc, Gy, S6b etc).
- ➢ Keep CPU power of the machine as low as possible.
- ➢ Introduce high configurability (in terms of adding the needed AVPs etc).
- ➢ Be robust under high load or big time periods of usage (e.g. in Stability testing).

In this implementation we highly supported the creation of this script by writing some of the used functions in pcrf script. In the end of the chapter C functions flow diagrams show the basic interconnections between them at program runtime.

6.5.2 Type of messages supported

Once the program has received a new CER message from a node, it will fork a new process that will handle from now on the connected node. This process will investigate every diameter message received and will send a reply accordingly. For example if the connected node sends a CCR, the program will respond with a CCA. Upon receiving the CCR, the program will analyze the CC-REQ-TYPE AVP included and will determine if the CCR is about session initiation, update or termination. It will then send a CCA message with the user-defined AVPs, as they are defined in the respective configuration section. Available message categories are:

- ✓ ccai : AVPs to be included for responses sent after a CCR-Initiate has been received.
- ✓ ccau : Same as the above, after a CCR - Update has been received.
- ✓ ccat : Same as the above, after a CCR – Terminate has been received.
- ✓ capabilities_exchange : AVPs to be included in Capabilities Exchange Request-Answer messages (during initial connection establishment).

- ✓ watchdog : AVPs included in watchdog keepalive messages.
- ✓ rar : AVPs to be included in outgoing RAR messages.

6.5.3 Volume based monitoring and metering (Scenario 1)

After a volume threshold is reached, gateway sends a CCR-U message to inform the PCRF that the user needs more quota. It is necessary and possible for the PCRF to apply a different policy for the PDP context/session or delete the session and stop the access.

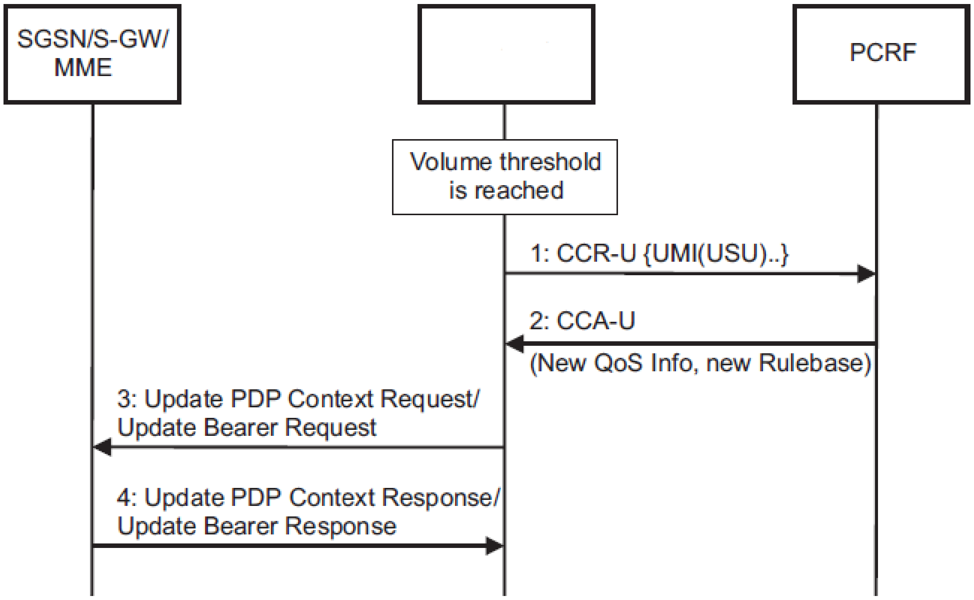

SGSN/S-GW/ MME
PCRF
Volume threshold is reached
1: CCR-U {UMI(USU)..}
2: CCA-U
(New QoS Info, new Rulebase)
3: Update PDP Context Request/ Update Bearer Request
4: Update PDP Context Response/ Update Bearer Response

Figure 41 : Based in Volume flow monitoring and metering

1. After the volume threshold is reached, the gateway sends a CCR-U message to the

PCRF.

2. The PCRF responds to the CCR-U message with a CCA-U message. In this example, the PCRF downgrades the QoS and therefore applying a new policy to the

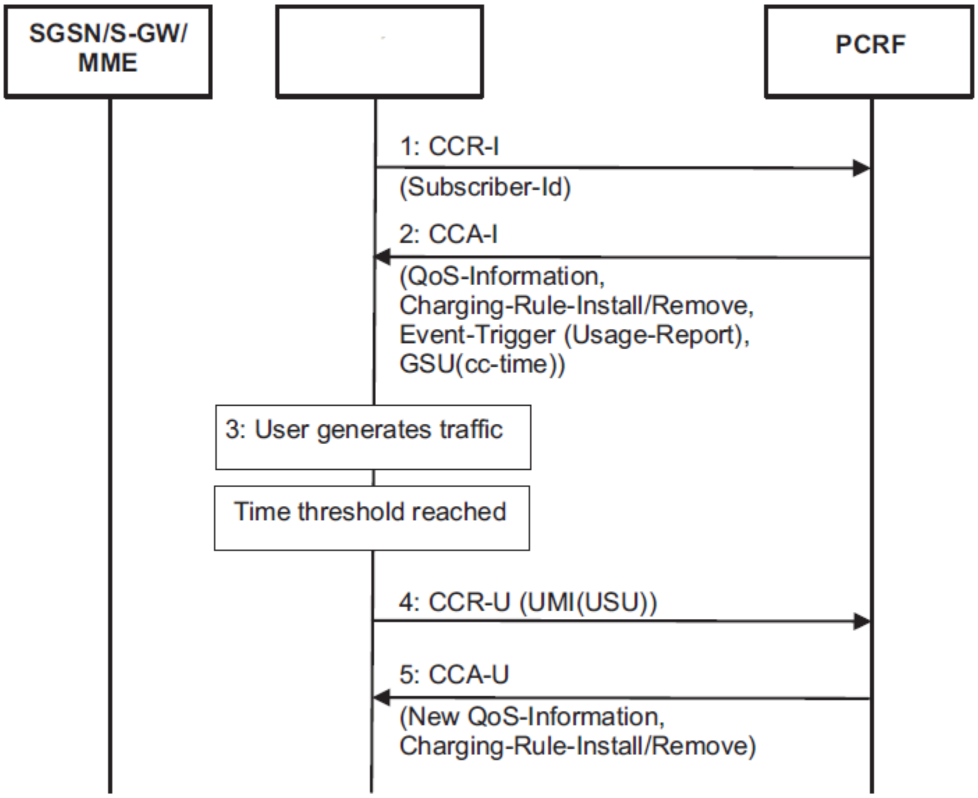
PDP context/session.

3. Gateway sends an Update PDP Context Request/Updated Bearer Request to the SGSN/S-GW/MME.

4. The SGSN/S-GW/MME responds to Gateway with an Update PDP Context Response/Update Bearer Response message.

6.5.4 Time based monitoring and metering (Scenario 2)

Time-based monitoring is done in a way similar to volume-based monitoring. The procedure is as follows:


SGSN/S-GW/ MME
PCRF
1: CCR-I
(Subscriber-Id)
2: CCA-I
(QoS-Information, Charging-Rule-Install/Remove, Event-Trigger (Usage-Report), GSU(cc-time))
3: User generates traffic
Time threshold reached
4: CCR-U (UMI(USU))
5: CCA-U
(New QoS-Information, Charging-Rule-Install/Remove)

1. During the context/bearer activation, Gateway contacts the PCRF by sending a CCRI message.

2. The PCRF responds to the CCR-I message with a CCA-I message and through this message installs a QoS and rulebases. Additionally, it allocates (grants) a time

threshold.

3. The context/bearer is activated and the user starts generating traffic.

4. When the user has generated traffic for the period allocated by the PCRF, Gateway informs the PCRF by sending a CCR-U message.

5. The PCRF responds to the CCR-U message with a CCA-U message. Through this message, the PCRF can reply with new QoS and/or new rulebases.

Time monitoring can be both on a session level, as well as on a rule level. For both levels the following applies: metering in Gateway starts with the first packet matching the corresponding monitoring level, after a quota has been granted from the PCRF. After this point, the metering continues even if no more traffic is generated. For example, if the PCRF has granted 60 seconds for Rule1 and the user starts generating traffic (that matches Rule1) as follows:

1. User generates traffic for 40 seconds.

2. User is idle for 20 seconds.

3. User generates traffic for 20 seconds.

then, the PCRF will be informed after example's step 2. That is, 60 seconds after the user started generating traffic.

6.5.5 Scenarios supported

The big difference with the former used Perl scripts is that this tool gives the opportunity to user for configuring his own scenario. Up to now five different scenarios and the default one have been implemented

1) ***Monitor***: Checks the received CCR-U for a specific AVP, checks its value and compares it with a user defined value. If the check is TRUE then sends a CCA-U with AVPs declared under message section ccau_sc. Otherwise the normal CCA-U message will be sent as a response.

   syntax:

```
scenario monitor 421 INT64 300000

                          |       |          |-------VALUE
                           |      |---------------VALUE TYPE (INT32/INT64 or FLO32/FLO64)
                          |---------------------AVP Code to be monitored
```

2) ***Delay RAR:*** This instructs the program to send a RAR message. 3 Options are available, presented here with the appropriate syntax:

   a) *scenario delay RAR 0* : The program will send the RAR message for each session right after the CCA-I message. That was the default behavior in most Perl scripts. Database is also disabled.

   b) *scenario delay RAR X Y* : Will wait for X seconds then start sending RARs for all created sessions (by that time..) at Y messages/sec. Setting SECONDS > 0 && defining a RATE that represents messages per second, will cause the program to sleep for SECONDS and then start sending RARs at the predefined RATE (almost). This differs from (b) since no checking is done on the timestamp, plus once the algorithm goes through all active sessions it will exit and no RARs will be sent for any new sessions.

3) ***DRA*** : Diameter Routing Agent

   The DRA scenario causes the program to alternate between two sets of available AVPs, when sending a CCA-I. This is used when the program emulates a redirect server, redirecting the PGW/SGW/SAE node to a different PCRF Host. On this mode database is also disabled. Section ccai_alt MUST be set. If only 1 redirect server has to be used, then ccai_alt MUST mirror ccai contents.

   ✓ Program will act as a DRA server. Database is disabled and server will send CCA-I messages by alternating between ccai && ccai_alt sections.

   ✓ ccai_alt must be configured.

   ✓ Used to redirect target node to other PCRFs.

4) ***Normal Scenario*** : Normal scenario exists as a command and is the default behavior if no other scenario is set. When a CCR-U is received, a CCA-U is sent with the AVPs defined in ccau. No RARs sent.

5) ***Scenario gx_gxc SECONDS*** : This is used strictly with scenario delay RAR option, in the case where the program expects both Gx and GXc requests and

must send RARs in a specific manner towards the NG. Specifically the NG sends a CCR-I over both Gx and Gxc and the program triggers a RAR for the GXc. The NG receives this RAR, responds with a RAA and sends a CCR-U over the GXc. The program then responds with a CCA-U over the GXc and ONLY THEN it is supposed to initiate a RAR over the Gx. To emulate this behavior, along with scenario delay RAR option, the scenario gx_gxc X must be set where X is the number of seconds after which the program will start sending RARs over the Gx after it has sent the first RAR-GXc. So for example, assume user has set scenario delay RAR 60 2000 and scenario gx_gxc 5. After 60 seconds the program will start sending GXc RARs and after 5 seconds from that moment it will start sending GX RARs. The rate for the GX RARs will be the same as with the GXc, so user should have this in mind when calculating the desired rate (in our example 2000 in runtime is 4000). Possible values are 1 to 30.

6) ***Empty_cca*** : The EMPTY_CCA scenario forces the program to send empty CCA messages and ignore completely the ccaX AVP sections.

7. Conclusions

After the modification of the scripts that we mentioned in Gy and Gx interface the daily life of a tester in Nokia is easier. The test scenarios can be more detailed and the tester knows the exact reason that a session is failed during his run. The implementation from scratch of the PCRF scripts was very useful for the whole Testing team that I was part of. The script in C now is more powerful and it can support the sending/receiving of more CCR/CCA/RAR/RAA messages without any failed session or script failure (stop unexpectedly).

References

http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

http://www.netmanias.com/en/post/techdocs/5904/architecture-lte/lte-network-architecture-basic

http://www.rfwireless-world.com/Tutorials/UMTS-Network-Architecture.html

http://www.rfwireless-world.com/Tutorials/LTE-tutorial.html

https://sites.google.com/site/lteencyclopedia/lte-network-infrastructure-and-elements#TOC-3.5-The-PCRF-Policy-and-Charging-Rules-Function-Server

https://en.wikipedia.org/wiki/History_of_mobile_phones

University of Alberta – Overview of the Evolved Packet Core

UMTS System Architecture and Protocol Architecture, Oliver Waldhorst, Jens Mückenheim, Oct 2011

3GPP TR 25.913: Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (EUTRAN).

Motorola, Long Term Evolution (LTE): A Technical Overview, Technical White Paper.

3GPP TS 24.301: Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS): Stage 3.

UMTS – Universal Mobile Telecommunications System, tutorialspoint simplyeasylearning

Digital cellular telecommunications system (Phase 2+), Universal Mobile Telecommunications System (UMTS), LTE Policy and charging control architecture (3GPP TS 23.203 version 10.8.0 Release 10).

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Gx reference point (Release 10).

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging architecture and principles (Release 11).

UMTS Networks, Andreas Mitschele-Thiel and Jens Mückenheim, Nov. 2010

3G Long-Term Evolution (LTE) and System Architecture Evolution (SAE), Ilmenau University of Technology, June 2011

Towards Global Mobile Broadband - Standardising the future of mobile communications with LTE (Long Term Evolution), UMTS Forum February 2008.

SAE and Evolved Packet Core, Farooq Bari, Seattle Communications (COM-19) Society Chapter Nov. 13, 2008

Internet Engineering Task Force (IETF), Diameter Base Protocol

UMTS Forum Report: “Market Potential for 3G LTE”, January 2008

“UTRA-UTRAN Long Term Evolution (LTE) and 3GPP System Architecture Evolution (SAE)” – www.3gpp.org

3G Americas White Paper: “UMTS Evolution from 3GPP Release 7 to Release 8 – HSPA and SAE/LTE”, June 2007

Peter Rysavy, “EDGE, HSPA & LTE: The Mobile Broadband Advantage”, 3G Americas, September 2007

www.umts-forum.org/content/view/2270/109/

ECC Decision of 18 March 2005 on harmonised utilisation of spectrum for IMT-2000/UMTS systems operating within the band 2500 – 2690 MHz (ECC/DEC/(05)05)

GSMA report, “HSDPA Operators Commitments”, 19 November 2007

GSM GPRS and EDGE Performance, Second Edition, Timo Halonen Juan Melero

Evolution of Mobile Wireless Communication Networks:1G to 4G, Amit Kumar, Dr. Yunfei Liu, December 2010

ITU (2009). “Measuring the Information Society; The ICT Development Index”, [Online] Available: http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf

Mishra, Ajay K. “Fundamentals of Cellular Network Planning and Optimization, 2G/2.5G/3G…Evolution of 4G”, John Wiley and Sons, 2004.

John Wiley & Sons, Ltd, Intelligent Networks for the GSM, GPRS and UMTS Network – Introduction to GSM Networks,2006