UNIVERSITAT POLITÈCNICA
DE CATALUNYA

ESCOLA TÈCNICA SUPERIOR D'ENGINYERIA DE TELECOMUNICACIÓ DE BARCELONA

Departamento de Ingeniería Telemática

Proyecto Final de Carrera Plan 92

Estudio de la arquitectura de protocolos de LTE

Tutor:
José Luis Muñoz

Autor:
Javier Gualda Muñoz

Barcelona, Septiembre 2016

A Pau e Ian
caminad,
caminad,
que nadie barra vuestro paso

Contents

Chapter 1

Objetivo

Resum

L'objectiu d'aquest projecte és fer un anàlisi en profunditat de les xarxes LTE que actualment estan disponibles dins la tecnologia de 4a i 5a Generació. L'analisi preten mostrar les principals característiques d'una manera ordenada i detallada. Així mateix s'intentarà dotar del màxim de coneixements possibles a partir d'exemples reals del funcionament d'aquesta.

Aquest anàlisi en profunditat sera la base per entrar d'una forma detallada en l'explicació d'un protocol que està present en moltes de les interfaces existents entre els elements dins de la xarxa LTE, el protocol Diameter. En primer lloc explicarem les característiques principals del protocol per posar la base dels coneixements necessaris.

Ja per últim, al tenir aquest projecte una vessant molt didàctica, ens recolzarem en una serie de pràctiques que tenen com a finalitat, asseure els coneixements dels alumnes. Totes aquestes pràctiques, estan destinades a anar conduint als alumnes a entendre el protocol Diameter d'una forma relaxada introduint a poc a poc nous termes a base de la prova i error.

Resumen

El objetivo de este proyecto es hacer un análisis en profundidad de las redes LTE que actualmente están disponibles dentro de la tecnología de 4a y 5a Generación. El análisis pretende mostrar las principales características de una manera ordenada y detallada. Así mismo se intentará dotar de los máximos conocimientos posibles a partir de ejemplos reales del funcionamiento de la misma.

Este análisis en profundidad, será la base para entrar de una forma especifica en la explicación de un protocolo que está presente en muchas de las interfaces existentes entre los elementos dentro de la red LTE, el protocolo Diameter. En primer lugar explicaremos las características principales del protocolo para poner la base de los conocimientos necesarios.

Ya por último, al tener este proyecto una vertiente muy didáctica, nos apoyaremos en una serie de practicas, que tienen como finalidad asentar los conocimientos de los alumnos. Todas estas

practicas están destinadas a ir conduciendo a los alumnos a entender el protocolo Diameter de una forma relajada introduciendo poco a poco nuevos términos utilizando como base, la prueba y error.

Abstract

The goal of this project is to make a thorough analysis of LTE networks that are currently available within the technology 4rd and 5th Generation. The analysis aims to show the main features from an orderly and detailed manner. Likewise we will try to provide the maximum knowledge using real examples of the operation thereof.

This in-depth analysis will be the basis for entering a specific way in explaining a protocol that is present in many of the interfaces between the elements within the LTE network, the Diameter protocol. First we explain the main protocol's features to assure the necessary base knowledge.

And finally, having this project a very educational perspective, we will rely on a series of practices, which aim to lay the knowledge of students. All these practices are intended to be driving students to understand the Diameter protocol in a gradually way relaxed introducing new terms using as a basis, the trial and error format.

Chapter 2

Introducción

2.1 2ª Generación - 2G

Se conoce como telefonía móvil 2G a la segunda generación de telefonía móvil. La telefonía móvil 2G marca el salto de una telefonía analógica, como era la 1G, a una telefonía digital.

Las mayores ventajas que ofreció 2G respecto a 1G fueron una mayor calidad frente a interferencias y mejor utilización del espectro.

Gracias a los avances en las tecnologías digitales se logró la miniaturización de los equipos terminales, reducción del costo y del consumo de potencia. Asimismo, permitió aplicar **técnicas de procesado digital de la información** como la modulación digital, codificación de canal, codificación de fuente, sistemas entrelazados, cifrado de las comunicaciones, entre otras. Se consiguieron tambien, mejoras en cuanto a calidad, velocidad de transmisión, capacidad del sistema y la posibilidad de agregación de nuevos servicios como el buzón de voz, identificador de llamadas y mensajes de texto.

2G abarcaba diferentes protocolos desarrollados por diferentes compañías cosa que implicaba limitaciones respecto a las áreas donde se podía utilizar estos móviles. Algunos de los protocolos utilizados serían:

- **GSM** (Global System for mobile Communications):
  - Utiliza la técnica de duplexado FDD (Frequency Division Duplex) en la banda de 900 MHz.
  - Como técnica de acceso emplea una combinación de frecuencia y tiempo, es decir, utiliza FDMA (Frequency Division Multiple Access)
  - El éxito del sistema GSM rápidamente se extendió por países de todo el mundo.
  - Teléfonos tribanda 900, 1800 y 1900 MHz -> más fácil roaming internacional permitiendo establecer comunicaciones en cualquiera de los cinco continentes.
  - GSM fue sin duda el sistema de segunda generación con mayor extensión en el mundo (aunque hay otros).

- **IS-95** también conocido como CDMAOne:
  - 1993 en USA y utilizado también en varios países asiáticos.
  - Único sistema de segunda generación basado en CDMA (Code Division Multiple Access).

2.2 2.5G

Para alcanzar mayores velocidades surgieron una serie de tecnologías conocidas como generación 2.5. Esta generación conocida como 2.5G (o 2.75G) marco una transición entre los sistemas de segunda y de tercera generación. Los móviles conocidos como de 2.5G aún sin definir un estándar como tal, incorporaron algunas mejoras del sistema GSM como HSCSD o tecnologías del estándar 3G como el GPRS y EDGE. Adicionalmente, soportaban tasas de transferencia superiores a los teléfonos 2G (e inferiores a los de 3G)

HSCSD (High-Speed Circuit-Switched Data) es principalmente una mejora del mecanismo de transmisión de datos de GSM. La idea es emplear más de un time slot por usuario de forma paralela para la transmisión de datos (hasta cuatro). Este sistema funcionaba muy bien para aplicaciones en tiempo real pero seguía empleando conmutación por circuito. Este hecho representaba una disminución drástica de los recursos disponibles para los usuarios de voz que implicaba, que los canales debían ser reservados para un usuario por el tiempo total de la conexión sin importar si se estuviera transmitiendo información o no.

El servicio **GPRS** (General Packet Radio Services) fue propuesta por la ETSI, como una extensión del sistema GSM. GPRS utiliza conmutación de paquetes que permite tener una mayor eficiencia espectral y por tanto, que los recursos no sean asignados de manera exclusiva sino compartidos entre varios usuarios. Además se toma en cuenta la asimetría de los servicios de paquetes de datos facilitando que la asignación de los recursos en los enlaces ascendente y descendente, se realice de manera separada. Una factor a su favor, fue la posibilidad de realizar una tarificación del servicio más atractiva al usuario, basada en la cantidad de paquetes transmitidos y no en la duración de la conexión. El coste de implementación del sistema GPRS fue bajo ya que era una extensión de GSM.

Características de GPRS

- Se utiliza todo el hardware existente añadiendo solo dos nuevos nodos SGSN (Serving GPRS Support Node) y GGSN (Gateway GPRS Support Node) para el tráfico de paquetes.
- Se incorporando una unidad PCU (Packet Control Unit) en las BSC (Base Station Controller), con la capacidad de que los canales sean asignados dinámicamente a GSM o GPRS dependiendo de los niveles de tráfico.
- Dando siempre prioridad a los servicios de voz.
- GPRS utiliza distintos esquemas de codificación dependiendo de la calidad del radio enlace, el tipo de terminal y el tráfico de datos de la celda.

- CS1: 9.05 kbps, CS2: 13.4 kbps, CS3: 15.6 kbps y CS4: 21.4 kbps.
- Permite utilizar varios time slots por conexión, con lo cual se lograría una velocidad máxima teórica de 171.2 kbps utilizando 8 time slots y el esquema CS4.

La tecnología **EDGE** (Enhanced Data Rates for Global Evolution) es una mejora a GSM/GPRS. GPRS implementa una codificación adaptativa. EDGE complementa a GPRS con la introducción de la modulación adaptativa. Además de la modulación GMSK empleada en GSM/GPRS, EDGE introduce la modulación 8PSK que permite triplicar la tasa de transmisión de datos de GPRS a cambio de una menor área de cobertura. La máxima velocidad de transmisión en EDGE es de 384 kbps utilizando 8 time slots y el más eficiente de los esquemas de modulación/codificación (MCS9).

Los cambios principales de este sistema se encuentran a nivel de capa física y MAC/RLC. La arquitectura de la red GPRS no necesita ser modificada excepto en las BTS donde debe agregarse una nueva unidad transceptora. Adicionalmente había que actualizar el software en las BSC para permitir la conmutación de GSM/GPRS a EDGE cuando es necesario. Los terminales móviles con un software que permita codificar y decodificar los nuevos esquemas de modulación utilizados en EDGE.

Por último, **IS-95B** ofrecía velocidades de transmisión de datos de hasta 14.4 kbps. La tecnología 2.5G para este sistema es IS-95B que emplea conmutación de paquetes. Permite velocidades de 64 kbps utilizando múltiples canales de códigos ortogonales para un mismo usuario.

2.3 3G

2G marcó un éxito en la historia de las comunicaciones móviles. Las crecientes demandas de tráfico de datos y las expectativas de nuevos servicios multimedia se hacían insuficientes para 2G/2.5G. La ITU empezó el desarrollo de un sistema de tercera generación universal llamado IMT-2000 (International Mobile Telecommunications). Posteriormente pasó a ser más bien una familia de sistemas 3G en vista de no poder englobar los intereses de todos los países en un único sistema.

IMT-2000 abarca el sistema europeo UMTS y el norteamericano CDMA2000 entre otros de menor importancia. Cabe destacar que la evolución desde el estándar IS-95 a los sistemas CDMA2000 de tercera generación es mucho más simple que la equivalente de GSM/GPRS/EDGE a UMTS. CDMA2000 permite la reutilización de la mayor parte de la infraestructura de la red. Practicamente el hecho de pasar a CDMA2000, implicaba mejoras basadas en actualizaciones de software.

Los principales objetivos que fueron marcados para los sistemas 3G, se plantearon en las tasas objetivo de:

- 144 kbps para entornos vehiculares de gran velocidad.
- 384 kbps para espacios abiertos
- velocidades de hasta 2 Mbps para entornos interiores de baja movilidad.

Con estas velocidades los usuarios pueden utilizar sus terminales móviles en una variedad de servicios:

- Llamadas telefónicas
- Acceso a redes LAN corporativas
- Acceso a Internet
- Envío de correo electrónico
- Transferencia de archivos e imágenes de calidad
- Video conferencias (audio/video en tiempo real)

La primera publicación del sistema UMTS estuvo disponible en 1999 conocida como Release 99. En ella se especifican dos modos de operación en cuanto al acceso radio:

- Modo FDD/W-CDMA (Wideband CDMA). El canal físico lo define un código y una frecuencia.
- Modo TDD/TD-CDMA (Time Division-CDMA). El canal físico lo define un código, una frecuencia y un time slot.

El uso de la tecnología CDMA implica un cambio en la arquitectura de red de acceso radio GSM/GPRS/EDGE. Si se tienen controladas las interferencias intercelulares, permite lograr una una gran eficiencia espectral.

Las mejoras más importantes en el acceso radio UMTS se describen en:

- R5 con la adición de HSDPA (High Speed Downlink Packet Access)
- R6 con HSUPA (High Speed Uplink Packet Access)

Juntas se conocen como HSPA (High Speed Packet Access). HSPA mejora los servicios de paquetes de datos introduciendo mayores velocidades y menores retardos. Mantiene una buena cobertura y una gran capacidad en el sistema. Para lograr esto, HSPA introduce:

- Nuevos esquemas de modulación de mayor nivel.
- Control de potencia rápido.
- Fast scheduling.
- Mecanismos de retransmisión híbrida HARQ con redundancia incremental.
- Se logran velocidades de hasta 14.4 Mbps en HSDPA y 5.7 Mbps en HSUPA.

El sistema de tercera generación **CDMA2000** fue desarrollado por la 3GPP2 como evolución del sistema IS-95 siendo compatible con el mismo. En CDMA2000 se incorporaron básicamente las mismas tecnologías que en WCDMA/HSPA en el acceso para lograr mejores tasas en la transmisión de datos y mejorar el rendimiento de la red. La evolución de CDMA2000 ocurrió en distintas fases:

- Primero surgió CDMA2000 1xRTT
- Luego dos ramas paralelas se iniciaron EV-DO (Evolution-Data Only) y EV-DV (Evolution for integrated Data and Voice).

Se consiguieron velocidades de transmisión superiores a 2 Mbps.

2.4 4G

La motivación principal del sistema de cuarta generación (4G) fue el crecimiento de servicios de paquetes de datos, y la posibilidad de elaborar terminales avanzados llevó a la necesidad de crear una nueva generación de comunicaciones móviles. La ITU-R estableció los requisitos para las redes 4G bajo el nombre de IMT-Advanced.

Algunos de los requisitos son (entre otros):

- Red basada completamente en conmutación por paquete.
- Arquitectura plana basada en el protocolo IP (Internet Protocol).
- Velocidades de transferencia de datos mayores a 100 Mbps para altas movilidades.
- 1 Gbps para entornos relativamente fijos.
- Interoperabilidad con estándares existentes.
- canalización flexible
- menores tiempos de latencia, etc.

Existen tres organizaciones que se han encargado de desarrollar estándares para cumplir requisitos de IMT-Advanced:

- La 3GPP (Third Generation Paterntship Project) empezó a finales de 2004 la primera especificación del sistema LTE (Long Term Evolution) que fue concluida a finales de 2008 y ha evolucionado posteriormente a LTE-Advanced.
- IEEE ha creado la familia 802.16 conocida como WiMAX donde la versión 802.16m, también conocida como WirelessMAN-Advanced, ha sido aprobada por la ITU-R como una tecnología IMT-Advanced.
- 3GPP2 comenzó el desarrollo del sistema UMB (Ultra Mobile Broadband) como evolución del sistema CDMA2000 con las intenciones de convertirse en un sistema de 4G pero el proyecto fue dejado inconcluso para pasar a apoyar a LTE.

La ITU aclara acerca de las tecnologías consideradas IMT-Advanced:

*Tras una detallada evaluación acerca de estrictos criterios técnicos y operativos, la ITU ha determinado que **LTE-Advanced** y **WirelessMAN-Advanced** deben recibir la designación oficial de IMT-Advanced. Siendo las tecnologías más avanzadas actualmente en comunicaciones de banda ancha móvil, IMT-Advanced es considerada como "4G", aunque se reconoce que este término, mientras no estuvo definido, también puede ser aplicado a los precursores de estas tecnologías, **LTE** y **WiMAX**, y a otras tecnologías que evolucionaron de sistemas 3G proporcionando un importante nivel de mejora en el rendimiento y en las capacidades con respecto a los sistemas iniciales de 3G desplegados.*

Chapter 3

Arquitectura

3.1 Arquitectura

La red LTE, también llamada EPS *(Evolved Packet System)*, es una red IP extremo a extremo (E2E) que se divide en dos partes como veremos en la Figura 3.1 de [1]:

- La parte LTE que trata de la tecnología relacionada con una red de acceso de radio E-UTRAN *(Evolved Universal Terrestrial Radio Access Network)*
- EPC que trata de la tecnología relacionada con la red troncal.

Que sea una red IP E2E, extremo a extremo, significa que todo el tráfico fluye mediante IP desde el terminal de usuario (UE), es decir el dispositivo con acceso a IP que utiliza el usuario, hasta la red de paquetes o PDN *(Packet Data Network)* donde está conectada la entidad o entidades que proporcionan el servicio.

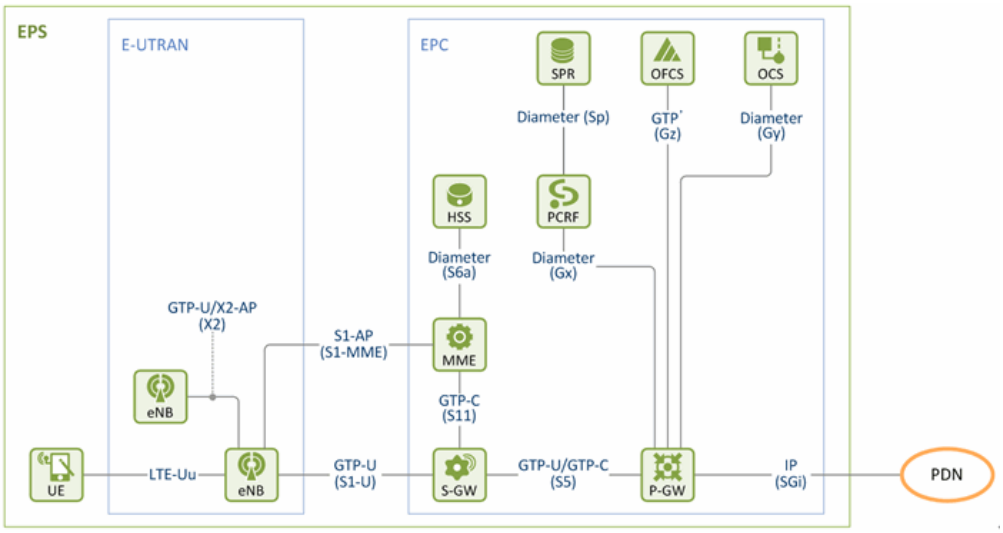


Figure 3.1: Arquitectura de Red LTE

Una red PDN *(Packet Data Networks)* es un dominio IP interno o externo al operador, con el cual un UE quiere comunicarse. Estas PDN's proporcionan servicios a los terminales de usuario (UE) tales como, acceso a Internet o Voz/Video mediante el IMS *(IP Multimedia Subsystem)* tal como veremos en en la Figura 3.2 de [1]:

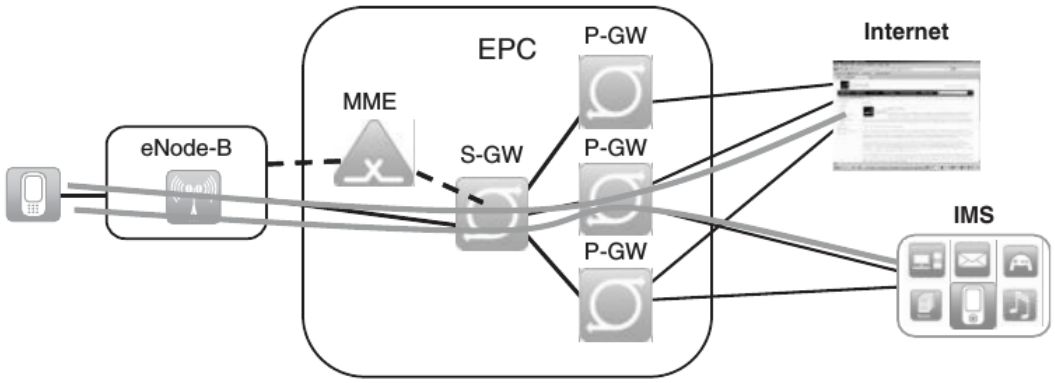


Figure 3.2: Acceso a red PDN de un UE

3.2 Entidades

La red LTE esta compuesta por múltiples entidades que interactúan entre ellas para permitir dar servicio IP punto a punto. Tal como hemos comentado anteriormente, la red LTE se puede dividir en dos partes, la parte propiamente de LTE y luego la parte EPC. Dentro de la parte propiamente LTE, podemos diferenciar los siguientes elementos (Podemos identificar todos los elementos en 3.1 de [1]):

UE - User Terminal

- El equipo de usuario (UE) es cualquier dispositivo utilizado directamente por un usuario final para comunicarse.
- Puede ser un teléfono de mano, un ordenador portátil equipado con un adaptador de banda ancha móvil, o cualquier otro dispositivo.
- Se conecta a una estación base o nodo eNB.
- La interfaz de radio entre el UE y el eNB se llama LTE-Uu.
- El UE también se comunica con el MME de la red EPC mediante señalización NAS (Non-access stratum) para:
  - Gestión de llamadas y movilidad
  - Gestión de sesiones/identidad
- El UE es un dispositivo que inicia todas las llamadas y es el dispositivo terminal en una red.

eNB - Evolved Node B

- El eNB proporciona a los usuarios las interfaces radioeléctricas
- Lleva a cabo la Gestión de Recursos Radio (RRM)
- Realiza el scheduling para la asignación dinámica de recursos
- Control de admisión radio
- Control de la movilidad entre eNBs
- Control de los recursos radio (bearers radio o RB)
- Coordinación de la interferencia inter-celda (ICIC)

Los elementos que forman parte de la parte EPC serían los siguientes:

MME - Mobility Management Mobility

- El MME es la principal entidad de control para el E-UTRAN.
- Se comunica con un HSS (interfaz S6a) para autenticar al usuario y obtener su perfil.

- ESM (EPS Session Management). Gestiona la sesión de los UE con la red.
- EMM (EPS Mobility Management). Gestiona con los UE la movilidad en el EPS. Esto incluye: paging, gestión de la tracking area list y gestión de los handovers.
- Para implementar EMM, ESM y la seguridad utiliza señalización NAS.
- Para calidad de servicio gestiona los bearers EPS.

S-GW - Serving Gateway

- Un S-GW termina la interfaz hacia una E-UTRAN.
- Sirve como punto fijo o 'ancla local' para las conexiones de datos cuando se produce movilidad entre nodos eNB y entre redes 3GPP.

P-GW - Packet Data Network Gateway

- Un P-GW proporciona acceso a un UE a una PDN mediante la asignación de una dirección IP del rango del PDN.
- El P-GW sirve como punto de anclaje para los handover entre redes 3GPP y redes no-3GPP.
- También realiza la aplicación de políticas, el filtrado de paquetes y la tarificación basada en las reglas PCC (Policy and Charging Control) que le proporciona un PCRF.
- Las principales funciones soportadas por un P-GW son los siguientes:
  - Enrutamiento y forwarding IP
  - Filtrado de paquetes por SDF (Service Data Flow) o por usuario. *Veremos en el capitulo 5 QoS que es el SDF*
  - Asignación de direcciones IP a los UE
  - Anclaje para movilidad entre 3GPP y no-3GPP
  - Funciones PCEF (Policy Enforcement and Charging Function)
  - Tarificación por SDF o por usuario

HSS - Home Subscriber Server

- Un HSS es la base de datos central donde se almacenan los perfiles de usuario.
- El HSS le proporciona los parámetros para la autenticación de usuario y los perfiles de usuario a los MME.

PCRF - Policy and Charging Rule Function

- El PCRF es la entidad encargada de la gestión de políticas y de tarificación.
- Toma decisiones por cada SDF.
- Proporciona las reglas PCC (Reglas de Qos y tarificación) al PCEF (P-GW).

SPR - Subscriber Profile Repository

- Un SPR proporciona información de suscripción (perfil de acceso por subscriptor) al PCRF.
- Cuando el PCRF recibe la información, éste utilizando una política basada en suscriptor crea reglas PCC.

OCS - Online Charging System

- El OCS proporciona control de crédito en tiempo real.
- También funciones de tarificación basadas en volumen, tiempo y eventos.

OFCS - Offline Charging System

- Un OFCS proporciona información de tarificación offline.
- La tarificación se basa en CDRs (Charging Data Records).

3.3 Interfaz Radio

En la interfaz radio se utiliza una pila de protocolos específica que se puede dividir en 2, un plano de usuario y un plano de control como se muestra en las Figuras 3.3 y 3.5 de [1]. En esta interfaz se establecen canales:

- Para el envío de paquetes IP de usuarios denominados Data Radio Bearers (DRBs).
- Para señalización denominados Signalling Radio Bearers (SRBs).

Describiremos a continuación los protocolos que podemos encontrar en el plano de usuario:

PDCP

- El protocolo PDCP soporta el transporte eficiente de los paquetes IP a través del enlace de radio.
- Lleva a cabo la compresión de cabecera.
- La estrato de acceso (AS) de seguridad (cifrado y protección de la integridad).
- El reordenamiento/retransmisión de paquetes durante la entrega de llaves.

RLC

- En el lado de transmisión, el protocolo RLC PDU RLC construye y proporciona la PDU RLC a la capa MAC.
- El protocolo RLC realiza la segmentación/concatenación de PDU de PDCP durante la construcción de la PDU RLC.
- En el lado de recepción, el protocolo RLC realiza el reensamblaje de la PDU RLC para reconstruir la PDU de PDCP.
- El protocolo RLC tiene tres modos de funcionamiento (modo transparente, reconocido y sin acuse de recibo).
- Cada modo ofrece diferentes niveles de fiabilidad.
- También realiza paquete (la PDU RLC) reordenamiento y la retransmisión.

MAC

- La capa MAC está conectada a la capa RLC a través de canales lógicos.
- Se conecta a la capa PHY a través de canales de transporte.
- El protocolo de MAC soporta la multiplexación y de-multiplexación entre canales lógicos y canales de transporte.
- Las capas superiores utilizan diferentes canales lógicos para diferentes métricas de calidad de servicio.
- El protocolo MAC soporta QoS mediante la programación y los datos de priorización de canales lógicos.
- El scheduler del eNB hace que los recursos de radio seguro que se asignan dinámicamente a los UE y realiza QoS de control para asegurar que cada portador se asigna la QoS negociados.

3.4 Plano Usuario

El tráfico de usuario se genera en el terminal del mismo fluyendo entre el eNB, el S-GW y P-GW. A través de túneles GTP-U en las interfaces S1-U y S5. Cada uno de los túneles, tiene un identificador llamado TEID que permite su identificación de forma única. El S-GW establece un mapping 1-a-1 entre cada túnel GTP-U en el interfaz S1 y cada túnel en el interfaz S5. El S-GW se sirve de los TEIDs de cada túnel para realizar el mapeo. Se crea un túnel por Bearer y dirección (uplink/downlink) tal como podemos observar en la siguiente figura.

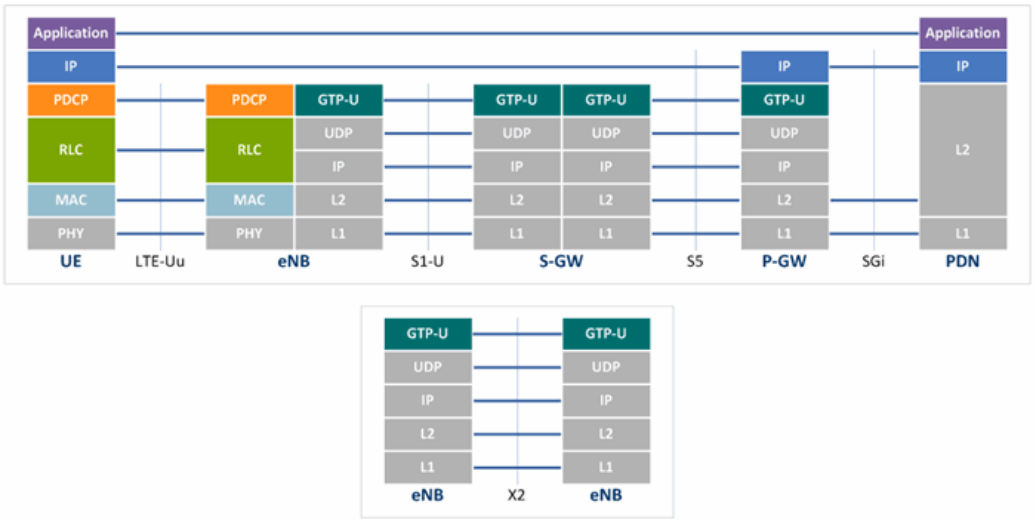


Figure 3.3: Pila Protocolos Plano Usuario

Punto	Protocolos	Descripción
LTE-Uu	E-UTRA	Interfaz entre un UE y un eNB. Por el LTE-Uu el usuario envía sus paquetes IP.
S1-U	GTP-U	Interfaz entre un eNB y un S-GW. Proporciona un túnel GTP-U por bearer.
S5	GTP-U	Interfaz entre un S-GW y un P-GW para el plano de usuario.
SGi	IP	Interfaz entre el P-GW y una PDN.
X2	GTP-U	Interfaz entre eNBs. Para el plano de usuario se utiliza en los handovers entre eNBs para transferir los paquetes de usuario pendientes.

Tráfico uplink (UE a Internet)

1. El **UE** envía paquetes IP de usuario a un eNB sobre la interfaz LTE-Uu.
2. El **eNB** encapsula los paquetes IP de usuario con la cabecera GTP-U en S1, reenvíando los paquetes con la IP externa resultante al S-GW. Para la cabecera del túnel GTP-U en S1, el eNB selecciona un TEID, Dirección IP de destino (IP del S-GW), y la IP origen (IP del eNB).
3. Después de recibir los paquetes IP externos, el **S-GW** elimina el encabezado GTP. El S-GW encapsula los paquetes IP del usuario (paquetes internos) con una nueva cabecera GTP para el interfaz S5. El S-GW reenvía los paquetes IP externos al P-GW. Para la cabecera del túnel GTP-U en S5, el S-GW selecciona un TEID, IP destino (IP del P-GW), y la IP origen (IP del S-GW).
4. Después de recibir los paquetes IP externos, el **P-GW** desencapsula los paquetes internos y los transfiere a Internet a través de enrutamiento IP.

Tráfico downlink (desde Internet a UE)

1. Un **P-GW** recibe paquetes IP destinados para un UE a través de Internet.
2. El P-GW encapsula los paquetes IP de usuario con GTP en S5 y reenvía los paquetes IP externos resultantes al **S-GW** usando, TEID, IP del S-GW y su IP para hacer la cabecera del túnel.
3. **S-GW** elimina el encabezado del túnel S5 GTP, encapsula los paquetes IP del usuario (los paquetes IP internos) con la cabecera del túnel GTP S1 y reenvía los paquetes IP externos resultantes al eNB.
4. Después de recibir los paquetes IP externos, el **eNB** obtiene los paquetes IP del usuario eliminando la cabecera del túnel GTP S1. El eNB transfiere los paquetes al UE a través del enlace radio mediante un portador de datos radio o DRB (Data Radio Bearer).

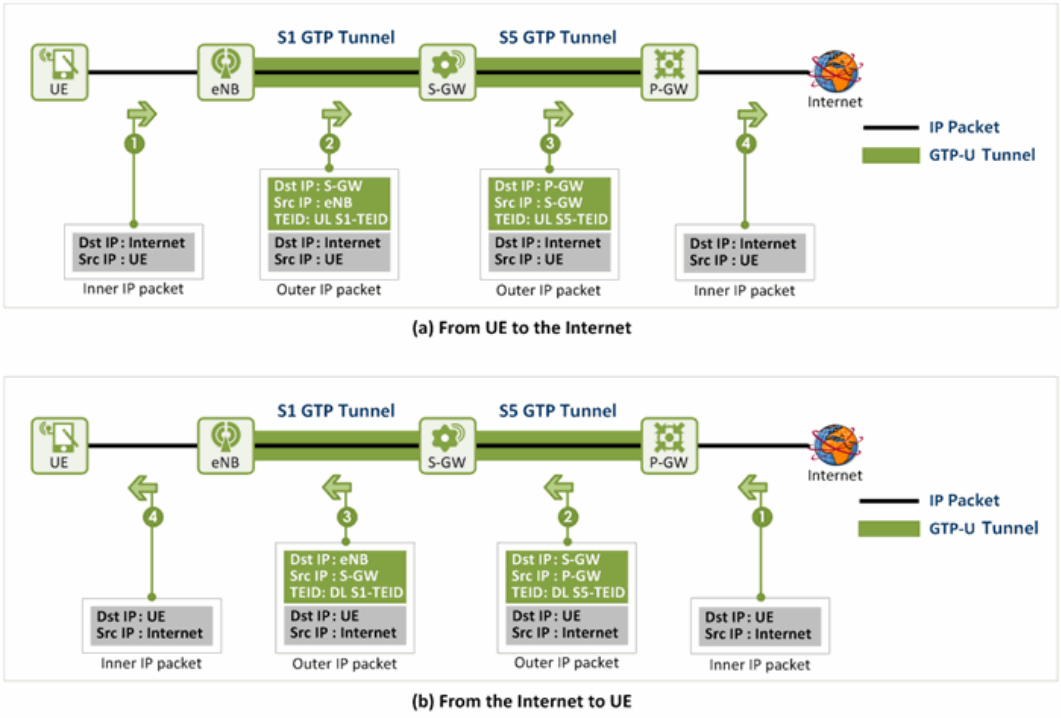


Figure 3.4: Flujo de trafico IP uplink/downlink

3.5 Plano Control

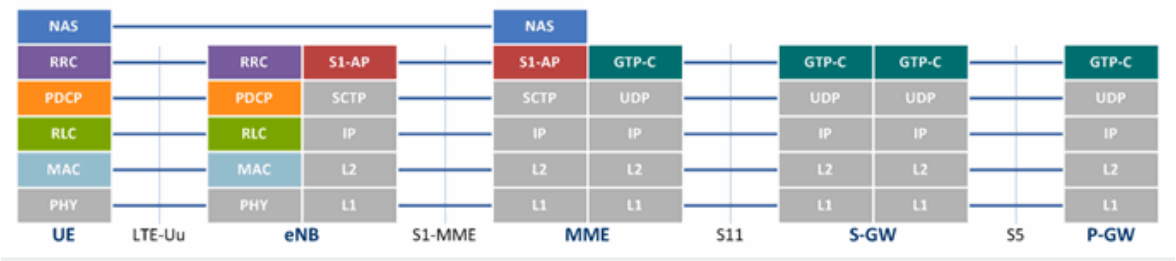


Figure 3.5: Pila Protocolos Plano Control

Los interfaces y protocolos de señalización previos, entre otros, se utilizan para establecer los túneles GTP-U. Para establecer los túneles GTP-U en S1-U, se establecen los siguientes puntos:

- S-GW asigna un identificador TEID para el tráfico Up Link (UL S1-TEID en la figura del flujo del tráfico en el plano de usuario).
- eNB asigna un TEID para el tráfico Down Link.
- Los valores TEID del túnel GTP se intercambian entre el eNB y el S-GW a través del MME mediante mensajes S1AP y GTP-C.

Del mismo modo cuando se establece un túnel GTP en la interfaz S5:

- P-GW asigna un TEID (UL S5-TEID) para el uplink.
- S-GW asigna un TEID (DL S5-TEID) para el tráfico downlink.
- Los TEID se intercambian entre la S-GW y el P-GW usando el protocolo GTP-C.

En GTP-C se utiliza un túnel para la señalización por usuario.

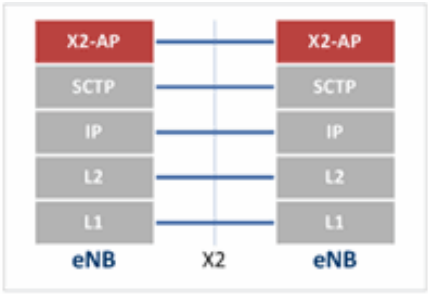


Figure 3.6: Protocolo X2

El protocolo X2-AP en el interfaz X2 se utiliza para gestionar la movilidad de los UE entre nodos eNB y también para las tareas de auto organización o SON (Self-Organizing Network).

Para la movilidad:

- Gestión de handovers entre eNB.
- Gestión de la transferencia de datos de usuario de un eNB a otro.

Para las funciones SON, X2-AP se utiliza para el intercambio de información entre eNB tal como:

- Información de estado.
- Información de la carga de tráfico.
- Información de configuración o actualización de la configuración.
- Información para coordinar entre eNB el ajuste de parámetros de movilidad.

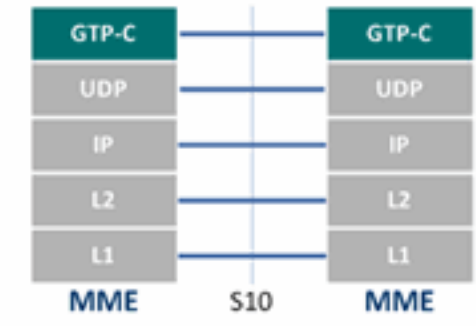


Figure 3.7: Interfaz S10

El interfaz S10 se identifica por ser aquel:

- Es la interfaz entre MMEs.
- Utiliza el protocolo GTP-C.
- Se utiliza para la transferencia de información de los usuarios cuando se realizan handovers que no son del tipo X2 (que no son entre eNBs).
- También sirve para gestionar la reubicación de MMEs.

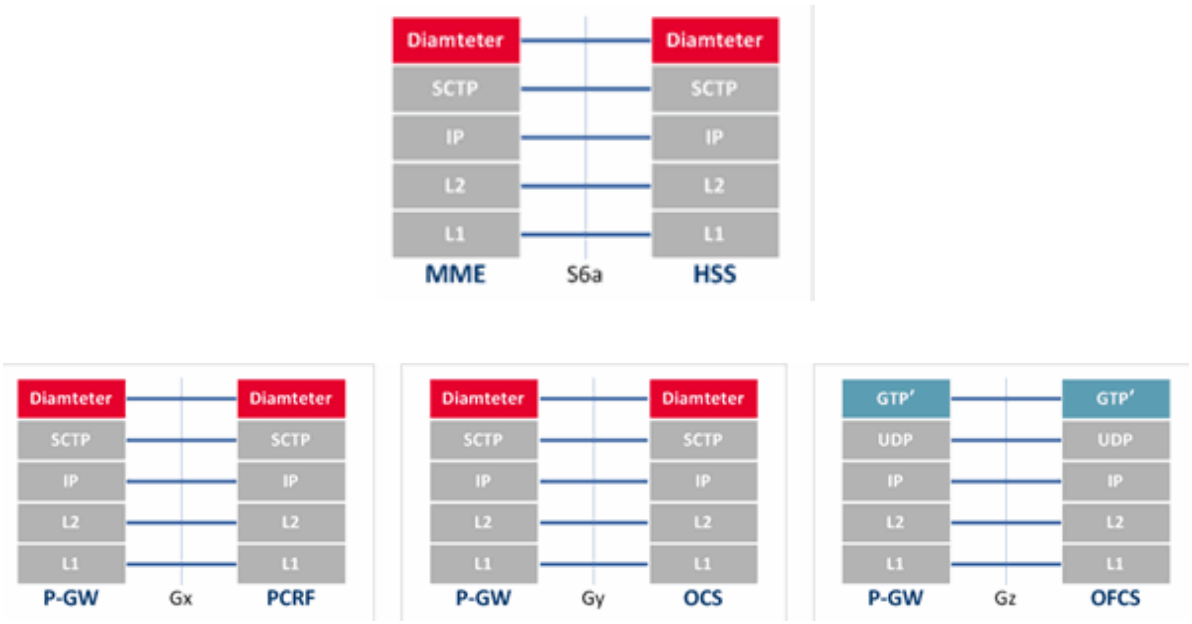


Figure 3.8: Otros Interfaces Protocolo Diameter

Todas las interfaces anteriores se implementan con el protocolo Diameter (la interfaz Gz también se puede implementar con Diameter). El protocolo Diameter será descrito más adelante en un capitulo especifico

Las distintas interfaces son:

- **S6a**: entre HSS y un MME para intercambio de datos de suscripción de usuario y la información de autenticación.
- **Sp**: entre SPR y PCRF para intercambio de perfiles de usuario.
- **Gx**: entre PCRF y un P-GW. Transferencia de políticas de control desde el PCRF al P-GW para gestionar la calidad de servicio y la tarificación.
- **Gy**: entre OCS y P-GW para tarificación online.
- **Gz**: Entre OFCS y un P-GW para tarificación offline.

Chapter 4

Identificación

4.1 Introducción

Un identificador (ID) es un nombre que identifica a un único objeto o a una clase única de objetos donde dicho objeto puede ser una idea, un objeto físico o sustancias.Un identificador puede ser un nombre, número, letra, símbolo o cualquier combinación de ellos en las redes LTE diferentes IDs (Identificadores) son utilizados para identificar cada entidad. Entender los IDs y las entidades EPS es necesario para entender la tecnología LTE

Se puede realizar diferentes clasificaciones de los identificadores dependiendo de algunos atributos propios

- **Fecha de Creación**. La fecha de creación de un ID LTE puede ser:
  - Asignada con la instalación del equipo
  - Provisionada por el operador durante el uso del servicio
  - Creada bajo demanda cuando el usuario accede a la red o utiliza el servicio
- **Tipo**
  - Permanente. Fija una vez definida.
  - Temporal. Cambia cada vez que se activa
- **Rango**. Cada identificador en las redes LTE es único en tanto en el mundo, en el operador de red, en las entidades o canales

Existen diferentes tipos de identificadores como podemos ver en la Figura 4.1 de la [2]. Dependiendo de su naturaleza, si nos fijamos en los identificadores para las **entidades EPS**, estos pueden dividirse en 3 grandes grupos:

- **UE** User Equipment
  - IMSI. International Mobile Subscriber Identity
  - GUTI. Globally Unique Temporary Identifier
  - S-TMSI. SAE Temporary Mobile Subscriber Identity
  - Dirección IP
  - C-RNTI. Cell Radio Network Temporary Identifier
  - UE S1AP ID. UE S1 Application Protocol Identifier
  - UE X2AP ID. UE X1 Application Protocol Identifier
- **ME** Mobile Equipment
  - IMEI. International Mobile Equipment Identity
  - IMEISV. IMEI Software Version
- **NE** Network Equipment. Entidades de red operadas por un operador LTE

- GUMMEI. Globally Unique MME Identifier
- MMEI. Mobility Management Entity Identifier
- Global eNB ID. Global Evolved Node B Identifier
- eNB ID. Evolved Node B Identifier
- ECGI. E-UTRAN Cell Global Identifier
- ECI. E-UTRAN Cell Identifier
- P-GW ID. PDN Gateway Identifier

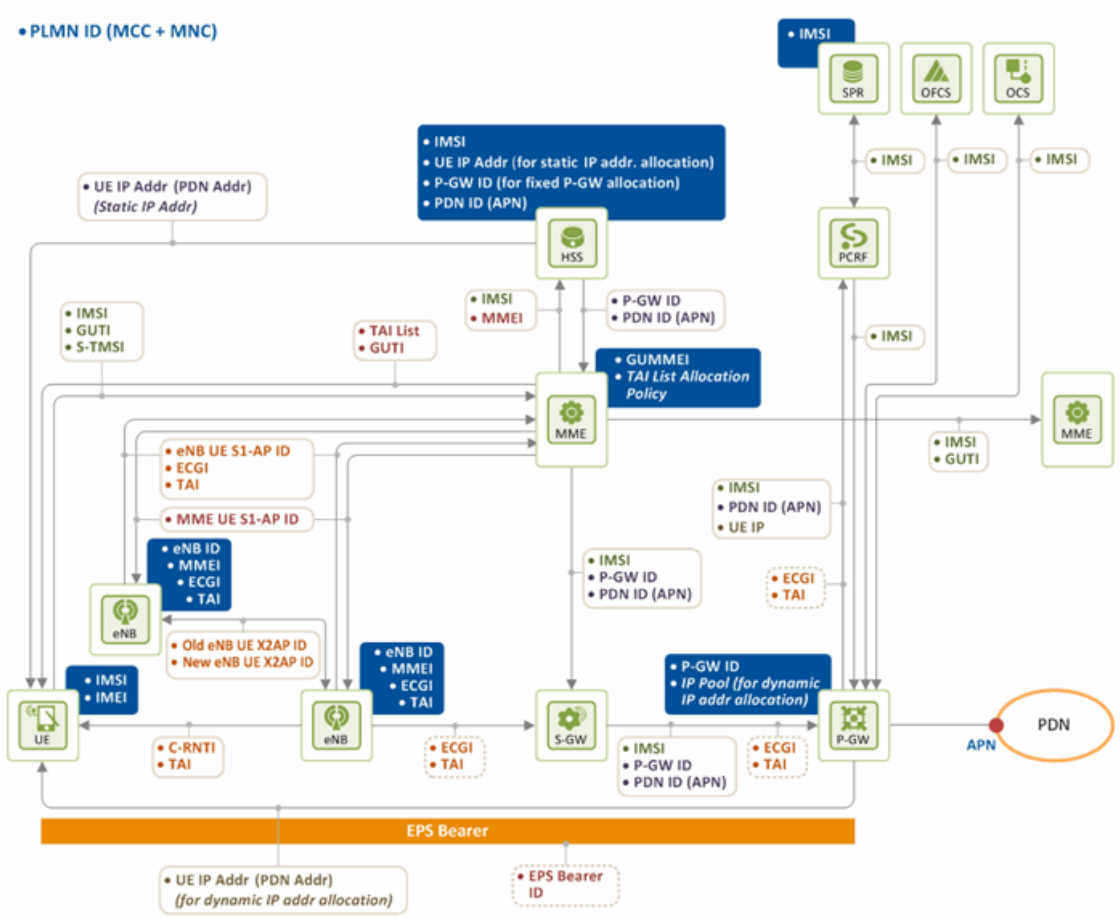


Figure 4.1: Identificadores involucrados en las redes LTE

Asimismo podemos encontrar otro tipo de identificadores utilizados para identificar las **localizaciones** donde se ubica el usuario

- TAI. Tracking Area Identity
- TAC. Tracking Area Code

Por último, podemos realizar otro tipo de identificación dependiendo del trafico entregado. En este caso podrían identificar sesiones y bearers EPS

- PDN ID. Packet Data Network Identifier
- EPS BearerID. Evolved Packet System Bearer OD
- E-RAB ID. E-UTRAN Radio Access Bearer Identifier

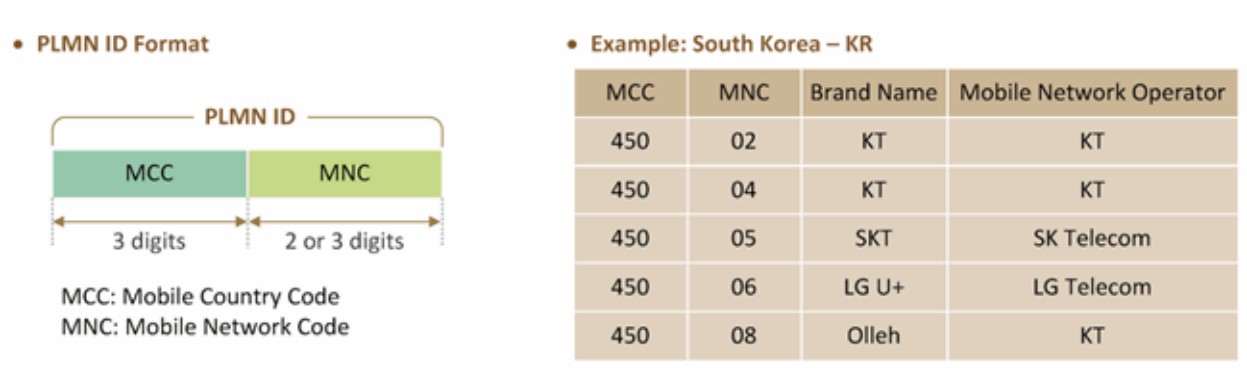
- DRB ID. Data Radio Bearer Identifier
- TEID. Tunnel Endpoint Identifier
- LBI. Linked EPS Bearer Identity

4.2 UE. User Equipment ID

Las redes LTE son redes **all IP** donde los terminales de usuario (UE) comparten los recursos de red y radio. La red LTE asigna un identificador único a cada UE. Cada equipo LTE por lo tanto, tiene su propio identificador denominado **User Equipment ID**.

PLMN son las siglas de Public Land Mobile Network. Están constituidas y gestionadas por operadores de red. El **PLMN ID**, como veremos en la Figura 4.2 de [2] identifica a un operador de una red y tiene un uso global. Esto implica que identifica de forma única en todo el mundo al operador de red. El PLMN ID esta compuesto de un **MCC**(Mobile Country Code) y un **MNC** (Mobile Network Code) donde:

- **MCC** identifica al país donde la red esta localizada
- **MNC** identifica al operador de la red y es asignada para cada país



MCC	MNC	Brand Name	Mobile Network Operator
450	02	KT	KT
450	04	KT	KT
450	05	SKT	SK Telecom
450	06	LG U+	LG Telecom
450	08	Olleh	KT

Figure 4.2: Formato del identificador PLMN ID y Ejemplo

En el ejemplo anterior vemos que para Corea del Sur hay 3 operadores de red diferente: KT, SK Telecom y LT Telecom. En este caso, KT administra 3 redes diferentes: 02, 04 y 08

IMSI son las siglas de International Mobile Subscriber Identity. IMSI es un número único que identifica de forma global a un suscriptor móvil. El IMSI esta compuesta del **PLMN ID** y del **MSIN** (Mobile Subscriber Identification Number) asignado por el operador. El tamaño máximo del MSIN es 15 dígitos. El **IMSI** identifica a un suscriptor móvil dentro del PLMN. El IMSI, como veremos en la Figura 4.3 de [2], es un valor permanente en el **USIM, HSS y SPR** y tiene un valor temporal para **MME, S-GW, P-GW y PCRF**

En el ejemplo anterior, el terminal móvil del usuario UE dentro de Corea del Sud, habiendo contratado con el operador SK Telecom tiene un IMSI de 450050123456789

El proceso de obtención del IMSI lo podemos describir con las siguientes etapas:

- Cuando un usuario compra un **USIM** (UMTS Subscriber Identity Module) y se suscribe a una red, se le asigna el IMSI
- El **IMSI** es almacenado en el **USIM** dentro del móvil
- El IMSI es facilitado por el operador al **HSS** y al **SPR**
- Una vez asignado, el UE envía su IMSI cuando se conecta a la red
- El **MME**, una vez recibido el IMSI, establece el bearer por defecto

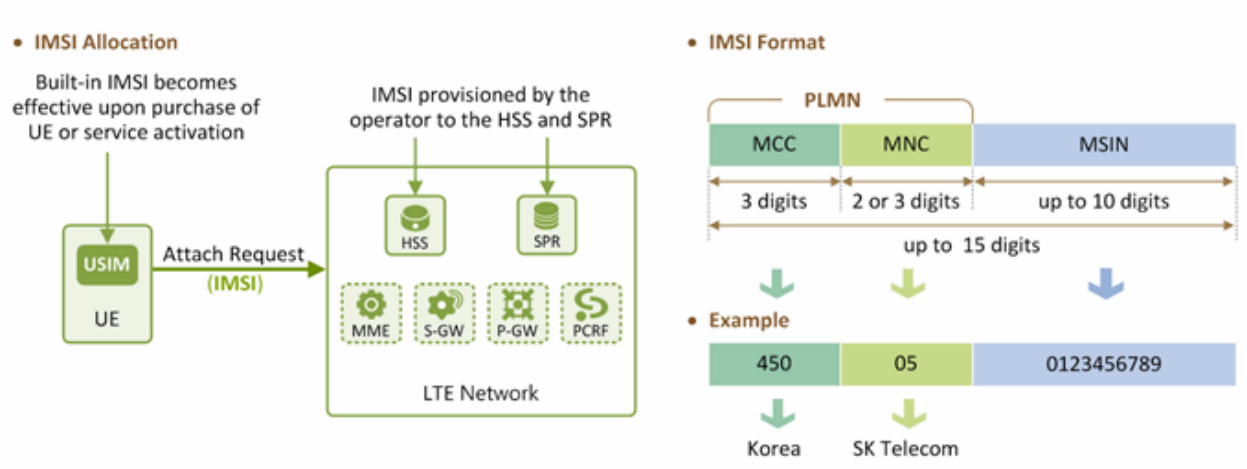


Figure 4.3: Formato del identificador IMSI y Ejemplo

Tal como hemos visto anteriormente, el IMSI es un valor permanente que identifica de forma única a un suscriptor móvil. Este valor se expone frecuentemente en el canal radio por lo que se expone a problemas de seguridad de forma constante. Para mejorar la seguridad apareció el **GUTI** (Globally Unique Temporary Identifier), valor que es asignado al UE por el MME y es utilizado en vez del IMSI.

Para realizar la asignación del GUTI se realizan las siguientes acciones:

- La primera vez que se conecta el UE a la red usa su IMSI para solicitar acceso
- El operador asigna el identificador GUTI al UE
- El UE utiliza, a partir de este momento, el GUTI en vez del IMSI para acceder a la red
- Que el UE utilice el IMSI o GUTI para acceder a la red, depende de que valor es seteado en el **TIN** (Temporary Identifier used in Next Update)
- El valor definido en el TIN será el GUTI en el caso de que el proceso de conexión a la red o el **TAU** (Tracking Area Update) sea satisfactorio

El formato del GUTI, como se muestra en la Figura 4.4 de [2], se compone de diferentes segmentos separados cada uno de los cuales identifica un elemento de la red LTE

- Un operador de red puede tener uno o más de un grupo MME, compuesto de múltiples MMEs
- Un **MMEI** es un identificador de MME. El **MMEI** esta compuesto de un **MMEGI** (MME Group Identifier), que representa al grupo MME, y de un **MMEC** (MME Code) que representa al MME dentro del grupo
- El **GUMMEI** (Globally Unique MME Identifier) esta compuesto del **PLMN ID** y del **MME ID**
- El **M-TMSI**(MME Temporary Mobile Subscriber Identity) es un valor único asignado al suscriptor por el MME. Con este valor se pretende mantener la confidencialidad del suscriptor. Este valor es único dentro del MME
- El **GUTI** esta compuesta de un **GUMMEI** y de un **M-TMSI**
- El **S-TMSI** esta compuesto de **MMEC** y un **M-TMSI**, y es utilizado para identificar a un UE dentro de un grupo MME. Al ser más corto que el GUTI permite mejorar la eficiencia de transmisión en los enlaces radio

La **dirección IP**, también llamada **dirección PDN**, es asignada por la red LTE al UE. Dado que un UE puede conectarse a varios PDN a la vez, la red LTE debe asignar una dirección IP para cada PDN. La dirección IP es utilizada para identificar al UE dentro de las redes. La asignación de IP puede ser:

- Dinámica. El operador de red asigna cada vez una IP distinta de la pila, cuando el UE se conecta a la red
- Estática. El operador asigna una IP en el momento de la suscripción y cada vez que el UE se conecta a la red, siempre le es asignada la misma IP

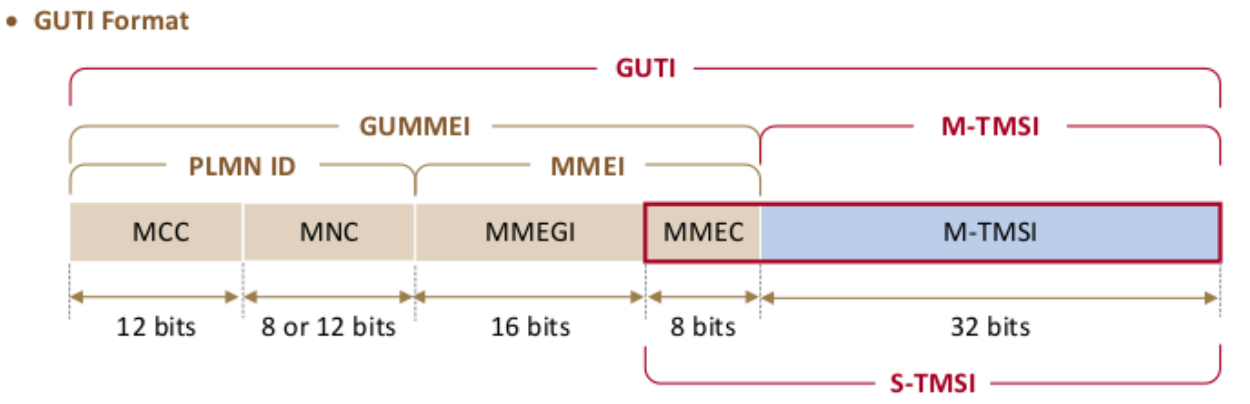


Figure 4.4: Formato del identificador GUTI

El **C-RNTI** es un identificador utilizado para distinguir equipos de usuario diferentes dentro de una celda.El **C-RNTI** (Cell Radio Network Temporary Identifier) es asignado al **UE** por el **eNB**. El **C-RNTI**, como veremos en la Figura 4.5 de [2] permite identificar de forma única un UE dentro de una celda del eNB siendo este valor solo valido dentro de esa celda. En el momento que el UE se mueve a una celda diferente, un nuevo C-RNTI es asignado al UE. El **eNB** es responsable de asignar los recursos radio a los UE asignados a él. El eNB notifica a cada UE que puede utilizar el canal radio en el próximo **TTI** (Transmission Time Interval) enviando un mensaje de broadcast con el C-RNTI mediante el **PDCH** (Physical Downlink Control Channel). El UE cuyo C-RNTI corresponde al mensaje de broadcast, puede utilizar el canal radio en el próximo TTI.

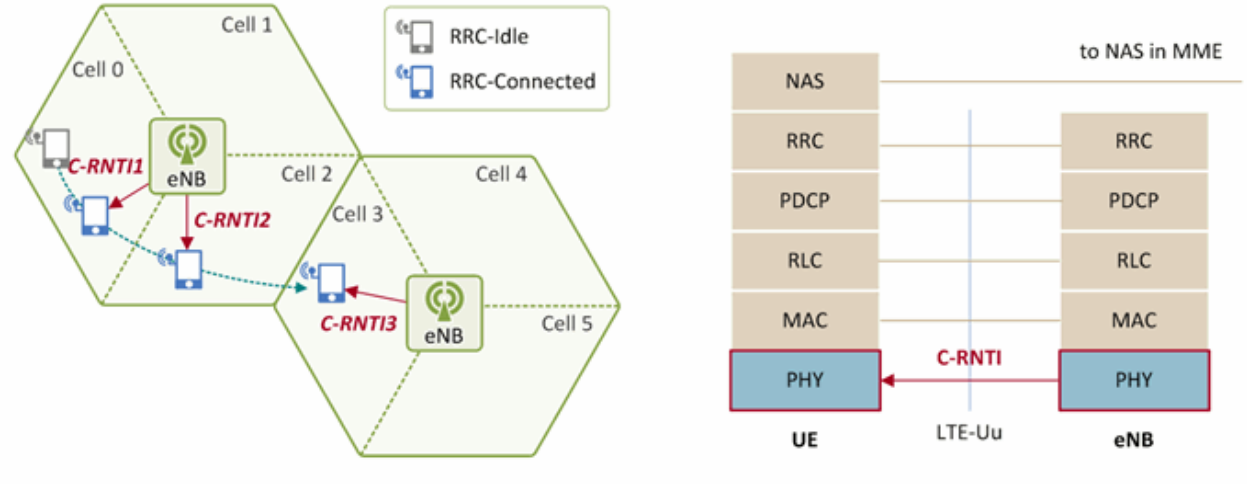


Figure 4.5: Asignación Identificador C-RNTI

Identificadores UE S1AP se utilizan para distinguir UEs dentro de la interfaz S1-MME. La capa **S1AP** se encarga de los mensajes de control entre el eNB y el MME a través de la interfaz **S1-MME**. Como cada eNB tiene múltiples UE conectadas a él, y el enlace S1 es único, es necesario identificar de forma única los mensajes S1AP para cada UE. El eNB asigna un identificador **eNB UE S1AP ID**, como veremos en Figura 4.6 de [2] a cada UE en la primera conexión. Asimismo, un MME tiene múltiples eNB conectados a través de múltiples enlaces S1, por lo que, es necesario identificar de forma única estos mensajes. El MME asigna un identificador **MME UE S1AP ID** a cada UE en la primera conexión. Después de la primera conexión, todos los mensajes de control intercambiados en el enlace S1-MME son entregados con la combinación de 2 identificadores **(eNB UE S1AP ID,MME UE S1AP ID)** Los **Identificadores UE X2AP** se utilizan para distinguir UEs dentro de la interfaz X2.La capa **X2AP** se encarga de los mensajes de control entre 2 eNBs vecinos sobre la interfaz **X2**. Como cada eNB tiene múltiples UE conectadas a él, es necesario identificar de forma única los mensajes X2AP para cada UE. El eNB origen asigna un identificador **Old eNB UE X1AP ID** a cada

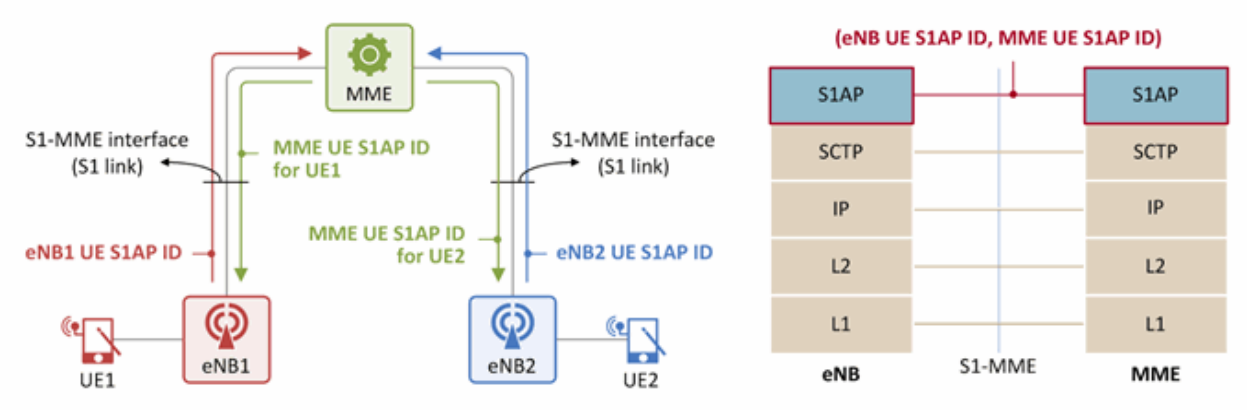


Figure 4.6: Asignación S1AP

UE con el primer mensaje enviado a un eNB destino. El eNB destino asigna un identificador **New eNB UE X1AP ID** a cada UE con el primer mensaje recibido del eNB origen. Después del primer intercambio de mensajes, todos los mensajes X2AP (como muestraa la Figura 4.7 de [2] sobre la interfaz X2 son intercambiados con el par **(Old eNB UE X1AP ID, New eNB UE X1AP ID)**

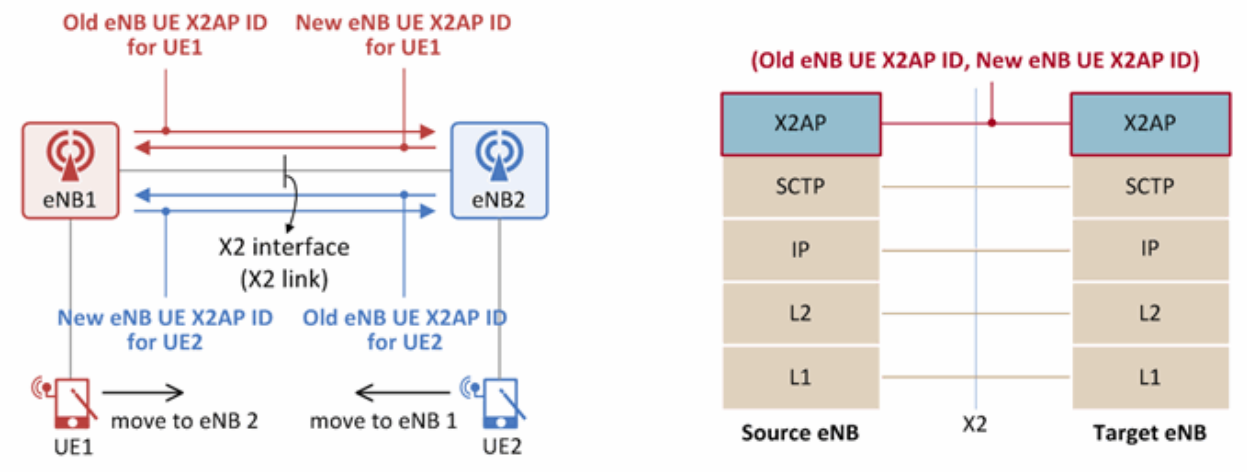
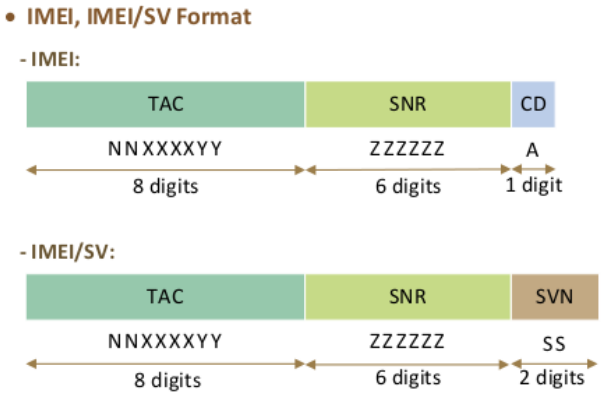


Figure 4.7: Asignación X2AP

4.3 ME. Mobile Equipment ID

Un UE esta compuesto de un **ME** y un **USIM** (UMTS Subscriber Identity Module). Un ME puede estar compuesto de un **TE** (Terminal Equipment) y un **MT** (Mobile Terminal). El MT es donde se ejecutan los protocolos de acceso radio. El TE es donde se ejecutan las funciones de control del MT. El MT y el TE están normalmente integradas en un móvil pero separadas en un PC

IMEI & IMEISV son aquellos identificadores permanentes en un ME. En la Figura 4.8 de [2] podemos comprobar su formato. El **IMEI** (International Mobile Equipment Identity) es un identificador único asignado a cada **ME**. El IMEI se asigna a cada ME en el momento de su fabricación contiendo información del fabricante, el modelo y el número de serie. El **IMEI** esta compuesto del **TAC** (Type Allocation Code), **SNR** (Serial Number) y el **CD** (Check Digit). El **IMEISV** esta compuesto del **TAC** (Type Allocation Code), **SNR** (Serial Number) y el **SVN** (Software Version Number). El **TAC** esta compuesto, a su vez, del **RBID** (Reporting Body Identifier) y del **ME Type ID** que representa el nombre del fabricante y el modelo. Los números de serie son asignados por el fabricante. Los operadores mantienen una base de datos con todos los IMEI. De esta forma, pueden denegar el acceso a la red a IMEIs reportados como perdidos o robados



	Format	Description [4]
TAC*	NN	Reporting Body ID
	XXXXYY	ME Type ID defined by Reporting Body
SNR	ZZZZZZ	Serial No, Allocated by Reporting Body but assigned per ME by the manufacturer
CD	A	Check Digit, defined as a function of all other IMEI digits
SVN	SS	Software Version Number, 00 – 98. 99 is reserved for future use.

* TAC: Type Allocation Code

Figure 4.8: Formato Identificador IMEI y IMEI/SV

4.4 NE. Network Equipment ID

Los identificadores de NE (Network Equipment) se pueden clasificar en 2 dependiendo de si están identificados únicamente de forma global o no

- Con PLMN ID
- Sin PLMN

El **MME**(Mobility Management Entity), que veremos en la Figura 4.9 de [2], se localiza entre el **E-UTRAN** y el **EPC**, y se encarga del control de conexiones de UEs a la red LTE. Se encarga también, de la **gestión de bearers**. Intercambia mensajes de control con el **HSS**, con el **S-GW** y con **eNB**. En definitiva, es el cerebro de la red LTE. Los operadores de red agrupan los MMEs y los operan de forma grupal. Existen 4 identificadores para MMEs:

- **MMEGI**. Identificador que representa a un grupo de MMEs
- **MMEC**. Identificador que representa a un MME especifico dentro del grupo de MMEs
- **MMEI**. Se utiliza para identificar un MME en la red de un operador. Esta compuesto de un MMEGI y un MMEC
- **GUMMEI**. Combinación de PLMN ID y MMEI, para identificar globalmente el MME

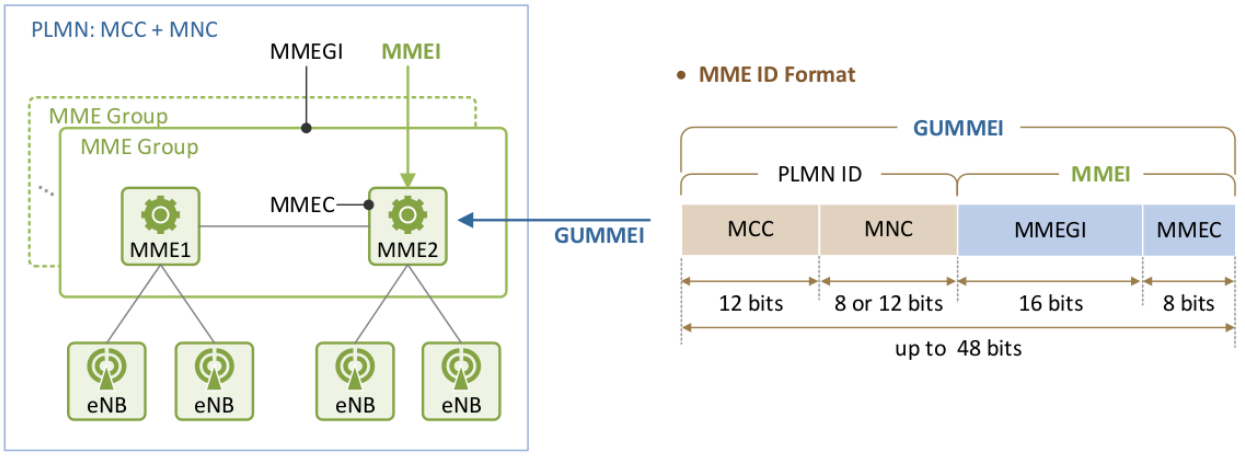


Figure 4.9: Identificadores de MME y formato

Para poder identificar eNBs existen 2 valores diferentes, el **eNB ID** y el **Global eNB ID**, que podemos revisar en la Figura 4.10 de [2]. El identificador **eNB ID** se utiliza para identificar un eNB dentro de la red del operador. El identificador **Global eNB ID** se utiliza para identificar un eNB de forma global. El **Global eNB ID** es una combinación del **PLMN ID** y del **eNB ID**. El identificador **Cell ID** se utiliza para identificar la celda dentro del eNB. El identificador **CSG ID** se utiliza para identificar celdas accesibles solo a un cierto grupo de suscriptores

Los identificadores **Cell IDs** y **eNB IDs** son asignados por el operador de red cuando un eNB es instalado. Una vez instal-

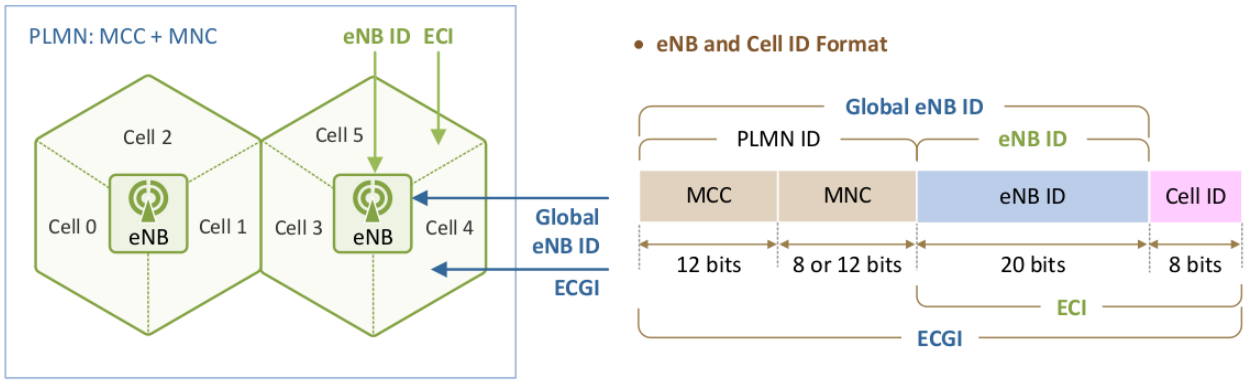


Figure 4.10: Formato identificador eNB

ado, el eNB intenta conectarse al **MME** mediante el **enlace S1** facilitando su **Global eNB ID** y el **TAS** soportado. En el caso que exista soporte para CSGs, también facilita su **CSG ID**. El MME responde enviando su **GUMMEI** al eNB.

Un P-GW se identifica con su P-GW ID. La provisión de P-GW puede realizarse de 2 formas

- **Fija**. El operador de red provee el P-GW dentro de los perfiles de suscripción del HSS. El HSS informa al MME del **P-GW ID** al que debe conectarse
- **Dinámica**. El MME selecciona un P-GW utilizando las reglas de derivación definidas por el operador de red. El MME obtiene la lista de P-GW a través de una consulta DNS y selecciona uno

El identificador **P-GW ID** se encarga de identificar al P-GW. El **P-GW ID** puede estar expresado como una dirección IP o un **FQDN** (Full Qualified Domain Name) La **Provisión Fija de P-GW** se detalla con las siguientes acciones y la podemos validar en la Figura 4.11 de [2]

- UE accede a la red LTE, el MME solicita al HSS información del perfil de usuario del UE

- El HSS informa al MME que los conexiones PDN son 2, PDN 1 (Internet) y PDN 2 (IMS)

- El P-GW 1 se utilizará para conectarse al PDN 1, y el P-GW 3 para conectarse al PDN 2

- MME establece la conexión PDN enr el UE e Internet a través del P-GW 1 y otra entre el UE e IMS a través del P-GW 3

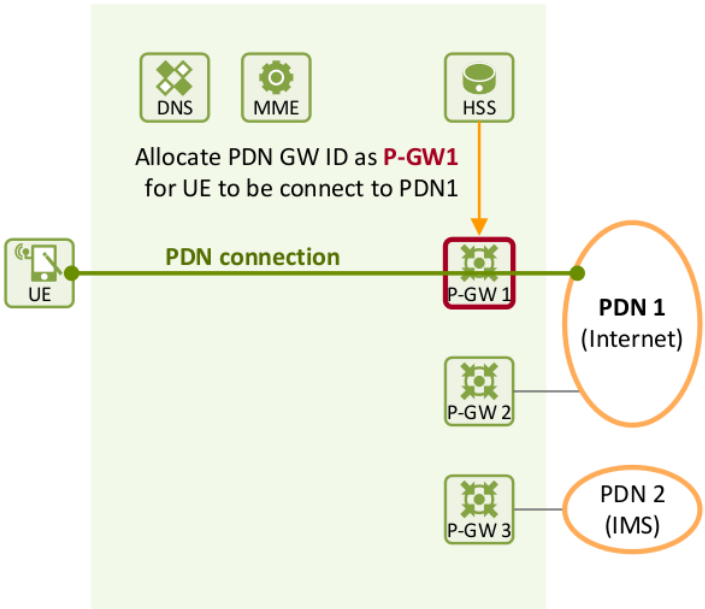


Figure 4.11: Asignacion P-GW

4.5 ID de Localizacion

El MME necesita tener información actualizada de la localización de cada UE ya que esta encargado de la gestión de movilidad. La red LTE conoce la localización del UE a **nivel de celda** si esta en estado activo y utilizando servicio. En el caso que el UE este inactivo y por lo tanto no utilizando ningún servicio, podrá ubicar al UE a **nivel de TA**

Los **Identificadores de Localización** son el TAC y el TAI tal como se muestra en Figura 4.12 de [2] . El identificador **Cell ID** se utiliza para identificar la celda dentro del eNB. Mientras, el identificador **TAC** (Tracking Area Code) se utiliza para identificar el TA en la red del operador. Por ultimo, el identificador **TAI** (Tracking Area Identifier) se utiliza para identificar el TA de forma única globalmente. El **TAI** esta compuesto de **PLMN ID** y un **TAC** Una vez el UE se conecta a una red LTE, el MME

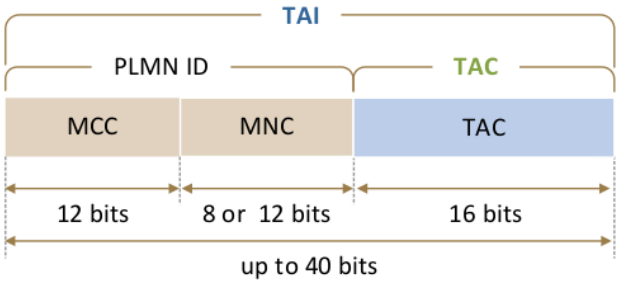


Figure 4.12: Formato del identificador TAI

le asigna un **TAI** y a partir de entonces, mantiene trazabilidad de su ubicación. El UE informa al MME de su nueva ubicación y solicita una actualización del TA en el caso que deje el TA donde esta registrado. El MME mantiene la información del TA en el que esta ubicado el UE y actualiza su listado de TAI. En el caso que un UE se mueve a un TA dentro de la lista de sus TAI, no será necesario que solicite una actualización de TA. En el caso que el periodo de renovación de su actual TA expire, se deberá informar al MME de su actual ubicación

Cuando el MME recibe información destinada a un UE, necesita saber su localización para remitir los datos correctamente. Cuando el UE esta activo, el MME conoce la localización exacta. Mientras, cuando el UE esta inactivo, el MME no sabe en que celda estará localizado. En el caso que esté inactivo, el MME envía un mensaje de **Pagging** a todas los eNBs que pertenezcan al TA donde el UE reporto que estaba, informando que existen datos para él. Los UE en estado inactivo se activan cada cierto tiempo para chequear los mensajes de Pagging. Si se encuentra que existe un mensaje de Pagging para él responde para recibir los datos

En el ejemplo anterior podemos comprobar como el eNB1 esta en TA1, eNB2 en TA2 y eNB3 y eNB4 en TA3. El UE1 esta registrado en MME1 y tiene asignada una lista TAI de TAI1, TAI2. Mientras, el UE2 esta registrado en MME2 y tiene asignada una lista TAI de TAI2, TAI3. El UE1 accede a eNB1 y se vuelve inactivo. Mientras tanto se mueve de eNB1 –> eNB2 –> eNB3. El comportamiento sería el siguiente:

- Mientras esta en eNB1, UE1 esta en TA1
- Mientras se mueve de eNB1 a eNB2, UE1 identifica que su nueva TA es TA2. Revisa su lista de TAI y como esta allí el valor, sabe que no debe solicitar una actualización de TA
- Mientras se mueve de eNB2 a eNB3, UE1 identifica que su nueva TA es TA3. Revisa su lista de TAI y como no esta allí el valor, sabe que debe solicitar una actualización de TA. Realiza un **TAU Request** al MME para actualizar su localización

4.6 ID Sesiones/Bearers EPS

La conexión IP entre un UE y un PDN se llama conexión PDN o **sesion EPS**. Cada sesión EPS se representa por una **dirección IP** del UE y un **PDN ID**. Existen múltiples EPS bearers para entregar el trafico. Aplica la **QoS** obtenida del **PCRF** a los EPS bearers

Algunas características importantes de la sesion EPS serían

- Tener un PDN a través del cual obtener los servicios solicitados
- Se asigna una dirección IP al usuario

- Se seleccionan la política de reglas a aplicar a los paquetes IP
- Se establece un bearer por defecto para entregar los paquetes IP
- Se intercambian los mensajes entre el UE y el PDN siguiendo las reglas establecidas por el operador

El **EPS Bearer** es un canal a través del cual, los paquetes IP son entregados a la red. Un UE puede tener múltiples EPS bearers al mismo tiempo siendo, cada EPS bearer identificado con su **EPS Bearer ID**. El **EPS Bearer ID** es asignado por un **MME**. Un **EPS Bearer** es la combinación de 3 bearers

- **DRB**. Establecido sobre la interfaz LTE-Uu entre el UE y el eNB
- **S1 Bearer**. Establecido sobre la interface S1-U entre el eNB y el S-GW
- **S5 Bearer**. Establecido sobre la interface S5 entre el S-GW y el P-GW

Existe adicionalmente otro bearer **E-RAB**. Este es un bearer desde el UE hasta el S-GW que además, esta compuesto de un **DRB** y un **S1 bearer**. Los E-RABs están identificados con su **E-RAB ID** que es asignado por el MME. En la Figura 4.13 de [2]

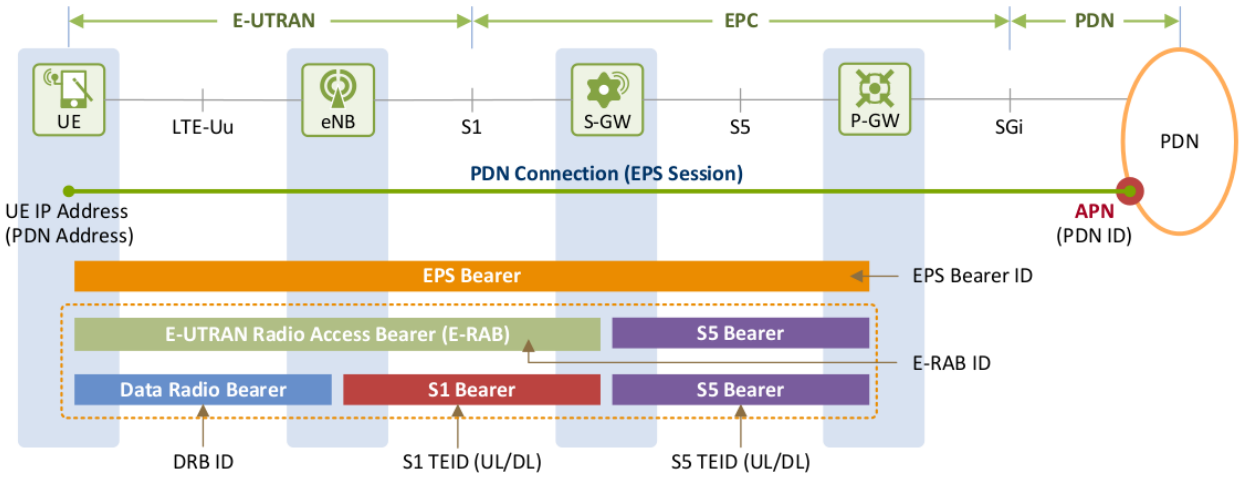


Figure 4.13: Vision General Identificadores sobre Bearer

- **[UE] - [eNB]: Data Radio Bearer**
  - EPS Bearer establecido sobre una **interfaz LTE-Uu**
  - El trafico IP es entregado a través de un DRB
  - Diferentes DRBs son identificados por su **DRB ID**
  - El **DRB ID** es asignado por el MME
- **[eNB] - [S-GW]: S1 Bearer**
  - EPS Bearer establecido sobre una **interfaz S1-U**
  - El trafico IP es entregado a través de un **túnel GTP**
  - Diferentes S1 Bearers son identificados por su **TEID** (Tunnel Endpoint Identifier)
  - El **TEID** es asignado por eNB y S-GW
- **[S-GW] - [P-GW]: S5 Bearer**
  - EPS Bearer establecido sobre una **interfaz S5**
  - El trafico IP es entregado a través de un **túnel GTP**
  - Diferentes S5 Bearers son identificados por su **TEID** (Tunnel Endpoint Identifier)
  - El **TEID** es asignado por P-GW y S-GW

Existen 2 tipos de EPS Bearers como muestra la Figura 4.14 de [2]:

- Por defecto
- Dedicados

Cada PDN debe tener un EPS Bearer por defecto, y puede tener uno o múltiples Bearers dedicados.

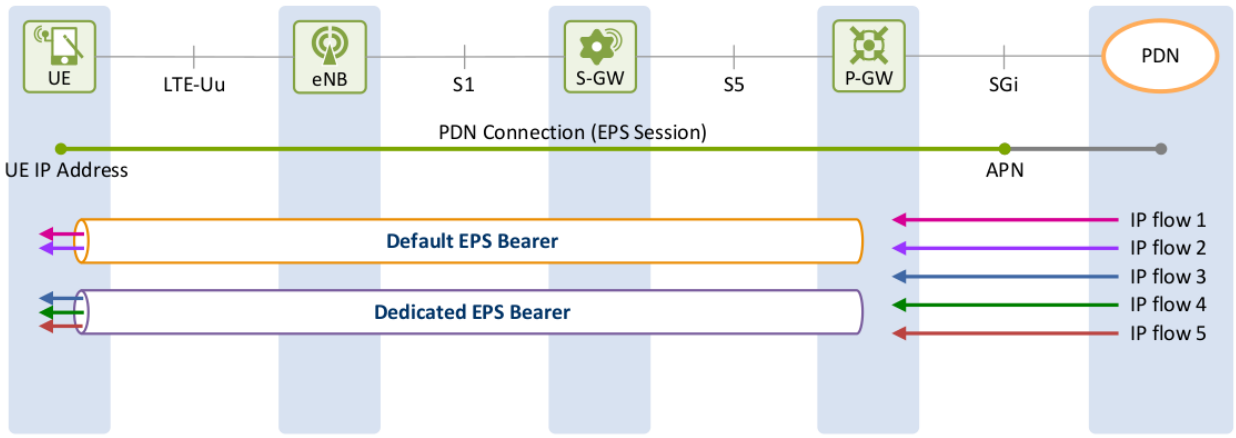


Figure 4.14: Tipos de Bearers EPS

La red LTE es una red **all-IP** por lo que, siempre provee conectividad IP. Una vez el usuario se conecta al PDN, es establece un EPS bearer, que se mantiene activo hasta que el UE se desconecta de la red. Pueden establecerse otro tipo de EPS bearers si la EPS bearer por defecto no es suficiente, de forma que, aseguremos una determinada QoS. El bearer establecido se llama **EPS bearer dedicado**. En el momento que no existe trafico, el EPS bearer dedicado se elimina. Los bearer dedicados están unidos a bearer por defecto. Los bearers enlazados son representados por un **LCI** (Linked EPS Bearer Identity)

El identificador **PDN ID** (o Access Point Names (**APN**)) identifica a PDNs tal como se ve en la Figura 4.15 de [2]. Un **APN** es la combinación de un **Network ID** y un **Operator ID**. El **Network ID** se utiliza para identificar PDNs (como Internet o VPN Corporativas) o servicios (como IMS). El **Operator ID** identifica al operador de red.

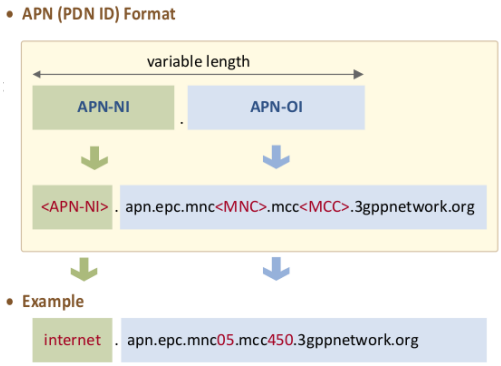


Figure 4.15: Formato APN

Cuando un UE se conecta a la red por primera vez, un APN por defecto es descargado del perfil de suscripción del **HSS** al **MME**. El **MME** selecciona un PDN basándose primero en el APN y después en el P-GW, a través del cual se conecta el UE a la PDN.

El **EPS Bearer** es una conexión establecida entre el UE y el P-GW para entregar trafico IP. Los bearers se identifican con el **EPS Bearer ID** que esta compuesto por 4 bits. Un UE puede tener hasta 11 EPS Bearer y sus IDs van del valor 5 al 15. El **EPS Bearer ID = 0** no se asigna nunca. El **EPS Bearer ID = 1 - 4** esta reservado

Los **EPS Bearer ID** son asignados por el **MME**. Cuando el UE se conecta a la red, el MME obtiene el perfil de QoS del HSS par establecer el bearer por defecto. El procedimiento para establecer el bearer se inicia cuando el **EPS Bearer ID** es asignado por el MME A continuación se describirán los identificadores de bearer EPS

El **E-RAB** es un EPS bearer establecido entre el **UE** y el **S-GW**. Este bearer se identifica con el **E-RAB ID**. El **E-RAB ID** es asignado por el **MME** una vez establecida el EPS bearer. El **E-RAB ID** se mapea contra un **EPS Bearer ID** en una escala 1:1. En el momento de establecer el EPS bearer,el MME solicita al eNB la configuración del E-RAB, el eNB crea el DRB con el UE y Bearer S1 con S-GW. Cuando no hay trafico de usuario, y por lo tanto el usuario pasa a estado inactivo, el E-RAB es desactivado y solo el Bearer S5 es mantenido. En el momento que el trafico de usuario vuelve, el E-RAB es restablecido

El **DRB** es un EPS bearer establecido sobre el canal radio entre el **UE** y el **eNB**. Este bearer se identifica con el **DRB ID** de 4 bits. El **DRB ID** es asignado por el **eNB** una vez establecida el EPS bearer. El **DRB ID** se mapea contra un **EPS Bearer ID** en una escala 1:1. En el momento de establecer el EPS bearer,el MME solicita al eNB la configuración del E-RAB, el eNB crea el DRB con el UE y le asinga el **DRB ID**

El **Bearer S1 y S5** son establecidos entre el **eNB** y el **S-GW** en forma de tuneles **GTP**. Los tuneles GTP se identifican con su **TEID** (Tunnel Endpoint Idenfier) de 32 bits. En el momento de establecer el EPS bearer, para S5 bearer, el S-GW asigna un **DL S5 TEID** y el P-GW asigna **UL S5 TEID**. En el momento de establecer el EPS bearer, para S1 bearer, el S-GW asigna un **UL S1 TEID** y el enB asigna **DL S1 TEID**

Una sesion EPS puede tener más de un EPS bearer. El **EPS Bearer por defecto** es activado/desactivado cuando la sesión se activo o desactiva. El **EPS Bearer dedicado** puede ser creado o eliminado cuando la sesión EPS se crea. Como los 2 bearers pertenecen al mismo PDN para el mismo usuario, es requerido identificar de forma única los 2 bearers. El **LBI** se utiliza para identificar cada EPS Bearer

Chapter 5

Seguridad

5.1 Introducción

Las redes LTE ofrecen tres bloques básicos de seguridad como podemos ver en la Figura 5.1 de [3]:

- **Autenticación LTE**. La Autenticación LTE es el proceso para determinar si un usuario es un suscriptor autorizado de la red a la que está tratando de acceder.
- **Seguridad NAS** (Non Access Stratum). Mecanismos necesarios para entregar de forma segura (integridad/cifrado) los paquetes NAS entre un UE y un MME.
- **Seguridad AS** (Access Stratum). Mecanismos necesarios para entregar de forma segura (integridad/cifrado) los paquetes AS entre un UE y un eNodeB:
  - Paquetes de señalización RRC.
  - Paquetes de usuario (a redes PDN).

Para realizar la autenticación mútua en LTE se utiliza EPS AKA (Authentication and Key Agreement). EPS AKA consta de dos pasos.

1. Un HSS (Home Server Suscriptor) genera uno o normalmente varios vectores de autenticación del tipo: (RAND, AUTN, XRES, K_{ASME}) y los entrega al MME que está en contacto con el usuario.
2. El MME selecciona uno de los vectores de autenticación, lo utiliza para la autenticación mutua con el UE y para compartir una clave de autenticación (K_{ASME}).

La red debe ser autenticada porque el usuario puede estar en roaming.

Una ASME (Access Security Management Entity) se define como la entidad que recibe las clave(s) de alto nivel desde un HSS para una red de acceso. En EPS, el MME es el que sirve como ASME. Para evitar cualquier posible espionaje o manipulación de datos a través de enlaces de radio, K_{ASME} no se entrega a la UE a través de E-UTRAN. El procedimiento sería el siguiente:

- El MME proporciona parte del vector autenticación al UE.
- El UE utiliza esta información para autenticar la red y generar K_{ASME}.
- Una vez el UE y el MME se han autenticado mutuamente, comparten la misma clave K_{ASME}.

La seguridad NAS se diseña para entregar de forma segura mensajes de señalización entre UE y MMEs a través de enlaces de radio. Se realiza la comprobación de integridad y cifrado de mensajes de señalización NAS utilizando para ello, claves diferentes para la comprobación de la integridad:

1. K_{NASint}: integridad de paquetes NAS.
2. K_{NASenc}: cifrado de paquetes NAS.

La comprobación de integridad es obligatoria siendo el cifrado es opcional. Las claves de seguridad de NAS (integridad y cifrado) los UE y MMEs la derivan de la calve K_{ASME}.

El propósito de la seguridad AS es garantizar la entrega segura de datos entre un UE y un eNB a través de enlaces de radio. Esta seguridad AS proporciona:

- Integridad/cifrado de los mensajes de señalización RRC en el plano de control (integridad obligatorio, cifrado opcional).
- Solo cifrado de los paquetes IP en el plano de usuario.

Las claves involucradas serían las siguientes:

1. K_{RRCint}: integridad de paquetes de señalización RRC.
2. K_{RRCenc}: cifrado de paquetes de señalización RRC.
3. K_{UPenc}: cifrado de paquetes IP de usuario.

Las claves se derivan de una clave denominada K_{eNB}. El UE deriva K_{eNB} de K_{ASME}. Sin embargo, la clave K_{ASME} no se transfiere a los eNB. El MME genera la clave K_{eNB} y la reenvía al eNB. Por último, la comprobación de integridad y cifrado AS las realiza la capa PDCP (Protocolo de Convergencia de Datos por Paquetes).

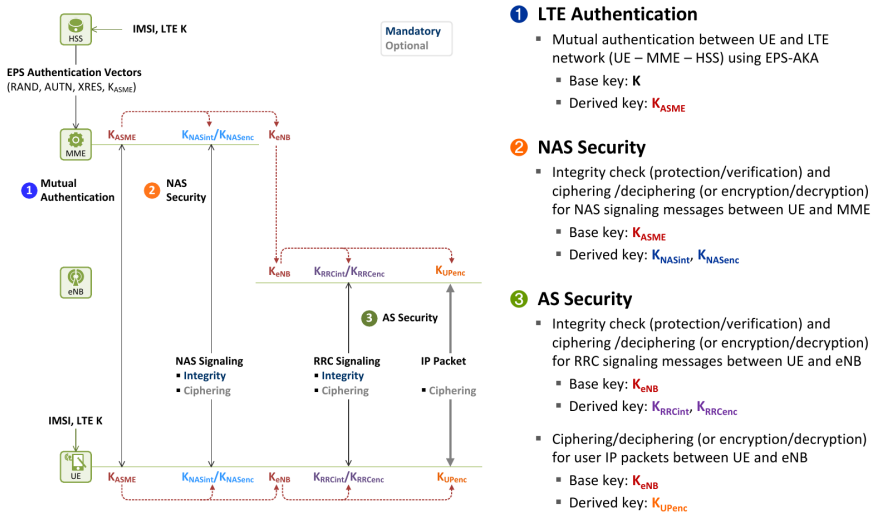


Figure 5.1: Seguridad LTE

5.2 Autenticación LTE

Cuando un usuario solicita el acceso a una red LTE, se utiliza EPS AKA para autenticación mutua usuario/red. En la Figura 5.2 de [3] podemos ver el proceso de forma gráfica. El procedimiento de autenticación es tal como sigue:

- El UE envía una dicha solicitud (attach request) al MME.
- El MME identifica al usuario usando su IMSI.
- El MME pide un vector (o varios) de autenticación (AV) a un HSS.
- El HSS genera AV(s) utilizando el algoritmo EPS AKA y las envía a la MME:
  $AV = \{RAND, XRES, AUTN_{HSS}, K_{ASME}\}$
- Después de almacenar los AVs, el MME selecciona uno de ellos y lo utiliza para realizar la autenticación mutua con el UE.
- El MME reenvía $RAND$ y $AUTN_{HSS}$ a la UE.
- El UE calcula RES, $AUTN_{UE}$ y K_{ASME} utilizando el algoritmo EPS AKA.
- El UE compara $AUTN_{UE}$ con el $AUTN_{HSS}$ que recibió del MME.
- Si son iguales, envía RES al MME.
- MME comprara RES con el XRES recibido desde el HSS para autenticar al usuario.
- Si el UE y la red se han autenticado entre sí, comparten la misma clave K_{ASME} (aunque esta clave **no se transfiere nunca** entre el UE y MME).

La información de aprovisionamiento @HSS/AuC sería que sigue a continuación:

- K (master Key) y AMF (Authentication Management Field) provisionados en el AuC en el momento de suscripción.
- IMSI: aprovisionado en HSS/AuC en el momento de suscripción.

Por último, la información almacenada en USIM en el momento de fabricación: K, AMF e IMSI.

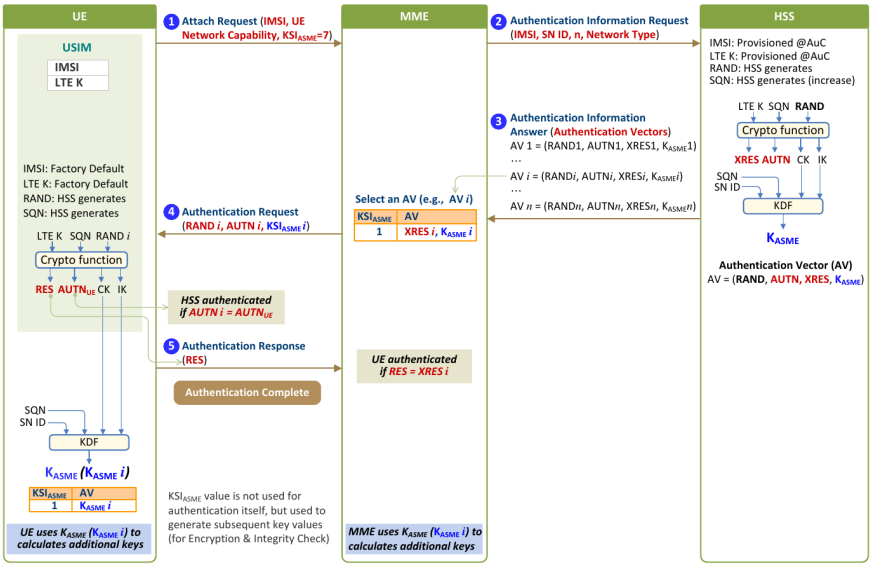


Figure 5.2: Autenticación AKA en LTE

El procedimiento para la autenticación en la red LTE lo describiremos dependiendo de los actores involucrados.

1. **UE->MME Request by UE for Network Registration**.
   - El UE envía un mensaje Attach Request a un MME con la siguiente información:
     - IMSI: Identidad de Abonado Móvil Internacional.
     - UE Network Capability: algoritmos EIA (EPS Integrity Algorithms) y EEA (EPS Encryption Algorithms) están disponibles en el UE para seguridad NAS/AS.
     - KSI_{ASME} = 7: indica UE aún no tiene clave de autenticación.
2. **MME->HSS Request by MME for Authentication Data**.
   - El MME envía un mensaje Authentication Information Request (IMSI, SN ID, n, Network Type) al HSS:
     - SN ID (Serving Network ID): identifica a la red visitada por el usuario. Consta de Identificación PLMN (MCC + MNC).
     - n (número de vectores de autenticación): Número de vectores de autenticación que solicita el MME.
     - Tipo de red: tipo de la red visitada por el UE (E-UTRAN para LTE).
   - El HSS genera RAND (aleatorio) y SQN (número de secuencia se incrementa con re-autenticaciones).
   - A partir de RAND, SQN, AMF y K unas funciones generadoras "f" se generan los siguientes parámetros de seguridad:
     - **IK (Integrity Key)**: Generada por HSS y USIM.
       (K, RAND)->f4->IK
     - **CK (Ciphering Key)**: Generada por HSS y USIM.
       (K, RAND)->f3->CK
     - **AK (Anonymity Key)**: Generada por el HSS.
       (K, RAND)->f5->AK
     - **XRES (eXpected RESponse)**: Generada por el HSS que debe coincidir con RES generado por el USIM.
       (K, RAND)->f2->XRES
     - **MAC (Message Authentication Code)**: Generado por el HSS, el USIM debe generar XMAC.
       (K, SQN, RAND, AMF)->f1->MAC

  - **AUTN (Authentication Token):** Generado por el HSS.
    $AUTN = SQN \otimes AK || AMF || MAC$
- Mediante una función KDF se deriva K_{ASME}.
- En general la función KDF usada en EPS es:
  - $KDF = HMAC - SHA - 256(Key, S)$
  - Key: Input key
  - S: Input string = FC ‖ P0 ‖ L0 ‖ P1 ‖ L1 ‖ ... ‖ Pn ‖ Ln
  - FC: function code
  - P0 = parameter 0
  - L0 = length of parameter 0
- En particular, para derivar K_{ASME}:
  - Key = CK‖IK
  - $FC = 0x10$
  - $S = 0x10 || SN\ ID || length\ of\ SN\ ID || SQN \otimes AK || length\ of\ \ SQN \otimes AK$
- Si se requieren varios vectores se envían:
  $(Rand_i, AUTN_i, XRES_i, K^i_{ASME})$ i = 0..n.

3. **HSS -> MME Response to Authentication Data Request**
   - El HSS envía un mensaje Authentication Information Answer con los AVs al MME.
4. **MME -> UE Request for User Authentication**
   - MME que almacena los AVs recibidos desde el HSS.
   - Selecciona un AV para utilizar en la autenticación del UE y asigna un indice al vector seleccionado KSI_{ASME}.
   - Envía un mensaje Authentication Request $(KSI^i_{ASME}, RAND_i, AUTN_i)$ al UE.
   - El UE, al recibir el mensaje:
     - Manda el $RAND_i$ y el $AUTN_i$ a la USIM.
     - De $AUTN_{UE}$ puede obtener SQN.
     - El USIM deriva RES, $AUTN_{UE}$, CK e IK con K.
     - El UE compara entonces $AUTN_{UE}$ generado con el AUTN recibido del MME ($AUTN_i$) para autenticar la red LTE (serving network).
5. **UE -> MME Response to User Authentication**
   - El UE envía una Authentication Response (RES) incluyendo el valor RES generado.
   - Si la autenticación de red utilizando AUTN falla, el UE envía un mensaje Authentication Failure (CAUSE) que contiene un campo que indicará los motivos.
   - Cuando la MME recibe el mensaje compara RES con $XRES_i$ del AV_i para autenticar al usuario.
   - El USIM entrega CK e IK al UE.
   - El UE obtiene la K_{ASME} usando la KDF y lo almacena utilizando el KSI_{ASME} que recibió del MME como su índice.
   - A partir de entonces, se referenciará este índice durante la configuración de seguridad NAS entre la UE y el MME.

El resumen de las claves utilizadas en la autenticación en la red LTE lo encontraremos en la figura 5.3 de [3]:

5.3 Seguridad NAS

Después de la autenticación LTE se realiza la configuración de la seguridad NAS como vemos en la Figura 5.4 de [3].

1. **El MME selecciona los algoritmos de seguridad NAS.**
   - El MME selecciona los algoritmos de cifrado e integridad para NAS.

Key	Length	Location	Derived from	Description
K	128 bits	USIM, AuC	-	EPS master key
CK	128 bits	USIM, HSS	K	Cipher key
IK	128 bits	USIM, HSS	K	Integrity key
K_{ASME}	256 bits	UE, HSS, MME	CK, IK	MME base key

Figure 5.3: Resumen Autenticación LTE

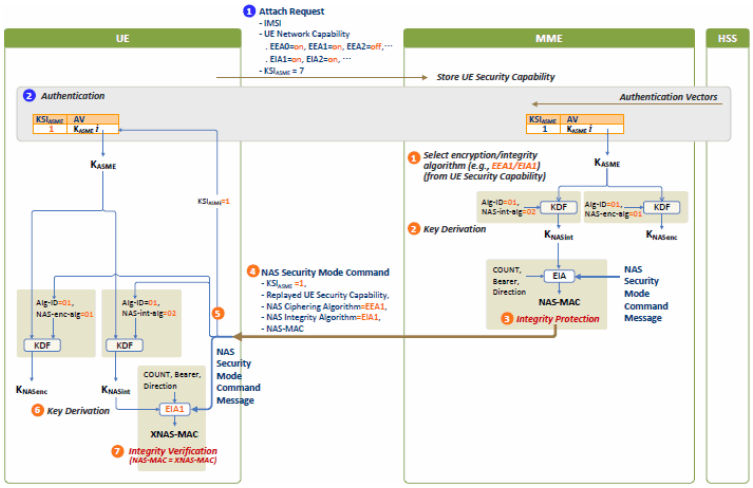


Figure 5.4: Conf. Seguridad NAS

- Esta selección se basa en la capacidad del UE (recibida en el mensaje Attach Request en la autenticación LTE).
- En el ejemplo se considera EEA=1 y EIA=1 (algoritmo SNOW 3G).

2. **El MME deriva las claves de seguridad NAS.**
   - El MME deriva K_{NASint} y K_{NASenc} de K_{ASME}:
     - $KDF = HMAC - SHA - 256(Key, S)$
     - $Key = K_{ASME}$
     - $S = FC(0x15)||algorithm\ Distinguisher||\ length\ of\ algorithm\ Distinguisher||algorithm\ ID||\ length\ of\ algorithm\ ID$
3. **El MME genera NAS-MAC para la protección de la integridad.** En la figura 5.5 de [3] veremos como se describe el proceso
   - El MME forma un mensaje Security Mode Command para enviar al UE.
   - Para ello calcula el NAS-MAC de dicho mensaje.
   - Utiliza el algoritmo EIA seleccionado (EIA=1):
     - Count (32 bits): cuenta NAS de enlace descendente.
     - Message: Mensaje NAS (Security Mode Command)
     - Dirección (1 bit): 0 para el enlace ascendente y 1 para el enlace descendente (el valor 1 en el presente documento)
     - Bearer (5 bits): ID del portador (la señalización NAS no usa portadores, siempre vale 0 en este caso).
     - K_{NASint} (128 bits): clave de integridad NAS
4. **El MME envía al UE el Security Mode Command**

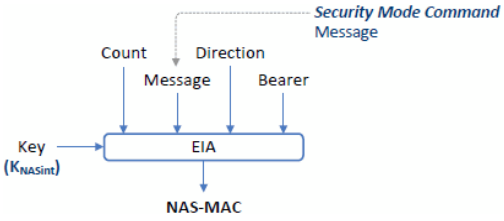


Figure 5.5: Calculo del NAS-NAC

- El mensaje tiene la integridad protegida pero no está cifrado.

- Lleva los siguientes parámetros:

  - KSI_{ASME}: valor de 3 bits asociado con una K_{ASME} utilizado para identificar dicha clave.

  - Repetición de las capacidades de seguridad del UE: el mensaje incluye las capacidades de seguridad incluidas en el Attach Request que envió el UE.

  - Algoritmo Cifrado NAS: algoritmo de cifrado NAS seleccionado por el MME.

  - Algoritmo de Protección de la Integridad NAS: algoritmo de protección de la integridad NAS seleccionado por el MME.

5. **Usando KSI_{ASME} el UE selecciona K_{ASME}**

6. **El UE deriva las claves NAS igual que hizo el MME**

7. **El UE verifica el NAS-MAC**. Todos los puntos anteriores están descritos en la figura 5.4

8. **El UE cifra el mensaje Security Mode Complete** como se describe a continuación en la figura 5.6 de [3]

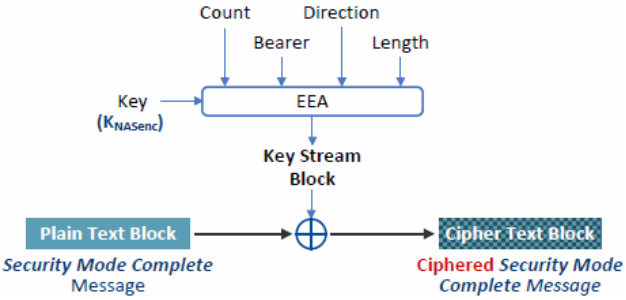


Figure 5.6: Cifrado Security Mode Complete

9. **El UE genera el NAS-MAC** como vemos en la siguiente figura 5.7 de [3]

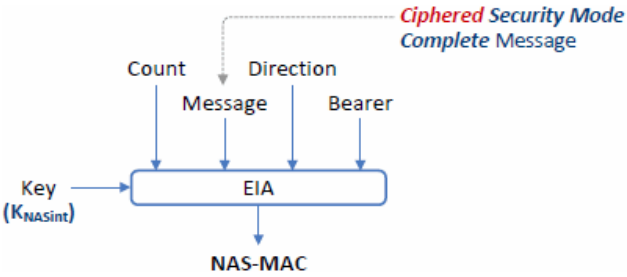


Figure 5.7: Calculo NAS-MAC a partir del Mensaje Security Mode Complete

10. **El UE envía el Security Mode Complete**.

11. **El MME comprueba la integridad del Security Mode Complete**.

12. **El MME descifra el Security Mode Complete** como vemos en la figura 5.8 de [3]

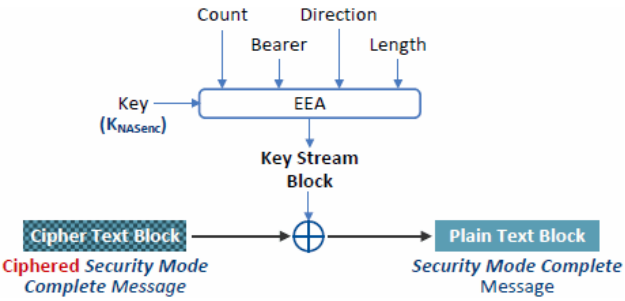


Figure 5.8: Descifrado mensaje NAS

Los últimos puntos del proceso se describe en la figura 5.9 de [3]

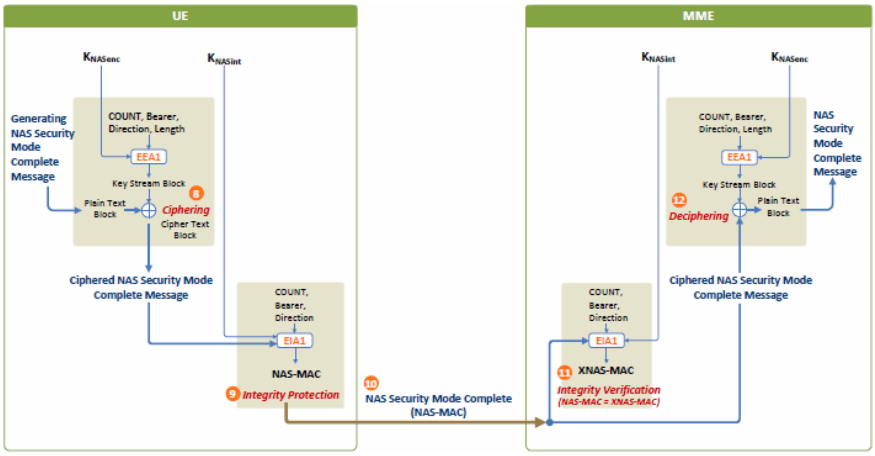
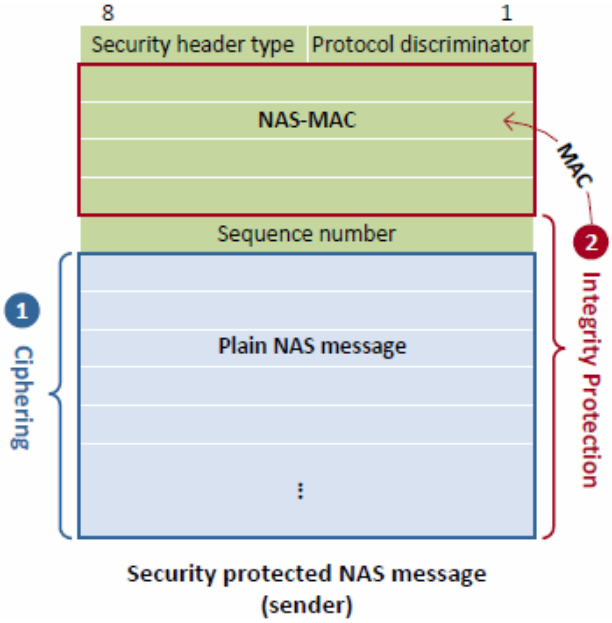


Figure 5.9: Mensaje Completo

- Después de la configuración NAS de seguridad los mensajes NAS están protegidos en ambos sentidos respecto a su integridad y confidencialidad.
- Cuando se envían mensajes NAS, se cifran primero y luego les protege la integridad.
- Cuando se reciben primero se comprueba la integridad y luego se descifran.



La figura 5.10 de [3] muestra el esquema de cifrado y protección final después de la configuración de la seguridad

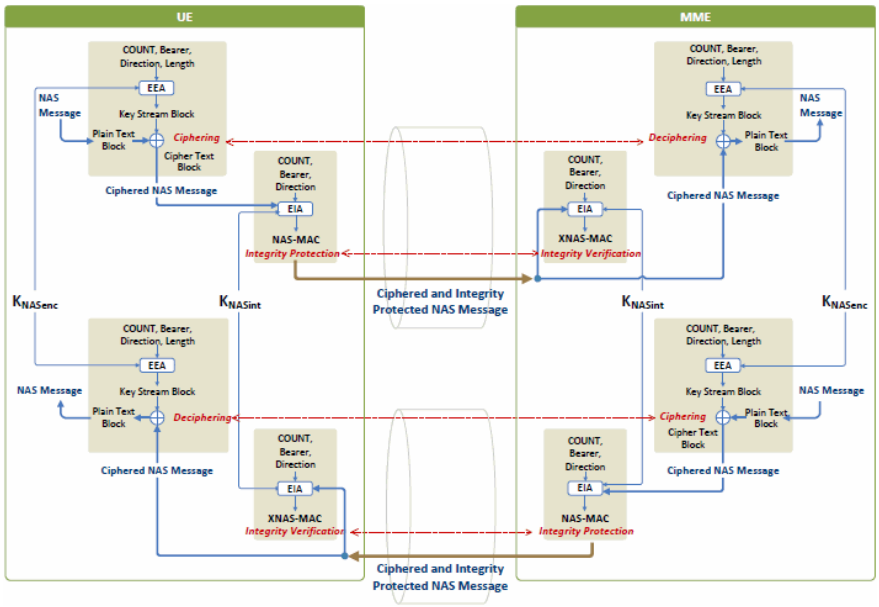


Figure 5.10: Descifrado mensaje NAS

5.4 Seguridad AS

La Figura 5.11 de [4] describe el inicio del proceso una vez se ha realizado la Autenticación LTE

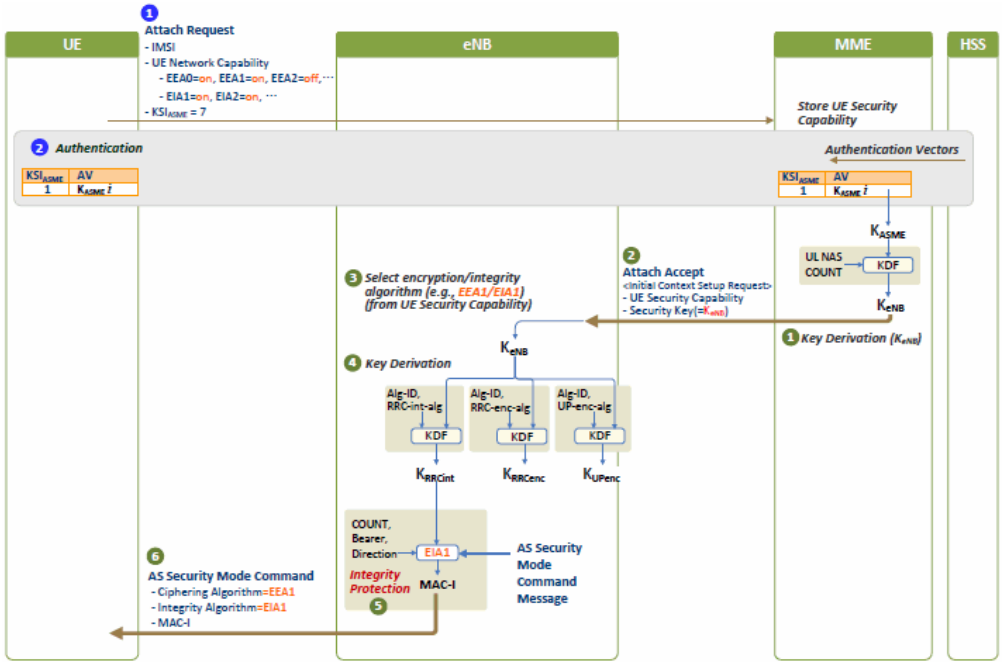


Figure 5.11: Conf. Seguridad AS

1. **El MME deriva la clave máster AS.**
   - $= HMAC - SHA - 256(Key, S)$

- $Key = K_{ASME}$
- $S = FC(0x11)||UL\ NAS\ Count||Length\ UL\ NAS\ Count$

2. **El MME responde al UE y envía la clave máster AS al eNB.**
   - El MME envía un mensaje Attach Accept (NAS) aceptando al UE.
   - El Attach Accept va encapsulado en un mensaje Initial Context Setup Request.
   - El Initial Context Setup Request es un mensaje entre el eNB y el MME (S1AP) con los siguientes parámetros:
     - UE Security Capability: algoritmos de seguridad seleccionados por el MME.
     - Clave K_{eNB} (256 bits).
3. **El eNB selecciona los algoritmos de seguridad.**
   - El eNB selecciona los algoritmos de cifrado e integridad que deben aplicarse a los mensajes RRC y los paquetes IP.
   - Esta selección se basa en la información de la capacidad de seguridad del UE recibida por el eNB en el mensaje Initial Context Setup Request desde el MME.
4. **El eNB deriva las claves de seguridad AS.**
   - El eNB deriva K_{RRCint} y K_{RRCenc} de K_{UPenc}:
     - $KDF = HMAC - SHA - 256(Key, S)$
     - $Key = K_{eNB}$
     - $S = FC(0x15)||algorithm\ Distinguisher||\ length\ of\ algorithm\ Distinguisher||algorithm\ ID||\ length\ of\ algorithm\ ID$
5. **El eNB calcula el MAC (MAC-I) para el mensaje Security Mode Command.**
   - Parámetros:
     - Count (32 bits): contador PDCP del enlace descendente.
     - Mensaje: Mensaje de RRC (Security Mode Command).
     - Dirección: 0 para el enlace ascendente y 1 para el enlace descendente.
     - Bearer (5 bits): ID del radio bearer.
     - K_{NASint} (128 bits): clave AS de integridad.
6. **El eNB envía el mensaje Security Mode Command.**
   - Parámetros:
     - Algoritmo cifrado AS.
     - Algoritmo protección integridad AS.
7. **El UE identifica los algoritmos de seguridad AS.**
8. **El UE deriva las claves de seguridad AS.**
9. **El UE verifica el MAC-I de integridad.**
10. **El UE calcula el MAC-I del Security Mode Complete.**
    - Para completar el establecimiento de la configuración de seguridad AS, el UE genera un mensaje Security Mode Complete.
    - Calcula el MAC-I de este mensaje.
11. **El UE envía el Security Mode Complete.**
12. **El eNB verifica el Security Mode Complete.**

Los últimos puntos del proceso están descritos en las figura 5.12 y 5.13 de [4]

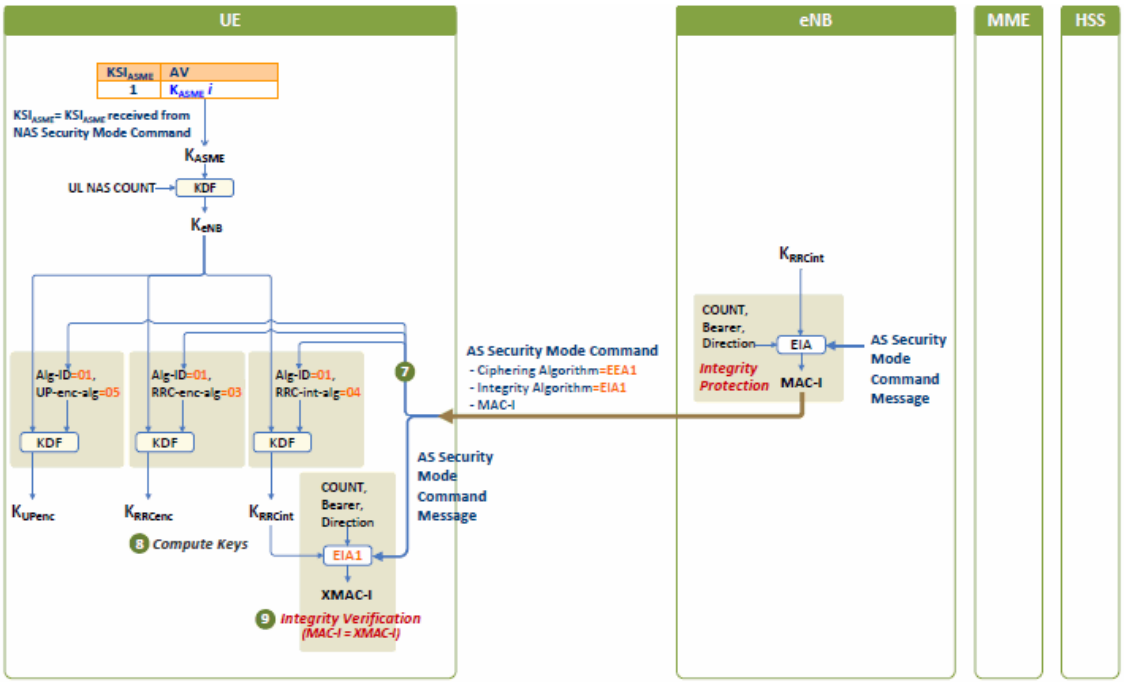


Figure 5.12: Configuración seguridad AS

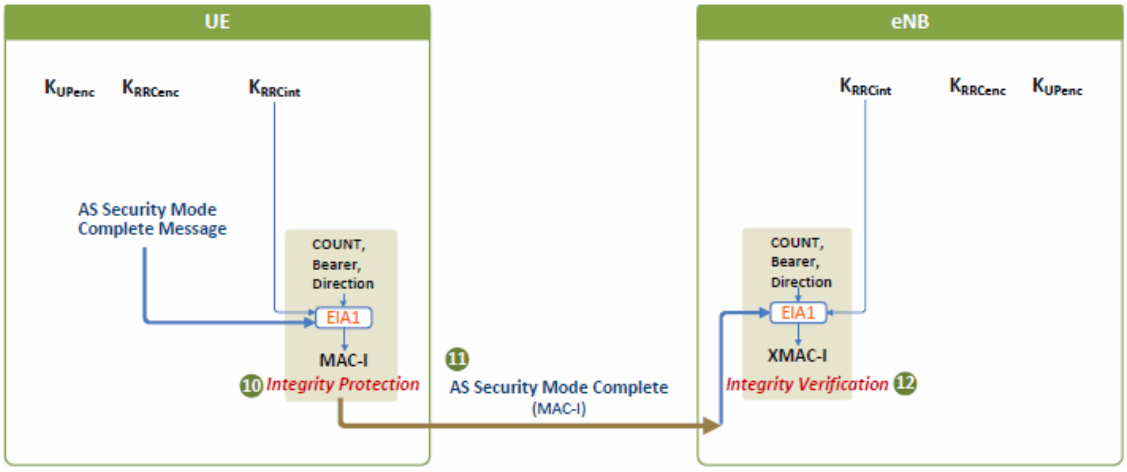
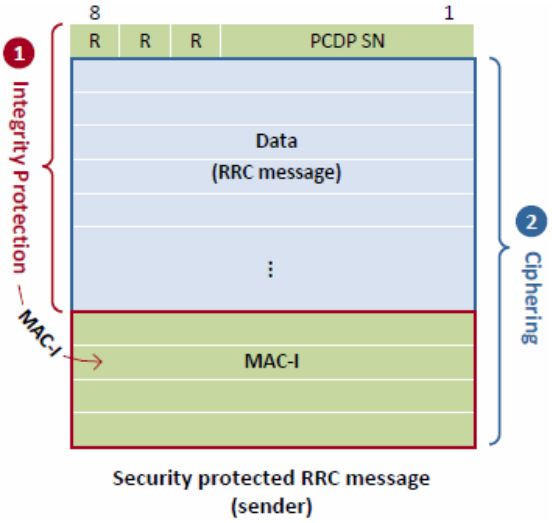


Figure 5.13: Configuración seguridad AS 2

- Todos los mensajes RRC entregados entre el UE y eNB tienen la integridad protegida y pueden ir encriptados.
- Todos los paquetes IP de usuario pueden ir encriptados.
- Cuando se envían mensajes RRC, están protegidos de integridad primero y luego encriptados (diferente a mensajes NAS).



La figura 5.14 de [4] muestra el esquema de cifrado y protección final después de la configuración de la seguridad

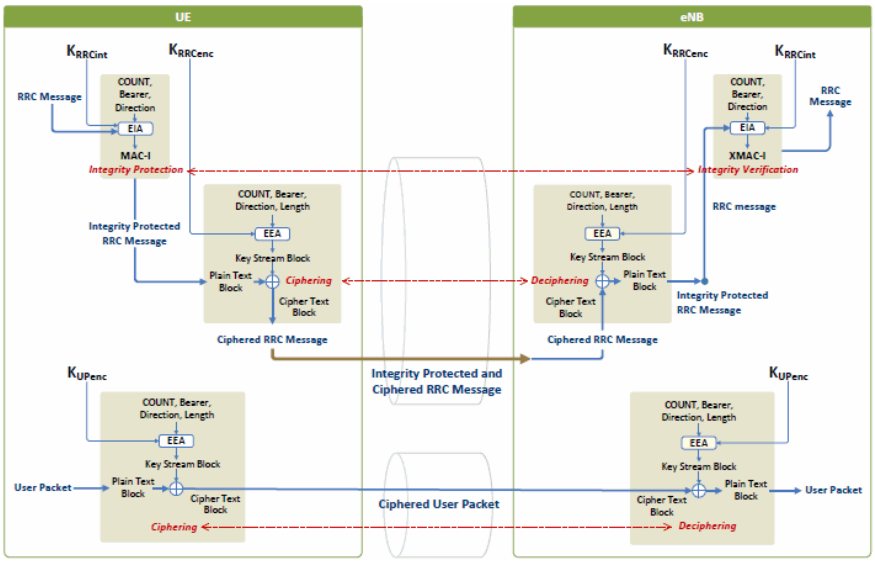


Figure 5.14: Cifrado y protección Seguridad mensajes RRC

- El contexto de seguridad son los parámetros de seguridad establecidos.
- Tenemos contexto de seguridad NAS y contexto de seguridad AS como podemos comprobar en la figura 5.15.
  - Un contexto de seguridad NAS puede ser nativo completo o nativo parcial.
  - Un contexto de seguridad de NAS se llama parcial después del AKA EPS pero antes del procedimiento SMC (Security Mode Command).
  - Un contexto nativo parcial de seguridad NAS se transforma en completo después de que se complete el SMC.

Partial Native EPS NAS Security Context	Full Native EPS NAS Security Context	EPS AS Security Context
UE Security Capability	UE Security Capability	UE Security Capability
K_{ASME}	K_{ASME}	K_{eNB}
KSI_{ASME}	KSI_{ASME}	
UL NAS Count	UL NAS Count	UL NAS Count
DL NAS Count	DL NAS Count	DL NAS Count
	EIA ID	EIA ID
	EEA ID	EEA ID
	K_{NASint}	K_{RRCint}
	K_{NASenc}	K_{RRCenc}
		K_{UPenc}

Figure 5.15: Contextos seguridad NAS

Chapter 6

QoS

6.1 Introducción

Los proveedores de servicios en redes LTE deben ser capaces de ofrecer servicios con diferente **calidad de servicio(QoS)** dependiendo del usuario y su suscripción. Para mediar la calidad de una red existen varios conceptos:

- Tasas de errores
- Ancho de banda
- Rendimiento
- Retraso en la transmisión
- Disponibilidad
- Tasa de bit transferidos

Alguno ejemplos existentes, de mecanismos para garantizar QoS podrían ser

- Priorización de trafico, de esta forma usuarios con un mejor servicio podrían ver su trafico priorizado sobre otros usuarios con un peor servicio contratado
- Garantía de ancho de banda mínimo

Existen diferentes servicios que necesitan disponer de diferentes QoS (p.e, la telefonía necesita una QoS más alta que un una conexión a Internet). Adicionalmente, los usuarios contratan suscripciones con un nivel establecido de QoS. A partir de la información de la suscripción de usuario y servicio, se debe asignar los recursos de radio y red necesarios

6.2 SDF y Canal EPS

Podemos categorizar la QoS en las redes LTE en 2 tipologías:

- QoS en el nivel de servicio **(Service Data Flow -SDF)**
- QoS en el nivel de canal **(EPS bearer)**

El tráfico en las redes IP (flujo IP y paquetes IP) se clasifica en:

- Tráfico SDF **(Service Data Flow)**. Grupo de flujos IP asociados a un servicio
- Tráfico canal EPS **(EPS Bearer)**. Flujos IP que, habiendo sido agregados previamente en SDF, requieren del mismo QoS

La clasificación del flujo IP, como veremos descrito en la Figura 6.1 de [5], se realiza por:

- **SDF**. Se realiza por las denominadas Plantillas SDF (SDF Templates) que aplican filtros IP dependiendo de una política establecida previamente por el operador de red
- **EPS Bearer**. Se realiza por las denominadas plantillas de flujo de trafico (TFT)

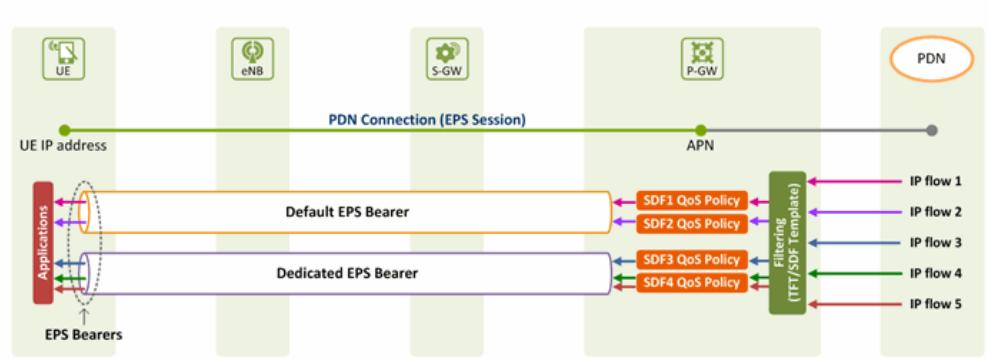


Figure 6.1: Bearer EPS y SDFs

Por tanto, la política consiste en un *tuple* de 5 (Dirección IP origen, Dirección IP Destino, Número de puerto destino, Número de puerto origen y ID de Protocolo)

Podríamos definir el **SDF** como un grupo de flujos asociados que se clasifican juntos por el tipo de servicio que proveen. Estos, son clasificados por las plantillas SDF (SDF Templates) de forma que, diferentes SDFs tienen diferentes QoS. La QoS es determinada por el **PCRF**. Cada SDF es mapeado por un P-GW contra un canal EPS dependiendo de los requisitos QoS. Cada SDF es entregado a través de un canal EPS que satisface su QoS

En cambio el **Bearer EPS** sería la ruta de transmisión entre UE y P-GW para entregar tráfico de usuario con una determinada QoS. Existen dos tipos diferentes de canales EPS:

- Por defecto. Canal asignado por defecto al UE cuando se conecta a la red LTE
- Dedicado. Canal asignado al UE cuando solicita utilizar un servicio que requiere un QoS superior al que provee el canal por defecto

A cada conexión entre el UE y un PDN se le asigna un canal EPS por defecto. Un UE puede conectarse al mismo tiempo a más de un PDN por lo que un UE puede tener asignados varios canales EPS al mismo tiempo. El máximo número de canales son 11. Cuando el UE se conecta a la red, el MME necesita información de como establecer el canal por defecto. Esta información es facilitada por el HSS a través de la información de suscripción. El MME descarga la información de suscripción, selecciona un P-GW para conectar al PDN y activa el canal por defecto basándose en la información QoS del perfil de suscripción

Los flujos IP que llegan al P-GW a través del PDN, son filtrados por los SDF Templates creando SDFs. Diferentes QoS se aplican a cada uno de los SDFs. Dependiendo del QoS aplicado a cada SDF, se le asigna el canal por defecto, o el canal dedicado. Esta asignación se hace por el filtrado TFT. Una vez los flujos IP llegan al UE, son enviados a sus aplicaciones de destino

6.3 Parámetros QoS

Los parámetros QoS se definen a 2 niveles:

- QoS en el nivel de servicio (Service Data Flow -SDF). También llamado **nivel SDF**
- QoS en el nivel de canal (EPS bearer). También llamado **nivel agregado SDF**

Cada nivel agrupa una serie de parámetros de QoS, algunos de los cuales son comunes:

- **QCI** (QoS Class Identifier). Referencia para indicar las características de rendimiento del SDFs y de los canales EPS (tipo de recurso, tasa de paquetes perdidos, retrasos..)
- **ARP** (Allocation and Retention Priority). Controla el acceso a llamadas. Indica la prioridad para decidir si activar nuevos SDF/canales.
- **MBR** (Maximum Bit Rate). Máximo ancho de banda que se puede utilizar. Este valor marca el máximo pero depende de la conexión y como este compartida con otros usuarios/aplicaciones
- **GBR** (Guaranteed Bit Rate). Ancho de banda garantizado en la conexión

- **APN-AMBR** (Access Point Name - Agregated Maximum Bit Rate). Máximo ancho de banda permitido para todos los canales non-GBR asociados a una conexion PDN de un UE
- **UE-AMBR** (User Equipment - Agregated Maximum Bit Rate). Máximo ancho de banda permitido para todos los canales non-GBR asociados a una conexión a un UE

Parámetros QoS por nivel

- Parámetros QoS para SDF:
  - **QCI** (QoS Class Identifier) es un mecanismo utilizado en redes LTE para asegurar que el trafico del bearer se ha asignado de forma apropiada su QoS. Para asegurar que el trafico es el apropiado, existe un mecanismo que permite clasificar los bearer en diferentes clases cada una de ellas con su correspondiente QoS
  - **ARP** (Allocation and Retention Priority). Parámetro que define la prioridad del SDF
  - **GBR** (Guaranteed Bit Rate). Máximo ancho de banda que debe ser garantizado por el SDF
  - **MBR** (Maximum Bit Rate). Máximo ancho de banda permitido en el SDF
- Parámetros QoS para canal EPS:
  - **QCI** (QoS Class Identifier) es un mecanismo utilizado en redes LTE para asegurar que el trafico del bearer se ha asignado de forma apropiada su QoS. Para asegurar que el trafico es el apropiado, existe un mecanismo que permite clasificar los bearer en diferentes clases cada una de ellas con su correspondiente QoS
  - **ARP** (Allocation and Retention Priority). Parámetro que define la prioridad del bearer EPS
  - **GBR** (Guaranteed Bit Rate). Máximo ancho de banda que debe ser garantizado por el bearer EPS
  - **MBR** (Maximum Bit Rate). Máximo ancho de banda permitido en el bearer EPS
  - **APN-AMBR** (Access Point Name - Aggregate maximum Bit-Rate) es un parámetro servido por el PCRF para limitar el máximo ancho de banda permitido en un APN
  - **UE-AMBR** (User Equipment - Aggregate maximum Bit-Rate). Ancho de banda total permitido para todos los bearers que un UE tiene asociados a un P-GW

Existen 2 tipos de SDFs cada uno con sus parámetros:

- **GBR SDF**. Se dedican recursos de red específicos de acuerdo al tipo de recurso que marca su QCI
- **Non-GBR SDF**. No se asignan recursos específicos Los parámetros que hemos explicado en el punto anterior están asociados a cada uno de los tipos de SDFs :
  - GBR SDF. QCI, ARP, GBR(UL/DL) y MBR(UL/DL)
  - Non-GBR SDF: QCI, ARP y MBR(UL/DL)

Existen 2 tipos de canales EPS cada uno con sus parámetros:

- **GBR Bearer**. Se dedican recursos de red específicos de acuerdo a su QCI. En este caso, solo puede ser un canal EPS dedicado
- **Non-GBR Bearer**. No se asignan recursos específicos. Puede ser tanto un canal EPS dedicado como uno por defecto

Los parámetros por tipo:

- GBR Bearer. QCI, ARP, GBR(UL/DL) y MBR(UL/DL)
- Non-GBR Bearer: QCI, ARP, APN-AMBR(UL/DL) y UE-MBR(UL/DL)

En la figura anterior 6.2 de [5], el UE esta conectado a 2 PDNs (por lo tanto tiene 2 direcciones IP). Existen 2 canales dedicados y uno por defecto por cada PDN. El trafico IP es filtrado en SDFs en el P-GW gracias a los SDF Templates. Para esos SDFs se asignan recursos de red dependiendo de las reglas QoS aplicadas por el P-GW. Se mapea cada SDF contra un canal EPS siguiendo el filtrado realizado por los TFT. Los canales non-GBR asociados a un PDN están controlados por el APN-AMBR (se comparte el ancho de banda en el APN). Los asociados al UE se controlan con el UE-AMBR

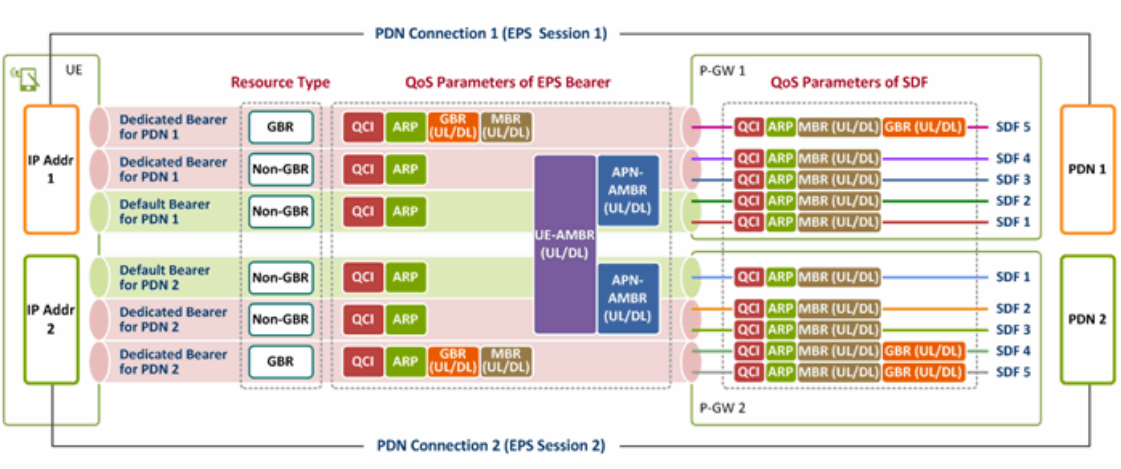


Figure 6.2: Parámetros QoS para Bearer EPS y SDF

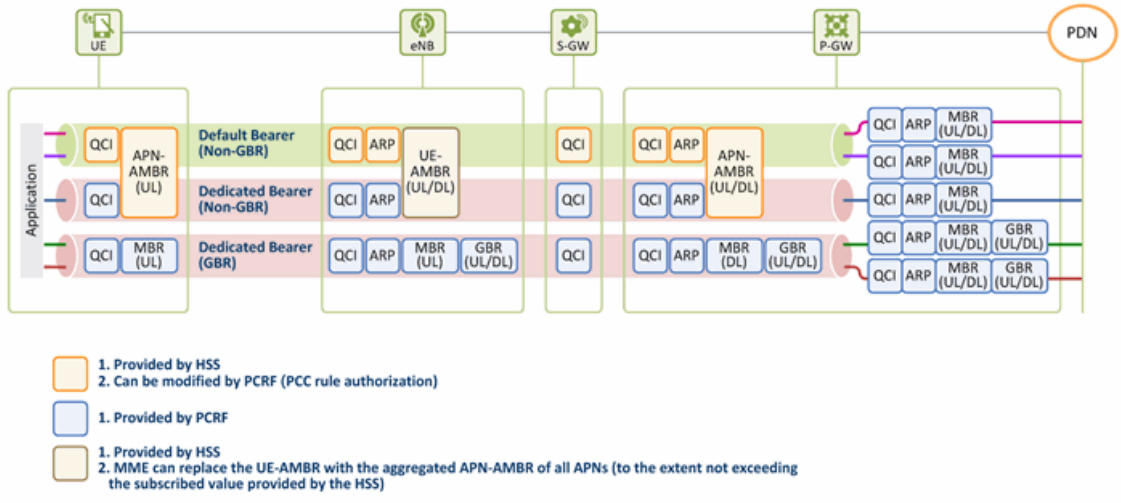


Figure 6.3: Provisionamiento QoS

6.4 Provisionamiento de QoS

Durante el provisionamiento, descrito en la Figura 6.3 de [5] de **QoS en SDF**, todos los parámetros de QoS aplicados a SDF son provisionados por el PCRF (Policy and Charging Rules Function). En cambio, en el provisonamiento de **QoS para canal EPS**, los parámetros de QoS son provisionados al HSS como una información de suscripción por los operadores de red.

Cuando el **canal por defecto** se activa:

- MME descarga el perfil de QoS del HSS y lo envía a las entidades EPS
- Se provee al eNB con el UE-AMBR

Cuando se activa un **canal dedicado**, los parámetros QoS son facilitados por el PCRF a partir de la información recibida por el SPR(Subscriber Profile Repository)

6.5 Forzado de QoS

Se modifican los parámetros QoS dependiendo del trafico en SDFs y canales EPS

- **Forzado QoS en SDF**. Los parámetros QoS son instalados en un P-GW. Los flujos IPs son filtrados usando SDF Templates y asignados a SDFs. Cada SDF es conrolado por los parámetros QoS instalados en el P-GW
- **Forzado QoS en canales EPS**. Los parámetros QoS son forzados en las entidades EPS (UE, eNB, S-GW y P-GW) que entregan trafico entre el UE y el P-GW.

Los Parámetros forzados en SDF son

- QCI. Aplicado a todos los SDFs por el P-GW
- ARP. Aplicado a todos los SDFs por el P-GW
- MBR. Aplicado a todos los SDFs por el P-GW
- GBR. Aplicado solo a GBR SDFs por el P-GW

Los parámetros forzados en canales EPS son

- QCI. Aplicado a todos los canales por todas las entidades EPS(UE, eNB, S-GW y P-GW)
- ARP. Aplicado a todos los canales por todas las entidades EPS(UE, eNB, S-GW) menos P-GW
- MBR. Solo aplicado a los canales GBR
  - UL(Uplink). Aplicado solo a canales non-GBR por UE y eNB
  - DL(Dowlink). Aplicado solo a canales non-GBR por S-GW y P-GW
- GBR. Aplicado a todos los canales por todas las entidades EPS(UE, eNB, S-GW) menos P-GW
- APN-AMBR. Solo aplicado a los canales non-GBR
  - UL(Uplink). Aplicado solo a canales non-GBR por UE y P-GW
  - DL(Dowlink). Aplicado solo a canales non-GBR por P-GW
- UE-AMBR. Aplicado solo a canales non-GBR por eNB

6.6 Ejemplos

Operación Qos en Enlace de Bajada

A continuación describiremos un Ejemplo de Operación de QoS en un Enlace de Bajada tal como esta descrito en la Figura 6.4 de [5]

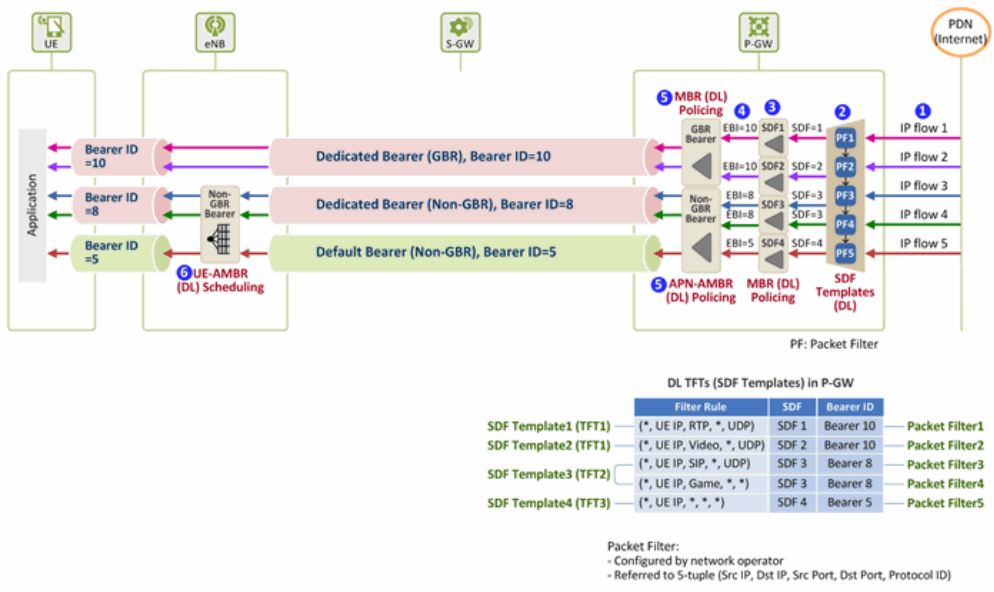


Figure 6.4: Ejemplo de QoS de Bajada

- **[P-GW] DL IP Flujos de llegada**

  Los flujos IP llegan al P-GW, cada uno de ellos con información de servicios diferentes(RTP, señalización de voz, streaming de video, juego, etc..)

- **[P-GW] IP filtrado de paquetes (SDF Templates)**

  A su llegada al P-GW, los flujos IP se filtran a través de los SDF Templates creandose varios SDFs. Para realizar el filtrado se basa en un 5-tuple(número de puerto de origen, número de puerto de destino, Dirección IP de origen, dirección IP de destino, ID de protocolo) Los diferentes flujos son clasificados: IP Flow 1 como GBR SDF 1, IP Flow2 como GBR SDF 2, IP Flows 3 y 4 como non-GBR SDF 3 y IP flow 5 es clasificado como non-GBR SDF4

- **[P-GW] SDF QoS Aplicación: Política de tasa MBR**

  Política de tasa MBR se realiza por SDF siendo cualquier trafico que supere el máximo, descartado.

- **[P-GW] SDF - Mapeo Canal EPS : filtrado de paquetes IP (plantillas de flujo de tráfico; TFT)**

  Los SDFs son filtrados usando TFT en diferentes canales EPS. SDF 1 y SDF 2 son mapeados contra un canal dedicado GBR (EBI=10), SDF 3 es mapeado contra el canal dedicado non-GBR(EDI=8) y por último, el SDF 4 es mpaeado contra el canal por defecto non-GBR (EDI =5)

- **[P-GW] Forzado de Qos para Canal EPS: MBR / APN-AMBR Rate Policing**

  Se aplica a cada canal un QoS. Para los canales GBR, se asigna un MBR usando el valor MBR DL siendo cualquier paquete que excesa el ancho de banda descartado. Para los canales non-GBR, se asigna un APN-AMBR. Por lo tanto, para todos los flujos IP de EBI 8 y EBI 5 , se aplica la politica y cualquier paquete que exceso el ancho de banda es descartado

- **[eNB] Forzado de Qos para Canal EPS: UE-AMBR Programación**

  El eNB realiza el control del ancho de banda UE-AMBR contra los canales EPS non-GBR. Para todos los flujos IP de EBI 8 y EBI 5, se aplica la política UE-AMBR.

Operacion Qos en Enlace de Subida A continuación describiremos un Ejemplo de Operación de QoS en un Enlace de Subida tal como esta descrito en la Figura 6.5 de [5]

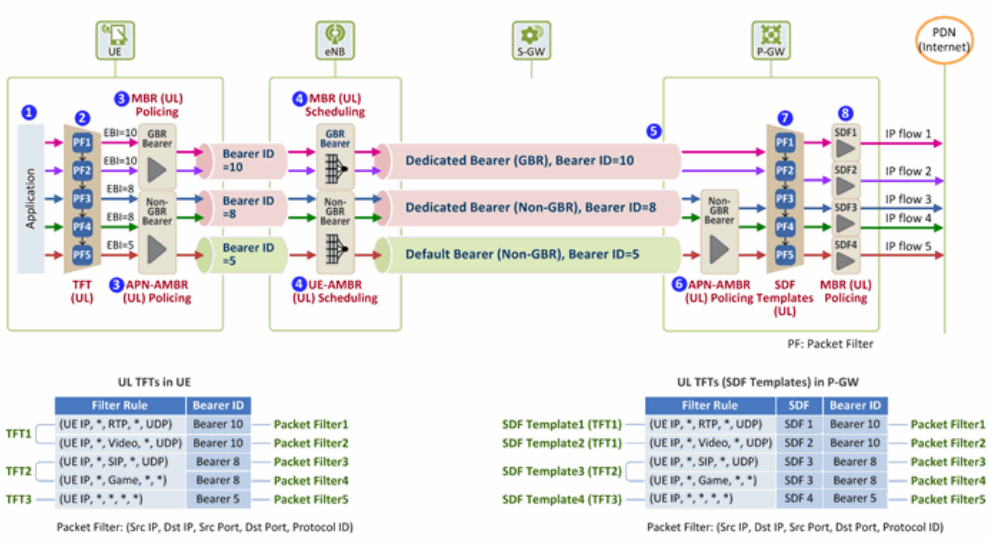


Figure 6.5: Ejemplo de QoS de Subida

- **[UE] UL IP Flujos de llegada**

  Los flujos IP de las aplicaciones de usuario han llegado al UE.

- **[UE] IP filtrado de paquetes (TFT)**

  Los flujos IP son filtrados usando TFT en los canales EPS correspondientes. Una 5-tuple es usado para realizar el filtrado. Los flujos 1 y 2 son mapeados contra un canal dedicado GBR(EBI=10), los flujos 3 y 4 son mapeados contra el canal dedicado non-GBR(EBI=8) y por último, el flujo 5 es mapeado contra el canal por defecto (EBI=5)

- **[UE] Forzado de Qos para Canal EPS: MBR / APN-AMBR Rate Policing**

  Se aplica un QoS a cada canal. Para los flujos IP de canales dedicados GBR(EBI=10), se aplica la política usando UL MBR, para los canales dedicados non-GBR (EBI=8 y EBI=5), se aplica UL APN-AMBR

- **[eNB] Forzado de Qos para Canal: MBR / UE-AMBR Rate Policing** eNB aplica una polita de control usando UL MBR para los canales GBR (EBI=10) y una política usando UL UE-AMBR para los non-GBR(EBI=8 and EBI=5). Debido a que solo hay un PDN, el UL UE-AMBR tiene el mismo valor que el UL APN-AMBR

- **[P-GW] Portador de Tráfico de llegada**

  Llega el trafico de canal al P-GW a través del S-GW

- **[P-GW] EPS Portador QoS Aplicación: APN-AMBR Rate Policing**

  La política APN-AMBR es aplicada contra los flujos IP recibidos a través de canales non-GBR (EBI=8 y EBI=5), descartando cualquier paquete que exceda el ancho de banda marcado.

- **[P-GW] Filtrado de paquetes IP (SDF Templates)**

  Los canales son filtrados a través de los SDF templates y se crean SDFs. Los flujos 1 y 2 del canal dedicado GBR(EBI=10) se mapean contra los SDFs 1 y 2. El flujo 3 y 4 de los canales dedicados non-GBR (EBI=8) son mapeados contra el SDF 3 y 4, y por último el flujo 5 del canal por defecto (EBI=5) se mapea contra el SDF 5.

- **[P-GW] Forzado QoS de SDF: Policing MBR Rate**

  Se aplica la política MBR contra cada SDF, siendo descartado el paquete que exceda el ancho de banda marcado.

Chapter 7

Gestión de Movilidad EPS (EMM)

7.1 Introducción

Con anterioridad hemos visto como un usuario se ha conectado a una red LTE. Los pasos a realizar serían, según hemos visto, los siguientes:

- El usuario se autentica y se registra en la red
- Se establece una sesión EPS y un bearer
- Se ejecutan las funciones de gestión a la movilidad para dar soporte al movilidad del usuario

Todas las tareas anteriores son llevadas a cabo por la Entidad de Gestión a la Movilidad (EMM) que es la entidad encargada de las tareas de:

- Establecimiento de una conexión de señalización
- Intercambiando de los mensajes de control

La gestión de movilidad entre el usuario y la red es controlada siguiendo los protocolos del NAS en el panel de control. Este protocolo utilizado esta definido bajo el documento **3GPP TS 24.30** y es el utilizado entre las 2 entidades, UE y MME, para su comunicación. Por último, podemos dividir el NAS en:

- EPS Mobility Management (EMM)
- EPS Session Management (ESM)

Tipos	**Procesos EMM**
Procesos Comunes EMM	Asignación GUTI Autenticación Seguridad del Modo de Control Identificación UE Información EMM
Procesos Específicos EMM	Conectar Desconectar Tracking Area Update
Procesos de Gestión de Conexión EMM	Petición de servicio Paging Transporte de mensajes NAS

Table 7.1: Procesos involucrados en la gestión de movilidad EMM

Existen por tanto una seria de **Procesos Comunes**. Estos procesos se caracterizan por:

- Se refiere a aquellas que pueden ser iniciados aunque ya exista una conexión de señalización entre UE y MME
- Asignación GUTI, Autenticación, Identificación, Seguridad del Modo de Control (SMC) y Información

También identificamos los **Procesos Específicos** con las características que se indican a continuación

- Se refiere a la movilidad del usuario
- Conexión, Desconexión y actualización TA (TAU)

Y por último hemos visto los **Procesos de Gestión de la movilidad**

- Se refiere al establecimiento de una conexión de señalización NAS
- Petición de Servicios, Paging y Transporte de mensajes NAS

Un usuario **(UE)** puede tener uno de los siete estados EMM:

- EMM-Null
- EMM-Deregistered
- EMM-Deregistered-Initiated
- EMM-Registered
- EMM-Registered-Initiated
- EMM-TAU-Initiated
- EMM-Service-Request-Initiated

En cambio si nos fijamos en el **EMM**, puede tener alguno de los siguientes estados:

- EMM-Deregistered
- EMM-Deregistered-Initiated
- EMM-Registered
- EMM-Common-Procedure-Initiated

Por lo tanto, como hemos visto con anterioridad cada elemento puede tener un estado diferente dependiendo de la situación en la que se encuentre.

Para que UE y MME puedan intercambiar mensajes NAS se debe establecer una conexión de señalización. A esta conexión se le llama **conexión EPS Connection Management (ECM)**. Es una conexión lógica que consta de una conexión RRC entre el UE y el eNB, y una conexión S1 entre el eNB y el MME. En el momento que se establece una conexión ECM, se establecen también las conexiones RRC y S1

EMM puede estar principalmente en 2 estados dependiendo si esta el UE conectado o no

- EMM-Registered
- EMM-Deregistered

ECM puede estar en 2 estados dependiendo si la conexión NAS de señalización esta establecida o no

- ECM-Connected
- ECM-Idle

RRC puede estar en 2 estados dependiendo si la conexión RRC esta establecida o no

- RRC-Connected
- RRC-Idle

Capa	Estado	Entidad	Descripción
EMM	EMM-Deregistered	UE, MME	UE no esta conectado a ninguna red LTE. MME desconoce la ubicación actual del UE pero puede tener información de la TA de la última vez que reporto su localización
	EMM-Registered	UE, MME	UE se ha conectado a la red y se le ha asignado una IP. Se ha establecido un bearer EPS. El MMEd conoce la ubicación del UE la exactitud de una celda o, como mínimo, de una TA
ECM	ECM-Idle	UE, MME	No se ha establecido aún una conexión de señalización NAS. No se han asignado aún recursos físicos al UE ni recursos de red (Bearer S1, Conexión señalización S1)
	ECM-Connected	UE, MME	Se ha establecido una conexión de señalización NAS. Se han asignado recursos físicos y recursos de red al UE
RRC	RRC-Idle	UE, eNB	No se ha establecido aun conexión RRC
	RRC-Connected	UE, eNB	Se ha establecido una conexión RRC

Table 7.2: Tabla Descriptiva con los estados por entidad

Los diferentes estados de los elementos EMM, ECM y RRC van cambiando a medida que los procesos EMM se ejecutan.

Caso	Estado	Experiencia de usuario
A	EMM-Deregistered + ECM-Idle + RRC-Idle	• UE se enciende por primera vez después de la suscripción • UE se enciende después de estar apagado durante un periodo largo de tiempo • No existe contexto UE en la red LTE
B	EMM-Deregistered + ECM-Idle + RRC-Idle	• UE se enciende después de estar apagado un cierto periodo de tiempo • Cuando se pierde la conexión ECM debido a un problema en el enlace radio • Cierto contexto UE se ha guardado en la red de la última conexión
C	EMM-Registered + ECM-Connected + RRC-Connected	• UE esta conectado a la red y esta utilizando los servicios • La movilidad del UE esta siendo gestionada por un proceso de Handover
D	EMM-Registered + ECM-Idle + RRC-Idle	• Cuando el UE esta conectado a la red pero no utiliza los servicios • La movilidad del UE esta siendo gestionada por un proceso de reselección de celda

Table 7.3: Tabla descripción de los diferentes estados a nivel de usuario

A continuación describiremos algunas características que identifican cada uno de los estados descritos en la tabla 7.3.

Los estados A y B implican que el UE aún no esta conectado a la red. Las diferencias entre ambos las mostramos en la siguiente tabla 7.4

A	B
La red no tiene más información del UE que la de la provisión	La red mantiene el GUTI y el contexto de Seguridad NAS obtenido en la última conexión del UE a la red
Una vez la información de usuario es eliminada después de cierto tiempo se transita a este estado	La red mantiene la información de usuario necesaria para autenticación y la configuración de seguridad en caso que se vuelva a querer conectar

Table 7.4: Diferencias entre estado A y B

El UE averigua con que celda de la red se puede comunicar.Una vez el UE solicita permiso para conectarse a la red, el proceso de conexión se inicia haciendo que el UE transite al estado C (EMM-Registered, ECM-Connected y RRC-Conected)

El Estado del EMM en los escenarios C y D se describe por que en ambos, el UE esta conectado a la red. Los estados de ECM y RRC pueden ser

- Escenario C –> ECM-Connected/RRC-Connected
- Escenario D –> ECM-Idle/RRC-Idle

Una vez conectado a la red y mientras el UE utiliza la red, se mantiene en el escenario C. En el momento que deja de utilizar los servicios transita al escenario D. Mientras el **estado C** se identifica con las siguientes características

- Los recursos de red y radio están asignado a las conexiones de señalización en el panel de control
- Los bearers EPS en el panel de usuario
- Un UE puede ejecutar un Handover a otra celda para tener una mejor calidad de señal mientras esta comunicando con su celda actual

El **Estado D** se diferencia y se identifica como

- El UE se desactiva liberando las conexiones ECM/RRC
- Se liberan todos los recursos (ni conexión ECM ni bearers) a excepción del bearer S5
- No puede entregarse trafico de usuario y en el caso que quisiera hacerlo, se debería establecer conexión ECM de forma que el UE transitará al escenario C
- El UE selecciona una celda donde mantenerse, utilizando los criterios de calidad de señal radio

Las transiciones del estado D al C se realiza en las siguientes situaciones

- Cuando existe trafico para el UE (ya sea UL o DL)
- Estando el UE en estado desactivado realiza una petición de TA
- Estando el UE desactivado, expira el temporizador TAU

Las transiciones de C a D en cambio, se realizan cuando

- No se detecta actividad en el UE durante un periodo de tiempo
- El UE libera los recursos utilizados durante la petición de TA o una vez ha renovado el temporizador TAU

Si nos fijamos en el momento en el que el UE se desconecta de la red, pasando al escenario B:

- El UE se apaga
- El enlace radio falla
- Cuando el UE en el escenario C ejecuta un Handover a una red no LTE
- Cuando la conexión a una red es rechazada (Attach Reject)
- La solicitud de actualización del TA es rechazada (TAU Reject)

7.2 Características EMM

En la tabla 7.5 veremos la información de la que dispone la red. La red conoce la localización del UE a nivel de celda si está conectado (estado C), o a nivel de TA si esta desconectado (Estado D)

Caso	Estado	UE	eNB	S-GW	P-GW	MME	HSS	PCFR	SPR
A	EMM-Deregistered + ECM-Idle + RRC-Idle								
B	EMM-Deregistered + ECM-Idle + RRC-Idle					TAI del último TAU	MME		
C	EMM-Registered + ECM-Connected + RRC-Connected		Cell/eNB	Cell/eNB	Cell/eNB	Cell/eNB	MME	Cell/eNB	
D	EMM-Registered + ECM-Idle + RRC-Idle			TAI del último TAU	TAI del último TAU	TAI del último TAU	MME	TAI del último TAU	

Table 7.5: Información por elemento en cada estado

Tal como hemos comentado anteriormente, la red conoce la localización del UE a nivel de celda o a nivel de TA. A continuación se indica los puntos claves dependiendo de la característica del EMM

- Movilidad
  - Un UE encendido en estado EMM-Deregistered (Estado A o B) averiga en que celda y en que red esta ubicado seleccionando una red PLMN y una celda.
  - Un UE utilizando servicios en EMM-Registered (Estado C) ejecuta un Handover desde su actual celda a otra celda vecina, para mejorar la calidad de la señal radio
  - Un UE es estado EMM-Registered pero sin utilizar servicios (Estado D) ejecuta una reselección de celda buscando otra celda vecina con mejor calidad de señal radio que su celda actual, de forma que se mantiene en una con mejor calidad
- Tracking Area Update
  - Un UE en estado EMM-Registered (Estado C o D), utilizando o no servicios, actualiza su TA cuando cambia.
  - En Estado D (EMM-Registered+ECM-Idle+RRC-Idle), el UE actualiza su TA de forma regular cada vez que el timer TAU expire, aún cuando no cambia de TA. Cuando necesita, transita a estado C para poderactualizar su TA. Una vez en estado C, envía un mensaje de solicitud TAU (TAU Request) y recibe un mensaje TAU Accept del MME, quedando completo el proceso de TAU. Despues, libera la conexión ECM/RRC, y el UE vuelve al estado D (ECM-Idle/RRC-Idle)
- Paging
  - Cuando el UE se conectada a la red en estado D, cuando existe trafico a entregar, la red inicia el proceso de Paging para despertar al UE. De esta forma, el UE transita al estado C.
  - El proceso de paging esta basado en la información TAI (Tracking Area Identifier) que se facilita al UE durante la ultima actualizacion TA

Caso	Estado	Movilidad	Tracking Area Update	Paging
A	EMM-Deregistered + ECM-Idle + RRC-Idle	Selección PLMN-Celda		
B	EMM-Deregistered + ECM-Idle + RRC-Idle	Selección PLMN-Celda		
C	EMM-Registered + ECM-Connected + RRC-Connected	Handover • Intra eNB Handover • XA Handover • S1 Handover	TAU cuando cambia la TA	
D	EMM-Registered + ECM-Idle + RRC-Idle	Reselección de celda	• TAU cuando cambia la TA • TAU periodico	Control Paging

Table 7.6: Puntos claves de las características del EMM dependiendo del estado

7.3 Conexion Inicial

En el siguiente capitulo describiremos el proceso de Conexión inicial a la red LTE por parte de un UE. Dependiendo del tipo de conexión a la red LTE, el MME inicia un proceso diferente. El proceso se inicia cuando el usuario envía un mensaje de **Attach Request** al MME . En este mensaje, el UE se identifica incluyendo su UE ID, ya sea IMSI o Old GUTI. El proceso finaliza con un mensaje de **Attach Accept** enviado del MME al UE. En el mensaje de **Attach Accept** el MME inluye el GUTI, un identificador que el UE puede utilizar en vez del IMSI, y la lista TAI, que contiene las áreas donde el UE puede acceder sin tener que realizar un proceso de **TAU update**

El proceso de Aceptación de la Conexión a la red se describe a continuación. Una vez el MME ha recibido el mensaje de **Attach Accept** puede iniciar uno de los siguientes procesos

- **Adquisición UE ID.**
  - La red obtiene el UE ID para identificar al UE y autenticarlo. El UE ID puede ser IMSI o Old GUTI
  - IMSI se obtiene del UE a través de los mensajes **Attach Request** o **Identity Response**
  - El Old GUTI puede obtenerse del UE a través de un mensaje **Attach Request**
- **Autenticación**
  - Si la red ha obtenido un UE ID a través de un mensaje **Attach Request** pero la comprobación de seguridad falla, la red debe saber si el usuario puede conectarse o no ejecutando un proceso de seguridad $EPS - AKA$. El HSS deriva la clave K_{asme}, clave base del MME, generando vectores de autenticación y enviándolos al MME, que a su vez ejecuta la misma autenticación con el UE.
- **Configuración de la seguridad NAS**
  - Una vez la autenticación se ha completado, se generan las claves de seguridad NAS para la entrega de mensajes NAS seguros entre UE y MME
- **Actualización Localización**
  - MME descarga la información del HSS, y el HSS actualiza la información de localización del UE con el MME actual
  - MME realiza actualización de localización

- **Establecimiento Sesión EPS**

  - Se establece una sesión EPS y se asigna un bearer EPS por defecto

La decisión del tipo de proceso a seguir depende del tipo de conexión que el UE intenta. Los procesos de Aquisicion UE ID y Establecimiento Sesión EPS son necesarios en cualquier tipo de conexión.El tipo de conexión se basa:

  - Que UE ID tiene el usuario (IMSI o Old GUTI), es decir, si ya ha se ha conectado anteriormente a la red, por lo tanto que el MME ya le ha facilitado un GUTI
  - Si la información de la última conexión todavía existe en la red
  - A que MME el UE se está intentando conectar

En la figura 7.1 de [6] veremos el tipo de preguntas utilizados como criterio de selección de los identificadores a utilizar

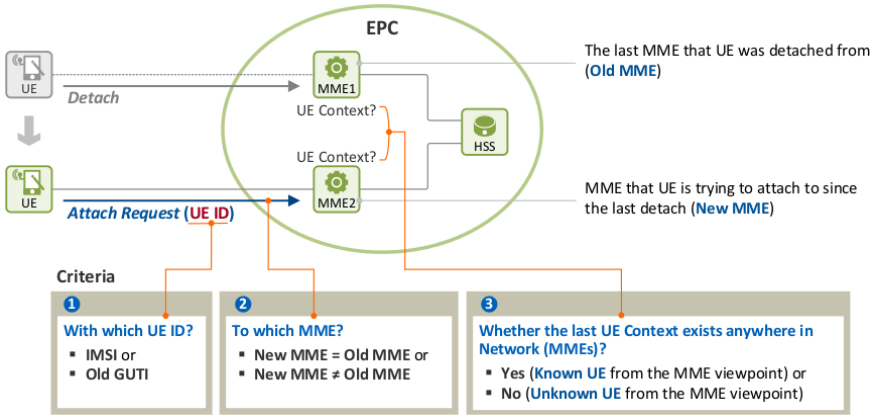


Figure 7.1: Descripción del proceso de conexión inicial e identificadores involucrados

Se debe introducir el concepto de **UE no conocido** que podemos describir con alguno de los conceptos a continuación descritos

- Los UE no conocidos serán aquellos donde el MME no se mantiene información de la última conexión
- El proceso se inicia cuando el UE envía un mensaje **Attach Request** a la red y el MME no tiene ningún contexto valido del UE
- Diferenciaremos entre **New MME**, aquel MME al que el UE se esta intentando conectar ahora, y **Old MME**, aquel al que se conecto la última vez

En la figura 7.2 de [6] se muestran los diferentes tipos de conexión que un UE puede generar respecto un MME.

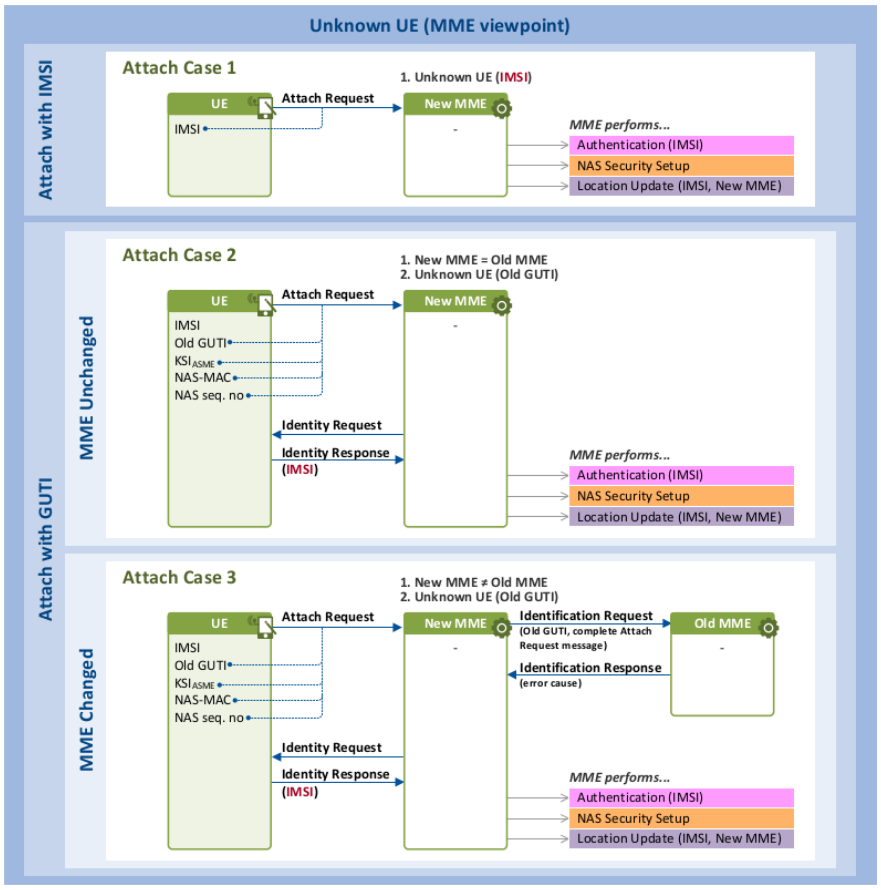


Figure 7.2: Diferentes tipos de conexión con UE no conocido

En el primer caso de la figura 7.2, se describe el proceso que sigue un UE no conocido para realizar la conexión a la red LTE. Este caso sucede cuando ni UE ni MME tienen el último contexto UE. El proceso sería el siguiente

- UE envía al MME un mensaje **Attach Request** usando su IMSI como UE ID. El MME por tanto, obtiene el IMSI del mensaje
- El MME inicia el proceso de autenticacion y configuración de seguridad NAS
- El MME envía una actualización de la localización al HSS, informándole que el UE se ha registrado con el, y descarga la información de suscripción del usuario

El siguiente caso identificado en la Figura 7.2 era la conexión del UE al mismo MME al que se había conectado con anterioridad. El UE, teniendo la información de contexto de la última conexión, se intenta conectar al último MME con el que estuvo conectado, pero el MME no tiene ninguna información valida del último contexto. El proceso sería el siguiente:

- UE envía un mensaje **Attach Request** utilizando el **Old GUTI**. El mensaje se envía protegido por una clave de integridad NAS
- Como el GUTI incluye el GUMMEI, un ID de MME, el **New MME** averiga que el **Old MME** fue él mismo, pero falla al intentar localizar el contexto de UE
- El MME envía al UE un mensaje **Identity Request**, solicitando el IMSI
- El UE envía al MME un mensaje **Identity Response**, facilitando el IMSI solicitado
- El MME ejecuta los proceso de autenticación y configuración de seguridad NAS utilizando el IMSI obtenido
- El MME envía el mensaje de actualización de localización al HSS

El último tipo de conexión que vimos en la Figura 7.2 es el caso en el que el UE, aun teniendo información de la última conexión, se intenta conectar a un MME diferente y el Old MME no tiene información de contexto valida del UE. El proceso sería el siguiente

- UE envía un mensaje **Attach Request** utilizando su Old GUTI como UE ID
- MME recibe el mensaje e identifica que el Old GUTI corresponde a otro MME, no él
- El New MME envía al Old MME un mensaje **Identification Request** reenviando el Old GUTI y el mensaje **Attach Request** recibido del UE. Con este paso, el New MME pretende obtener la información de contexto de conexión del UE
- El Old MME intenta localizar la información de contexto de conexión pero no es capaz de localizarla
- El Old MME envía un mensaje de **Identification Response** informando que no ha encontrado información de contexto
- El UE envía al MME un mensaje **Identity Response**, facilitando el IMSI solicitado
- El MME ejecuta los proceso de autenticación y configuración de seguridad NAS utilizando el IMSI obtenido
- El MME envía el mensaje de actualización de localización al HSS

Con anterioridad habíamos descrito que era un UE no conocido. Ahora, en cambio, describiremos los **UE conocidos** como aquellos donde el MME mantiene información de la última conexión.

Por lo tanto, en el caso que el UE sea conocido para el MME, el tipo de conexión que un UE intenta también se puede separar en diferentes escenarios o casos como veremos en la Figura 7.3 de [6]

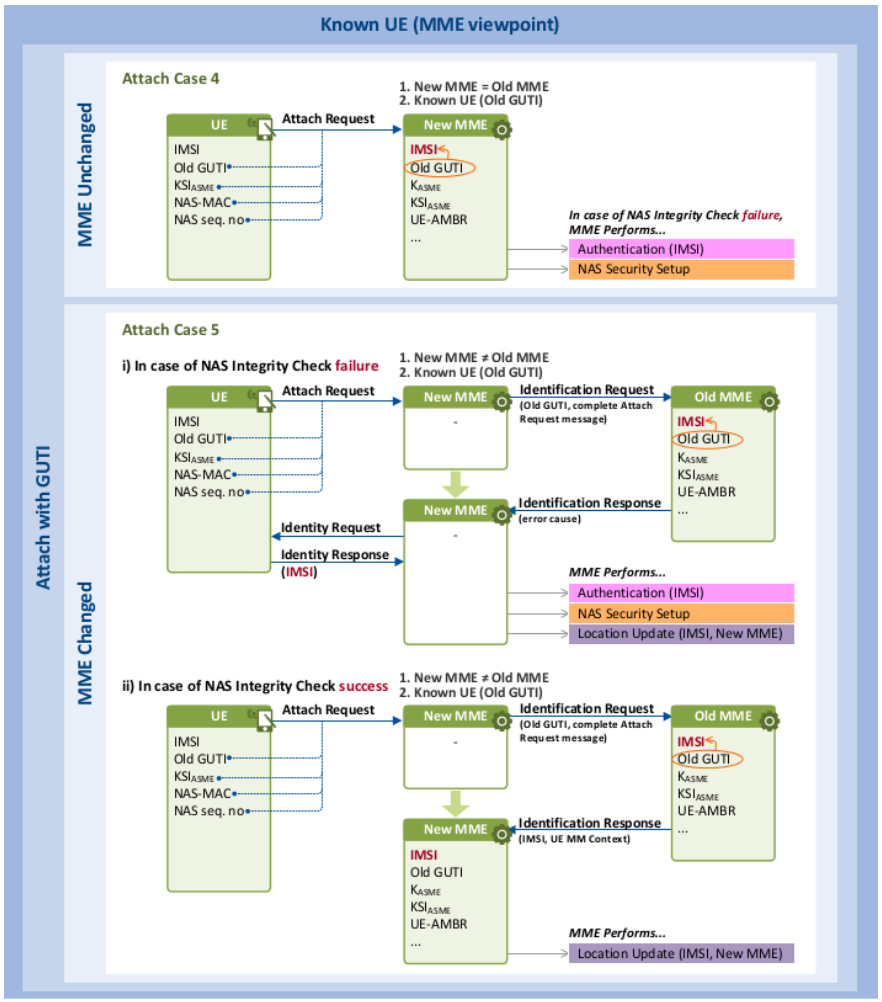


Figure 7.3: Diferentes tipos de conexión para UE conocidos

A continuación describiremos los casos descritos en 7.3. En el primero de ellos (Caso 4), el UE todavía tiene información de contexto de la última conexión (Old GUTI, conexto de seguridad NAS) e intenta conectarse al MME al que estuvo conectado la última vez, teniendo este la información de contexto de la última conexión. El proceso será el siguiente

- UE envía al New MME un mensaje **Attach Request** utilizando su Old GUTI como UE ID. En este punto, el mensaje **Attach Request** esa protegido con una clave de integridad NAS
- El New MME conoce por el Old GUTI que fue él quien lo asigno. Revisa la información y localiza la información de contexto de conexión del UE (IMSI, MM Conexto [Conexto Seguridad NAS, UE-AMBR])
- El MME realiza una comprovación de integridad al mensaje **Attach Request**
  - Si la comprobación falla, el MME debe autenticar al UE utilizando el IMSI y realizando el proceso de configuración de seguridad NAS
  - Si la comprobación es correcta, el MME obvia el proceso de autenticacion y configuración de seguridad. En este caso, si que el New MME realiza una actualización de la localización con el HSS

El siguiente sería el Caso 5 donde el UE tiene la información de la última conexión, intenta conectarse a un New MME teniendo el Old MME información de contexto valida del UE. El proceso sería el siguiente

- UE envía al New MME un mensaje **Attach Request** utilizando su Old GUTI como UE ID
- El New MME conoce por el Old GUTI recibido que fue asignado por otro MME (Old MME)
- El New MME envía un mensaje **Identificaction Request** que incluyed Old GUTI y el mensaje de Attach REquest, reenviando el mensaje de **Attach Request**. De esta forma el New MME solicita la información de contexto de la última conexión del UE
- El Old MME mira el contexto UE y localiza el IMSI y el contexto MM(Contexto Seguridad NAS, UE-AMBR)
- El Old MME realiza una comprovación de integridad del mensaje **Attach Request**
  - Si la comprobación falla, el Old MME responde al mensaje con las causas del error
  - Si la comprobación es correcta, reenvía el contexto UE(IMSI, Old GUTI y contexto MM)
- En el caso que la comprobación fallara
  - El New MME envía al UE un mensaje **Identity Request**, solicitando el IMSI
  - El UE envía al New MME un mensaje **Identity Response**, facilitando el IMSI solicitado
  - El New MME ejecuta los proceso de autenticación y configuración de seguridad NAS utilizando el IMSI obtenido
  - El New MME envía el mensaje de actualización de localización al HSS
- En el caso que la comprobación era correcta
  - El New MME envía el mensaje de actualización de localización al HSS

7.4 Desconexion de la red EMM

Existen varias posibilidades del origen de la desconexión del usuario (UE) de la red EMM

- El UE se desconecta una vez ha utilizado los servicios de la red, por tanto, es el usuario quien inicia el proceso de desconexión
- El usuario puede ser desconectado de la red sin su petición expresa, de forma que no puede seguir utilizando los servicios, por tanto, es la red quien inicia la desconexión

Una vez el usuario es desconectado, todos los recursos de radio/red que habían sido asignados y los bearers establecidos, son liberados. Esta liberación implica que el contexto MM del usuario y los bearers EPS asignados son eliminados. El estado transita de **EMM-Registered a EMM-Deregistered**. En el caso que el usuario sea correctamente desconectado, la información del contexto del usuario, GUTI y el user-id a nivel de NAS, se mantiene valida tanto en el usuario como en el MME, de forma que puede ser utilizada la próxima vez que se conecte a la red

Es posible categorizar los escenarios de desconexión dependiendo de quien inicia el proceso. Es posible que sea el usuario o la red, y en este ultimo caso, es posible que lo inicie el MME o HSS

- Caso 1. UE Inicia la Desconexión

  - UE se apaga
  - La tarjeta USIM es sacada del UE
  - UE intenta utilizar una red no-EPS
- Caso 2. MME Inicia la Desconexión
  - Desconexion Implícita. El MME inicia la desconexión avisando al usuario de su intencion de desconectarlo de la red
    * MME no puede comunicar con el usuario debido a problemas en la calidad del enlace radio
  - Desconexión Explicita. El MME inicia la desconexión sin comunicar nada al usuario
    * Debido a mantenimiento de red
    * Problemas en la autenticación
    * Si no es posible asignar recursos al usuario
- Caso 3. HSS Inicia la Desconexión
  - En el caso que el perfil del usuario cambio en el HSS y sea necesario actualizar el perfil en el MME
  - Para restringir el acceso ilegal de un UE a su red

En la figura 7.4 de [7] se describen los pasos que se realizan durante el proceso de desconexión de un UE de la red

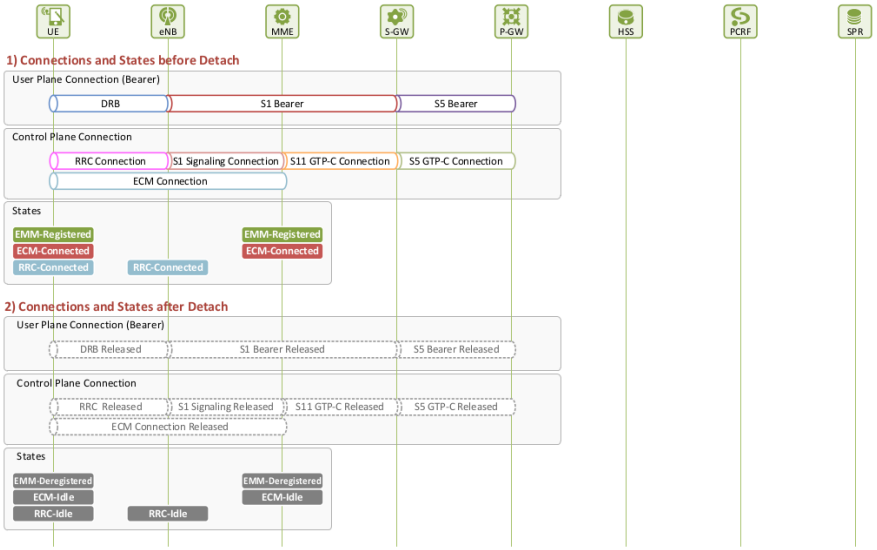


Figure 7.4: Proceso de desconexión iniciado por el UE

- **1 - Desconexión iniciada por UE**
  - **1) [UE –> MME] Solicitud de Desconexión**. El UE solicita la desconexión enviando un mensaje de **Detach Request** al MME.
  - **2) [UE] Gestionando Seguridad y Contextos**. Después de enviar el mensaje **Detach Request** , el UE almacena su contexto de seguridad NAS, GUTI e información del TA, y elimina el contexto del Bearer EPS
  - **3) [MME] Notificando la intención de desconectar y Gestionando el Contexto de Seguridad**. Después de recibir el mensaje **Detach Request**, el MME conoce al intención del UE de desconectarse. Almacena el contexto de seguridad NAS del usuario y valida el tipo de desconexión (si es normal o que el terminal se ha apagado). Dependiendo de la tipología envía un mensaje de confirmación de la desconexión o no
- **2 - Terminación de la sesión EPS**.
  - **(1) Liberación del Bearer EPS y Eliminación de la Regla PCC**

* **4) [MME –> S-GW] Solicitando la liberación de la Sesión EPS**. El MME y el S-GW se comunican a través de la interfaz S11 utilizando el protocolo GTP (GTP-C). El MME inicia los procesos para eliminar la sesión EPS del usuario y el bearer EPS enviando al S-GW un mensaje **Delete Session Request**. En este momento, se eliminan el ID del Bearer EPS por defecto y la información de la localización del UE (ECGI, TAI)

* **5) [MME] Eliminando el Contexto del Bearer EPS**. El MME elimina la información de contexto del Bearer EPS enviando un mensaje de **Delete Session Request**

* **6) [S-GW –> P-GW] Solicitando la liberación de la Sesion EPS**. S-GW y el P-GW se comunican a través de la interfaz S5 utilizando el protocolo GTP. El S-GW le reenvia el mensaje **Delete Session Request** recibido del MME

* **7) [S-GW] Eliminando el Contexto del Bearer EPS**. El S-GW elimina la información de contexto del bearer EPS enviando un mensaje de **Delete Session Request**

* **8) [P-GW –> PCRF] Notificación de la terminación de la sesión EPS**. El P-GW y el PCRF se comunica a través del interfaz Gx utilizando el protocolo Diameter. El P-GW envía al PCRF un mensaje **CCR (CC-Request)** notificándole que el usuario ha dejado de utilizar los servicios de red.

* **9) [PCRF] Eliminando la regla RCC**. El PCRF elimina la regla PCC del usuario una vez ha recibido el mensaje **CCR**

* **10) [P-GW <–PCRF] Puesta en conocimiento de la terminación de la sesión EPS**. El PCRF informa de la eliminación de la regla PCC del usuario enviando un mensaje **CCA(CC-Answer)** al P-GW

* **11) [S-GW <– P-GW] Respondiendo a la petición de liberación de la sesión EPS**. Cuando el P-GW recibe el mensaje **CCA**, envía al S-GW un mensaje de **Delete Session Response** como respuesta a la solicitud del punto 4

* **12) [P-GW] Eliminando el Contexto de Bearer EPS**. El P-GW elimina el contexto del Bearer EPS una vez ha enviado el mensaje de **Delete Session Response**

* **13) [UE <–MME] Puesta en conocimiento Desconexión**. Una vez el MME ha recibido el mensaje de **Delete Session Response**, este envía un mensaje al UE de **Detach Accept** en el caso que la tipología de desconexión sea diferente a que el UE se ha apagado.

– **(2) Liberación de la conexión de señalización S1**

* **15) [eNB <– MME] Puesta en conocimiento liberación de la conexión de señalización S1**. El MME envía un mensaje **UE Context Release Command** al eNB para liberar la conexión de señalización S1

* **16) [UE <– eNB] Liberación Conexión RRC**. El eNB envía un mensaje **RRC Connection Release** al UE para liberar cualquier conexión pendiente RRC

* **17) [eNB] Eliminando el Contexto UE**. El eNB elimina toda la información relacionada con el UE

* **18) [eNB –> MME] Liberación Conexión RRC Completada**. Por ultimo, el eNB envía al MME un mensaje **UE Context Release Complete** como respuesta a la petición enviada en 15)

En la siguiente Figura 7.5 de [7] se describe la desconexión iniciada por el MME

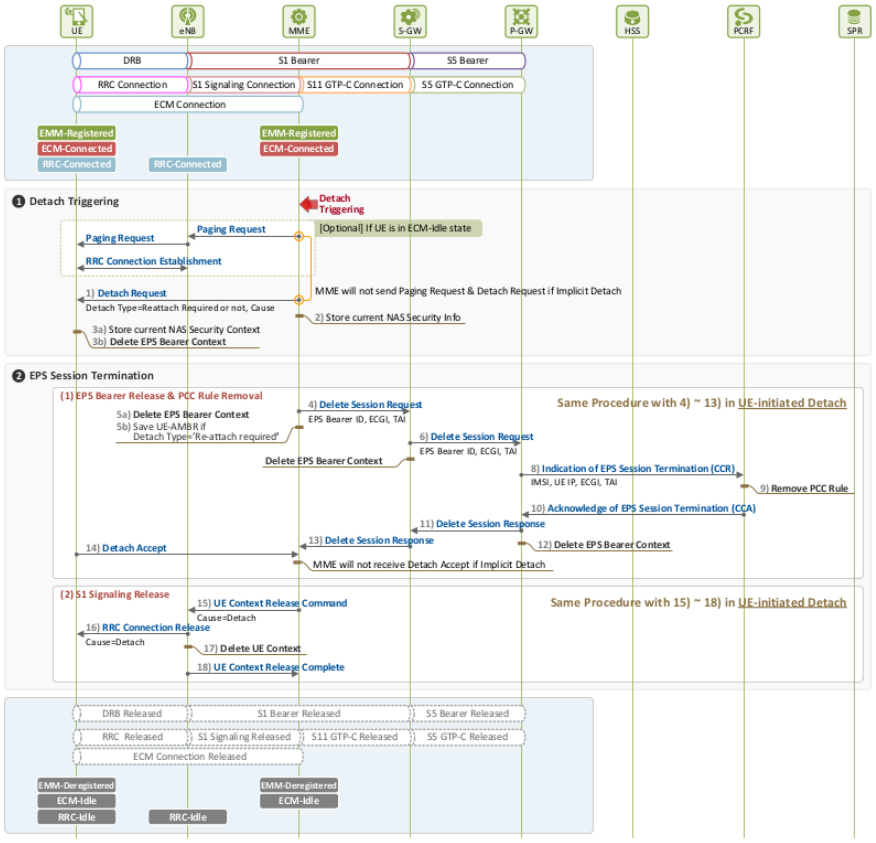


Figure 7.5: Proceso de Desconexión iniciado por el MME

- **1 - MME Inicia la desconexión**
  - **1) [UE <– MME] Solicitud Desconexión**.En desconexión explicita, el MME envía un mensaje **Detach Request** la UE para desconectar. En caso de desconexión implícita, el MME no envía ningún mensaje al UE
  - **2) [MME] Gestionando el Contexto de Seguridad**.Después de enviar el mensaje de **Detach Request**, el MME almacena la información de contexto de seguridad NAS antes de eliminar la sesión EPS. De esta forma la próxima vez que el UE intente conectarse, el MME puede utilizar la información almacenada y obviar los procesos de autenticación y configuración de seguridad NAS
  - **3) [UE] Notificando la intención de desconectar y Gestionando el Contexto de Seguridad**. Después de recibir el mensaje **Detach Request**, el UE conoce al intención del MME de desconectarlo. Almacena el contexto de seguridad NAS del usuario y elimina el contexto del Bearer EPS. En el mensaje de desconexión se le indica si es necesario reconectar o no
- **2 - Terminación de la sesión EPS**
  - **(1) Liberación Bearer EPS y Eliminación Regla PCC**.
    - **4) [MME –> S-GW] Solicitando la liberación de la Sesion EPS**. El MME y el S-GW se comunican a traves de la interfaz S11 utilizando el protocolo GTP (GTP-C). El MME inicia los procesos para eliminar la sesión EPS del usuario y el bearer EPS enviando al S-GW un mensaje **Delete Session Request**. En este momento, se eliminan el ID del Bearer EPS por defecto y la información de la localización del UE (ECGI, TAI)
    - **5) [MME] Eliminando el Contexto del Bearer EPS**. El MME elimina la información de contexto del Bearer EPS enviando un mensaje de **Delete Session Request**. En el caso que el tipo de conexión solicite la reconexión posterior del UE, el MME puede almacenar el valor actual del UE-AMBR

        * **6) [S-GW –> P-GW] Solicitando la liberación de la Sesion EPS**. S-GW y el P-GW se comunican a través de la interfaz S5 utilizando el protocolo GTP. El S-GW le reenvia el mensaje **Delete Session Request** recibido del MME
        * **7) [S-GW] Eliminando el Contexto del Bearer EPS**. El S-GW elimina la información de contexto del bearer EPS enviando un mensaje de **Delete Session Request**
        * **8) [P-GW –> PCRF] Notificación de la terminación de la sesión EPS**. El P-GW y el PCRF se comunica a través del interfaz Gx utilizando el protocolo Diameter. El P-GW envía al PCRF un mensaje **CCR (CC-Request)** notificándole que el usuario ha dejado de utilizar los servicios de red.
        * **9) [PCRF] Eliminando la regla RCC**. El PCRF elimina la regla PCC del usuario una vez ha recibido el mensaje **CCR**
        * **10) [P-GW <–PCRF] Puesta en conocimiento de la terminación de la sesión EPS**. El PCRF informa de la eliminación de la regla PCC del usuario enviando un mensaje **CCA(CC-Answer)** al P-GW
        * **11) [S-GW <– P-GW] Respondiendo a la petición de liberación de la sesión EPS**. Cuando el P-GW recibe el mensaje **CCA**, envía al S-GW un mensaje de **Delete Session Response** como respuesta a la solicitud del punto 4
        * **12) [P-GW] Eliminando el Contexto de Bearer EPS**. El P-GW elimina el contexto del Bearer EPS una vez ha enviado el mensaje de **Delete Session Response**
        * **13) [UE <–MME] Puesta en conocimiento Desconexión**. Una vez el MME ha recibido el mensaje de **Delete Session Response**, este envía un mensaje al UE de **Detach Accept** en el caso que la tipología de desconexión sea diferente a que el UE se ha apagado.
        * **14) [UE –> MME] Puesta en conocimiento Desconexión**. Después de almacenar el contexto de seguridad NAS y eliminar el contexto del Bearer EPS tras recibir el mensaje **Detach Request** del MME el UE envía un mensaje de **Detach Accept**
    - **(2) Liberación Conexión de Señalización S1**.
        * **15) [eNB <– MME] Puesta en conocimiento liberación de la conexión de señalización S1**. El MME envía un mensaje **UE Context Release Command** al eNB para liberar la conexión de señalización S1
        * **16) [UE <– eNB] Liberación Conexión RRC**. El eNB envía un mensaje **RRC Connection Release** al UE para liberar cualquier conexión pendiente RRC
        * **17) [eNB] Eliminando el Contexto UE**. El eNB elimina toda la información relacionada con el UE
        * **18) [eNB –> MME] Liberación Conexión RRC Completada**. Por ultimo, el eNB envía al MME un mensaje **UE Context Release Complete** como respuesta a la peticion enviada en 15)

El último caso, descrito en la Figura 7.6 de [7] el caso en el que la desconexión es iniciada por el HSS

- **1 - HSS Inicia la desconexión**
    - **1) [MME <– HSS] Solicitud Desconexión**. HSS y MME se comunican a través de la interfaz S6a utilizando el protocolo Diameter. El HSS solicita al MME la desconexión del usuario enviando un mensaje **Cancel Localition Request (CLR)**
    - **2) [UE <– MME] Solicitud Desconexión**.En desconexión explicita, el MME envía un mensaje **Detach Request** la UE para desconectar. En caso de desconexión implicita, el MME no envía ningún mensaje al UE
    - **3) [MME] Gestionando el Contexto de Seguridad**.Después de enviar el mensaje de **Detach Request**, el MME almacena la información de contexto de seguridad NAS antes de eliminar la sesión EPS. De esta forma la próxima vez que el UE intente conectarse, el MME puede utilizar la información almacenada y obviar los procesos de autenticación y configuración de seguridad NAS
    - **4) [UE] Notificando la intención de desconectar y Gestionando el Contexto de Seguridad**. Después de recibir el mensaje **Detach Request**, el UE conoce al intención del MME de desconectarlo. Almacena el contexto de seguridad NAS del usuario y elimina el contexto del Bearer EPS. En el mensaje de desconexión se le indica si es necesario reconectar o no
- **2 - Terminación de la sesión EPS**
    - **(1) Liberación Bearer EPS y Eliminación Regla PCC**.
        * **5) [MME –> S-GW] Solicitando la liberación de la Sesion EPS**. El MME y el S-GW se comunican a través de la interfaz S11 utilizando el protocolo GTP (GTP-C). El MME inicia los procesos para eliminar la sesión EPS del usuario y el bearer EPS enviando al S-GW un mensaje **Delete Session Request**. En este momento, se eliminan el ID del Bearer EPS por defecto y la información de la localización del UE (ECGI, TAI)

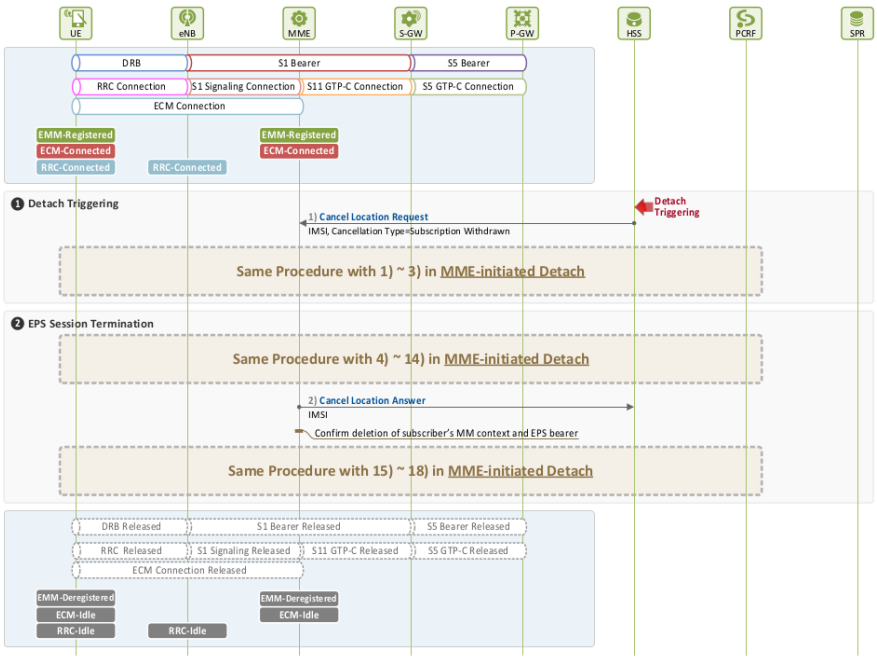


Figure 7.6: Proceso Desconexión iniciado por el HSS

* **6) [MME] Eliminando el Contexto del Bearer EPS**. El MME elimina la información de contexto del Bearer EPS enviando un mensaje de **Delete Session Request**. En el caso que el tipo de conexión solicite la reconexión posterior del UE, el MME puede almacenar el valor actual del UE-AMBR
* **7) [S-GW –> P-GW] Solicitando la liberación de la Sesion EPS**. S-GW y el P-GW se comunican a través de la interfaz S5 utilizando el protocolo GTP. El S-GW le reenvia el mensaje **Delete Session Request** recibido del MME
* **8) [S-GW] Eliminando el Contexto del Bearer EPS**. El S-GW elimina la información de contexto del bearer EPS enviando un mensaje de **Delete Session Request**
* **9) [P-GW –> PCRF] Notificación de la terminación de la sesión EPS**. El P-GW y el PCRF se comunica a través del interfaz Gx utilizando el protocolo Diameter. El P-GW envía al PCRF un mensaje **CCR (CC-Request)** notificándole que el usuario ha dejado de utilizar los servicios de red.
* **10) [PCRF] Eliminando la regla RCC**. El PCRF elimina la regla PCC del usuario una vez ha recibido el mensjae **CCR**
* **11) [P-GW <–PCRF] Puesta en conocimiento de la terminación de la sesión EPS**. El PCRF informa de la eliminación de la regla PCC del usuario enviando un mensaje **CCA(CC-Answer)** al P-GW
* **12) [S-GW <– P-GW] Respondiendo a la petición de liberación de la sesión EPS**. Cuando el P-GW recibe el mensaje **CCA**, envía al S-GW un mensaje de **Delete Session Response** como respuesta a la solicitud del punto 4
* **13) [P-GW] Eliminando el Contexto de Bearer EPS**. El P-GW elimina el contexto del Bearer EPS una vez ha enviado el mensaje de **Delete Session Response**
* **14) [UE <–MME] Puesta en conocimiento Desconexión**. Una vez el MME ha recibido el mensaje de **Delete Session Response**, este envía un mensaje al UE de **Detach Accept** en el caso que la tipología de desconexión sea diferente a que el UE se ha apagado.
* **15) [UE –> MME] Puesta en conocimiento Desconexión**. Después de almacenar el contexto de seguridad NAS y eliminar el contexto del Bearer EPS tras recibir el mensaje **Detach Request** del MME el UE envía un mensaje de **Detach Accept**
* **16) [MME –> HSS] Respondiendo a la petición de Desconexión**. Después de recibir el mensaje de **Dettach Accept** del UE, y el mensaje del S-GW **Delete Sesion Response**, el MME envía un mensaje al HSS **Cancel Location Answer** como respuesta a la petición en 1)

– **(2) Liberación Conexión de Señalización S1**.

* **17) [eNB <– MME] Puesta en conocimiento liberación de la conexión de señalización S1**. El MME envía un mensaje **UE Context Release Command** al eNB para liberar la conexión de señalización S1
* **18) [UE <– eNB] Liberación Conexión RRC**. El eNB envía un mensaje **RRC Connection Release** al UE para liberar cualquier conexión pendiente RRC
* **19) [eNB] Eliminando el Contexto UE**. El eNB elimina toda la información relacionada con el UE
* **20) [eNB –> MME] Liberación Conexión RRC Completada**. Por ultimo, el eNB envía al MME un mensaje **UE Context Release Complete** como respuesta a la peticion enviada en 15)

7.5 Liberación S1

Cuando se habla de liberación S1, significa liberar tanto la señalización S1 y conexión RRC en el panel de control como el bearer S1 (de bajada)y DRB en el panel de usuario. La solicitud de liberación del interfaz S1 puede ser creada tanto por MME como eNB. Las causas para la solicitud dependerán de quien la crea. Si la solicitud es generada por eNB

- Inactividad de usuario
- Repetido error de comprobación de integridad en la señalización RRC
- UE genera señalización de liberación de conexión
- Error no especificado
- Mantenimiento

Si la solicitud es generada por MME

- Fallo de autenticación
- Desconexión
- Celdas CSG no permitidas

En el panel de usuario, una vez establecida la conexión, se establece un bearer EPS. El bearer EPS esta compuesta de un DRB (bearer del UE al eNB), un Bearer S1 (del eNB al S-GW) y un Bearer S5 (de S-GW a P-GW). En el panel de control, una vez establecida la conexión, se asigna una conexión de señalización. La conexión de señalización esta compuesta de un ECM (RRC + conexión de señalización S1), conexión S11(de MME a S-GW) y S5 (de S-GW a P-GW).

En la liberación S1 solo se liberan los recursos radio por lo que el UE se mantiene en estado EMM-Registered y el transito se hace a ECM-Idle

En la Figura 7.7 de [8] veremos descritas las conexiones que se establecen tanto en el panel de control como en el panel de usuario respecto la conexión S1. *En el anexo podemos encontrar descrito el proceso de liberación del enlace S1 por inactividad del usuario*

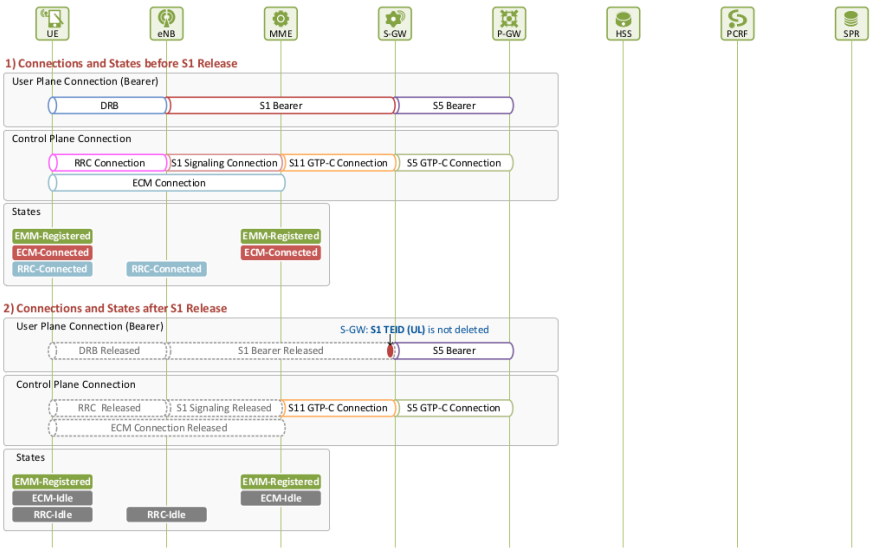


Figure 7.7: Conexiones y Estados en los escenarios de liberación de S1

Cuando el UE sigue registrado en la red pero la conexión S1 ha sido liberada por inactividad, el UE no tiene recursos radio asociados para poder recibir o entregar trafico (EMM-Registered, ECM-Idle). En esta situación, el UE debe realizar una solicitud de servicio para que le sean asignados otra vez los recursos y poder entregar-recibir trafico. El UE solicita servicio enviando un mensaje **Service Request** al EMM de forma que transita al estado EMM-Registered+ECM-Connected+RRC-Connected . Entonces, se le asigna una conexión ECM (RRC + Conexión de señalización S1) y un E-RAB (DRB+Bearer S1) permitiéndole recibir y entregar trafico.

Las solicitudes de servicio puede ser iniciadas tanto por el UE como por la red, y las podemos dividir

- Caso 1: UE inicia el proceso, ya que tiene trafico de subida que entrega
- Caso 2: Red inicia el proceso, ya que tiene trafico de bajada que entregar

En el anexo podemos encontrar descrito el proceso de iniciación del proceso por parte de la red

7.6 TAU Tracking Area Update

El proceso de TAU identifica el momento en el que es necesario actualizar la lista de Tracking Areas de su lista de TAIs. El proceso de TAU se inicia

- Cuando un UE accede a un nuevo TA (Tracking Area) que no esta en su lista de TAIs permitidos por el MME
- Cuando el Temporizador TAU expira

Un UE en estado inactivo reporta su localización actual al MME enviando un mensaje **TAU Request** cuando el temporizador TAU expira. Una vez transitado al estado **ECM/RRC-Connected**, y ejecutado el proceso de TAU periódico, el UE vuelve al estado inactivo

Cuando el temporizador TAU expira se producen una serie de acciones cuyo objetivo, entre otros, sería liberar los recursos asignados. Una vez el UE entra en estado inactivo, las conexiones de señalización y bearers son liberados. El MME,por tanto, pierde la pista de la localización del UE. La red tiene que estar atenta a la localización del UE, tanto si esta esté activo o inactivo, para poder entregarle trafico.

Los UE en estado inactivo tiene que reportar de forma periódica su localización aún cuando no tengan datos a entregar. Un TA es un grupo de celdas, gestionadas por el MME. La localización del UE en estado inactivo es reconocida a nivel de TA. El MME en el momento que el UE se conecta a la red, le provee con una lista TAI y un temporizador TAU incluidos ambos en el mensaje **Attach Accept**. Con esta información, el UE ejecuta el procedimiento TAU cuando el Temporizador TAU ha expirado. Cuando el MME

recibe información del UE, actualiza la localización actual (TA, celda). En el caso que exista trafico para el UE cuando este está en estado inactivo, el MME informa al UE enviando un mensaje **Paging Message** a todas las celdas en el TA donde el UE ha reportado su localización anteriormente. En el ejemplo de la figura 7.8 de [8], UE se conecto a la celda 2 en eNB1 siendole asignado una TAI

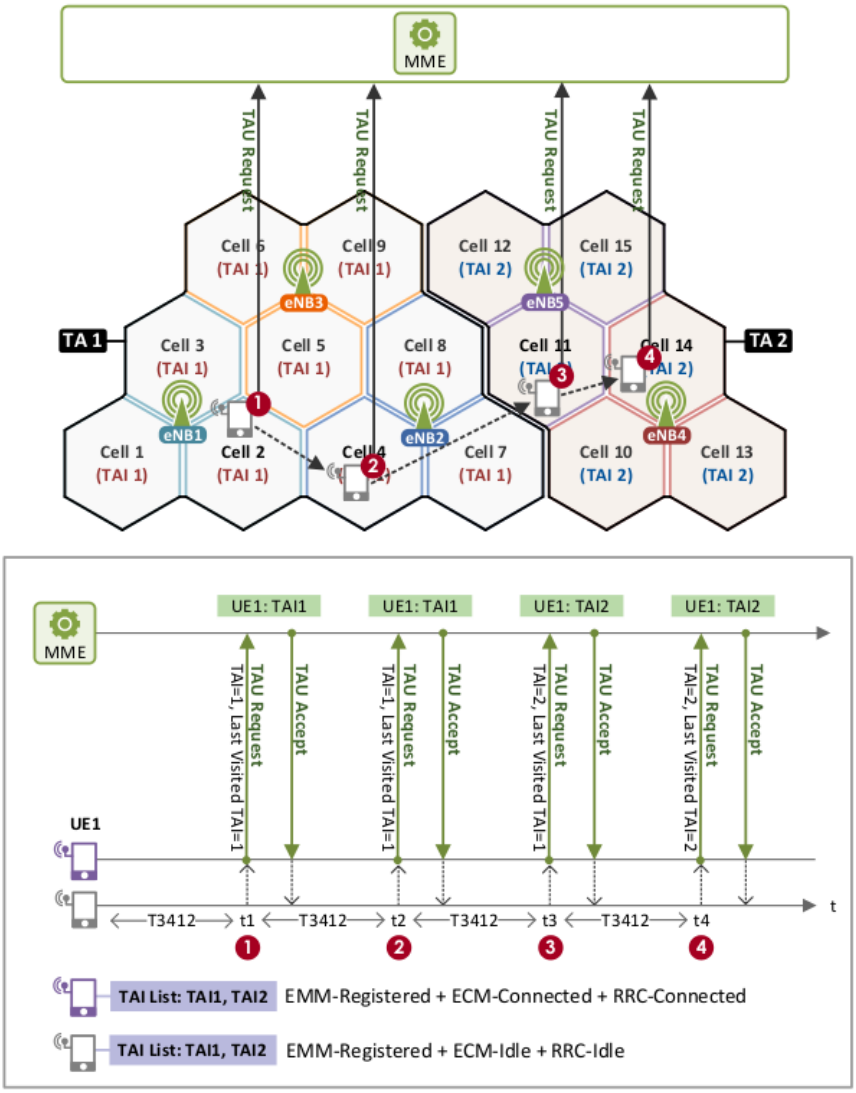


Figure 7.8: Ejemplo TAU Periódico

List TAI1, TAI2 y un temporizador TAU (60m) a través de un mensaje **Attach Accept** del MME. Posteriormente, el UE se inactivo, y durante este periodo viajó de 1 –> 2 –> 3 –> 4

1 - Temporizador TAU - T1

- Tras conectarse y transitar a estado Inactivo en la celda 2, el UE se despierta y establece una conexión de señalización con MME cuando el temporizador TAU expira en T1.
- El UE envía al MME un mensaje **TAU Request** (TAI = TAI1, Last Visited TAU=TAI1)
- El MME revisa si la localización del UE ha cambiado desde la última vez y actualiza la información en el caso que fuera necesario
- El UE vuelve a estado inactivo una vez ha recibido el mensaje **TAU Accept**

- En el caso que existiera trafico de bajada a entregar al UE, el MME averiguaría cual fue el última TA donde el UE reporto su localización, y enviaría un mensaje **Paging Message** a todas las celdas de este TA

2 - Temporizador TAU - T2

- El UE se mueve a la celda 4, y el temporizador expira en T2
- El UE envía al MME un mensaje **TAU Request** (TAI = TAI1, Last Visited TAU=TAI1)

3 - Temporizador TAU - T3

- El UE se mueve a la celda 11, y el temporizador expira en T3
- El UE envía al MME un mensaje **TAU Request** (TAI = TAI2, Last Visited TAU=TAI1)
- El MME actualiza la última localización de UE a TAI2

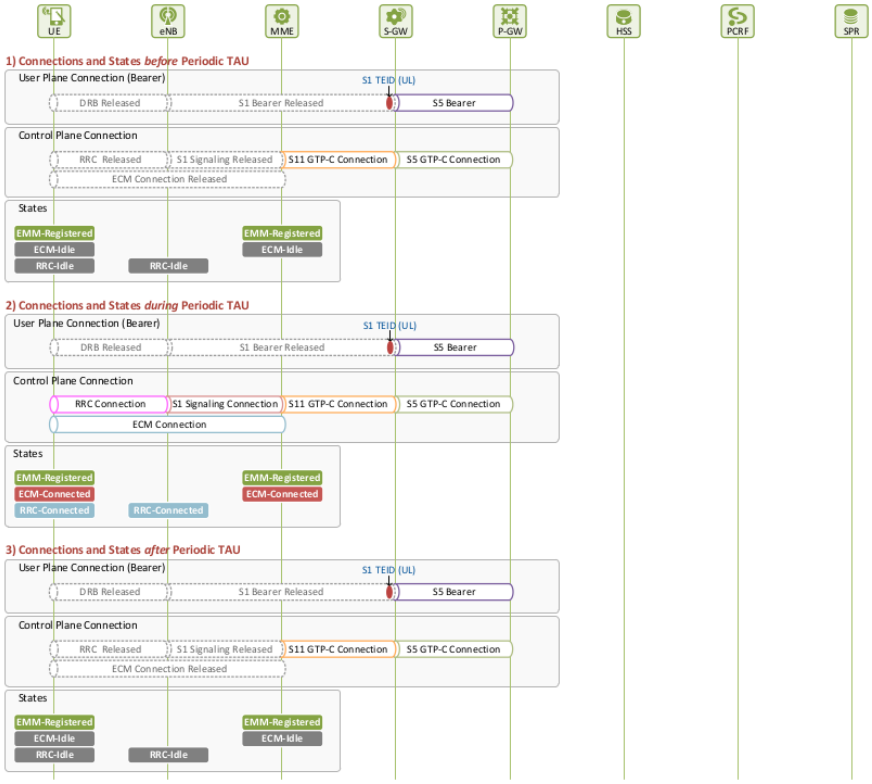


Figure 7.9: Conexiones y Estado en el proceso de TAU

En la figura anterior 7.9 de [8] vemos que antes del proceso de TAU periódico, el UE esta en estado **EMM-Registered, ECM/RRC-Idle** estando todos los recursos liberados. Durante el proceso TAU, el UE transita a estado **EMM-Registered, ECM/RRC-Connected**. Solo se establece la conexión de señalización para poder entregar la información relacionada con el TAU. Después del proceso, la señalización de conexión es liberada. El UE transita de nuevo a **EMM-Registered, ECM/RRC-Idle**

A continuación se muestra la figura 7.10 de [8] donde podemos ver la evolución del estado de los elementos de la red durante el proceso de TAU.

En el anexo podemos encontrar descrito el proceso de TAU Periódico

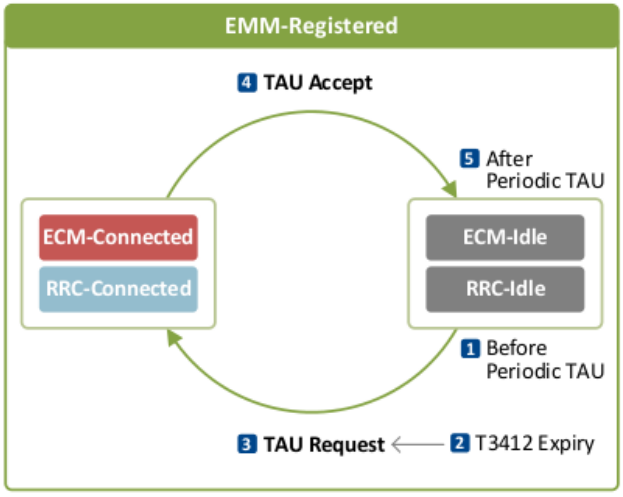


Figure 7.10: Cambios de estado durante el proceso TAU

7.7 Handover

Los suscriptores móviles pueden utilizar los servicios mientras se mueven dado que las redes móviles soportan el proceso de **Handover**. Los UE se pueden cambiar de estación base/celda sin perdida de información, y seguir comunicándose con la red sin ninguna interrupción durante el cambio.

Proceso	**Dirección**	**Descripción**
Medición de Configuración	eNB –> UE	Especifica la medición a realizar por el UE
Reporte de medición	UE –> eNB	Resultados de la medición
Decisión de Handover	Origen eNB	Toma la decisión de la celda destino y el tipo de Handover (X2 o S1 Handover)
Preparación Handover	Varios tipos dependiendo del Handover	Prepara el path para reenviar información
Ejecución Handover		Reenvio de datos
Finalización Handover		Cambia el path de datos

Table 7.7: Procesos afectados durante el Handover

El proceso de Handover se produce cuando la potencia de la señal recibida por el UE de la celda de servicio actual se va volviendo débil mientras viaja el UE, y la señal de una celda vecina empieza a volverse fuerte. Una vez iniciado el proceso de Handover, se establece una nueva conexión RRC con la celda vecina. En el momento que se establece la conexión RRC con el eNB, el eNB informa al UE en que evento la señal recibida debe ser reportada, enviando un mensaje de configuración **RRC Connection Reconfiguration**. El UE mantiene traza de las señales recibidas por ambas celdas, la que da servicio y la vecina. Cuando uno de los eventos marcados por el eNB se produce, el UE reporta la potencia de la señal al eNB mediante un mensaje **Measurement Report**. Una vez el eNB recibe el mensaje, toma la decisión de iniciar o no el Handover

(1) Configuración de Medición

- El eNB informa al UE que tipo de información de medición debe ser reportada. Esta información es reportada por el eNB mediante un mensaje **RRC Connection Reconfiguration**
- El contenido del mensaje es el siguiente:
  - Objetivo Medición: facilita la información de las celdas E-UTRA a ser medidas por el UE (número de canales de frecuencia, Identificador de Celda Fisica - PCI, lista negra de la celda, offset, etc..)

  - Configuración de Reporte: especifica los eventos que requieren al UE enviar un mensaje de reporte
  - Identificador de Medición: ID que identifica los objetos de la medición
  - Configuración de Cantidad: identifica los valores a ser medidos por el UE
  - Medición de GAP: indica a que intervalo de celdas vecinas debe realizar mediciones el UE

- En el caso de celdas intrafrecuencia (celdas vecinas que utilizan la misma frecuencia de portadora de la celda de servicio actual), UE puede realizar la medición sin utilizar medición de gaps
- En el caso de celdas inter-frecuencia(celdas vecinas no utilizan la misma frecuencia), UE debe sincronizar con la frecuencia de las celdas vecinas antes de realizar las mediciones

(2) Generación Reporte Medición

- UE reporta el resultado de la medición de forma periódica o cuando se genera el evento de medición (establecido por el eNB)
- Existen diferentes tipos de eventos, A1, A2, A3, A4,A5, B1 y B2

Dependiendo de los resultados de las mediciones de señal, el eNB decide que tipo de Handover realizar a la celda destino, e inicia el proceso. Los Handovers pueden categorizarse

- **(1) Categorización 1 - Si las entidades EPC Cambian o no**
  - **Intra-LTE Handover**
    - **Intra-MME/S-GW Handover**. Ni el MME ni el S-GW que dan servicio al UE cambian después del Handover
  - **Inter-LTE Handover**. MME y/o S-GW cambian después del Handover
    - **Inter-MME Handover**. Cambia el MME pero no el S-GW
    - **Inter-S-GW Handover**. Cambia el S-GW pero no el MME
    - **Inter-MME/S-GW Handover**. Cambian tanto MME como S-GW
  - **Inter-RAT Handover**. Handover entre redes que utilizan diferente tecnología radio
    - **UTRAN a E-UTRAN**
    - **E-UTRAN a UTRAN**
- **(2) Categorización 2 - Si las entidades EPC son involucradas o no**
  - **Handover X2**. La interfaz X2 conecta ambos eNBs y esta disponible para realizar el Handover. Una vez completado el Handover, ambos eNBs se comunican para controlar el Handover, sin la necesidad de intervención del MME
  - **Handover S1**. La interfaz S1 conecta E-UTRAN (eNB) y EPC (MME para el control de mensajes, o S-GW para control paquetes de usuario). Si i) no existe conexión X2 entre los eNBs origen y destino, ii) existe conexión X2, pero no se le permite realizar Handovers, o iii) la preparación del Handover falla entre ambas celdas, se inicia el Handover S1. Una vez completado el Handover, la celda de servicio se comunica con la celda de destina a través del MME para controlar el Handover

El proceso de Handover consiste en 3 fases, preparación, ejecución y finalización

- **(1) Fase Preparación Handover** como veremos en la figura 7.11 de [8]
- **(2) Fase Ejecución Handover** como veremos en la figura 7.12 de [8]
- **(2) Fase Finalización Handover** como veremos en la figura 7.13 de [8]

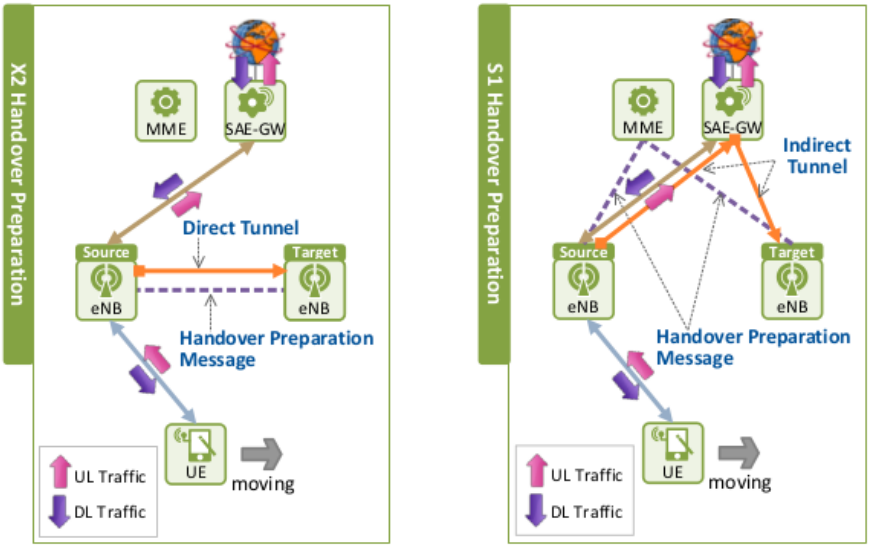


Figure 7.11: Fase de Preparación del Handover

Las etapas en las fase de preparación del Handover serían las siguientes:

- El eNB origen y el eNB destino se preparan para el Handover
- Si es un Handover X2, ambos eNBs se comunican entre ellos, en el caso de Handover S1, el MME se involucra a través de la señalización S1
- El eNB origen envía el contexto de usuario del UE al eNB destino para comprobar que el eNB destino pueda dar la calidad de servicio esperada
- Si el eNB destino es capaz, establece un bearer de transporte para el reenvío de paquetes
- El eNB destino asigna un valor C-RNTI para que el UE pueda acceder al eNB
- Al finalizar esta fase tendremos por tanto
  - En el caso de Handover X2, un bearer de reenvio que es un túnel de conexión directo entre los 2 eNBs
  - Handover S1,un túnel de conexión indirecto uniendo las entidades involucradas (eNB origen, eNB destino y MME)

En la fase de Preparación del Handover, como podemos observar en la Figura 7.12:

- UE desconecta el radio enlace del eNB origen y lo conecta al eNB destino, accediendo a la nueva celda
- Una vez los recursos necesarios para el reenvío de paquetes entre los 2 eNBS han sido asignados y los nuevos recursos para el UE también han sido asignados, los 2 eNBs están preparadas para realizar el Handover
- El eNB origen ordena al UE realizar el Handover enviándole un mensaje **Handover Command**
- UE accede a la nueva celda usando el C-RNTI que le había sido asignado en la Fase de Preparación
- Una vez llegan paquetes al eNB origen esté, los reenvía a través del bearer de reenvío al eNB destino que los almacena hasta que el UE haya completado el acceso
- Los paquetes de subida (UE –> eNB) no son reenviados hasta que el proceso de conexión al nuevo eNB destino este completo
- Una vez el UE haya completado el acceso radio al eNB destino, los paquetes de subida pueden ser inmediatamente reenviados al S-GW a través del eNB destino

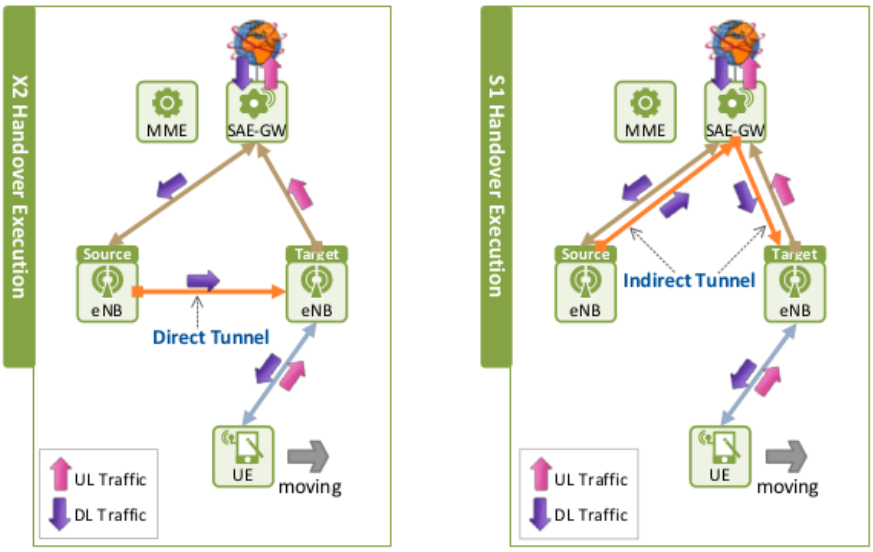


Figure 7.12: Fase de Ejecución del Handover

Una vez el UE completa su acceso radio al eNB destino, el nuevo bearer(DL) es conectado al eNB destino. Una vez el path se ha cambiado, el bearer de reenvío es liberado dando por finalizado el proceso de Handover En el Handover existe lo que se denomina

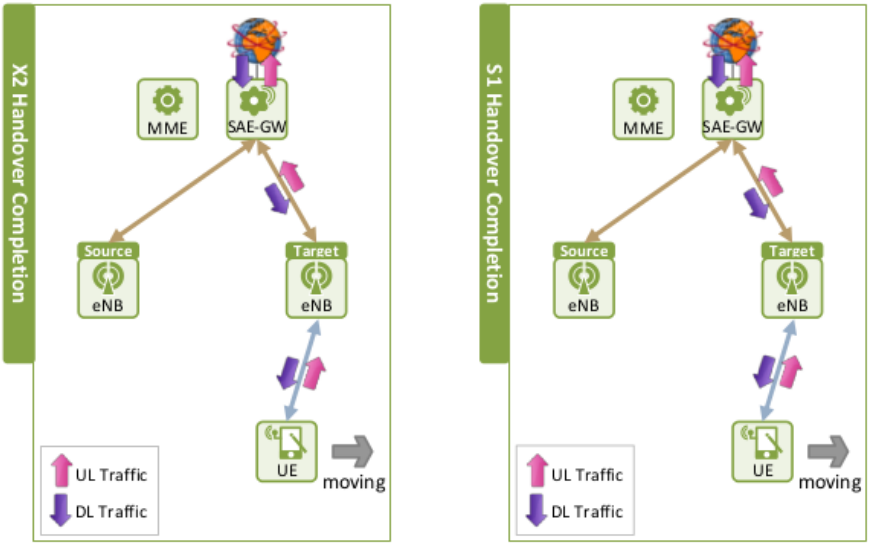


Figure 7.13: Fase de Finalización del Handover

Tiempo de Interrupción. Durante la fase de preparación del Handover, los entidades de red asignan recursos para asegurar que no se pierda ningún paquete. Sin embargo, es inevitable que exista un tiempo de interrupción. Durante este tiempo, los paquetes no pueden ser entregados entre el UE y las celdas. Si este tiempo es largo, no se puede dar un servicio sin interrupciones, y los usuarios sufren de una calidad pobre de servicio

El tiempo de interrupción de Handover incluye:

1. Tiempo necesario para la sincronización DL con el eNB destino
2. Tiempo de espera RACH

3. Tiempo necesario para enviar el preámbulo dedicado RACH para solicitar recursos UL
4. Tiempo necesario para que el eNB destino detecte el preámbulo y lo procese
5. Tiempo necesario para preparar el mensaje respuesta al RACH
6. Tiempo necesario para decodificar el mensaje respuesta al RACH
7. Tiempo necesario para informar al eNB destino que el UE ha completado el Handover
8. Tiempo necesario para obtener la confirmación del eNB destino de la finalización del Handover

Tal como hemos descrito con anterioridad, existían 2 tipos de Handover S1 y X2. El Handover X2 se realiza entre un eNB origen y un eNB destino a través de la interfaz X2. En las redes LTE, a diferencia de redes anteriores (2G y 3G), se permiten que eNBs realicen Handover sin la intervención de entidades EPC, utilizando el interfaz X2

- En el panel de control:
  - eNBs proveen a los usuario con señalización X2AP (X2 Application Protocol) a través de una conexión SCTP
  - En la capa X2AP, los usuarios son identificados por el eNB UE X2APID (Old eNB UE X2AP ID, New eNB UE X2AP ID)
- En el panel de usuario:
  - Los eNBs están conectados a través de un tunel GTP (GPRS Tunneling Protocol), como con los bearers S1/S5
  - Un único túnel GTP es creado para cada usuario, siendo identificado el túnel por su Tunnel Endpoint Identifier (TEIDs)

Función	**Procesos**
Gestión Movilidad	Preparación Handover Transferencia Estado SN Liberación Contexto UE Cancelación Handover
Gestión Carga	Indicación de Carga Iniciación del Reporte de Estado de Recursos Reporte de Estado de Recursos
Reporte de la Situación General de Errores	Indicación de Errores
Reconfiguración del X2	Reconfiguración
Configurando X2	Configuración X2
Actualización Configuración eNB	Actualización Configuración eNB Activación Celda
Gestión Parámetros Movilidad	Cambio en la Configuración de Movilidad
Optimización de la Robustez de la Movilidad	Indicación de Fallo en el Radio Enlace Reporte Handover
Ahorro Energía	Actualización Configuración eNB Activación Celda

Table 7.8: Funciones X2AP

En las redes LTE, el protocolo X2AP, provee funcionalidad Self-Organing Networks (SON). SON permite a un eNB conectar con un eNB vecino, recoger información de su estado, y utilizar esta información para automatizar la configuración y optimizar sus parámetros.

Entre las funciones X2AP las siguientes están relacionadas con SON:

- **Gestión Carga**. Mejora el rendimiento de interceptación entre celdas al intercambiar información de carga e interferencia
- **Actualización Configuración eNB**. Ejecuta la configuración automática de eNB
- **Gestión de Parámetros de Movilidad**. Negocia la información de configuración del inicio del proceso de Handover entre peers y utiliza esa información para optimizar el proceso
- **Optimización de la Robustez de la Movilidad**. Provee información de los eventos en el fallo del Handover

- **Ahorro Energía**. Ayuda al eNB a consumir menos energía intercambiando información de la activación/desactivación de la celda

Durante el proceso de Handover, se utilizan diferentes mensaje para la gestión de la movilidad. Entre ellos los siguientes mensajes:

- **Handover Request**. Mensaje utilizado durante la fase de preparación del Handover. Se envía del eNB origen al destino para informar del contexto de UE

- **Handover Request Acknowledge**. Preparación Handover. Lo envía el eNB destino al origen para informar que la asignación de recursos se ha completado con éxito

- **Handover Preparatin Failure**. Ejecución Handover. Se envía del eNB destino al origen informando si existe algún error en la asignación de recursos

- **SN Status Transfer**. Ejecución Handover. El eNB origen informa al destino desde que paquete de datos debe recibir y enviar

- **UE Context Release**. Finalización Handover. eNB destino informa al eNB origen que libere el contexto UE

- **Handover Cancel**. Preparación Handover. eNB origen envía al destino cuando necesita cancelar la preparación del Handover

A continuación en la tabla se describen en que etapas del proceso de Handover se utilizan los mensajes vistos con anterioridad

Proceso	**Mensaje Inicial**	**Mensaje Respuesta Éxito**	**Mensaje Respuesta Error**
Preparación Handover	Handover Request	Handover Request Acknowledge	Handover Preparatin Failure
SN Status Transfer	SN Status Transfer	-	-
UE Context Release	UE Context Release	-	-
Handover Cancel	Handover Cancel	-	-

Table 7.9: Mensajes utilizados en cada etapa del proceso de Handover

En el Anexo encontraremos la figura A.18 donde se describen las etapas del proceso de Handover X2

Con anterioridad había visto que existían 2 tipos de Handover y se ha explicado el proceso de Handover X2. El Handover S1 se produce entre un eNB origen y un eNB destino a través de la interfaz S1, que conecta el eNB con EPC. El eNB se conecta con MME a través de la señalización S1AP en el panel de control, y comunica con el S-GW a través del túnel GTP en el panel de usuario.

De forma general, cuando se introduce un nuevo eNB

- eNB envía un mensaje **S1 Setup Request** que contiene eNB ID, eNB Name, TAC, al MME
- El MME devuelve un mensaje **S1 Setup Response** con la información necesaria para establecer la conexión, GUMMEI, MME Name, Relative MME Capacity
- El Relative MME Capacity expresa la capacidad de gestionar conexiones UE, y es un parámetro que permite realizar un balanceo de carga entre MMEs
- Los eNBs conectados a más de un MME, utilizan este valor cuando seleccionan un MME para establecer la conexión

La conexión UE entre eNB y EPC

- En el panel de control, cada señalización de usuario entre eNB y MME se realiza a través de la conexión de señalización **S1 Application Protocol(S1AP)** identificándose mediante eNB UE S1AP, MME UE S1AP ID
- En el panel de usuario, cada Bearer S1 de UE entre el eNB y el S-GW se establece a través de un **túnel GTP (GPRS Tunneling Protocol)** identificándose con DL S1 TEID (S1 eNB TEID) y UL S1 TEID(S1 S-GW TEID)

Proceso	**Mensaje Inicial**	**Mensaje Respuesta Éxito**	**Mensaje Respuesta Error**
Preparación Handover	Handover Required	Handover Command	Handover Preparation Failure
Asignación Recursos Handover	Handover Request	Handover Request Acknowledge	Handover Failure
Cancelación Handover	Handover Cancel	Handover Cancel Acknowledge	-
Liberación Contexto UE	UE Context Release Command	UE Context Release Complete	-
Transferencia Estado SN	eNB Status Transfer MME Status Transfer	-	-
Notificación Handover	Handover Notify	-	-

Table 7.10: Procesos y Mensajes involucrados en el proceso de Handover S1

En paginas anteriores habíamos visto los mensajes existentes en el Handover X2. En el Handover S1 asimismo, existe otra variedad de mensajes utilizados. A continuación los describimos

- **Handover Required**. Se utiliza en el Handover Preparation. Lo envía el eNB origen al MME, y incluye información del eNB destino y los recursos asignados a la celda
- **Handover Request**. Se utiliza en el Handover Preparation. Enviado del MME al eNB destino incluyendo el contexto de UE
- **Handover Request Acknowledge**. Se utiliza en el Handover Preparation. Enviado por el eNB origen al MME cuando los recursos en el eNB destino son asignados correctamente. Recursos asignados
  - Bearer S1, identificado por su DL S1 TEID, para después del Handover
  - Bearer S1, identificado por su DL S1 TEID, para utilizar durante el proceso de Handover
- **Handover Command**. Se utiliza en el Handover Preparation. Enviado por el MME al eNB origen incluyendo la información necesaria para el acceso UE
  - Acceso al eNB destino, C-RNTI, Algoritmo Seguridad AS eNB destino, DRB ID
  - Bearer S1, identificado por su UL S1 TEID, para utilizar durante el proceso de Handover

- **eNB Status Transfer**. Se utiliza en el Handover Execution. Enviado por el eNB al MME informándole a partir de que paquete el eNB destino debe enviar o recibir
- **MME Status Transfer**.Se utiliza en el Handover Execution. Enviado por el MME al eNB destino informándole a partir de que paquete el eNB destino debe enviar o recibir
- **Hanover Notify**.Se utiliza en el Handover Completion. Enviado por el eNB destino al MME informándole que el UE ha completado el Handover
- **UE Context Release Command**. Se utiliza en el Handover Completion. Enviado por el MME al eNB origen indicándole que libere el contexto de UE
- **UE Context Release Complete**. Se utiliza en el Handover Completion. Enviado por el eNB origen al MME confirmando que se ha liberado el contexto de UE

En el Anexo encontraremos la figura A.19 donde se describen las etapas del proceso de Handover S1

Chapter 8

Control de Políticas y Facturación (PCC)

8.1 Introducción

En las redes LTE, un usuario establece con el operador de red el tipo de servicio que va a contratar. El operador de red determina para cada tipo de servicio, que recursos son necesarios asignar y como se va a facturar dicho servicio. Una vez que el usuario establece una sesión EPS el PCRF determina la regla **PCC (Policy and Charging Control)** a utilizar para cada uno de los **SDF (Service Data Flow)** basándose en la política del operador. El **PCEF (P-GW)** detecta cada SDF y aplica una regla PCC especifica para cada uno de los SDFs. El PCEF, asimismo, identifica la QoS a aplicar a los SDF y al canal. Esta información es gestionada por cada una de las entidades EPS(UE, eNB,S-GW, P-GW y MME)

8.2 Reglas PCC

El **Objetivo** de las reglas PCC lo podemos determinar en 4 puntos:

- Detectar los paquetes que pertenecen a un SDF
- Identificar los servicios asociados
- Aplicar los correspondientes parámetros para su facturación
- Proveer de las correspondientes políticas de control

Estas reglas aplican a diferentes SDF. Los paquetes IP son clasificados en SDF a partir de los SDF Templates. Por tanto, cada regla PCC es aplicada a cada uno de estos SDFs.

Las reglas pueden ser de 2 tipos:

- Dinámicas. Reglas dinámicamente asignadas por el PCRF al P-GW
- Estáticas. Predefinidas por el operador de red y activadas por el P-GW

Por definición, una regla PCC se compone de los siguientes elementos:

- Nombre de la Regla PCC
- Service ID. Identificador de servicio
- SDF Template
- Parámetros QoS
- Parámetros de Facturación
- Dependencias del operador

El funcionamiento básico de las reglas PCC sería el siguiente

- El PCRF determina una regla PCC para cada SDF y la remite al PCEF(P-GW) a través de la interfaz Gx
- El P-GW fuerza cada regla PCC a cada SDF
- El P-GW identifica cada flujo IP a cada SDF que pertenece y le aplica la regla PCC correspondiente

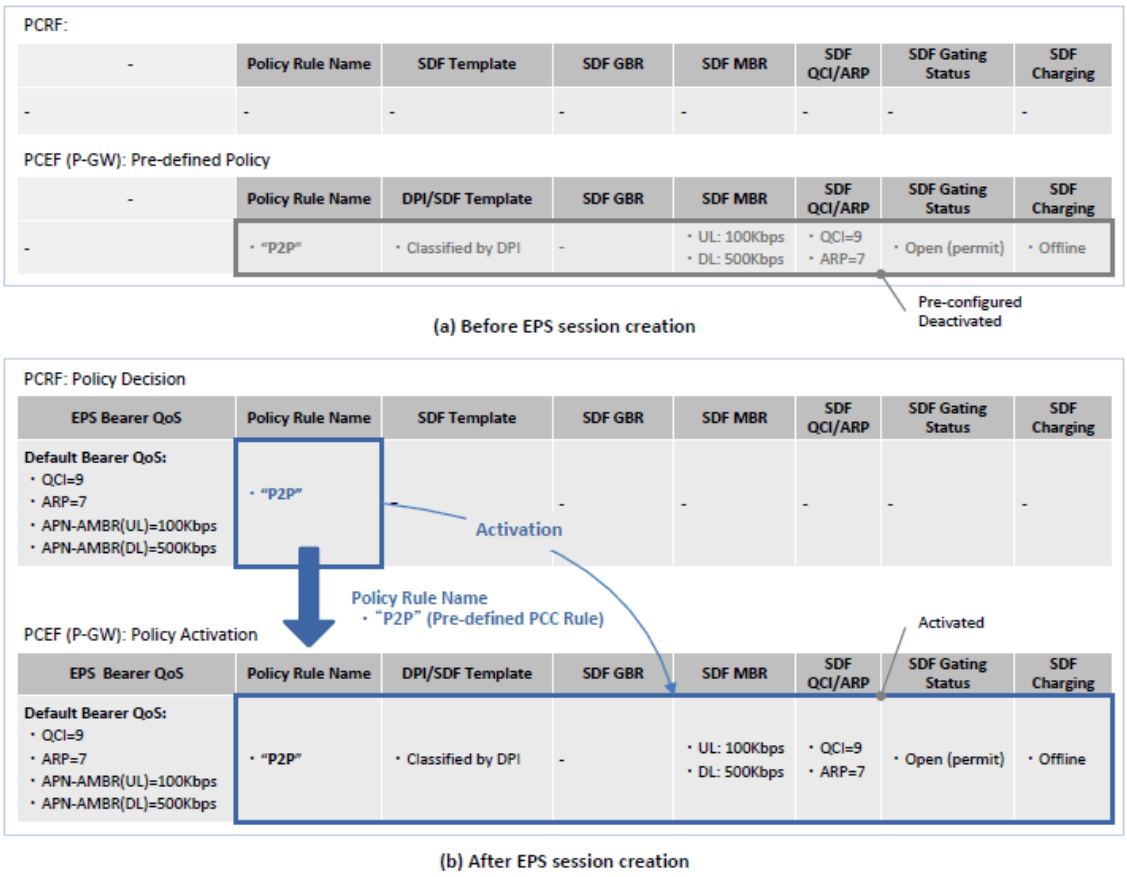


Figure 8.1: Ejemplo de reglas predefinidas

Existen reglas predefinidas por el operador e inicialmente inactivas (p.e. regla 'P2P' para limitar el ancho de banda de este servicio) en el P-GW. Una vez el PCRF identifica la necesidad de aplicar esta regla a un SDF, le pasa el nombre de la regla al P-GW. El P-GW activa y aplica esta regla al SDF correspondiente

Tal como hemos visto con anterioridad las reglas se pueden diferenciar a partir de su tipología al ser dinámicas o estáticas. Entraremos un poco más en detalle en la definición de la tipologia principal, Dinamica. En el caso de las reglas dinámicas algunas de sus características principales serían las siguientes:

- Se activan con determinados eventos
- Una vez creada la sesión el PCRF identifica la necesidad de crear reglas para cada tipos de servicio diferente
- El PCRF indica al P-GW las reglas a aplicar a cada trafico IP (SDF)
- El P-GW aplica esta regla y adicionalmente el QoS a cada SDF. Posteriormente, se crean los correspondientes canales para cada SDF
- Cada canal tiene asociado una serie de parámetros asociados a su QoS

En la siguiente figura podremos ver un ejemplo de regla PCC dinámica El PCRF identifica la necesidad de crear 3 reglas para

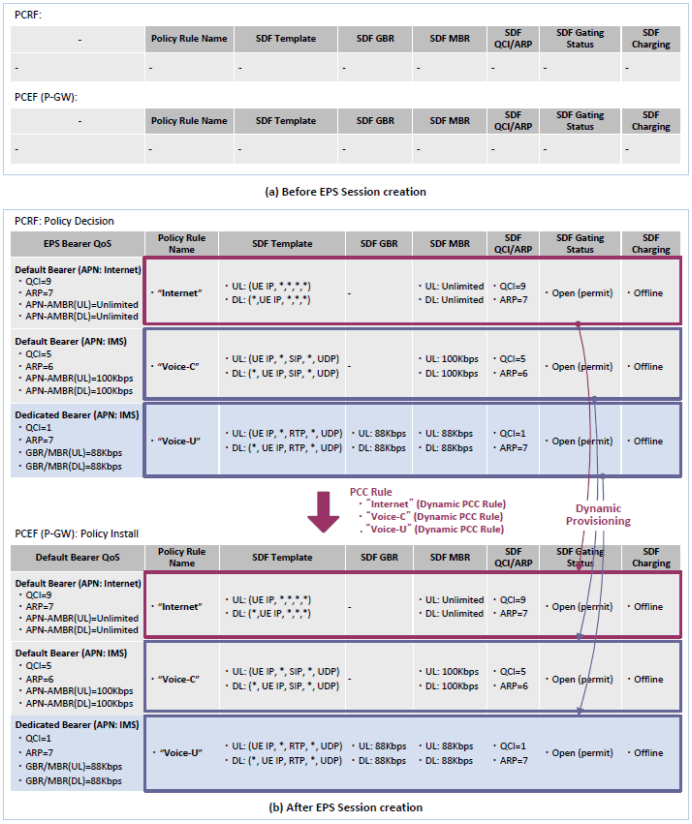


Figure 8.2: Ejemplo de regla PCC dinámica

diferentes tipos de servicio, tráfico 'Internet', tráfico de señalización de SIP 'Voice-C' y tráfico de voz 'Voice-U'.

- Regla Internet. Soporta un MBR ilimitado permitiendo máximo ancho de banda para el acceso a Internet. La regla aplica al canal por defecto. APN-AMBR(UL/DL) definido como ilimitado

- Regla 'Voice-C'. Aplica al canal por defecto soportando un APN-AMBR(UL/DL) de 100Kbps

- Regla 'Voice-U'. Aplica a trafico de voz. Mientras esta activa la llamada se establece un canal dedicado permitiendo un GBR(UL/DL) de 88Kbps.

El PCRF provisiona todas las reglas al P-GW a través de la interfaz Gx. El P-GW fuerza las reglas PCC a los paquetes IP

8.3 Procesos

Para poder entrar en detalle de los procesos involucrados en el establecimiento de sesiones EPS, veremos un ejemplo del establecimiento de una sesión de voz. La siguiente figura describe los procesos que se dan lugar durante el establecimiento. Seguiremos cada uno de los procesos que se producen para poder describirlos un poco más en detalle.

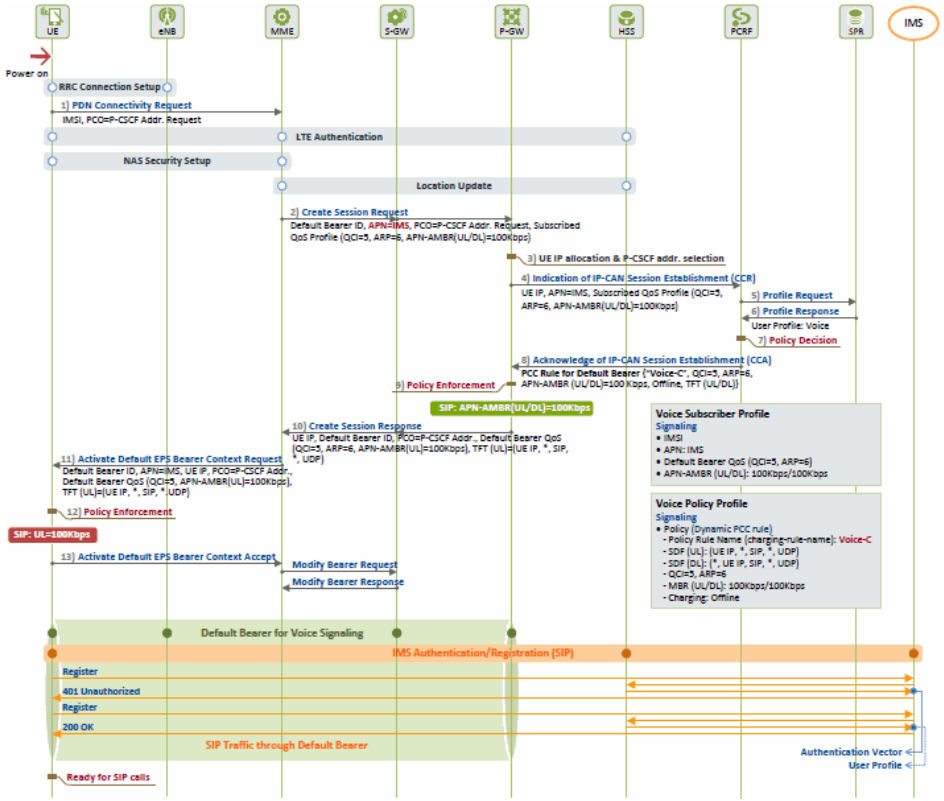


Figure 8.3: Sesion voz y Establecimiento del bearer por defecto

- **1) Solicitud [UE -> MME] PDN Conectividad**
  UE solicita acceso a la red IMS enviando un mensaje de Solicitud de Conexión PDN al MME. El campo de Opciones de Configuración del Protocolo(PCO) en ese mensaje EMS se utiliza para pedir la IP del P-CSCF (Proxy Call Session Control Function). El mensaje es incluido en un mensaje de Petición de Conexión y enviado al MME.
- **2) [MME -> P-GW] Solicitud de Creación de sesiones de voz**
  MME obtiene del HSS un APN y el perfil de suscripción durante una Actualización de localización. Del APN, MME recoge la necesidad de crear un canal por defecto para el servicio de voz y un ID para el canal (para la señalización SIP). El perfil de suscripción contiene un QoS (QCI=5, ARP=6, APN-AMBR=100Kbps) que debe ser aplicado al canal por defecto. MME prepara un mensaje de Petición de Creación de Sesión contiene el ID del canal por defecto, APN, PCOy el perfil de suscripción QoS, y se lo envía al P-GW. En eses momento, el campo PCO recibido por UE es enviado al P-GW de forma transparente.
- **3) Asignación de direcciones [P-GW] UE IP y P-CSCF**
  P-GW asigna una IP al UE para el APN IMS, y selecciona la dirección del P-CSCF y un nodo de control del IMS
- **4) [P-GW -> PCRF] Notificación de EPS Sesión Establecimiento**
  P-GW envía el perfil de suscripción QosS del usuario al PCRF enviándole un mensaje de Petición de Control de Crédito (CCR), solicitando autorización.
- **5) 6) [PCRF, SPR] Obtención del Perfil del usuario**
  PCRF puede obtener un perfil de suscripción del usuario del SPR, y lo utiliza para determinar una política PCC para el servicio de voz

- **7) [PCRF] Decisión Política**

  Basando en el perfil de suscripción, el PCRF dedica la política para la sesión EPS. Como el ejemplo era para señalización SIP,la regla seleccionada es 'Voice-C'

  - Regla 'Voice-C': QCI=5, ARP=6, APN-AMBR(UL/DL)=100Kbps, Regla de Facturación =Offline, Filtrado de paquetes SIP

- **8) [P-GW <- PCRF] Provisión de Regla PCC**

  PCRF envía la regla PCC ('Voice-C') a P-GW sobre la interfaz Gx.

- **9) [P-GW] Política de Cumplimiento**

  Una vez recibida la regla PCC('Voice-C'), P-GW fuerza los parámetros de la política, y mapea los parámetros QoS del SDF al canal por defecto:

  - P-GW (SDF): QCI = 5, ARP = 6, MBR (UL / DL) = 100 Kbps / 100 Kbps, SDF Plantilla (UL / DL) = (UE IP, *, SIP, *, UDP) / (*, UE IP, SIP, *, UDP)

  - P-GW (Default portador): QCI = 5, ARP = 6, la APN = AMBR (UL / DL) = 100 Kbps / 100 Kbps, TFT (UL / DL) = (UE IP, *, SIP, *, UDP) / (*, UE IP, SIP, *, UDP)

- **10) [MME <- P-GW] Respuesta a la Creación de sesiones de voz**

  Como respuesta a la petición realizada en el punto 2, el P-GW envia un mensaje de Respuesta a la Creación de Sesión al MME. Este mensaje contiene el perfil aprobado de QoS y los parámetros de la política UL para ser reenviado al UE (p.e, APN-AMBR(UL), TLF(UL))

- **11) [UE <- MME] Solicitud de Contexto de Activación del Canal por defecto**

  El MME le pide al UE para que active el canal por defecto enviándole un mensaje de Petición de Activación del Canal EPS por Defecto. Este mensaje ESM, contiene un APN, UE IP, la dirección P-CSCF y los parámetros de la política enviados por el P-GW en un mensaje de Aceptación de la Conexión.

- **12) [UE] Política de Forzado: Contexto de Activación del Canal por defecto** UE fuerza la política de UL y activa el contexto portador por defecto.

  - UE: QCI = 5, la APN-AMBR (UL) = 100 Kbps, TFT (UL) = (UE IP, *, SIP, *, UDP)

- **13) [UE -> MME] Notificación de Contexto de Activación del Canal por defecto**

  El UE notifica al MME que el canal por defecto necesario para la entrega de mensajes de señalización SIPha sido activado enviando un mensaje de Aceptación del Contexto de Activación del Canal por defecto

Una vez el canal para la señalización SIP ha sido activado, el registro en la red IMS es realizado a través del canal.
Si nos centramos ahora en el siguiente ejemplo de modificación de la sesión de voz estableciendo un bearer dedicado para tal efecto,

podemos identificar las etapas involucradas en esta situación. La siguiente figura describe el escenario:

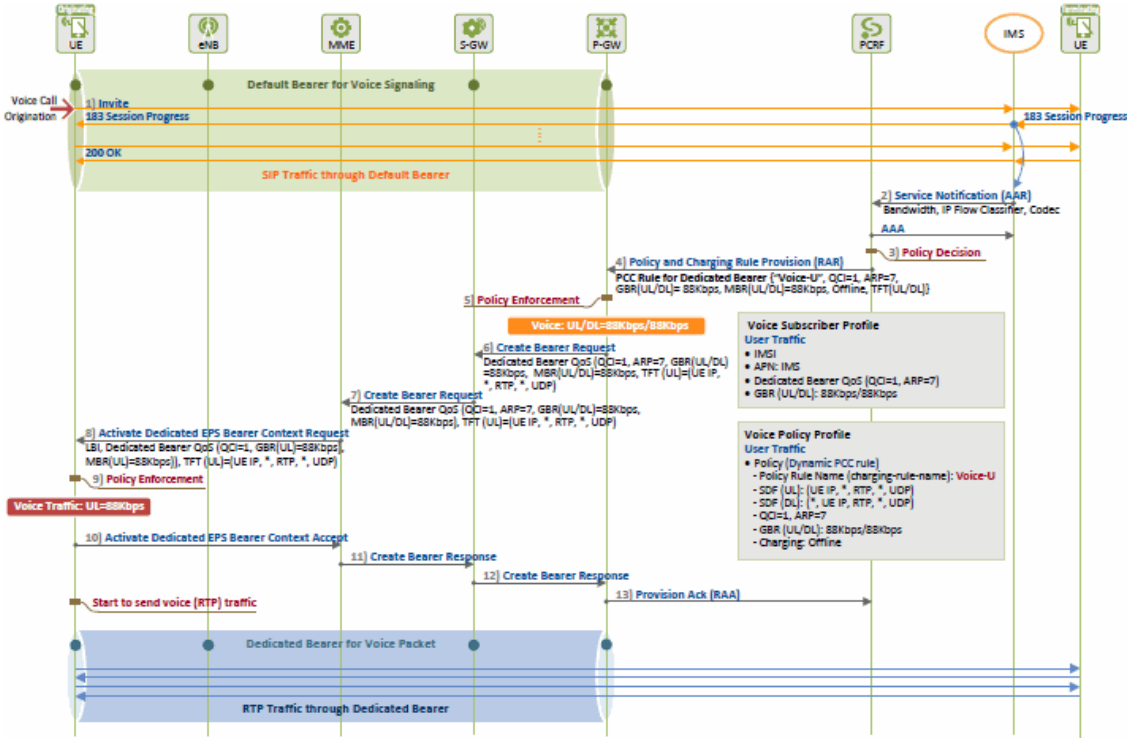


Figure 8.4: Modificación Sesión Voz y establecimiento Bearer Dedicado

- **1) [UE -> P-CSCF] Generación de la Llamada de voz**

  El UE solicita una llamada de voz enviando un mensaje **Invite** a la red IMS.

- **2) [PCRF <- P-CSCF] Información de Entrega de Servicios**

  Una vez recibido el mensaje SIP, la red IMS (P-CSCF) sabe que una llamada de voz ha sido solicitada. Entonces, envía un mensaje AAR al PCRF. El mensaje AAR contiene información como máximo/mínimo ancho de banda, identificador de flujo IP, etc..

- **3) [PCRF] Decisión Política**

  Basada en la información recibida del P-CSCF, el PCRF determina la política a aplicar a la sesión EPS seleccionando una regla PCC y un canal.Para la regla PCC, selecciona la regla 'Voice-U' que soporte paquetes de voz. Para la clase QoS y el canal, selecciona QCI=1. Como el canal por defecto no puede soportar este nivel, se crea un canal dedicado con un QoS deferente, modificando la sesión EPS existente

  – Regla 'Voice-U': QCI = 1, ARP = 7, GBR (UL / DL) = 88 Kbps / 88 Kbps, MBR (UL / DL) = 88 Kbps / 88 Kbps, la regla de carga: Desconectado, RTP Packet Filter

- **4) [P-GW <- PCRF] Regla PCC Provisión**

  PCRF entrega la regla PCC ('Voice-U') al P-GW sobre la interfaz Gx.

- **5) [P-GW] Forzado de Política**

  Una vez recibida la regla PCC('Voice-U'), el P-GW configura los parámetros Qos y la política de facturación, y mapea los parámetros Qos de SDF a los parámetros del canal dedicado

  – P-GW (SDF): QCI = 1, ARP = 7, GBR (UL / DL) = 88 Kbps / 88 Kbps, MBR (UL / DL) = 88 Kbps / 88 Kbps, SDF Plantilla (UL / DL) = (UE IP, *, RTP, *, UDP) / (*, UE IP, RTP, *, UDP)

  – P-GW (Canal Dedicado): QCI = 1, ARP = 7, GBR (UL / DL) = 88 Kbps / 88 Kbps, MBR (UL / DL) = 88 Kbps / 88 Kbps, TFT (UL / DL) = (UE IP, *, RTP, *, UDP) / (*, UE IP, RTP, *, UDP)

- **6) 7) [MME <- S-GW <- P-GW] Solicitud de Creación Canal Dedicado**

  P-GW envia al MME un mensaje de Solicitud de Creación de Canal,solicitando un canal dedicado. El mensaje contiene un Identificador de Canal Enlazado EPS (LBI), con el ID del canal dedicado, el QoS del canal y la información del TFT para el enlace de bajada. Los mensajes relacionados con el canal por defecto contienen el LBI, que indican el ID del canal al cual cada canal pertenece, y juega el papel de s

- **8) [UE <- MME] Solicitud de Activación de Contexto del Canal Dedicado**

  MME solicita la activación del canal dedicado enviando al UE un mensaje de Activación del Contexto del Canal EPS Dedicado. En este mensaje, se envían los parámetros de la política por el P-GW

- **9) [UE] Política de Cumplimiento: La activación de Dedicated Contexto Portador**

  UE fuerza la política de UL, y activa el canal dedicado.

  - UE: QCI = 1, GBR (UL) = 88 Kbps, MBR (UL) = 88K bps, TFT (UL) = (UE IP, *, RTP, *, UDP)

- **10) [UE -> MME] Notificación de Activación del Contexto del Canal Dedicado**

  UE notifica al MME que el canal dedicado para los paquetes de voz ha sido activado enviando un mensaje de Aceptación de Activación del Canal EPS Dedicado

- **11) 12) [MME -> S-GW -> P-GW] Notificación de la Creación Canal Dedicado**

  MME notifica al P-GW que el canal dedicado ha sido creado.

- **13) [P-GW -> PCRF] Notificación de la Regla Aplicada PCC**

  P-GW notifica PCRF que la regla de PCC ha sido forzada.

8.4 Trafico IP y Politicas PCC

Durante la gestión de la sesión EPS el flujo de paquetes IP se ve afectado siguiendo la política de las reglas PCC. En la siguiente figura se muestra como los bearer se modifican dependiendo del servicio actual.

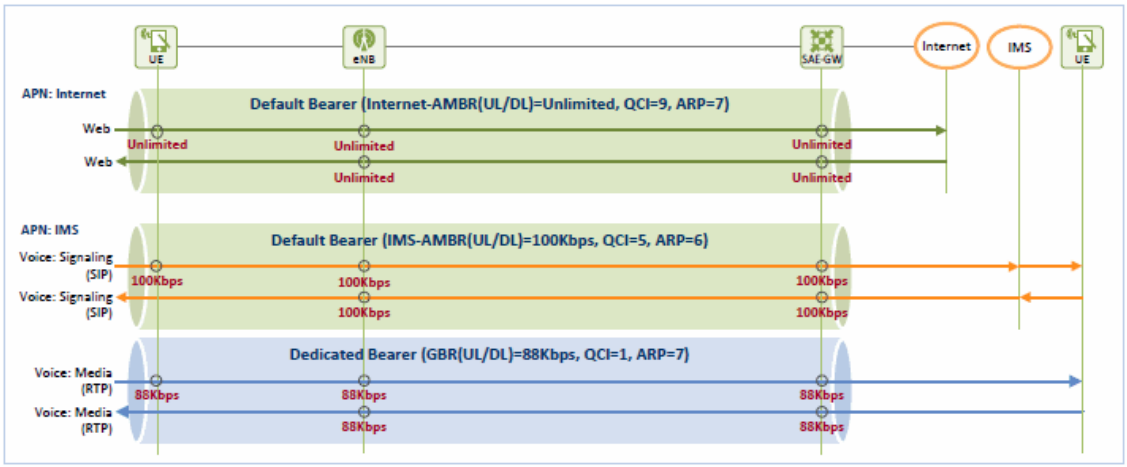


Figure 8.5: Flujos de paquetes IP en sesiones EPS

Tráfico IP generado por el UE es entregado al PDN Internet a través del canal por defecto que ha sido creado. En el caso del tráfico SIP de señalización es entregado al PDN IMS a través del canal por defecto. El tráfico de voz se entrega al receptor de la llamada a través de un canal dedicado creado específicamente para este servicio.

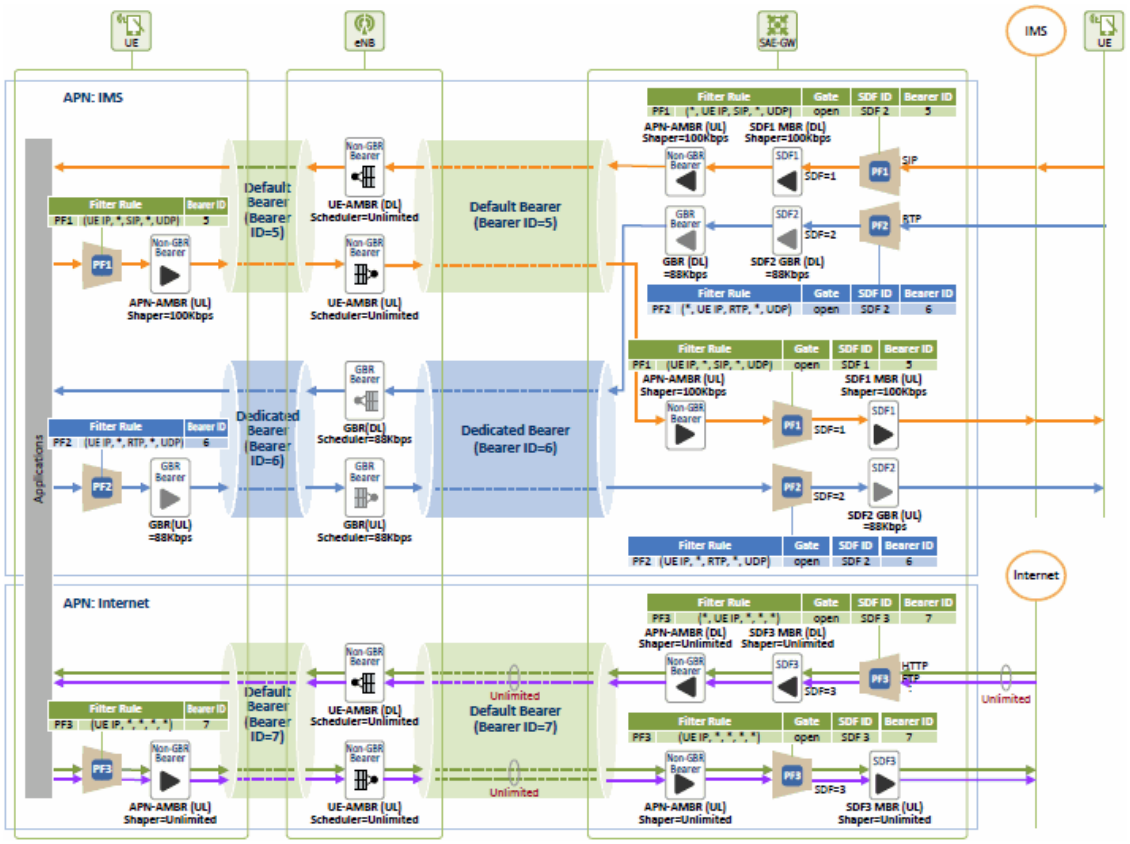


Figure 8.6: Ejemplo de aplicación de las políticas de control

La lista de políticas a aplicar son enviadas al P-GW. El P-GW identifica lo diferentes tipos de trafico IP a través de los SDFs y ejecuta la política de control especifica para cada uno de ellos. En el canal EPS, se han definido los parámetros QoS Correspondientes. La gestión de paquetes IP es diferente dependiendo del flujo de descarga: Bajada(Downlink o DL) o Subida(Uplink o UL). A continuación describiremos cada uno de los flujos identificacods

Ejemplo de aplicación de PCC: **Downlink**. Dependiendo del tipo de servicio

- **Tráfico SIP**
  - El tráfico es detectado como SDF1 por un filtro de paquete IP(PF1) en P-GW y se establece un MBR(100Kbps)
  - Se mapea el tráfico contra el canal por defecto estableciendo un APN-AMBR(100Kbps)
  - En el eNB se establece un UE-AMBR ilimitado
- **Tráfico Voz**
  - Es detectado como SDF2 por PF2 en el P-GW y se establece un GBR
  - Se mapea el tráfico contra un canal dedicado estableciendo un GBR hasta el P-GW
  - En el eNB se establece un GBR
- **Tráfico Internet**
  - Es detectado como SDF3 por PF3 en el P-GW y se establece un canal ilimitado
  - Se mapea el tráfico contra un canal por defecto estableciendo un APN-AMBR ilimitado
  - En el eNB se establece un UE-AMBR ilimitado

Ejemplo de aplicación de PCC: **Uplink**. Dependiendo del tipo de servicio

- Los paquetes llegan al UE de las aplicaciones de usuario.
- Los paquetes IP son mapeados por los filtros TFT a los canales correspondientes aplicando la QoS establecida
- El P-GW posteriormente, filtra este trafico IP que llega por los diferentes canales usando los SDF Templates, aplicando el correspondiente QoS a cada uno de ellos y reenviándolos a su destino
- **Tráfico SIP**
  - El tráfico es mapeado por PF1 al canal por defecto estableciendo un APN-AMBR de 100Kbps y enviado al eNB
  - En el P-GW, se establece un APN-AMBR de 100Kbps detectado por PF1 como SDF1
  - Por último, se establece un SDF MBR de 100Kbps y se envia a la red IMS
- **Tráfico Voz**
  - El tráfico es mapeado por PF2 al canal por defecto estableciendo un GBR y enviado al eNB
  - En el P-GW, se establece un GBR de 88Kbps detectado por PF2 como SDF2
- **Tráfico Internet**
  - El tráfico es mapeado por PF3 al canal por defecto estableciendo un APN-AMBR ilimitado y enviado al eNB
  - En el P-GW, se establece un APN-AMBR ilimitado detectado por PF3 como SDF3
  - Por último, se establece un SDF MBR ilimitado y se envía a la red Internet

Chapter 9

Facturación

9.1 Introducción

Un proceso importante dentro de las redes LTE es como los operadores de red, realizan la facturación de aquellos servicios ya consumidos o por consumir. La facturación de servicios en redes LTE puede ser categorizada de varias formas.

- Si categorizamos dependiendo del nivel:
  - Canal (p.e. EPC)
  - Subsistema (p.e. IMS)
  - Servicio (p.e. MMS)
- Si categorizamos dependiendo del tipo:
  - Online. Si la facturación se realiza a priori. Esto significa que primero se valida el saldo pendiente y se evalúa si es posible dar el servicio.
  - Offline. Si la facturación se realiza a posteriori

Podemos describir la facturación Offline como aquella en que al usuario se le factura por los servicios ya usados, es decir, el usuario primero recibe el servicio y posteriormente, el operador le factura por dicho servicio. El operador de red controla el servicio satisfecho por el usuario (recursos, bits, etc..) y envía un comando CDR (Charging Data Record) al dominio de facturación. La información del usuario es recogida al finalizar la sesión y facturada dependiendo del ciclo de facturación contratada por el usuario. A este tipo de servicio se le suele llamar 'de contrato'

En cambio la **Facturación Online** es aquella en que, una vez el usuario solicita acceso al servicio, el operador realiza una consulta a la cuenta del usuario y decide si dar permiso o no al servicio solicitado. En este caso, el servicio consumido por el usuario es controlado a tiempo real. Este control tiene un efecto inmediato en el servicio. En el caso que el usuario se quedará sin saldo, se dejaría de dar servicio de forma automática. A este tipo de servicio se le suele llamar de 'prepago'

9.2 Facturación Offline

En la figura anterior 9.1 de [9], podemos comprobar aquellas interfaces y elementos relevantes involucradas en el proceso de facturación offline:

- **Policy and Charging Rule Function (PCRF).** Encargado de seleccionar las reglas PCC a aplicar a los paquetes IP, SDF, y enviar dicha regla al P-GW a través de la interfaz Gx
- **P-GW.** Encargado de aplicar las reglas que el PCRF le transmite. En facturación Offline, genera mensaje CDR de acuerdo a las reglas de facturación del usuario y le remite dicho mensaje al Offline Charging System (OFCS) a través del interfaz Gz. En facturación Online, en cambio, primero obtiene la cuota de usuario y ,mide y reporta el uso del usuario al Online Charging System (OCS) a través de la interfaz Gy
- **Offline Charging System (OFCS).** Una vez recibidos los CDRs del P-GW a través del interfaz Gz, los postprocesa y envía la información necesaria al dominio de facturación

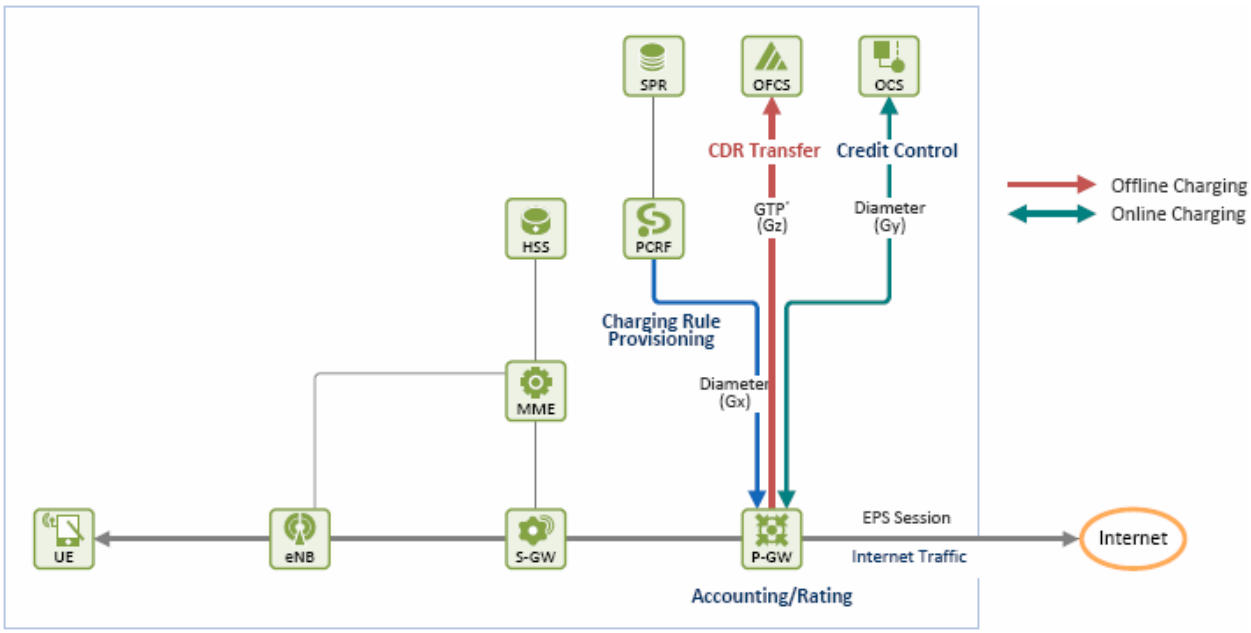


Figure 9.1: Arquitectura LTE de Facturación

- **Online Charging System (OCS).** Establece una cuota de usuario ejecutando un control de crédito con el P-GW a través del interfaz Gy

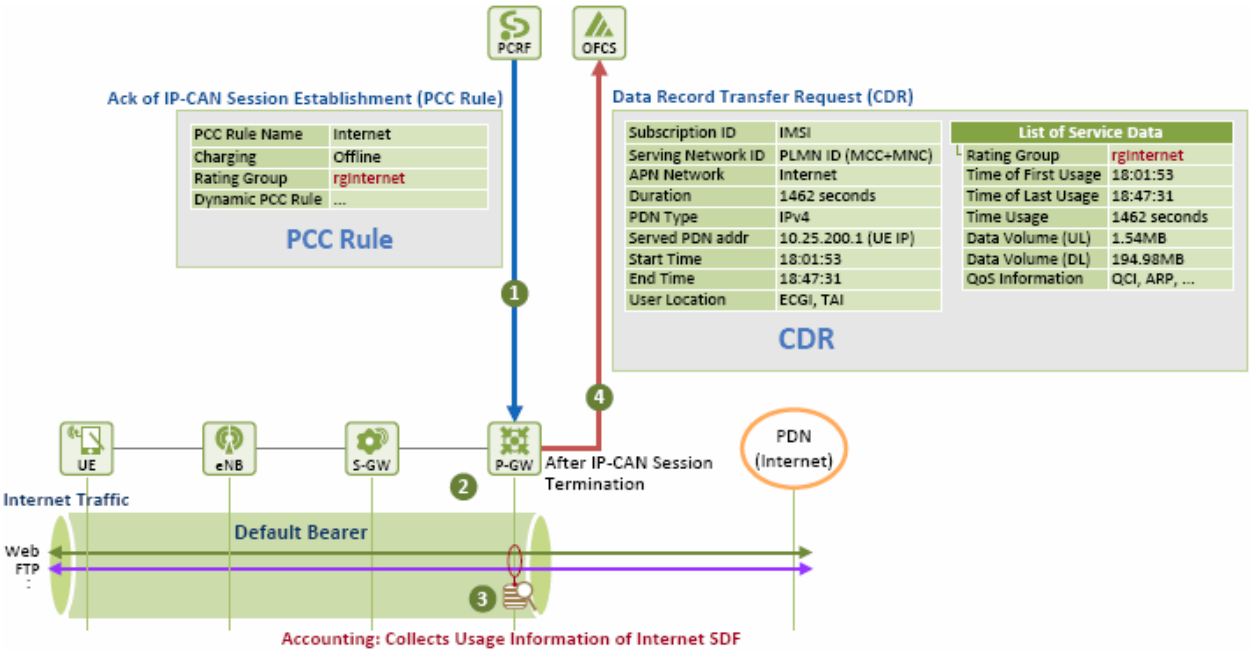


Figure 9.2: Regla de Facturación y Entrega CDR

1. PCRF selecciona una regla de facturación, como se describe en la Figura 9.2 de [9], y remite la regla, integrada en una regla PCC, al P-GW. En ese momento, el nombre de la regla de facturación es utilizado como nombre de la regla PCC. En dicha

regla se incluye información como tipo de facturación (online, offline), grupo facturación (precio/bits consumidos)

2. P-GW sabe a partir de la regla recibida que tipo de facturación es. Con esta dato determina que tipo de información de facturación debe ser controlada y a través de que interfaz debe remitir la información. Posteriormente, crea un canal por defecto, aplica la regla y genera un CDR, a partir del cual empezar a generar la información de facturación
3. P-GW empieza a controlar el tráfico IP que es entregado a través suyo y genera la información de facturación
4. Una vez terminada la sesión (o de forma periódica), el P-GW remite un mensaje CDR para registrar la información de facturación al OFCS. En este ejemplo se envía:
    - Información de usuario
    - Canal utilizado
    - Utilización de Recursos de red (bits entregados)
    - Información de uso
    - Información de servicio

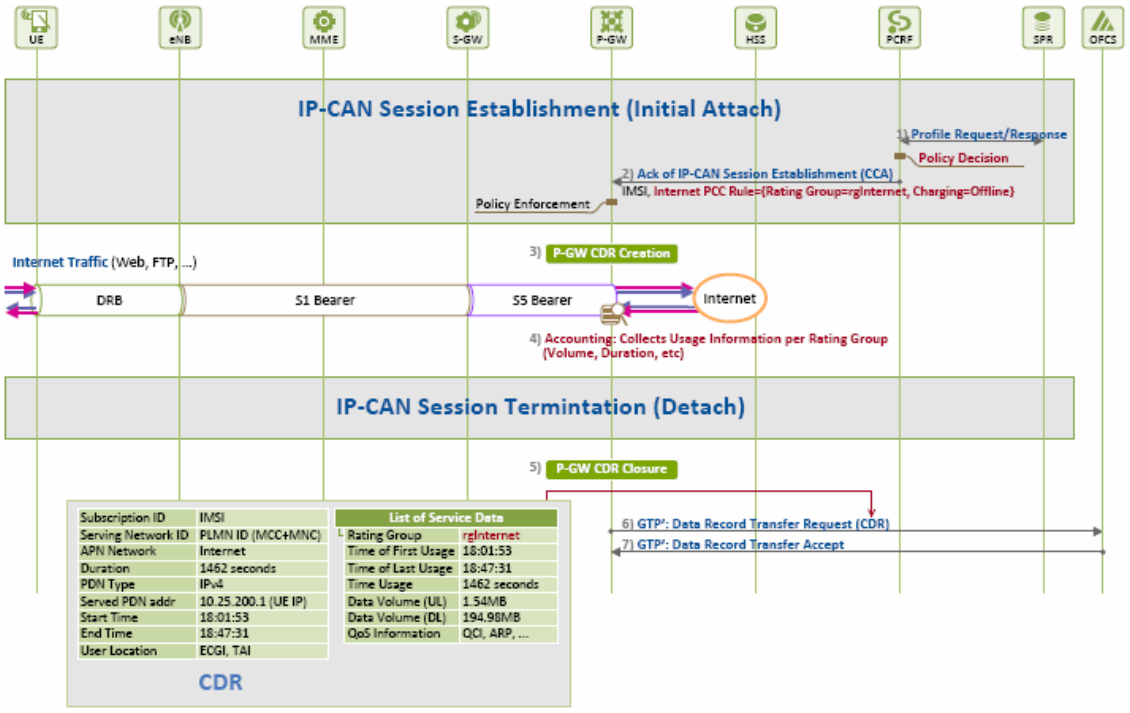


Figure 9.3: Procesos en Facturación Offline

A continuación describiremos cada una de las acciones involucradas durante el proceso de facturación, descrito en la Figura 9.3 de [9], así como los elementos que intervienen:

- **1) [PCRF <- SPR] Obtención de perfiles de usuario**

  Durante la conexión inicial, el PCRF solicita y obtiene la información de suscripción del usuario del SPR. Esta información servirá para determinar la regla PCC
- **2) [P-GW <- PCRF] Solicitud de establecimiento de sesión**

  PCRF determina la regla PCC a aplicar basándose en la suscripción de perfil. Esta información es remitida al P-GW mediante un mensaje CCA (Credit Control Answer). Este mensaje contiene el de regla de facturación
- **3) [P-GW] Creación CDR**

  El P-GW crea el canal por defecto de acuerdo a la regla PCC y fuerza la regla de facturación en el canal. Una vez forzada, el canal ya esta preparado para generar mensajes CDR

- **4) [P-GW] Generación de Información de Carga**
  Una vez el usuario empieza a utilizar el servicio de Internet, el P-GW guarda el uso de recursos de la red e información detallada del uso, para generar la información de facturación a entregar
- **5) [P-GW] Cierre CDR**
  El P-GW cierra el CDR una vez la sesión ha finalizado como consecuencia de la desconexión del usuario
- **6) [GW-P -> OFCS] Transferencia CDR**
  El P-GW envía el CDR al OFCS enviando un mensaje Data Record Transfer Request a través del protocolo GTP. Toda la información recopilada es entregada en dicho mensaje
- **7) [P-GW <- OFCS] Recepción de CDR Reconociendo**
  El OFCS informa al P-GW que ha recibido la información enviándole un mensaje de Data Record Transfer Accept
- Por último, una vez el OFCS ha recopilado todos los CDRs, los post-procesa y remite la información al dominio de facturación. Este se encarga de analizar la información para determinar cuanto debe cargar por el servicio.

Parámetro	**Descripción**	**Formato**
Subscription Identifier	Identifica el usuario al que se le factura	IMSI
Serving Networy Identify	Contiene el IP del PLMN del P-GW utilizado durante la solicitud de la localización	MCC+MNC
APN Network/Operator Identifier	Contiene el nombre lógico del APN que esta actualmente conectado al PDN	APN
APN Selection Mode	Indica como el MME selecciona el APN a utilizar	
Cause for Record Closing	Indica el motivo de la liberación del CDR	liberación normal/anormal
Charging ID	Idenficador de facturación. Utilizado para identificar el canal entre todos los registros creados en el S-GW y P-GW	
Duration	Duración del registro de datos	p.e. 3600sg
Dynamic Address Flag	Indica si la IP ha sido obtenida de forma dinámica o estática	Estática / Dinámica
Event Time Stamps	Identificador de tiempo para cada registro individual recogido	DD-HH:MM:SS
IMSI Unauthenticated Flag	Indica si el 'Served IMSI' no esta autenticado	
MS Time Zone	Contiene la 'Time Zone' facilitada por el MME. Esta información se transfiere del S-GW/P-GW durante la activación/desactivación del canal EPS	
P-GW Address Used	IP del P-GW	IP P-GW
P-GW PLMN Identifier	Identificador del PMLN del P-GW	MCC+MNC
PDN Connection ID	Utilizado para identificar los registros que corresponden a la misma conexión PDN. Con la IP del P-GW, identifica de forma única la conexión PDN	
PDN TYPE	Tipo de PDN	IPv4, IPv6
QoS Requested/QoS Negotated	QoS Requested: QoS solicitado por el UE cuando se activa el canal QoS Negotiated: QoS aplicado y aprobado por el PCRF	QCI, ARP
RAT Type	Tipo de tasa utilizado por el UE	EUTRAN(6)
Record Opening Time	Momento en el que se activa el canal EPS en el S-GW/P-GW	
Record Sequence Number	Contiene el numero de secuencia utilizado para linkar los registros parciales generador en el S-GW/P-GW para algun contexto MM o canal	
Record Type	Tipo de registro, p.e. SGW-CRD, P-GW CDR	PGW-CDR
S-GW Address Used	IP del S-GW	IP S-GW
Served IMSI	Indica el valor IMSI del UE	
Served PDN Address	IP asignada a la conexión PDN	IP UE
Serving Node Address	IP de los nodos de servicio (p.e. MME, S-GW)	
Serving Node PLMN Identifier	Identificador PLMN de los nodos de servicio	
Serving Mode Type	Tipo de nodo de servicio en el panel de control del P-GW o S-GW	
Start Time	Tiempo en el que la sesión EPS se inicia en el S-GW/P-GW	

Stop Time	Tiempo en el que la sesión EPS finaliza en el S-GW/P-GW	
User Location Information	Contiene la información de ubicación del usuario definida en el TS 29.274. Facilitada por el MME y transferida al S-GW/P-GW durante la activación/modificación del canal EPS	
List of Service Data	Incluye uno o mas contenedores de datos de servicio	
Charging Rule Base Name	Referencia al grupo de reglas PCC predefinidas en el PCEF	
Data Volume Downlink	Cantidad de datos en bytes transmitidos en el enlace de bajada	Bytes
Data Volume Uplink	Cantidad de datos en bytes transmitidos en el enlace de subida	Bytes
Local Sequence Number	Número de secuencia del contenedor de datos de servicio. Se va incrementando en 1 para cada contenedor de datos de servicio generado dentro de la vida de la sesión EPS	
QoS Information	QoS negociada y aplicada al canal	
Rating Group	ID del grupo de rating	
Report Time	Tiempo en que se cierra el contenedor de datos de servicio	
Service Condition Change	Motivo para cerrar el contenedor de datos de servicio	
Service Identifier	ID del servicio. Es utilizado para temas de reporting	
Service Specific Info	Mantiene información especifica del servicio para reglas PCC predefinidas	
Serving Node Address	IP del S-GW	IP S-GW
Time of First Usage	Tiempo cuando el primer paquete IP es transmitido	Fecha UTC
Time of Last Usage	Tiempo en el que el último paquete IP es transmitido	Fecha UTC
Time Usage	Tiempo utilizado	Segundos
User Location Information	Información de la ubicación del usuario mientras la información es recogida	TAI, ECGI

Table 9.1: CDR Parámetros

Chapter 10

Asignación de IPs

10.1 Introducción

La LTE es una red 'all IP' (todo IP) y proporcionan a los usuarios con 'always-on IP conectividad'. Cuando un UE se une a una red LTE, se le asigna una dirección PDN (Packet Data Network) y se establece un bearer (conexión UE a P-GW). Este bearer por defecto permanece conectado (es decir, la dirección IP asignada a la UE durante el primer adjuntar sigue siendo válida) hasta que la UE se separa de la red LTE. Se establece un bearer por defecto para cada APN (Access Point Name) que tiene un usuario por lo que una dirección IP única se le asigna por APN. Las direcciones IP asignadas pueden ser del tipo IPv4, IPv6 o IPv4/IPv6

10.2 Tipos de asignación de direcciones IP

A continuación describiremos el procedimiento de asignación de dirección IP

- UE se conecta a una red LTE y solicita una conexión al PDN
- P-GW asigna una dirección IP(es decir, dirección de PDN) que será utilizada por el UE en el PDN
- P-GW le envía la dirección IP al UE
- UE puede utilizar los servicios prestados a través del PDN
- Un P-GW asigna direcciones IP de 2 maneras: dinámica o estática
  - Dinámica. Se asigna automáticamente una dirección IP cada vez que el UE accede a la red
  - Estática. Asigna una dirección IP designada al UE a partir de su suscripción, a continuación, asigna la dirección IP designada cada vez que accede a la red

La asignación de IP dinámica es tal como sigue

- La red (por ejemplo, P-GW) selecciona automáticamente una dirección IP para UE
- El operador de red tiene IP de pool de provisión
- Cuando el UE se conecta ala red LTE, el P-GW asigna dinámicamente una dirección IP a la UE
- Conclusión, cada vez que un UE se conecta se le asigna una dirección IP dinámica

Mientras que la asignación de IP estática se describiría así:

- El operador de red asigna una dirección IP permanente a cada UE sobre su suscripción a la red.
- El operador tiene una dirección IP estática asignada reservada para el UE en la red (HSS), junto con otra información de suscripción
- Cuando el UE se conecta inicialmente a la red LTE, la P-GW obtiene la dirección IP estática de HSS, y lo envía al UE.
- Conclusión, esta dirección IP en particular se asigna a la UE cada vez que se conecta inicialmente a partir de entonces.

Al solicitar la conexión inicial, EL UE puede solicitar datos de protocolo relacionados con el protocolo externo / aplicación (por ejemplo, los parámetros de configuración) mediante el uso de opciones de protocolo de configuración (PCO) 2 parámetros (por ejemplo, la solicitud de la dirección del servidor DNS, la dirección P-CSCF) .

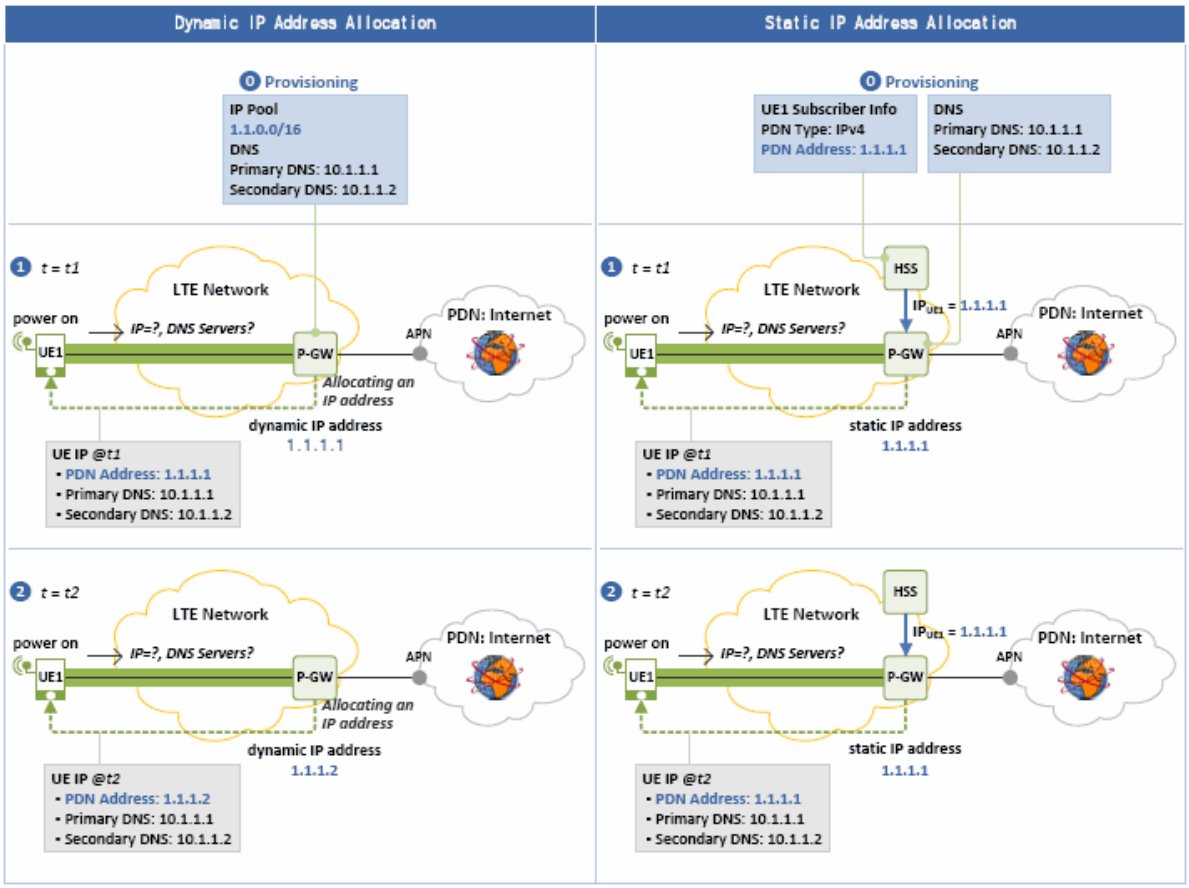


Figure 10.1: Tipos de Asignación dirección IP

10.3 Asignación de dirección IP dinámica

La red (P-GW) mantiene un listado de IP(s) para la UE, y dinámicamente asigna una dirección IP al UE en el momento de la conexión. Se muestra a continuación

Existe en el P-GW un listado de IP para asignar y las IPs de los servidores DNS ya provisionados A continuación describiremos el procedimiento que sigue un usuario A que intenta conectarse con su equipo UE a red LTE

1) [UE -> MME] Solicitud conexion por PDN.

El UE envía una solicitud de conexión al PDN enviando un mensaje a NME. Al mismo tiempo es solicitada una dirección IP para el servidor DNS. La petición de conexión es un mensaje ESM y además se adjunta en el mensaje, un mensaje EMM cuando es entregado.

2) 3) [MME -> S-GW -> P-GW] Solicitud Creación Sesión.

El MME, basándose en el perfil de usuario recibid del HSS,envía una mensaje de petición de creación de sesión al P-GW para la creación de una sesión EPS. Al ser una asignación de IP dinámica, no se actualiza el perfil de usuario con esta información. A la hora de enviar el mensaje de petición de creación de sesión se estable la dirección 0.0.0.0 en el campo de dirección, y la información de PCO recibida del UE se incluye en el campo PCO

4) [P-GW] Asignación de la dirección del PDN y del Servidor DNS.

El P-GW, después de chequear el tipo de PDN y la dirección [0.0.0.0], sabe que debe asignar una dirección IPv4. Selecciona una dirección IP de la pila y se la asigna al UE. Asimismo, le asigna una dirección IP al servidor DNS.

5) 6) [MME <- S-GW <- P-GW] Respondiendo a la Petición de Creación de Sesión.

Como respuesta a las peticiones realizadas en los puntos 2) y 3), el P-GW envía un mensaje de respuesta de Creación de Sesión

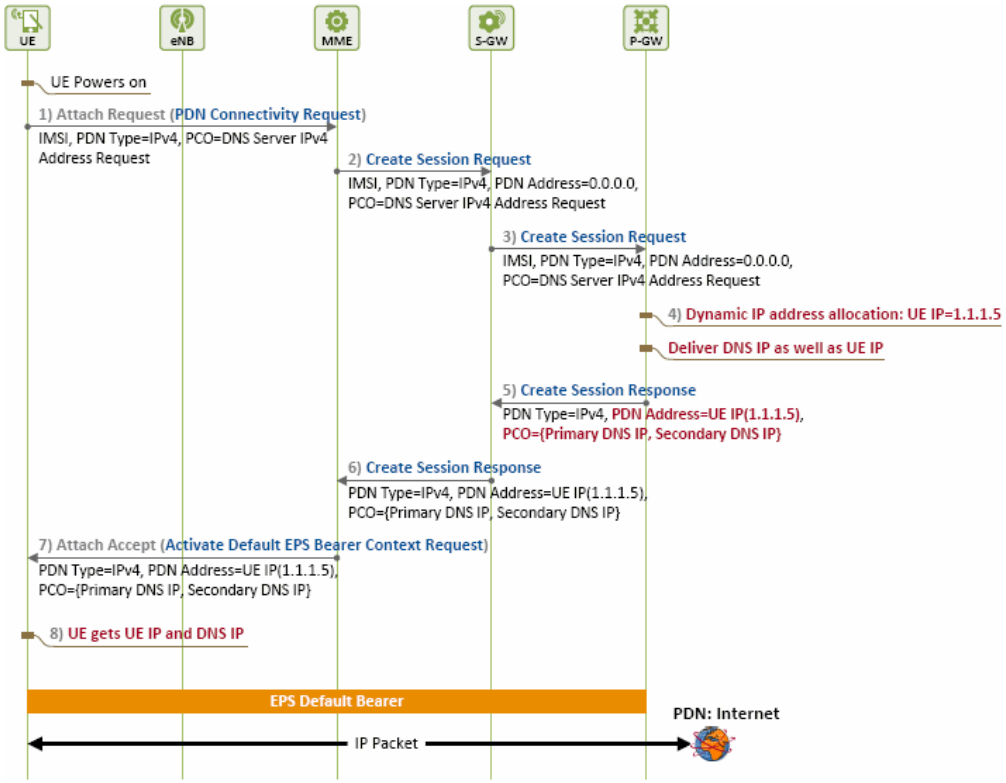


Figure 10.2: Proceso de asignación de IP dinámica

P-GW

- IP Pool: 1.1.0.0/16 (1.1.1.1 ~ 1.1.255.254)
- DNS server IP address: Primary DNS: 10.1.1.1
  Secondary DNS: 10.1.1.2

Figure 10.3: Provisionamiento IP en el P-GW

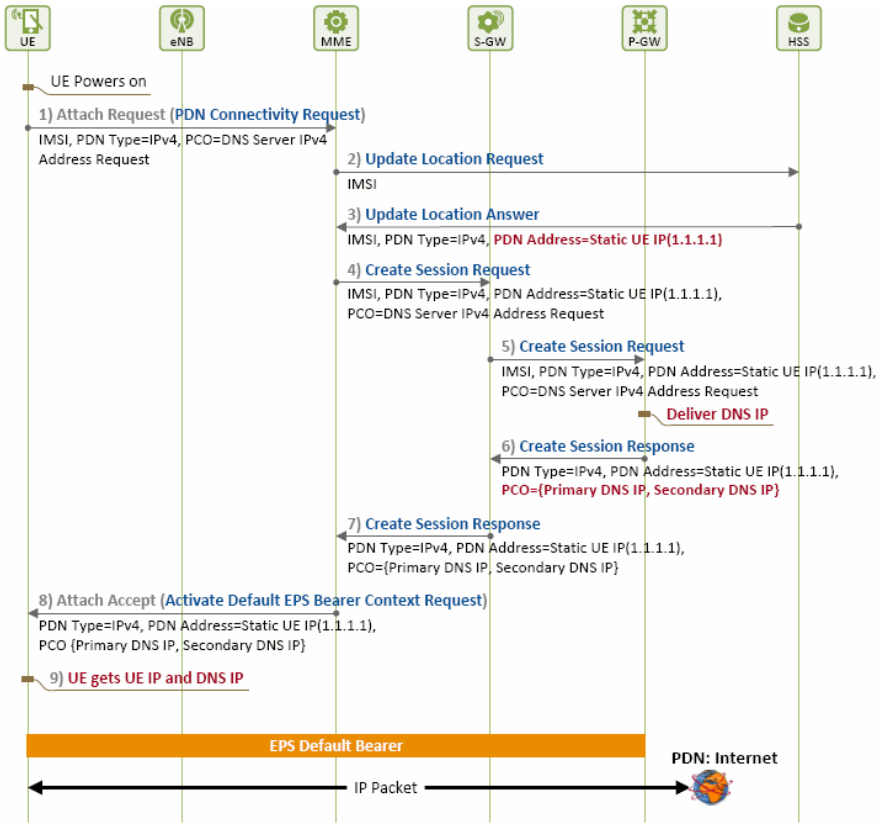


Figure 10.4: Procedimiento para la asignación de direcciones IP estáticas

al MME. Este mensaje incluye la IP asignada al UE en el campo dirección PDN, y la IP del servidor DNS en el campo PCO.

7) [UE <- MME] Petición de activación del canal por defecto.
El MME solicita la activación del canal por defecto enviando un mensaje de activación de solicitud de activación del EPS canal por defecto. Este mensaje ESM contiene la dirección IP del servidor DNS y del UE, y son añadidos al mensaje de aceptación EMM cuando es entregado.

8) [UE] Obtención dinámicamente de la dirección IP para usar el servicio PDN.
El UE obtiene la dirección IP y la dirección IP del servidor DNS. Un canal por defecto se establece entre el UE y el P-GW. El UE, ahora conectado al PDN(Internet) puede conectarse al servicio de Internet con su IP dinámica.

10.4 Asignación de dirección IP estática

El operador de la red asigna una dirección IP UE a un usuario cuando el usuario se suscribe a la red por primera vez, actualiza su perfil de suscripción en el HSS, y asigna la dirección IP estática almacenada en el perfil cada vez que intenta iniciar la conexion a la red. En HSS, se aprovisiona perfiles de suscripción de cada abonado. El perfil incluye un tipo de PDN y una dirección de PDN a usarse para la conexión PDN. En P-GW, las direcciones IP de servidor DNS ya se ha configurado. Un usuario se conecta a su UE intentando iniciar la conexión a la red LTE

1) [UE -> MME] Solicitud de conectividad PDN (Internet)
El UE solicita conexión PDN enviando un mensaje de petición de Conectividad PDN al MME (PDN type=IPv4, PCO=DNS Server IPv4 Address Request). En ese momento, además de una dirección IP para el UE, se solicita una dirección IP para los servidores DNS

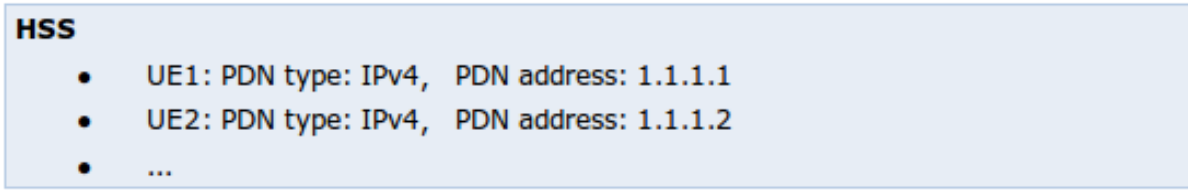


Figure 10.5: Provisionamiento IP en el HSS

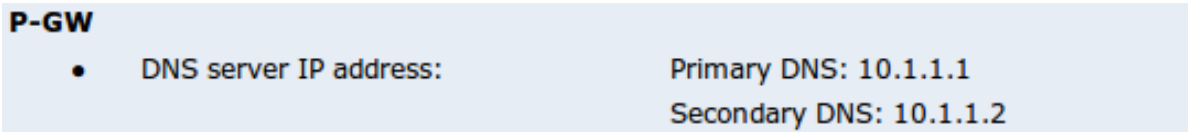


Figure 10.6: Provisionamiento IP en el P-GW

2) [MME -> HSS] Solicitando el registro a la Red LTE

El MME informa al HSS que la UE esta bajo su (por ejemplo MME1) Control enviando un mensaje de solicitud de actualización de la posición, y registra al UE en la red

3) [MME <- HSS] Respondiendo con el perfil de suscripción

El HSS, reconociendo que la UE se ha registrado en MME1, reenvía perfil de suscripción del UE a MME1 enviando un mensaje de respuesta de laActualización de su Ubicación (IMSI, PDN Type=IPv4, PDN Address=Static UE IP(1.1.1.1)). Este perfil de suscripción incluye la dirección IP estática asignada al UE.

4) 5) [MME -> S-GW -> P-GW] Solicitud de Creación Sesión

Después de recibir el perfil de suscripción de la UE desde el HSS, el MME conoce el UE tiene una dirección IP estática (1.1.1.1). El MME prepara un mensaje de petición de creación de sesión (IMSI, PDN Type=IPv4, PDN Address=Static UE IP(1.1.1.1), PCO=DNS Server IPv4 A y lo envía a la P-GW. En este momento el mensaje incluye la dirección IP estática recibida del HSS en el campo Dirección de PDN, y la información PCO recibida desde el UE en el campo PCO.

6) 7) [MME <- S-GW <- P-GW] En respuesta a la solicitud de Creación de sesión

Como respuesta a la solicitud formulada en los pasos 4) y 5), el P-GW y el S-GW envían un mensaje de solicitud de Creación de sesión (IMSI, PDN Type=IPv4, PDN Address=Static UE IP(1.1.1.1), PCO=Primary DNS IP, Secondary DNS IP) a la MME. Este mensaje incluye la dirección IP estática asignada al UE en el campo Dirección PDN, y las direcciones IP de los servidor DNS (solicitado por el usuario a través del campo PCO) en el campo PCO.

8) [UE <- MME] Petición de activación del canal por defecto

El MME solicita la activación del canal por defecto enviando un mensaje de solicitud de activación del canal de contexto por defecto EPS (PDN Type=IPv4, PDN Address=Static UE IP(1.1.1.1), PCO=Primary DNS IP, Secondary DNS IP). Este mensaje ESM contiene la dirección IP estática de la UE (1.1.1.1), así como las direcciones IP de servidor DNS y se incrusta en el mensaje de Adjuntar Aceptación, un mensaje EMM, cuando se entrega.

9) [UE] Obtención de dirección IP estática para el uso de servicio de PDN

La UE obtiene la dirección IP estática (1.1.1.1) y direcciones IP de los servidores DNS (Primary DNS IP = 10.1.1.1, IP DNS secundario = 10.1.1.2). Un canal por defecto se ha establecido entre la UE y el P-GW. La UE, ahora conectado a un PDN (Internet), puede utilizar el servicio de Internet con su dirección IP estática.

Como resumen podríamos concluir

- Existen 2 tipo de asignación IP: estática y dinámica
- Cuando un usuario solicita la conexión inicial, la red LTE provee al usuario con conectividad asignándole una IP y un canal
- Una vez validado el registro, la dirección IP y el canal se guardan en la información del perfil de suscripción

Chapter 11

Protocolo Diameter

11.1 Introducción

Diameter es un protocolo diseñado para proveer las funciones de **Authentication, Autorization y Accounting (AAA)**.

La **Authentication** es:

- Proceso por el que una entidad prueba su identidad ante otra.
- Normalmente la primera entidad es un cliente y la segunda un servidor.
- La Autenticación se consigue mediante la presentación de una propuesta de identidad y la demostración de estar en posesión de las credenciales que permiten comprobarla.
- Ejemplos de credenciales: contraseñas, tokens, certificados digitales, etc.

La **Authorization** es:

- El acto de determinar si la entidad que solicita un servicio/recurso tiene privilegios para acceder a éste.
- Se conceden privilegios específicos a una entidad o usuario basándose en su identidad, los privilegios que solicita, y el estado actual del sistema.
- Las autorizaciones pueden estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultaneas del mismo usuario, etc.
- Ejemplos: asignación de direcciones, asignación de rutas, asignación de QoS, cortafuegos, etc.

La **Accounting** es:

- El acto de recoger información de la utilización de recursos con el objetivo de planificar la capacidad, auditar, facturar o asignar coste.
- Para proporcionar accounting hay que hacer un seguimiento del consumo de los recursos de red por los usuarios.
- Típicamente se registra información tal como, identidad de usuario, tipo de servicio, fecha de inicio del uso o fecha fin de uso, etc.

11.2 Historia

Diameter se basa en el protocolo RADIUS. Como su nombre indica, Diameter proviene de la geometría (Diameter = 2 x Radius). Diameter fue estandarizado en Septiembre de 2003 a través del RFC3588 donde se establecen las bases del protocolo. En Octubre de 2012 apareció el RFC6733 que amplía y actualiza al RFC3588. Aunque Diameter esta diseñado para proveer funciones AAA, el protocolo base solo desarrolla la aplicación de Accounting. El resto de funciones/aplicaciones deben ser definidas a través de extensiones. Diversas aplicaciones Diameter se definen en su propios RFCs y hay aplicaciones propietarias.

Si hiciéramos una comparativa de Radius vs. Diameter podríamos remarcar las siguientes diferencias

- Control de errores:

  - RADIUS no implementa control de errores.
  - RADIUS se utiliza sobre UDP y una vez enviado un mensaje RADIUS/UDP se asume que probablemente llegará sin errores y en el orden adecuado al destino.
  - Diameter se implementa sobre transporte fiable (TCP o SCTP).
  - Diameter define ACKs de capa de aplicación y gestiona los errores.
- Seguridad:
  - RADIUS no proporciona confidencialidad.
  - Hay una opción de RADIUS sobre IPSec (RFC3162) pero no es obligatorio.
  - Diameter define que por defecto se debe aplicar confidencialidad a los mensajes mediante TLS o DTLS.
- Soporte para agentes:
  - El diseño RADIUS se basa en una arquitectura clásica cliente/servidor que no prevé un apoyo explícito a agentes (dispositivos intermedios).
  - Diameter define explícitamente los posibles agentes y su funcionalidad.
- Mensajes iniciados desde el servidor:
  - En RADIUS el soporte a mensajes iniciados desde el servidor es opcional.
  - Los mensajes iniciados desde el servidor permiten que el servidor inicie procesos reautenticación o reautorización.
  - En Diameter el soporte para mensajes iniciados desde el servidor es obligatorio.
- Auditabilidad
  - La auditabilidad permite detectar si agentes no confiables han alterado un mensaje (atributos o cabeceras).
  - RADIUS no define los mecanismos de seguridad y como resultado, dispositivos intermedios pueden modificar atributos o encabezados de paquetes sin ser detectados.
  - Diameter permite (de forma opcional) dar seguridad a cada atributo.
- Apoyo a la transición:
  - La unidad de datos de protocolo (PDU) de Diameter y RADIUS son distintas.
  - Sin embargo, se ha hecho un considerable esfuerzo para permitir la compatibilidad hacia atrás con RADIUS de modo que los dos protocolos puedan ser desplegados en la misma red.
- Negociación de capacidades:
  - RADIUS no soporta negociación de capacidades o flags obligatorio/opcional en sus atributos.
  - En RADIUS los clientes/servidores no son conscientes de las capacidades de cada uno.
  - Puede que no sean capaces de negociar con éxito un servicio aceptable para ambas partes, o en algunos casos, que ni siquiera sean conscientes de lo que ha sido implementado en un determinado servicio.
  - Esto si es soportado por Diameter.
- Descubrimiento y configuración de peers:
  - RADIUS requiere que el nombre o la dirección de los servidores o clientes se deban configurar de forma manual junto con los correspondientes secretos compartidos.
  - Esto da lugar a una gran carga administrativa y crea la tentación de reutilizar el secreto compartido (grave problema de seguridad).
  - En Diameter, a través del DNS se permite el descubrimiento dinámico de los peers.
- Soporte para roaming:
  - Diameter proporciona itinerancia segura y escalable utilizando encadenamiento de proxies (proxy chaining).
  - Ello facilita el roaming entre proveedores con Diameter.
  - Por su parte, RADIUS no proporciona apoyo explícito a proxies y carece de características auditabilidad y seguridad a nivel de transmisión.

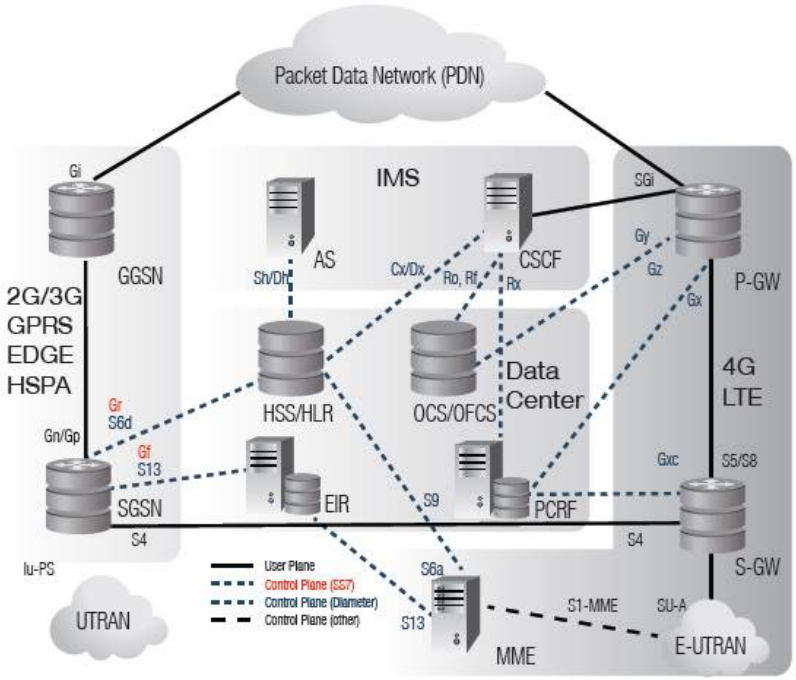


Figure 11.1: Diagrama de la red Diameter

11.3 Diseño

Siguiendo la estructura Lógica de Diameter, la aplicación se basa en una serie de comandos que amplían las capacidades del protocolo base (o vienen con él). Una aplicación esta formada por varios comandos y cada aplicación tiene un ID asignado por el IANA. Algunos ejemplos: Diameter Credit Control, Mobile IPv4, aplicaciones 3GPP como Cx, Gx, etc.

Tal como hemos comentado, dentro de cada aplicación Diameter existen los **Comandos Diameter**. Estos comandos definen una acción necesaria para poder ejecutar una aplicación Diameter. Cada comando tiene un ID (command code) y dos tipos de mensajes: **Solicitudes o Requests (R)** y **Respuestas o Answers (A)**. Algunos ejemplos de comandos Diameter serían: UAR (User Acceptance Request), UAA (User Acceptance Answer), etc.

Ya por último dentro de la estructura de Diameter, existen los **AVP (Attribute-Value Pairs)**. Los AVPs encapsulan información específica contenida en el comando y cada AVP tiene un ID. Algunos ejemplos: Origin-Host, Destination-Realm, etc.

El protocolo base especifica lo relativo a:

- Formato del mensaje
- Transporte
- Reporte de Errores
- Accounting
- Seguridad

Cualquier aplicación Diameter debe usar el protocolo Base de Diameter. El protocolo Diameter ha sido diseñado para ser muy extensible. Entre sus características principales:

- Definir nuevos valores AVP
- Creación de nuevos AVPs
- Crear nuevos comandos
- Crear nuevas aplicaciones

El perfil del transporte en Diameter ha sido definido en el RFC3539.

Los puertos por defecto para el protocolo base de Diameter son:

- 3868 para TCP y SCTP.
- 5658 para TLS y DTLS.

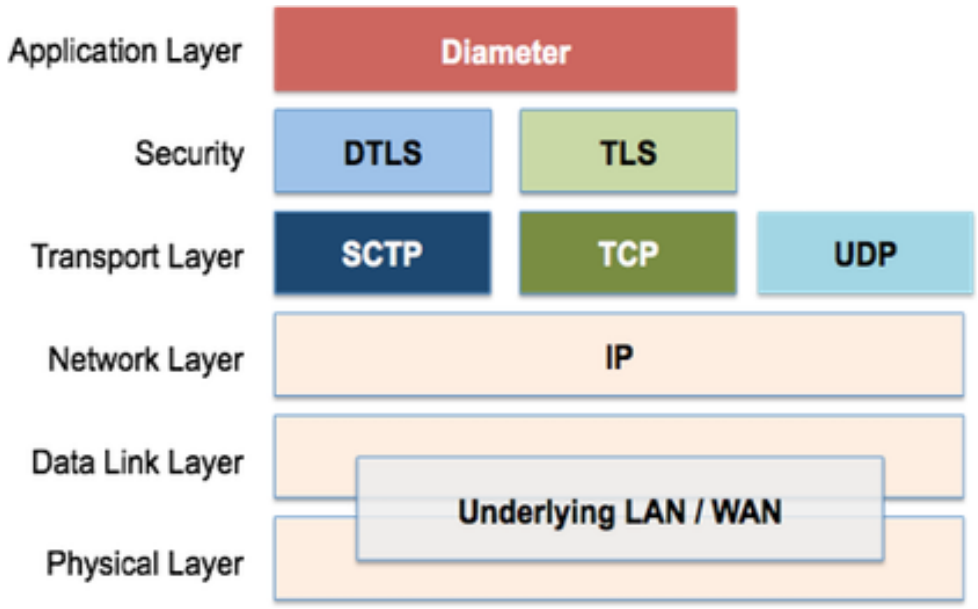


Figure 11.2: Pila Protocolos Seguridad en Diameter

Por tanto, los clientes Diameter deben soportar TCP o SCTP. Los agentes y servidores deben soportar ambos protocolos de transporte. El orden de protocolos de la capa de transporte a utilizar es la siguiente: primero TLS, seguido por DTLS, luego TCP y por ultimo SCTP.

Dentro de Diameter existe una **Terminología** importante que se debe tener claro a la hora de trabajar con el protocolo. Veremos a continuación algunos de los terminos que se deben conocer si se quiere trabajar con el protocolo

- **Peer**. Dos nodos Diameter que comparten una conexión de transporte se llaman 'peers'.
- **Nodo**. Un nodo es un host que implementa el protocolo Diameter.
- **Realm**. Es un dominio administrativo con el cual el usuario mantiene una relación de suscripción.
- **NAI (Network Access Identifier)**. Es un 'string' que contiene la identidad del usuario y de su realm. Ejemplo: alice@example.com.

Cuando dos peers Diameter establecen una conexión de transporte, deben intercambiar mensajes para anunciar sus capacidades (capabilities). Este proceso es denominado el **Intercambio de Capabilities**. Estos mensajes son:

- El CER (Capabilities-Exchange-Request).
- Su respuesta es CEA (Capabilities-Exchange-Answer).

El intercambio de estos mensajes permite el descubrimiento de la identidad del peer y sus capacidades (número de versión del protocolo, los identificadores de aplicaciones Diameter compatibles, mecanismos de seguridad, etc.).

Un peer solo envía comandos de una cierta aplicación a peers que han anunciado que soportan dicha aplicación.

Otro punto importante dentro de la terminología de Diameter, es saber la diferencia entre **Conexión vs Sesión**

- **Conexión** se refiere a una conexión a nivel capa de transporte entre dos peers que es utilizada para enviar y recibir mensajes.

- **Sesión** es un concepto lógico que existe entre un cliente y un servidor Diameter.

  Se identifica mediante el AVP Session-ID.

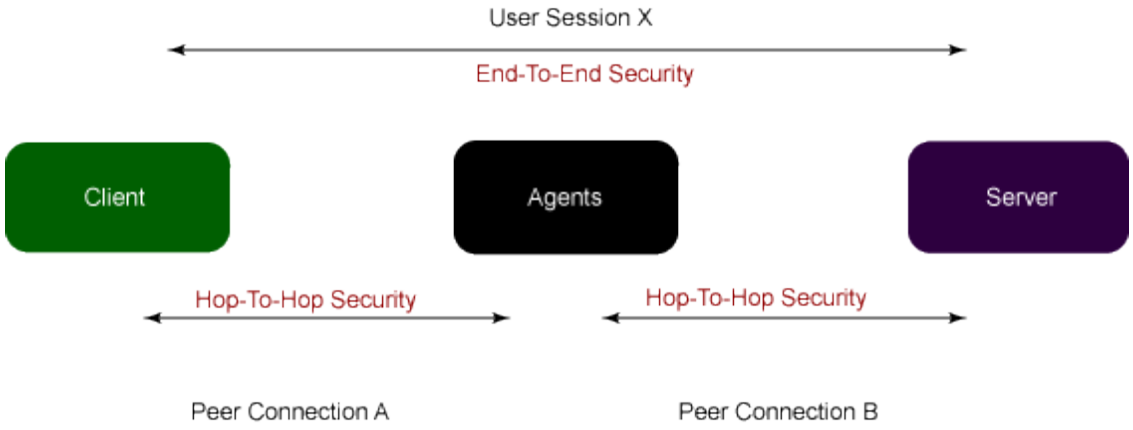


Figure 11.3: Sesión vs Conexión

Un **nodo Diameter** es un host que implementa Diameter. Existen tres tipos de nodos:

1. **Clientes**. Un cliente es un nodo Diameter que soporta aplicaciones Diameter y también, el protocolo base. Normalmente se sitúan en el limite de una red para facilitar el control de acceso a dicha red.
2. **Servidores**. Un servidor Diameter proporciona servicios de authentication, authorization y accounting. Debe soportar aplicaciones Diameter de servidor además del protocolo base.
3. **Agentes**. Un agente es un nodo Diameter que proporciona distintas funcionalidades tales como servicios de enrutamiento (relay y proxy), redirección (redirect) y traducción (translation).

Los **agentes Diameter** son útiles porque:

- Pueden ser utilizados para concentrar peticiones y distribuirlas (evitando tener un número de conexiones entre peers de orden N^2).
- Pueden distribuir la administración de sistemas de una forma mas configurable incluyendo la gestión de la seguridad.
- Pueden ser utilizados para balanceos de carga.
- Una red compleja puede tener múltiples orígenes de autenticación, los agentes pueden ayudar a filtrar solicitudes y redirigirlas a los nodos correctos.

Existen cuatro tipos de agentes: Relay, Proxy, Redirect y Translation.

Agente Relay

Los agentes Relay, aceptan peticiones y enrutan los mensajes a otros nodos Diameter basándose en la información que aparece en el mensaje. La decisión de enrutamiento se basa en una lista de realms soportados y peers conocidos. Esta información está en la **tabla de enrutamiento Diameter**. Los relays modifican el mensaje Diameter añadiendo o eliminando información de enrutamiento pero no modifican ninguna otra información del mensaje. No mantienen información del estado de la sesión pero si del estado de la transacción (Request/Answer).A continuación se muestra un ejemplo de Agente Relay.

1. Cliente Diameter hace una solicitud para acceder a un equipo.

   El cliente Diameter revisa en su tabla de enrutamiento cual es el siguiente nodo al que enviar el mensaje.

   Selecciona el Agente Relay y le remite el mensaje.
2. El Agente Relay realiza la misma operación, revisa la información del mensaje y la compara con su tabla de enrutamiento decidiendo que el siguiente nodo a quien enviar el mensaje, es el Servidor Diameter.
3. El servidor Diameter analiza la información y comprueba que puede dar servicio a la petición recibida.

   El servidor remite un mensaje de respuesta al Relay.

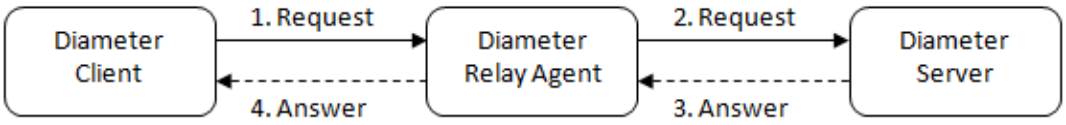


Figure 11.4: Agente Relay

4. El Relay remite la respuesta del servidor al cliente que inicio la petición.

Agente Proxy

Los agentes Proxy al igual que los relays enrutan los mensajes usando una tabla de enrutamiento Diameter. A diferencia de los relays modifican los mensajes Diameter y el hecho de poder modificar mensajes Diameter, permite a los proxies proporcionar servicios de valor añadido en la red Diameter. En el intercambio de capacidades, un proxy solo debe anunciar las aplicaciones que soporta (ya que debe entenderlas para modificarlas).

Agente Redirect

Los agentes Redirect, envían información del peer con el que el nodo que consulta debe comunicarse. No modifican mensajes ni mantienen información del estado de la sesión. Son útiles en escenarios donde la configuración de enrutamiento Diameter está centralizada. Algunos ejemplos de uso:

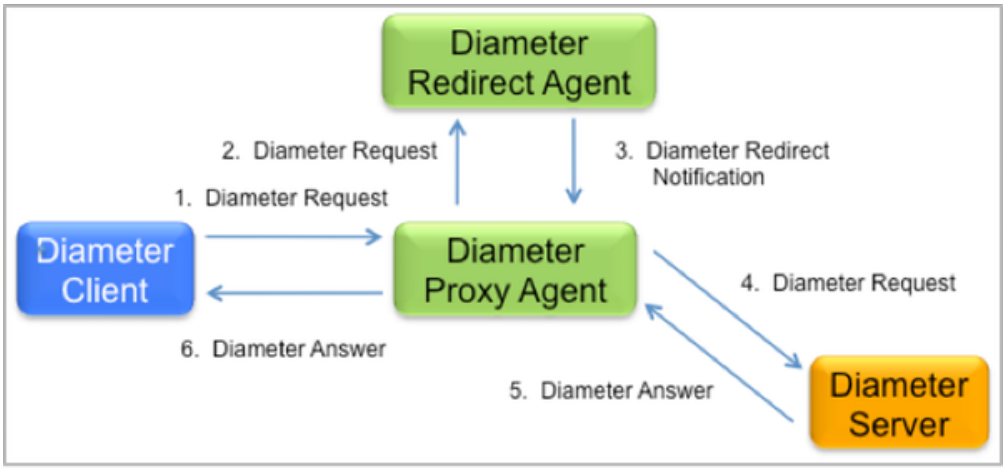


Figure 11.5: Agente Redirect

Agente de Traducción

Los agentes de traducción se encarga de hacer la traducción entre 2 protocolos. El caso más habitual sería realizar la traducción entre los protocolos RADIUS y Diameter. Mantienen el estado de la sesión y el estado de la transacción. La traducción sólo puede ocurrir si el agente es capaz de identificar la aplicación de la solicitud. Los agentes traductores sólo deben anunciar durante el intercambio de capacidades, las aplicaciones que soportan.

Figure 11.6: Agente de Traducción

11.4 Formato Mensajes

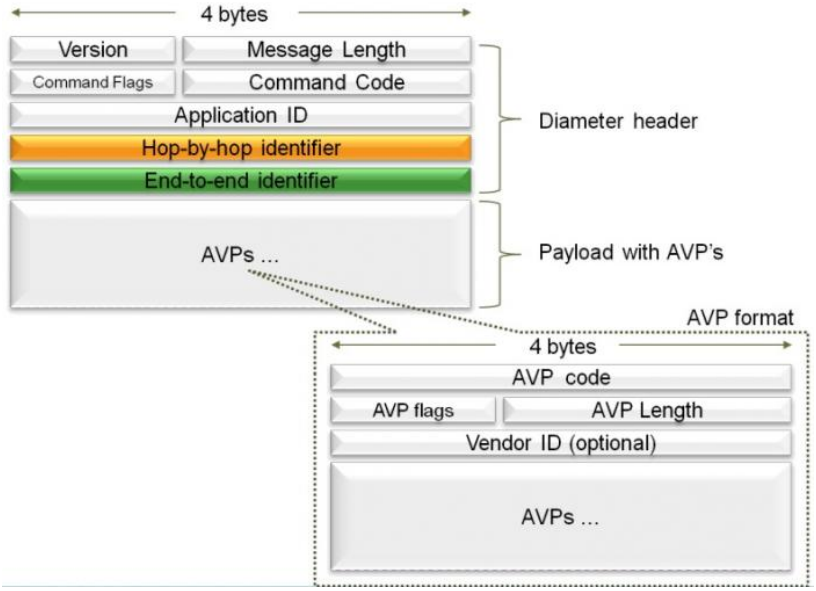


Figure 11.7: Formato AVP

Los mensajes en Diameter están formados por una cabecera o header que ocupa 20 octetos seguido por una cantidad variable de AVPs

- **Version**. 8 bits. Indica la versión de Diameter.
- **Message Length**. 3 bytes. Indica la longitud del mensaje Diameter incluyendo las cabeceras y los AVPs (múltiplo de 4 bytes).
- **Command Flags**. 8 bits.
  - **R(equest)**. Si es 1 es una petición (R).
    Si es 0 es una respuesta (A).
  - **P(roxiable)**. Si está a 1 significa que el mensaje puede ser gestionado por un agente relay, proxy o redirect.
    Si es 0, solo puede ser gestionado localmente.
  - **E(rror)**. Si es 1, el mensaje reporta un error de protocolo.
    Este bit sólo se considera en los mensajes respuesta (A).
  - **T(retransmission)**. El bit T indica si el mensaje es el original (cuando el T=0), o si es un mensaje retransmitido (T=1).
    Este bit debe ponerse a 0 cuando se envía una petición por primera vez.
  - **r(eserved)**. Reservados para uso futuro.

R	P	E	T	r	r	r	r

Table 11.1: Flags Command

Command Code

3 bytes. Se utiliza para identificar al comando asociado al mensaje. Los valores son gestionados por la IANA

Command Name	Abbrev.	Code	Section Reference
Abort-Session-Request	ASR	274	8.5.1
Abort-Session-Answer	ASA	274	8.5.2
Accounting-Request	ACR	271	9.7.1
Accounting-Answer	ACA	271	9.7.2
Capabilities-Exchange-Request	CER	257	5.3.1
Capabilities-Exchange-Answer	CEA	257	5.3.2
Device-Watchdog-Request	DWR	280	5.5.1
Device-Watchdog-Answer	DWA	280	5.5.2
Disconnect-Peer-Request	DPR	282	5.4.1
Disconnect-Peer-Answer	DPA	282	5.4.2
Re-Auth-Request	RAR	258	8.3.1
Re-Auth-Answer	RAA	258	8.3.2
Session-Termination-Request	STR	275	8.4.1
Session-Termination-Answer	STA	275	8.4.2

Figure 11.8: Ejemplos de Command Codes

Application-ID

4 octetos. Identifica la aplicación para la cual es aplicable el mensaje. La aplicación puede ser una aplicación de autenticación, de accounting o una especifica de proveedor:

Application	Application Id
Diameter Common Messages	0
NASREQ	1
Diameter Base Accounting, Rf , Gz	3
Diameter Credit Control, Ro, Gy	4
Relay	0xFFFFFFFF
Cx/Dx Interface Application	16777216
Rx Interface Application	16777236
Sh/Dh Interface Application	16777217
Re Interface Application	16777218
S6a/S6d Interface Application	16777251
S13/S13 ' Interface Application	16777252
S9 Interface Application	16777267
Gx Interface Application	16777238
Sy Interface Application	16777302
SWx Interface Application	16777265

Figure 11.9: Ejemplos de Application-Id

V	M	P	r	r	r	r	r

Table 11.2: Flags AVP

Hop-by-Hop Identifier

ID de 4 bytes que permite encaminar las respuestas al origen.

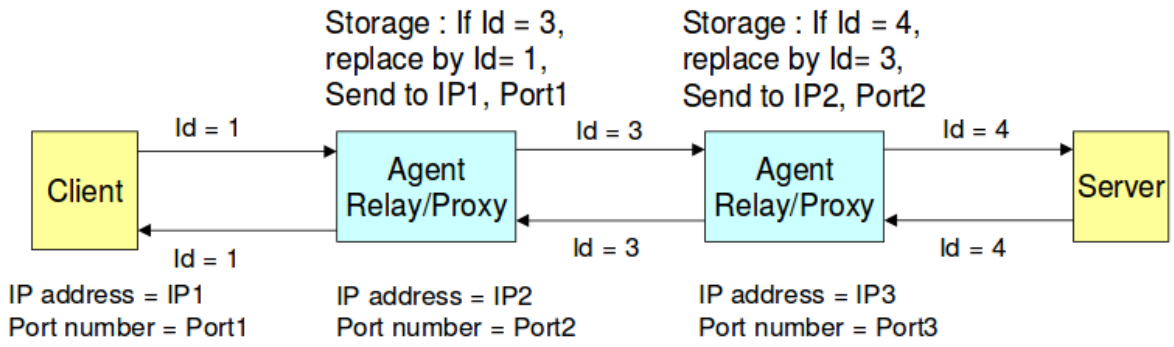


Figure 11.10: Ejemplos de Hop-by-Hop

El que envía las peticiones debe asegurarse que el Hop-by-Hop ID enviado sea único para la conexión dada. Posteriormente, el que envía una respuesta debe asegurarse que dicho valor sea el mismo que le llego de una petición.

End-to-End Identifier

Cuando un nodo Diameter recibe un mensaje:

- Si el mensaje es una petición y el End-to-End ID no está en su tabla de mapeo de mensajes se asume que es una nueva petición y se inserta la nueva entrada en la tabla.
- Si el mensaje es una respuesta y el End-to-End ID no está en la tabla, se descarta el mensaje (una respuesta debe seguir la misma ruta que la petición, por tanto, esto implica que mensaje ha sido encaminado indebidamente).

La combinación del AVP Origin-Host y este campo se utilizan para detectar mensajes duplicados. El End-to-End ID tiene 4 bytes. El emisor de una petición debe insertar un identificador único (al menos 4 minutos). El emisor de la respuesta debe poner el mismo End-to-End ID que encontró en la solicitud correspondiente. Este identificador no debe ser modificado por agentes de ningún tipo. Sin detección de duplicados, un duplicado podría generar una nueva entrada (innecesaria) en la tabla de mapeo para una request/answer finalizada.

En un agente además se pueden aplicar distintos comportamientos para duplicados:

- Descartar silenciosamente.
- Forward.

Los AVPs llevan información especifica de autenticación, autorización, accounting, routing y configuración especifica de solicitudes y respuestas.

- **AVP Code**. 4 octetos. Combinado con el campo Vendor-ID identifica de forma única el atributo. Los códigos del 1 al 255 están reservados para RADIUS. Del 256 en adelante son utilizados por Diameter. La IANA gestiona estos valores.
- **AVP Flags**. 8 bits. Indican al receptor como debe ser procesado cada atributo
  - **V**. Indica si el campo opcional Vendor-ID esta presente en el AVP o no.
  - **M**. Conocido como bit obligatorio, indica si el receptor del mensaje debe entender o no la semántica del mensaje. El receptor debe responder con un mensaje de error en el caso que reciba un AVP con M =1 y no sea capaz de entenderlo.
  - **P**. Reservado para uso futuro (para seguridad end-to-end).
  - **r**. Reservado para uso futuro.

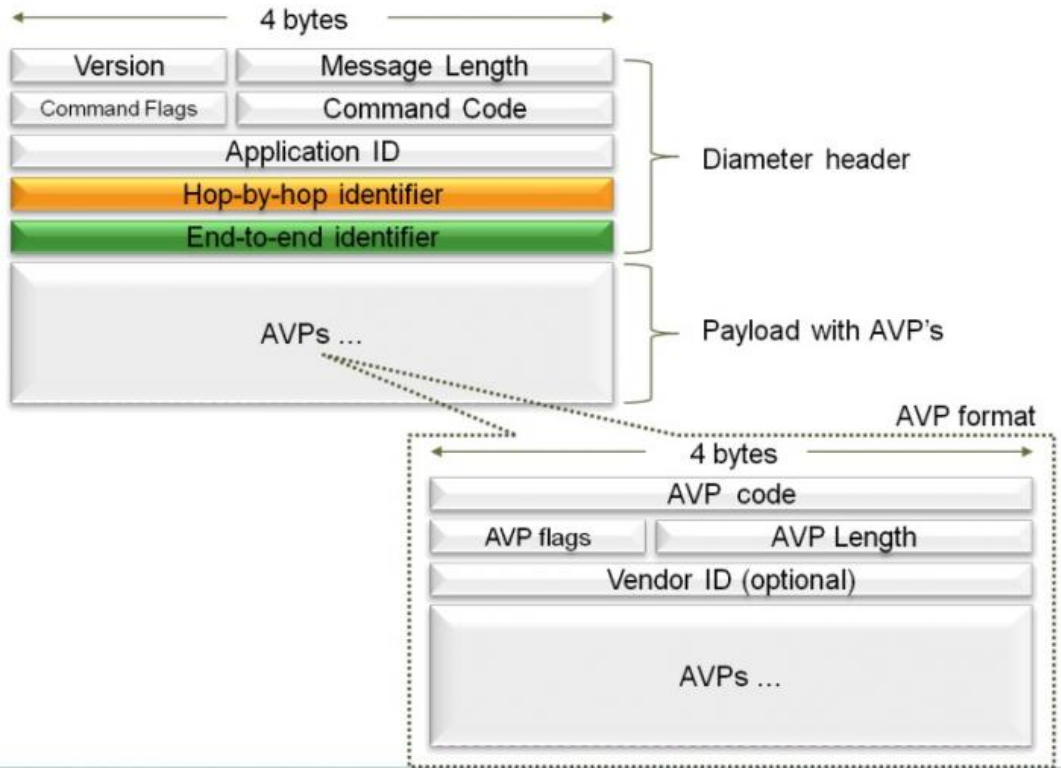


Figure 11.11: Formato AVP

- **AVP Length**. 3 bytes. Número de bytes del AVP. Los mensajes con longitudes erróneas debe rechazarse.
- **Vendor-ID**. Opcional. 4 bytes. Contiene el valor asignado por la IANA al vendor.

```
AVP: Service-Information(873) l=328 f=VM- vnd=TGPP
  AVP Code: 873 Service-Information
  AVP Flags: 0xc0
  AVP Length: 328
  AVP Vendor Id: 3GPP (10415)
Service-Information: 0000036ac000013c000028af00000002c0000010000028af...
  AVP: PS-Information(874) l=316 f=VM- vnd=TGPP
    AVP Code: 874 PS-Information
    AVP Flags: 0xc0
    AVP Length: 316
    AVP Vendor Id: 3GPP (10415)
  PS-Information: 00000002c0000010000028af000056ce00000003c0000010...
    AVP: 3GPP-Charging-Id(2) l=16 f=VM- vnd=TGPP val=22222
    AVP: 3GPP-PDP-Type(3) l=16 f=VM- vnd=TGPP val=3
    AVP: PDP-Address(1227) l=18 f=VM- vnd=TGPP val=12.27.12.27 (12.27.12.27)
    AVP: SGSN-Address(1228) l=18 f=VM- vnd=TGPP val=12.28.12.28 (12.28.12.28)
    AVP: GGSN-Address(847) l=18 f=VM- vnd=TGPP val=8.47.8.47 (8.47.8.47)
    AVP: 3GPP-CG-Address(4) l=16 f=VM- vnd=TGPP val=4.4.4.4 (4.4.4.4)
    AVP: 3GPP-IMSI-MCC-MNC(8) l=17 f=VM- vnd=TGPP val=test8
    AVP: 3GPP-GGSN-MCC-MNC(9) l=17 f=VM- vnd=TGPP val=test9
    AVP: 3GPP-NSAPI(10) l=18 f=VM- vnd=TGPP val=test10
    AVP: Called-Station-Id(30) l=14 f=-M- val=test30
    AVP: 3GPP-Selection-Mode(12) l=18 f=VM- vnd=TGPP val=test12
    AVP: 3GPP-Charging-Characteristics(13) l=18 f=VM- vnd=TGPP val=test13
    AVP: 3GPP-SGSN-MCC-MNC(18) l=18 f=VM- vnd=TGPP val=test18
    AVP: 3GPP-MS-TimeZone(23) l=18 f=VM- vnd=TGPP val=746573743233
    AVP: 3GPP-User-Location-Info(22) l=18 f=VM- vnd=TGPP val=746573743232
    AVP: 3GPP-RAT-Type(21) l=18 f=VM- vnd=TGPP val=746573743231
F5 Ethernet trailer
```

Figure 11.12: Ejemplo AVP

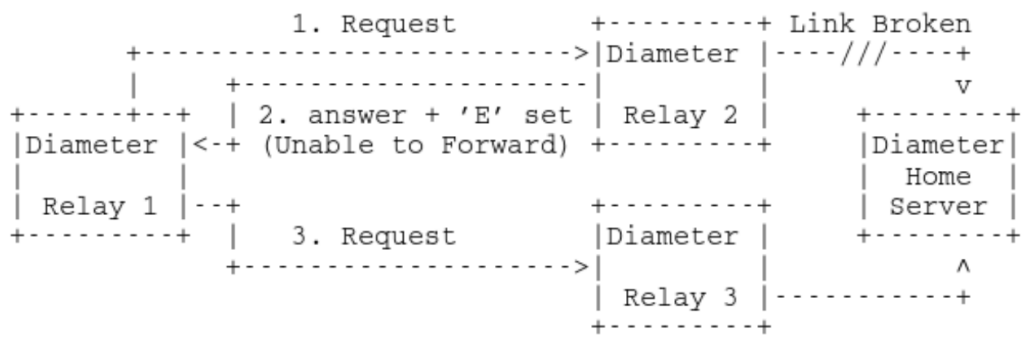


Figure 11.13: Ejemplos de error de protocolo

11.5 Accounting

En Diameter el proceso de **Accounting** está basado en el modelo denominado 'Server Directed Model'. En este modelo, el dispositivo que genera la información de accounting sigue las instrucciones de un servidor. Basado en los perfiles de usuario o en otras condiciones, un servidor Diameter informa a un cliente el comportamiento que debe seguir. Por ejemplo, la frecuencia con la que los registros de accounting deben ser enviados por el cliente al servidor. Un registro o record de Accounting es un resumen del consumo de recursos por parte de un usuario en una sesión. Los servidores de Accounting generan los 'accounting records' a través del procesamiento de eventos que ocurren en las sesiones.

Existen dos comandos relacionados con Accounting:

- Comando **Accounting-Request** (ACR)
  - Identificado con el **Command Code 271**.
  - Command Flag **R=1**.
  - Enviado por el nodo Diameter que actúa como cliente para intercambiar información de Accounting.
- Comando **Accounting-Answer** (ACA)
  - Identificado con el **Command Code 271**.
  - Command Flag **R=0**.
  - Responde con un **ACA** el nodo que actúa como Servidor.

11.6 Gestión de errores

Existen dos tipos de error en Diameter:

- Errores de protocolo. Ocurre en el protocolo base de Diameter y puede requerir atención en los diferentes saltos de la red.
- Errores de aplicaciones. Normalmente ocurren debido a un problema en las funciones especificas de cada aplicación.

Los códigos de los errores se encapsulan en AVP Result-Code:

- Un AVP Result-Code sólo debe estar presente en un mensaje respuesta.
- Los valores Result-Code tienen los significados:
  - 1xxx Información
  - 2xxx Éxito
  - 3xxx Errores de protocolo
  - 4xxx Errores transitorios
  - 5xxx Errores permanentes

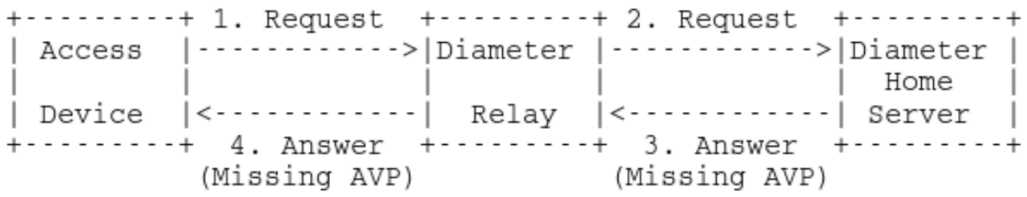


Figure 11.14: Ejemplos de error de aplicación

El Relay1 envía un request al Relay2 pero debido a fallos en el enlace, la petición no puede ser retransmitida al servidor. En este punto se genera una respuesta con el bit **E=1** indicando el error producido (en este ejemplo: DIAMETER_UNABLE_TO_DELIVER). Debido a que este error pertenece a la categoría de errores de protocolo, el Relay1 tratará de re-enrutar el mensaje a través del Relay3.

Cuando ocurre un error de tipo aplicación, el nodo Diameter que reporta el error añadiendo un Result-Code en la respuesta (pero se mantiene E=0). Los errores de aplicación no requieren que exista ningún agente Diameter implicado, por lo que, el mensaje es remitido al host que originó la petición.

11.7 Gestión de Peers

Para establecer una conexión con otro peer se necesita conocer su **DiameterIdentity**, la cual contiene los datos que identifican de forma unívoca como establecer una conexión con un peer:

- Permite identificar de forma única un nodo Diameter.
- Permite identificar de forma única un Realm y determinar si se pueden enviar los mensajes de forma local o si deben ser enviados a un agente.

En general, la **DiameterIdentity** tiene un formato de tipo Diameter URI:

- FQDN = Fully Qualified Host Name (nombre del nodo).
- Port = :<1*digit> (si ausente se usa el puerto por defecto el puerto de Diameter 3868).
- Transport= ;transport= (nombre del protocolo de transporte. Si ausente se usa por defecto SCTP).
- Protocol = ;protocol= (si ausente se usa Diameter).

```
aaa://FQDN[:Port];[Transport];[Protocol]  //No Transport security
aaas://FQDN[:Port];[Transport];[Protocol] //Transport security used
```

Ejemplos:

- Nodo con FQDN=host.example.com, escuchando en el puerto por defecto (3868), con el protocolo de transporte por defecto (SCTP) y con el protocolo por defecto (Diameter):

  ```
  aaa://host.example.com
  ```

- En este caso Port=6666, Transport=tcp , Protocol=diameter:

  ```
  aaa://host.example.com:6666;transport=tcp;protocol=diameter
  ```

- Radius con UDP:

  ```
  aaa://host.example.com:1813;transport=udp;protocol=radius
  ```

Los mensajes para el establecimiento y gestión de las conexiones Diameter tienen un Application Id=0.

Entre estos tenemos:

- Intercambio de capacidades: CER/CEA

  Capabilities-Exchange-Request/Capabilities-Exchange-Answer.

- Mensajes de watchdog: DWR/DWA

  Device-Watchdog-Request/Device-Watchdog-Answer.

- Desconexión del peer: DPR/DPA

  Disconnect-Peer-Request/Disconnect-Peer-Answer.

Durante el transcurso del tiempo, un peer con una conexión Diameter establecida puede pasar a estado 'sospechoso. Esto puede suceder por varias razones pero la razón más común es la de no recibir un DWA dentro de un periodo de tiempo asignado.

En ese caso:

- No se deben enviar más mensajes de petición al peer destino.
- El peer origen puede establecer conexiones Diameter adicionales para asegurar el servicio.

Existen dos formas de salir de la lista de peers sospechosos:

1. El peer se considera no disponible. Se cierra la conexión de transporte y se pasa el peer a estado 'cerrado'.
2. Se intercambian tres mensajes de watchdog en los tiempos requeridos, por lo que, la conexión se considera estabilizada de nuevo.

Se podría configurar un nodo Diameter con conexiones a todos los peers con los que puede tener comunicación. Sin embargo, consumiríamos una gran cantidad de recursos en ese caso. Una configuración óptima a nivel de fiabilidad/escalabilidad es la siguiente:

- Tener dos conexiones establecidas por realm a dos peers distintos, conocidos como primario y secundario.
- Entonces, los mensajes son enviados al peer primario pero, en caso de un eventual fallo, cualquier petición pendiente es enviada al secundario.
- Un peer que en un realm haga las funciones de primario puede ser un peer secundario en otro realm y viceversa.

La **tabla de peers** se utiliza en el envío de mensajes Diameter y es referenciada por la tabla de rutas Diameter (se comenta posteriormente). Se compone de los siguientes campos:

- **Host Identity**. Contiene la URI del nodo (DiameterIdentity).
- **StatusT**. Estado del nodo.
- **Static o Dynamic**. Especifica si la entrada fue añadida de forma estática o dinámica (mediante el descubrimiento de peers que explicamos a continuación).
- **Expiration Time**. Especifica el tiempo en el que las entradas dinámicas, deben ser eliminadas o refrescadas (para ello se utiliza el valor TTL proporcionado por el DNS).

Si se usan certificados con claves publicas, el valor del tiempo de expiración no puede ser superior a la fecha de validez del certificado.

- **Activación de TLS/TCP y DTLS/SCTP**. Especifica si el transporte utiliza seguridad.
- **Información adicional**. Información adicional para acceder al peer. Por ejemplo, si se utiliza un transporte con seguridad (TLS/DTLS), en este campo se deben almacenar las claves, los certificados, etc.

Identidad Host	StatusT	Estatico/Dinamico	Tiempo Expiración	Seguridad
nodeB.realm1.com transport=tcp port=12345	Idle	Dinámico	600	No
nodeE.realm1.com	Abierto	Estático		No
nodeI.realm1.com	Pendiente	Estático		No
nodeF.realm2.com	Abierto	Estático		Si

Table 11.3: Tabla peers nodo A

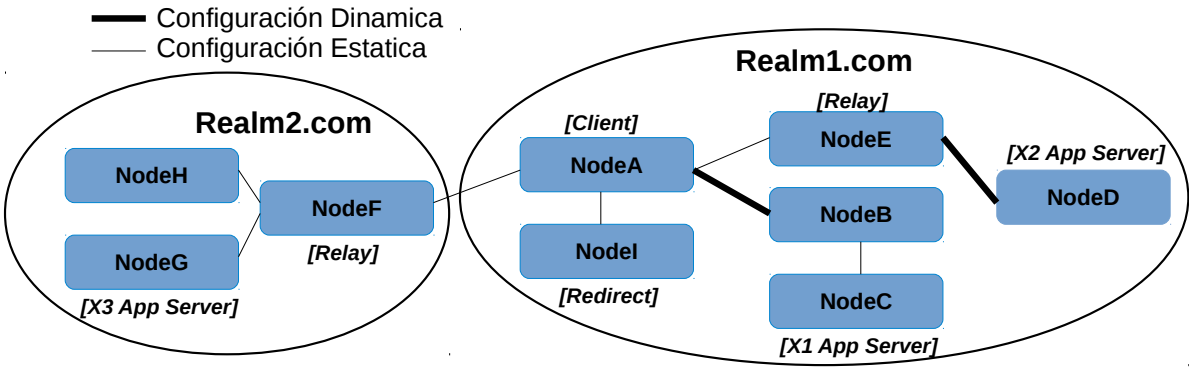


Figure 11.15: Ejemplo Tabla Peers

El RFC3588 define tres formas de configurar peers:

1. De forma manual: Se rellena manualmente la lista de peers. Los peers manuales son utilizados siempre en primer lugar.
2. De forma dinámica mediante el protocolo SLPv2 (Service Location Protocol). No es muy utilizado.
3. De forma dinámica mediante DNS usando los registros NAPTR/SRV.

El descubrimiento de peers Diameter de forma dinámica hace que sea más simple y robusto el despliegue de aplicaciones Diameter.

A continuación se detalla el descubrimiento de peers con DNS.

El RFC2782 define los registros SRV (SeRVice). Dado un servicio y un protocolo de transporte, un SRV define como se debe asignar un servidor para dicho servicio (incluyendo un esquema de reparto de carga). Para obtener los registros **hay que proporcionar el servicio, el protocolo de transporte y el dominio**. El cliente también consultará los registros A/AAAA para obtener las direcciones de los servidores en los SRV.

```
_service._protocol.name TTL class SRV priority weight port destination
```

- **priority** indica la prioridad del servidor. Un cliente deberá contactar, en primer lugar, al servidor con menor prioridad.
- **weight** sirve para seleccionar un servidor entre los de la misma prioridad. Un peso más grande significa que el candidato debe ser seleccionado con mayor probabilidad.
- **port** el puerto del protocolo de transporte.
- **destination** el FQDN del servidor que presta el servicio (el FQDN tendrá registros A o AAAA asociados).

Ejemplo de registros SRV para Diameter:

```
_diameters._tcp.example.com. 86400 IN SRV 10 60 12345 srv1.example.com.
_diameters._tcp.example.com. 86400 IN SRV 10 40 12345 srv2.example.com.
_diameters._tcp.example.com. 86400 IN SRV 20 100 12345 srv3.example.com.
_diameters._sctp.example.com. 86400 IN SRV 10 50 12345 srv4.example.com.
_diameters._sctp.example.com. 86400 IN SRV 10 50 12345 srv5.example.com.
```

En el ejemplo se configura:

- Un acceso Diameter a un dominio mediante TLS.
- Otro acceso Diameter mediante DTLS/SCTP.
- El acceso TLS en primera opción tiene dos servidores en reparto de carga 60%-40%.
- El acceso TLS en segunda opción tiene un servidor que asume el 100% de la carga.
- Para el acceso Diameter DTLS/SCTP se configura solo una opción con dos servidores en reparto de carga 50%-50%.

Para no obligar al cliente a conocer el protocolo de transporte y que el realm receptor pueda expresar sus preferencias se pueden utilizar registros NAPTR.Cuando un cliente realiza una consulta al DNS por NAPTR dando un nombre de dominio el resultado (si todo está bien configurado) es uno o más registros NAPTR. En el caso de Diameter, los registros NAPTR obtenidos nos proporcionarán información de los registros SRV correspondientes.

Formato genérico de registro NAPTR:

```
owner-name  ttl  class NAPTR  order preference flag params regexp replace
```

- **order** (16 bits) especifica el orden en el que los registros NAPTR debe ser procesados (más bajos más prioritarios).
- **preference** (16 bits) utilizado para priorizar registros NAPTR con el mismo valor order (más bajos más prioritarios).

Cuando un cliente encuentra un registro NAPTR con un servicio aceptable a su petición, no debe analizar otros registros con diferente order. El parámetro preference permite a los administradores dirigir a los clientes hacia los servidores más capaces o hacia los protocolos de transporte más eficientes. Un cliente puede preferir un NAPTR con preference menos prioritaria por que no soporta un cierto protocolo. Nota: el reparto de carga se implementa con SRVs.

Ejemplos para Diameter:

```
example.com. IN NAPTR 10  10 "s" "aaa+D2S" "" _diameter._sctp.example.com
example.com. IN NAPTR 20  10 "s" "aaa+D2T" ""  _aaa._tcp.example.com
```


```
example.com. IN NAPTR 10  10 "s" "aaa+D2S" "" _diameter._sctp.example.com
example.com. IN NAPTR 20  10 "s" "aaa+D2T" ""  _aaa._tcp.example.com
```


En el ejemplo los registros NAPTR indican que el realm soporta SCTP y también TCP en ese orden. Si el cliente soporta SCTP, se usará ese protocolo. Entonces, una vez obtenidos los NAPTR, el cliente lanzará una consulta por un registro SRV usando como nombre _diameter._sctp.example.com. Finalmente el DNS enviará los registros SRV (en realidad la mayoría de implementaciones del DNS enviarán NAPTR+SRV en la primera respuesta).

El protocolo de base de Diameter especifica mecanismos por los que un realm determinado puede anunciar nodos Diameter y un protocolo de transporte compatible. Sin embargo, estos mecanismos no revelan las aplicaciones Diameter que cada nodo soporta. Esto implica que los peers fuera del realm tendrían que realizar un intercambio de capacidades Diameter con cada nodo hasta descubrir uno compatible con la aplicación requerida. El RFC6480 (noviembre 2011) describe una mejora utilizando un formato ampliado utilizando los registros S-NAPTR (Straightforward-Naming Authority Pointer). La mejora permite el descubrimiento de las aplicaciones Diameter compatibles sin tener que hacer a priori el intercambio de capacidades. Dicha mejora es incluida en la actualización de Diameter en el RFC 6733.

El procedimiento S-NAPTR (Straightforward-Naming Authority Pointer) se define en el RFC 3958 y es una simplificación del procedimiento NAPTR (definido en el RFC 3403). Se utilizan en Diameter (y también en otras consultas DNS en la EPS de LTE). S-NATPR permite proporcionar información del servicio utilizando "nombres de recursos" (cuya sintaxis no es una URI). Para Diameter el campo service del NAPTR tiene el formato: "aaa+apX" donde "X" indica el Identificador de Aplicación Diameter. Si en el NAPTR recibimos un campo service con esa forma, significa que el realm soporta el formato extendido del registro NAPTR para Diameter (RFC6480).Ejemplo, considerar que un peer desea descubrir un servidor Diameter en el realm ex.com que soporte la aplicación control de crédito (Application ID =4). Para ello el peer realiza una consulta NAPTR para ese dominio (ex.com) y obtiene los siguientes registros NAPTR:

```
ex.com. IN NAPTR 10 10 "s" "aaa:diameter.sctp" "" _diameter._sctp.ex.com
ex.com. IN NAPTR 10 10 "s" "aaa+ap1:diameter.sctp" "" _diameter._sctp.ex.com
ex.com. IN NAPTR 10 10 "s" "aaa+ap4:diameter.sctp" "" _diameter._sctp.ex.com
```

- Los registros anteriores indican que el servidor soporta la aplicación Diameter NASREQ (ID = 1) y el Control Crédito (ID = 4) sobre SCTP.
- Si el cliente es compatible con SCTP, realiza un lookup por el SRV _diameter._sctp.ex.com.
- Otro ejemplo:

```
ex.com. IN NAPTR 150 50 "a" "aaa:diameter.sctp" "" srv1.ex.com.
ex.com. IN NAPTR 150 50 "a" "aaa:diameter.tls.tcp" "" srv2.ex.com.
ex.com. IN NAPTR 150 50 "a" "aaa+ap1:diameter.sctp"  "" srv1.ex.com
ex.com. IN NAPTR 150 50 "a" "aaa+ap1:diameter.tls.tcp"  "" srv2.ex.com
```

- Los registros anteriores indican que el realm ex.com soporta NASREQ (ID=1) sobre SCTP y sobre TLS/TCP via los hosts srv1.ex.com y srv2.ex.com respectivamente.
- Nota. Si un peer no localizara ningún registro NAPTR, puede consultar directamente por registros SRV de diameter.

11.8 Enrutamiento

El enrutamiento de peticiones Diameter se realiza utilizando dos AVPs: Destination-Realm y Destination-Host. Estos AVPs pueden aparecer en tres combinaciones distintas en las peticiones:

1. Una petición Diameter que no puede ser enrutada (proxied), como una petición CER, no debe contener ni Destination-Realm ni Destination-Host.
2. Una petición que necesita ser entregada a un servidor en un Realm especifico (pero no a un host especifico) debe contener el Realm destino pero no debe contener el Destination-Host.
3. Una petición que debe ser entregada a un host especifico en un Realm debe contener tanto el Realm destino como el Host destino.

Para realizar el envío de Peticiones se deben definir los siguientes valores

- El **Command Code** debe asignarse al valor apropiado.
- El **bit 'R'** debe asignarse a 1 (petición).
- El identificador **End-to-End** debe asignarse a un valor adecuado (único).
- Los identificadores **Origin-Host** y **Origin-Realm** deben incluirse en la petición con sus valores correspondientes.
- Los identificadores **Destination-Host** y **Destination-Realm** deben ser incluidos (o no) siguiendo lógica que se acaba de describir.

En cambio, cuando se recibe una petición Diameter se procesa en el siguiente orden:

1. Mirar si el mensaje es para el local host.
2. Mirar si el mensaje es para un peer con el cual el host local se puede comunicar directamente (esto se llama "Request Forwarding").
3. Encaminar la petición ("Request Routing").
4. Si nada de lo anterior es exitoso, se envía una respuesta con un Result-Code= DIAMETER_UNABLE_TO_DELIVER (con E=1).

Una petición Diameter es **procesada localmente** si se da alguna de las siguientes situaciones:

- La petición contiene como Destination-Host un valor local del nodo.
- El Destination-Host no esta presente pero el Destination-Realm contiene un valor que esta configurado para procesar los mensajes localmente, y la aplicación Diameter (del mensaje) esta soportada localmente.
- No están presentes ni el Destination-Host ni el Destination-Realm.

Una petición Diameter es procesada mediante **Request Forwarding**:

- Cuando se recibe una petición y el AVP Destination-Host es uno de los que está presente en la tabla de peers, entonces, el mensaje se envía al peer.

El encaminamiento de peticiones Diameter se realiza utilizando Realms e IDs de aplicación.Las decisiones de encaminamiento se realizan utilizando la tabla de enrutamiento Diameter.

Esta tabla contiene los siguiente campos:

- **Realm Name**. Clave primaria. Nombre del realm.

- **Application Identifier**. Application ID que identifica la aplicación. Los mensajes pueden ser enrutados de forma diferente dependiendo de la aplicación por lo que esta información debe estar contenida en la tabla de enrutamiento.

- **Local Action**. Identifica como deben ser gestionados los mensajes y puede tomar los valores:

  - LOCAL. Los mensajes pueden ser gestionados internamente (no es necesario que sean encaminados).

  - RELAY. Los mensajes deben ser enrutados al next-hop Diameter. No se modifica ningún AVP del mensaje.

  - PROXY. Los mensajes son enrutados al next-hop Diameter. Se modifica el mensaje (por ejemplo añadiendo nuevos AVPs).

  - REDIRECT. Se envía una respuesta al origen con los datos de la redirección.

- **Server Identifier**. Identidad de uno o más servidores a los cuales se les va a enviar el mensaje.

- **Static or Dynamic**. Identifica si la entrada fue configurada manualmente o descubierta dinámicamente.

- **Expiration Time**. Especifica el tiempo en el que las entradas dinámicas, deben ser eliminadas o refrescadas.

  Si se usan certificados con claves publicas, el valor del tiempo de expiración no puede ser superior a la fecha de validez del certificado.

La tabla de enrutamiento puede contener **una ruta por defecto** en el caso que ninguna otra entrada se ajuste a los parámetros de la petición.

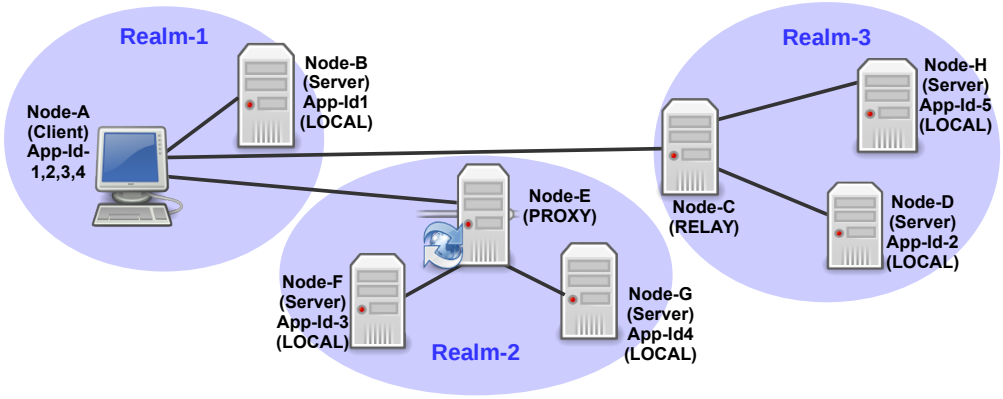


Figure 11.16: Ejemplo Tabla Enrutamiento

Host	**Status**	**Estatico/Dinamico**	**TLS**	**Tiempo Expiración**
Node-B	Abierto	Dinámico	Activo	
Node-C	Abierto	Dinámico	Activo	
Node-E	Abierto	Dinámico	Activo	

Table 11.4: Tabla Peers (nodo A)

Realm-Name	**Application-Id**	**Server-ID**	**Local Action**	**Descubrimiento Peer**	**Tiempo Expiración**
Realm-1	App-Id-1,2,3,4		LOCAL		
Realm-1	App-Id-1	Node-B	LOCAL	Dinámico	
Realm-2	App-Id-3	Node-E	PROXY	Dinámico	
Realm-2	App-Id-4	Node-E	PROXY	Dinámico	
Realm-3	App-Id-2	Node-C	RELAY	Dinámico	

Table 11.5: Tabla Enrutamiento Realms (nodo A)

Chapter 12

Conclusiones

Durante el desarrollo de este proyecto hemos visto las principales necesidades que la tecnología LTE pretendía cubrir:

- Una mayor tasa de subida y bajada en las conexiones de datos
- Una reducción tanto de la complejidad como de los costes de la arquitectura
- Redes basadas en conmutación por paquetes mediante el protocolo IP

Se ha cubierto todas las facetas de la tecnología LTE de una forma didáctica, introduciendo paulatinamente los conceptos e intentando asentarlos poco a poco. El hecho de reintroducir conceptos ya tratados con anterioridad, nos servía de refuerzo de las ideas del temario mostrado.

Adicionalmente, se ha utilizado el anexo para exponer información adicional relacionada con el tema principal, las redes LTE. De esta forma se han expuesto conceptos relacionados con la tecnología de 5ª Generación, como IoT (Internet de las Cosas) o Smart Things (Offices, houses, etc...). Este es un futuro muy presente, por lo que con la orientación tan educativa de este proyecto, se ha intentado recopilar información relevante así como interesante para dar una visión global de hacia donde se dirige la tecnología.

Se espera que el proyecto sirva de base práctica para desarrollar y aplicar los conocimientos del protocolo Diameter. El capitulo centrado en Diameter sirve como introducción teórica al protocolo. En él hemos intentado explicar, resumir y compilar toda la información recogida en el RFC6733 que sirve como base del protocolo. Para cumplimentar los conceptos introducidos, se ha diseñado una batería de practicas que a partir del hecho de introducir los conceptos poco a poco y basándonos en el método de prueba y error, pretende dotar y reforzar los conocimientos expuestos con anterioridad. Con esta orientación, la finalidad ha sido que sirva como apoyo para algún taller del Departamento de Telemática.

Appendix A

Anexos

A.1 5G

A.1.1 5g

A.1.1.1 Qué es el 5g

5G son las siglas utilizadas para referirse a la quinta generación de tecnologías de telefonía móvil que fue definida bajo el estándar de comunicación **IEEE_802.11ac** 5G es la sucesora de la tecnología 4G. Actualmente esta bajo desarrollo de prototipos y en previsión que su uso común sea en 2020

A.1.1.2 Por qué surge el 5g

Para explicar el porque de 5G se debería hacer un repaso de la situación existente con respecto a la tecnología 4G. Se podrían remarcar los siguientes puntos

- El número de dispositivos conectados ha aumentado
- El tráfico de datos móviles ha aumentado
- El impacto de las mayores capacidades de los nuevos terminales
- Los requisitos de mayores anchos de banda
- 4G no esta en disposición de dar servicio a este aumento de la demanda de datos

A partir de esos requerimientos tecnologicos que no podían ser cubiertos con la tecnologia existente 4G se pretendieron definir los retos u objetivos que debía cumplir la nueva tecnología. Algunos de los retos definidos son los siguientes:

- **Data Rates de varias decenas de Mb/s** deben ser soportados para decenas de miles de usuarios
- 1Gb/s a varios trabajadores dentro de la misma oficina
- **Cientos de miles de conexiones simultaneas** deben ser soportadas por instalaciones de sensores
- La **eficiencia espectral** debe ser mejorada sustancialmente respecto a 4G
- La cobertura debe ser mejorada
- La **eficiencia de la señal debe ser mejorada**
- La **latencia debe ser reducida** significativamente

Se han realizado varios estudios que muestran unas niveles de crecimientos espectaculares como se muestra en la figura A.1

- El número de dispositivos conectados al IoT se estima que llegará a los 50 Biliones en 2020
- El tráfico de datos se estima que crecerá a 24.3 Exabytes por mes en 2019
- El aumento de las capacidades de los teléfonos y los requerimientos de datos de los usuarios finales debido a nuevos servicios de Ultra-High Definition (UHD) como streaming multimedia y servicios con requerimientos de ultra baja latencia como cloud computing
- Estos nuevos requerimientos, evidencian que la 4G no puede dar soporte con la QoE necesaria, que en cambio 5G si daría

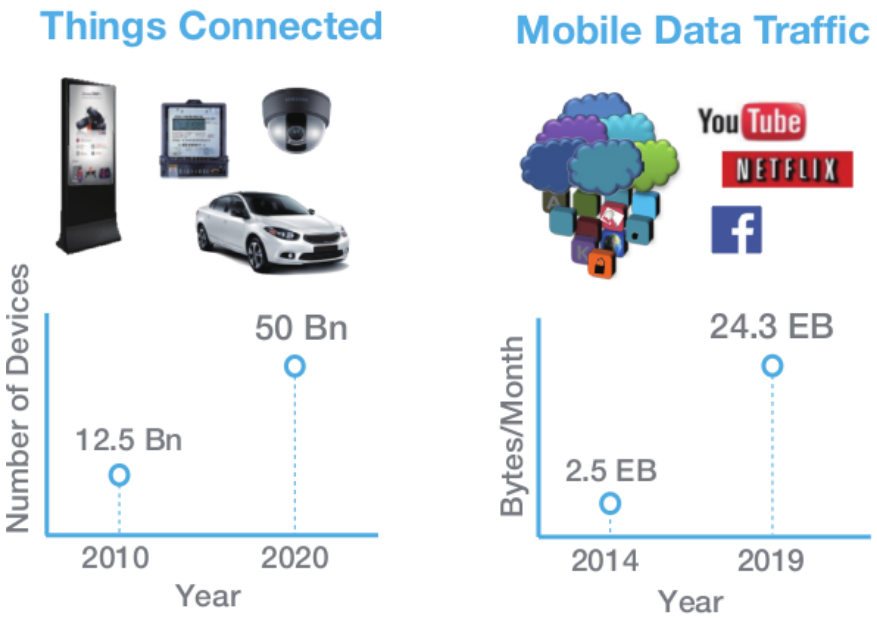


Figure A.1: Aumento del tráfico

A.1.1.3 Visiones

Los servicios 5G tienen como objetivo potenciar la revolución de la experiencia móvil. Así es como lo quieren hacer:

- **Internet of Things**
- **Casas Inteligentes** (Smart Home)
- **Fitness & Cuidado de Salud** (Healthcare)
- **Tiendas inteligentes** (Smart Store)
- **Oficinas inteligentes** (Smart Office)
- **Coches inteligentes** (Connected Car)

La **IoT (Internet de las cosas)** es un concepto que se refiere a la **interconexión digital de objetos cotidianos con Internet**. El concepto del IoT fue propuesto por Kevin Ashton del MIT en 1999. Con 5G el IoT se convertirá en una realidad donde se expera que un dispositivo pueda mantener la conectividad de red a pesar de su situación y del tiempo, abriendo la posibilidad de conectar todos los dispositivos sin la intervención humana. Se espera que con 5G se pueda tener hasta **un millón de conexiones simultaneas por Kilometro cuadrado**, habilitando una gran variedad de conexiones maquina-maquina posibles. Esta nueva era podría cambiar profundamente nuestra forma de vida ya que podríamos conectar virtualmente donde quisiéramos

El concepto de casas inteligentes (Smart Home) implica la **automatización de las actividades en casa**, el trabajo en casa y las actividades de mantenimiento (p.e. control centralizado de luces, ventilación, A/A, cierre automatizado de puertas, etc...). En la era del 5G podemos pensar que los lavavajillas se pueden arreglar de forma autónoma usando información de otros lavavajillas (peers) del mismo modelo. Otras aplicaciones:

- Neveras inteligentes podrían recomendar platos a cocinar basándose en los ingredientes que contiene
- Sistemas anti-incendio del barrio podrían colaborar para extinguir incendios

Los **Wearables devices (dispositivos llevables)** registraran tu actividad atlética mientras realizas actividades y serán capaces de recomendarte ejercicios, duración y frecuencia por día. Asimismo, estos dispositivos de control de salud enviaran tus señales vitales a un sistema de control que revisará y te avisará en caso que sea necesario una visita médica. Parte de la finalidad de todos estos sistemas de control de salud es prevenir urgencias antes que ocurran, esto supone unos requerimientos de latencia críticos

En grandes centros comerciales, con mucha gente caminando y viendo escaparates, la cercanía a ciertos productos será siempre traceada por servidores en el Cloud. A partir de esta información, una serie de alertas por artículos con descuentos podrán ser

enviados a tu dispositivo una vez detecten tu cercanía a las tiendas que los venden. Este servicio se puede customizar con una gran variedad de alternativas para mejorar la experiencia usuario. Podrían enviarse alertas a tu dispositivo si una vez en una tienda se encuentra alguna prenda similar a tu histórico de ventas alojado en el Cloud. Para entregar estos servicios se requiere una conexión masiva y baja latencia que pueda entregar los datos en el tiempo que estamos en las cercanías de las tiendas

A parte de los servicios habituales de navegación, con 5G se amplían las posibilidades relacionadas con la gestión del automóvil. Servicios como el diagnostico del vehículo para obtener información del nivel de batería, combustible o la situación del motor son cada vez más atractivos. Otro servicio con un gran valor añadido sería el eCall, sistema que automáticamente llamaría al servicio de urgencias en caso de necesitarla. A partir de 2020 se vislumbran servicios mucho más atractivos aprovechándose de la IoT, vehículos con cámaras y sensores podrán avanzarse a potenciales situaciones de emergencia recogiendo información propia y de los vehículos próximos y analizándola en tiempo real Estos servicios serán los potencialmente usados por los conductores inteligentes

En los entornos 5G **los usuarios experimentarán una vida multimedia a cualquier hora y cualquier lugar**. Para proveer esta experiencia, será necesaria una agilidad para responder de forma inmediata a las necesidades de usuario. Uno de los nuevos servicios que prevean dar esta experiencia, es el sistema de streaming UHD con un resolución altamente mejorada y claridad. Los servicios UHD empiezan a estandarizarse en algunos países. Asimismo, algunos móviles están siendo equipados con módulos que pueden grabar vídeo con calidad 4K UHD. Otros servicios que prevean dar un servicio ïmmersivoüque proveen revolucionar el entretenimiento son la realidad virtual (VR) y la realidad Aumentada (AR)

VR provee un nuevo mundo en el que la presencia física sera simulada por gráficos simulados por ordenador. El usuario puede de forma activa interactuar con los elementos simulados como por ejemplo en una retransmisión deportiva immersiva. Otros servicios interesantes de VR

- Peliculas 360
- Juegos online
- Educacion Remota
- Orquestas Simfonicas Virtuales

Los servicios AR permiten introducir información en tiempo real basada en el contexto de usuario y que se muestre de forma interactiva, dando un servicio añadido al usuario. Un ejemplo de AR lo encontramos en conducción donde podríamos tener en la luneta delantera información relacionada con el estado de nuestro vehículo como nivel de combustible, próxima gasolinera, estado de los neumáticos, etc..

5G dotará a los usuarios con una experiencia basada en la información en el Cloud. **Todo estará almacenado en el Cloud con acceso inmediato** gracias a la baja latencia. Con **interfaces de salida y entrada sencillas** en nuestro dispositivo móvil de forma que sea menos pesada, mas intuitivas y más user-friendly. Algún ejemplo lo podríamos encontrar yendo de compras donde podríamos tomar una foto a una prenda y el servicio computacional en el Cloud nos recomendaría complementos para llevar con ella

Los usuarios podrán controlar de forma remota maquinas y aplicaciones como si estuvieran delante de ellas, aun estando a miles de kilómetros. Gracias a las conexiones remotas y la latencia cercana a 0, los usuarios podrían controlar grandes maquinas industriales de forma remota en ubicaciones de acceso peligroso. También permitirá acceder a zonas inexploradas por el ser humano como el suelo marino

A.1.1.4 Requerimientos

Los sistemas **5G deben soportan rates de 10-50Gbps** para usuarios de baja movilidad. Las expectativas del 5G son de **proveer servicios de datos de Gbs a pesar de la ubicación**. Se espera que el despliegue de la red 5G sea mucho más densa de la realizada en 4G, por lo que es muy importante que el despliegue sea efectivo en coste. La **latencia de la red 5G en end-to-end debe ser menor a 5ms**mientras la **latencia over-the-air de menos de 1ms**. Si realizamos una comparación contra 4G, sería de 1 a 10. Los requerimientos de la tecnologia 5G los podemos revisar en la Figura A.2 **Mejora de la eficiencia espectral**:

- Los requisitos de eficiencia espectral son de 10bps/Hz.
- Utilización de MIMO, un esquema avanzado de modulación y codificación
- Un nuevo diseño de forma de onda

5G será 50 veces más eficiente que 4G entregando un coste y un uso de energía por bit mas reducido. Esto implica equipos de red de menor coste, despliegues de menor coste y funciones para mejorar el consumo de energía. Uno de los mayores retos a los que se enfrenta 5G es proveer servicio a la movilidad bajo demanda. El servicio bajo escenarios de movilidad debe estar

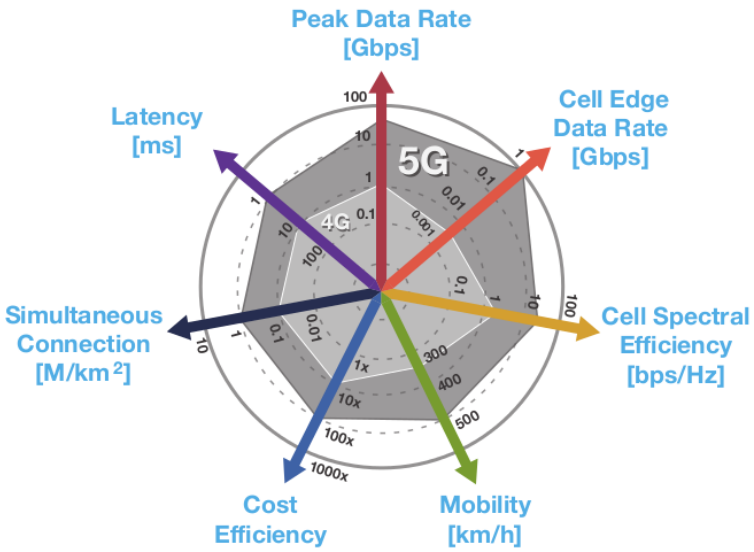


Figure A.2: Requerimientos 5G

garantizado. Para hacer la IoT verdad, el número de conexiones simultaneas se prevee del orden de 1000000 por kilometro cuadrado

Para poder cumplir unos requerimientos tan exigentes es necesaria la **utilización de una tecnología nueva y revolucionaria**. Los futuros sistemas 5G incluirán fundamentalmente, nuevos diseños para estimular la capacidad wireless utilizando:

- La **utilización de nuevas bandas de frecuencias**
- **Métodos avanzados para aumentar la eficiencias espectral** en la banda base
- La **integración de bandas licenciadas y no licenciadas**

La necesidad de **aumentar la capacidad de los sistemas 5G** será cubierta por:

- Un **nuevo sistema mmWave**
- **Celdas pequeñas de alta densidad**
- **MIMO** (Advanced Multiple-Input and Multiple-Output)
- Nuevos **esquemas de acceso múltiple** como p.e. Filter-Bank Multi-Carrier (FBMC)

La utilización de una **nueva codificación adaptativa y modulación** como Frequency and Quadrature Amplitude Modulation, en combinación con despliegue de mayor densidad permitirá:

- Mejora del rendimiento en los limites de la celda
- Promesa de entrega "Gbps anywhere"
- QoE uniforme

Mejora del ancho de banda con la integración de Multi-Radio Access Technology (Multi-RAT) que permite agregar las bandas licenciadas y no licenciadas. Por último, **nuevas topologías de red** donde se sitúan los **servidores de aplicaciones más cerca de los limites de la red** ayudaran a reducir la latencia de red. La tecnología Advanced Device-to-Device (D2D) puede ayudar a reducir la latencia en las comunicaciones y soporte un número mayor de conexiones simultaneas en la red

A.1.1.5 Tecnología 5G

El bandas **mmWave ofrecen 10 veces más ancho de banda que los bandas de 4G** por lo que, pueden soportar los mayores rates de datos necesarios en los futuros dispositivos móviles. Uno de los puntos a tener en cuenta cuando hablamos de las bandas mmWare s on las condiciones temporales, como lluvia, nieve o niebla. Sin embargo, la **perdida es pequeña en el rango de las comunicaciones 5G**. Uno de los retos existentes es debido a las características de la banda mmWave. Existe una **alta perdida de señal debido a la fragilidad debida las difracciones en el exterior**. Afortunadamente, la pequeña longitud de onda de la banda

mmWave también significa una alta direccionalidad del haz. Utilizando un número grande de antenas en una disposición correcta es clave para combatir la propagación de la perdida. Por lo tanto,los sistemas mmWave con la correcta utilización de antenas satisfacen 2 requerimientos del sistema 5G:

- **Cobertura geográfica suficientemente grande**
- **Soporta a la movilidad en ambientes NLoS** (None Line of Sight)

Los avances en la tecnología de semiconductores han echo que los sistemas comerciales mmWave estén rápidamente disponibles. Antenas de alto rendimiento son una pieza importante dentro del puzzle 5G. En entornos con constantes variaciones en la propagación de LoS y NLoS demandan un tipo especifico de antenas con mucha ganancia y una amplia capacidad de cobertura espacial. Una de los aspectos más importantes antes del lanzamiento comercial esta relacionado en como afectará la nueva banda mmWave al cuerpo humano. El Signal Absorption Rate(SAR) regulado por los gobiernos mundiales es utilizado como guia para validar el efecto de la nueva banda en el cuerpo humano La comparamos el efecto del SAR de media entre 4G y 5G es de 1 a 10. Aún así se estima que disminuya con el desarrollo de nuevas antenas

Para convertir en realidad los servicios 5G debe existir una mejora significativa en el rendimiento por usuarios asi como en la capacidad del sistema. Esta mejora puede ser obtenida mediante tecnologías avanzadas de PHY/MAC/network y metodos eficientes de despliegue de celdas y gestión de espectro. En particular, utilizar un mayor ancho de banda en el sistema garantiza el incremento en la capacidad por el simple hecho de poner más recursos de frecuencia por cada usuario. Por lo tanto, utilizar el espectro donde una gran cantidad de ancho de banda esta disponible, debe ser considerada una de las problemáticas mayores del despliegue del 5G

El Backhaul es una red de retorno. Porción de una red jerárquica que comprende los enlaces intermedios entre el núcleo y las subredes en sus bordes. Puede materializarse en una conexión entre computadoras u otros equipos encargados de hacer circular información. Las redes de retorno conectan redes de datos, redes de telefonía celular, y otros tipos de redes de comunicación, además de ser usadas para interconectar redes entre sí utilizando diferentes tipos de tecnologías alámbricas o inalámbricas.

En 4G el sistema especificaba la frecuencia operativa para cada uno de los operadores de red. Este despliegue era eficiente ya que los sistemas 4G no interferían con otros RATs. Obtener las licencias necesarias para utilizar el espectro no implican solo un alto coste de inversión asimismo, implican una serie de trabas burocráticas y un largo periodo de tiempo para su regulación. No solo eso, sino que una parte importante del espectro esta siendo actualmente usada. El reto principal de 5G es encontrar un ancho de banda del espectro suficientemente amplio para dar el servicio requerido. La última moda en gestión del espectro es agregar tanto la banda licenciada como la no licencia para poder extender el ancho de banda disponible. Para poder disponer de este ancho de banda no licencia una serie de imposiciones regulatorias deben ser consideradas

Para utilizar de forma eficiente el espectro no licenciado los sistemas 5G seguirán las siguientes características:

1. Diseño de **algoritmos PHY/MAC/network** ajustables a la naturaleza de la banda no licenciada. Cada una de las frecuencias dentro del ancho de banda tiene sus propias características por lo que un tratamiento especifico es necesario
2. Mecanismos de control y que permitan la **coexistencia con otros RATs** de forma que puedan operar todos al mismo tiempo
3. Técnicas que permitan **integrar y trabajar conjuntamente todas las RATs** operando en la misma frecuencia

Para poder cumplir con todos los requerimientos de la red 5G, se debe considerar también las tecnologías sobre el acceso radio deben considerarse. Es necesario desarrollar tecnologías a nivel de la arquitectura de sistemas desde el punto de vista de la red. 5G debe evolucionar hacia una arquitectura más plana y distribuida. Si pensamos en la actual topología de red existe un nodo dedicado en el Core que se encarga de gestionar una gran parte de la red así como centralizar todo el trafico a través suyo. Las consecuencias no deseables de este diseño serían:

- Incremento de la latencia de transmisión end-to-end debido a la longitud punto a punto
- Carga adicional del backhauling y del procesamiento de red en el Core
- Red poco confiable ya que se introduce un punto central de errores

En la arquitectura de red plana 5G, como muestra la Figura A.3, la movilidad de los usuarios será gestionada de forma eficiente y dinámicamente escalable poniendo la funcionalidad, en los limites de la red y adicionalmente, en los terminales móviles Los

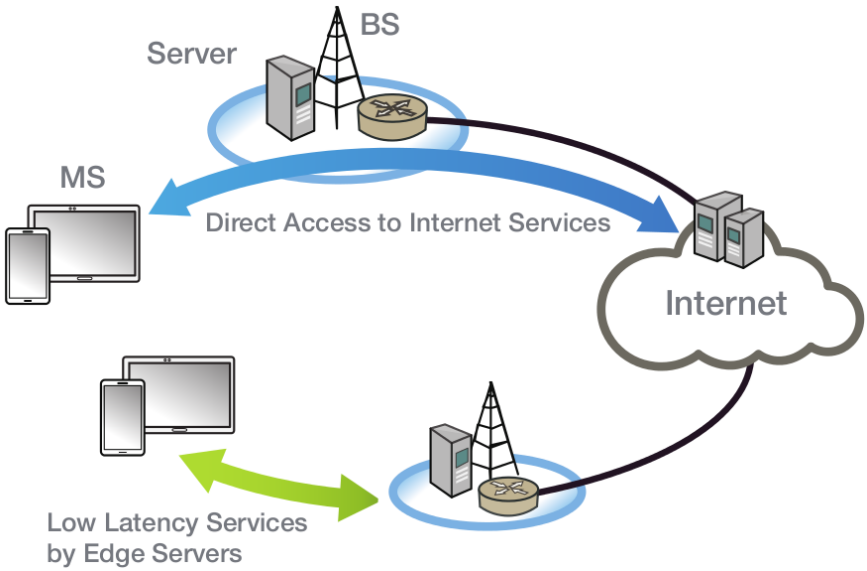


Figure A.3: Arquitectura 5G

principales beneficios serían

1. Esta gestión distribuida de la movilidad siempre facilita el camino más corto entre el terminal móvil e Internet sin tener que atravesar el centro de la red. Esto implica una reducción de la señalización y de los delays de transmisión. Asimismo situando servidores de aplicaciones en los limites de la red se consigue cumplir uno de los requerimientos claves de 5G, la baja latencia o latencia end-to-end inferior a 5ms
2. Facilita una solución altamente escalable comparado con una arquitectura centralizada donde un único nodo central gestionaba todo el trafico
3. Evita el riesgo de tener un único punto de errores. En un arquitectura plana el fallo de un nodo no afectaría al resto de nodos

Una de las tecnologías clave para poder dar respuesta a los requerimientos de la era 5G es el MIMO masivo. Los sistemas de MIMO masivo experimentan pequeñas interferencias inter-usuario e inter-celda y consecuentemente, consigue un mejor rendimiento que el MIMO original. Uno de los principales retos para construir sistemas de MIMO masivo es la limitación en el número de antenas que pueden ser equipadas en una estación base, debido a la forma de las ondas y las frecuencias de operación (ancho de banda, longitudes de onda, capacidad de la sala donde se aloja, etc...). Estas limitaciones practicas fueron las que motivaron la Full-Dimension MIMO (FD-MIMO), un sistema de comunicación entre celdas, que sitúa un gran número de antenas en un cuadro de 2 dimensiones en la estación base. Podemos verlo en la Figura A.4 El sistema FD-MIMO puede mejorar el rendimiento del sistema combinando la elevación, la dimension del azimuth y el Multi-Usuario MIMO (MU-MIMO). Estos sistemas están equipados con múltiples transceivers (TRX) que alimentan el cuadro de 2 dimensiones. Este tan elevado número de TRX incorporan nuevos retos tecnológicos, como la calibración de las antenas y problemáticas complejas relacionadas con el Channel State Information (CSI). El MU-MIMO asimismo, introduce nuevos retos relacionados con la complejidad de su programación y la adaptación del link

Comunicaciones D2D Avanzadas es una nueva tecnología que permite mejorar la eficiencia espectral y reduce la latencia end-to-end. Los terminales D2D pueden comunicarse de forma directa entre ellos siempre y cuando estén próximos. La comunicación D2D será utilizada para reducir la carga de la red. De esta forma, reduciremos el coste de procesamiento y señalización. La próxima versión mejorada del D2D fue recomendada posteriormente para ser utilizada en el Mission Critical Push-To-Talk (MCPTT) y Vehicle-to-Anything(V2X). Un único recurso radio puede ser reutilizado entre múltiples grupos que quieran comunicarse entre ellos si la interferencia producida entre ellos es tolerable. Con la utilización de comunicaciones D2D, es posible aumentar la eficiencia espectral y el número de conexiones simultaneas. Al enviar los datos directamente sin pasar por la red Core, la latencia end-to-end puede ser reducida de forma considerable.

Algunos ejemplos de comunicación D2D:

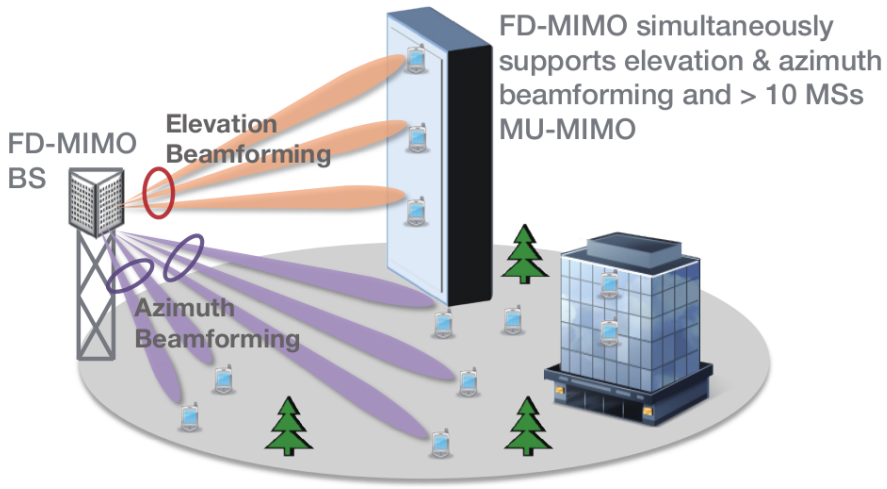


Figure A.4: Desarrollo FD-MIMO

- Vehículos pueden comunicarse entre ellos para intercambiar información de seguridad y obtener datos de entretenimiento sin necesidad de una estación base
- Los aparatos en casa se pueden comunicar entre ellos para automatizar servicios

En definitiva, si los dispositivos próximos pueden conectarse directamente, la IoT podrá ser una realidad próximamente

Para conseguir una mejora en el rendimiento será necesario desplegar un gran numero de celdas en una cierta área y poder gestionarlas de formas inteligente. Se prevee utilizar frecuencias más altas para poder utilizar el ancho de banda disponible en mmWave. La considerablemente alta propagación de perdidas en mmWave permite moldear un denso despliegue de pequeñas celdas que permitan un mayor reuso espacial . Mientras que en las topologías clásicas con un controlador central podemos encontrar limites, la nueva topología de cooperación en 5G donde existen estaciones base que cooperan entre ellas permitiendo que el usuario siempre se encuentre en el centro de la celda. Las nuevas tecnologías distribuidas y de "self-configuration" de red permitirán un despliegue más sencillo de muchas pequeñas estaciones base. Adicionalmente, el uso de in-band wireless backhaul en colaboración con las cooperativas estaciones base, reducen el coste y la complejidad del despliegue de la red

A.1.2 Arquitectura 5g

A.1.2.1 Vision Operador KT

Una de las empresas que ha sido pionera en el estudio y evolución de la tecnología 5G es el operador coreano KT. La visión de KT es la siguiente

- Core 5G Distribuido más cerca de las celdas. Más nodos en los limites
- RAN 5G: Rediseño del C-RAN y del Fronthaul
- Red Acceso 5G debe unificar acceso mobil y linea fija
- Arquitectura Software-Centric: Core 5G y el RAN 5G deben ser implementados como software en los servidores comerciales

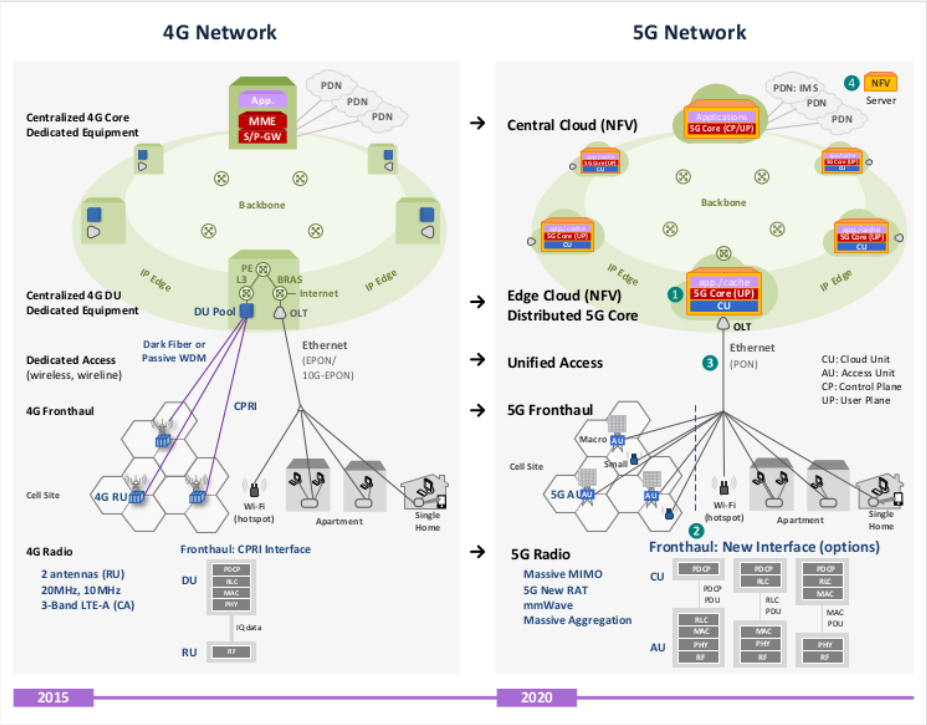


Figure A.5: 4G vs 5G

A.1.2.2 Core 5G Distribuido

La red 4G actual puede ser dividida como vemos en la Figura A.5 en:

- RAN (eNB)
- Core Network (SP-GW y MME). Encargado de movilidad, autenticación y facturación

En 4G todo el trafico debe pasar por el core de la red para acceder a los servicios. Esto implica que si existen pocos nodos de Core en una red, el trafico es intenso. P or ejemplo, en Korea el operador KT tiene 2 nodos en 2 ubicaciones en Seul, la capital

En cambio en la nueva tecnología 5G, el Core esta dividido en:

- MCU-UP (Core - User Plane) responsable de la entrega de bears
- MCU-CP (Core - Control Plane) responsable de las funciones de control

El plan del operador KT sería:

- Distribuir los nodos Core a decenas de nodos en las ubicaciones limítrofes a lo largo de la nación (Korea)
- Mantener el MCU-CP es su ubicación actual, en el cloud central NFV
- Redistribuir el MCU-UP a las decenas de nodos a lo largo de la nación en nodos cloud limítrofes (NFV)

Resumiendo, la idea es distribuir el Core 5G convirtiendo un Core Centralizado en un Core distribuido y plano

El hecho de mover el Core a ubicaciones limítrofes, cerca de las ubicaciones de las celdas, implica mover los servidores de aplicaciones. 5G permitirá comunicaciones a velocidades de 1Gbps haciendo que el trafico generado se dispare. Ubicando los Core a áreas locales, y asimismo los servidores de aplicaciones, el trafico backhaul se verá reducido de forma significativa, rebajando los costes de inversión también. La red 5G se supone que será capaz de proveer servicios en tiempo real como control remoto, control automático de vehículos, etc... Este tipo de servicios puede provocar un trafico inferior de vídeo pero requiere un delay ultra-corto. Estos delays tan bajos pueden ser conseguidos moviendo el Core cerca de los usuarios, y situando los servidores de estos servicios en tiempo real al lado del Core Una vez vista está distribución una pregunta que podría surgir sería si desaparece

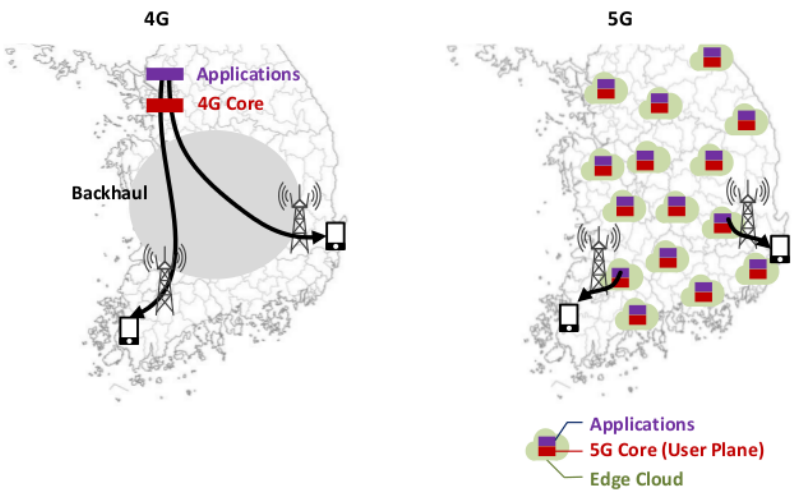


Figure A.6: Nodos

el nodo central. La respuesta es No. No todos las aplicaciones serán servidas desde los Cores Distribuidos. La ubicaciones del servidor de aplicaciones dependerá del tipo de aplicación servidas. Por ejemplo, el servicio IMS continuará siendo gestionado desde el Core Central mientras los servicios en tiempo real serán gestionados desde los Core Distribuidos. Resumiendo, MCU-CP y MCU-UP se mantendrán en el Core Central pero el MCU-UP tambien será distribuido desde los Core Distribuidos

A.1.2.3 RAN 5G

En la LTE C-RAN, Digital Unit (DU) y Radio Unit(RU) están conectados vía fibra dark o WDM pasivo, intercambiando trafico vía la interfaz CPRI. Actualmente, las señales base y datos IQ son transmitidos entre DI y RU requiriendo una tremenda capacidad CPRI. En la era 5G una vez que se empiecen a utilizar tecnologías como MIMO masivo, mmWare, New RAT que requieren de una gran capacidad, será necesario una capacidad de decenas o miles de Gbps por RU. Para gestionar los altos costes surgidos por la necesidad de una capacidad de trafico tan alta, varias ideas han sido propuestas:

- Compresión CPRI (Datos IQ)
- CPRI sobre Ethernet
- Radio analógica sobre fibra
- Función para separar el DU y el RU

De las ideas surgidas, el operador KT esta trabajando en la redefinicion de las funciones de DU y RU en el C-RAN actual, con la intención de mover las funciones del DU a las celdas. Con la idea de mover las funciones a las celdas, una nueva terminología ha sido tomada. Los términos nuevos, Cloud Unit (CU) y Acces Units (AU) serán utilizados en vez de DU y RU

A.1.2.4 Red Acceso 5G

- Integración de la red cableada con la red móvil.
- Actualmente, para la red cableada se utiliza E-PON, mientras que la red móvil utiliza el fronthaul CPRI
- La red cableada es una packet network que entrega frames Ethernet mientras la red móvil es un circuit network que entrega frames CPRI
- Entonces, serán unificadas las packet networks y circuit network? La respuesta será que en la futura 5G será más probable que exista una packet network entre CU y AU, que una red CPRI entre DU y RU
- Resumiendo, el plan sería agregar todo el trafico (casa, móvil y corporativo) a la red de acceso unificado

A.1.2.5 Arquitectura Software-Centric

Las funciones del RAN 5G y Core serán virtualizadas y implementadas como software en servidores comerciales. El Core 5G puede ser dividido en:

- Plano Usuario. Será instalado en los clouds limítrofes a lo largo de la nación
- Plao Control. Será instalado en el cloud central

Los servidores de aplicaciones serán ubicados en los clouds limítrofes. DU y RU serán redefinidos como el CU y AU. CU, basado en software, será instalado en el cloud limítrofe mientras el AU, basado en hardware, sera instalado en la celda. Resumiendo, en el cloud limítrofe, los servidores de aplicaciones, el plano de usuario del Core 5G y el CU del RAN 5G, son todos instalados como virtualizados. Todos estos son software por lo que pueden ser virtualizados

A.1.3 5G Slicing

A.1.3.1 5G Slicing

El **Slicing** es una nueva tecnología que permite al operador **separar (slice) una red física en múltiples , virtuales, end-to-end (E2E) redes, cada una de ellas asilada de forma lógica** incluyendo dispositivos, acceso, transporte y red Core, y dedicada para diferentes tipos de servicio con diferentes características y requerimientos. Para cada red separada **se garantizan recursos dedicados**. Como redes separadas y aisladas del resto, **un error o fallo ocurrido en una red separada no afecta a las comunicaciones en el resto de redes**

Hasta 4G la función principal de las redes móviles era ser utilizadas por los teléfonos móviles. A partir de la era 5G, **las redes móviles, deben servir a una variedad amplia de dispositivos** con diferentes características y necesidades. Algunas de las necesidades más importantes son:

- **IoT Masivo**
- **Misión Critica de IoT**
- **Ancho de banda móvil**

Todos los servicios tienen diferencias en términos de movilidad, facturación, seguridad, política de control, latencia, confianza, etc... Esto implica que debemos tener redes dedicadas para cada servicio? Una para teléfonos 5G, otra para IoT masiva y más? La respuesta es No, ya que **el Slicing nos permite tener múltiples redes lógicas sobre una única red física**

En la Figura A.7 podemos ver un ejemplo de **Slicing** y como se traduce en **Slices** en la Figura A.8

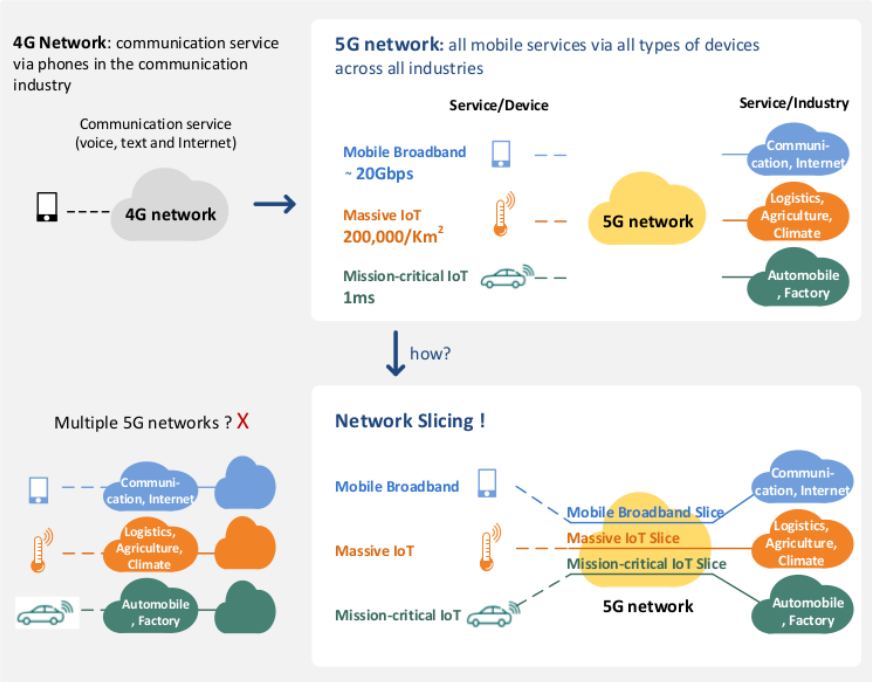


Figure A.7: Network Slicing

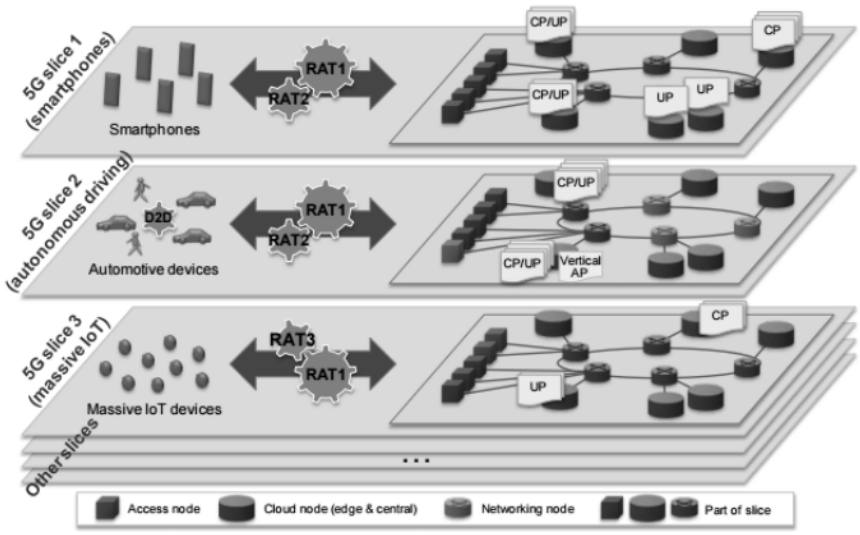


Figure A.8: Network Slice

A.1.3.2 Implementación Slicing

En la red móvil actual, los dispositivos principales son los móviles y las funciones RAN (DU y RU) y Core están desarrolladas con equipos de red dedicados, que han sido suministrados por los fabricantes RAN. Uno de los prerequisitos para implementar el Slicing, es el Network Function Virtualization (NFV). La principal idea del NFV es instalar las funciones de red S/W (p.e. MME, SP-GW y PCRF en Packet Core, y DU en RAN), en Maquinas Virtuales (VMs) instaladas en servidores comerciales virtualizados. Así, el RAN trabaja como un cloud limítrofe, mientras el Core trabaja como un cloud Core. La conectividad entre ambos esta provista usando SDN Entonces, las separaciones (Slices) se crean para cada servicio

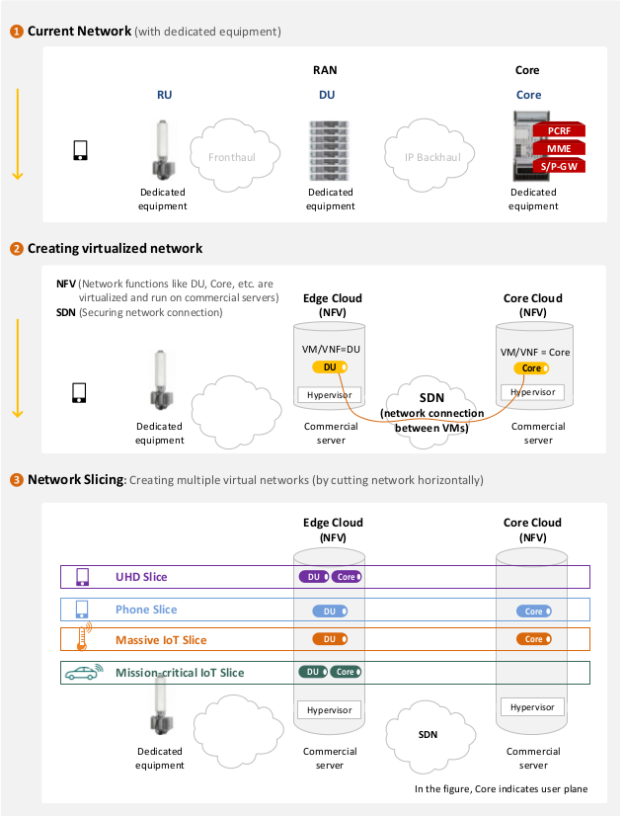


Figure A.9: Como se implementa el Slicing

Las separaciones (Slices) pueden ser configuradas como:

- **UDH**
  - DU Virtualizados, Core 5G (UP) y Servidor Cache en el cloud limitrofe
  - Core 5G Virtualizado (CP) y Servidor MVO en el cloud Core
- **Teléfono**. Core 5G (UP y CP) con características completas de movilidad, servidor IMS, todos virtualizados en el cloud Core
- **IoT Masiva**. Core 5G sin gestión de movilidad en el cloud Core
- **Mision Crítica de IoT**: Core 5G (UP) y los servidores asociados todos en el cloud limítrofe para minimizar los delays de trasmisión

Resumiendo:

- Se crean **Slices dedicados para servicios con diferentes requerimientos**
- Las **funciones de red virtualizadas se sitúan en diferentes ubicaciones** en cada Slice dependiendo del servicio
- Diferentes funciones de red son esenciales en alguna Slice pero innecesarias en otras Slices
- Los operadores de red, pueden **customizar las Slices** como ellos quieran, probablemente utilizando la fórmula de reducción de coste más efectiva

El siguiente ejemplo, en la Figura A.10, nos permitirá revisar como funciona la seguridad en la conexión de red entre VMs La conectividad Inter-VM se debe realizar sobre IP/MPLS SDN y su sub SDN, el Transport SDN. Centrándonos en el área de los routers IP/MPLS SDN suministrados por Ericsson y Juniper, ambos han presentado un arquitectura de red IP/MPLS SND bastante similar en términos de como se conectan las VMS a través de SDN. Aun las similitudes, si presentan alguna diferencia menor.

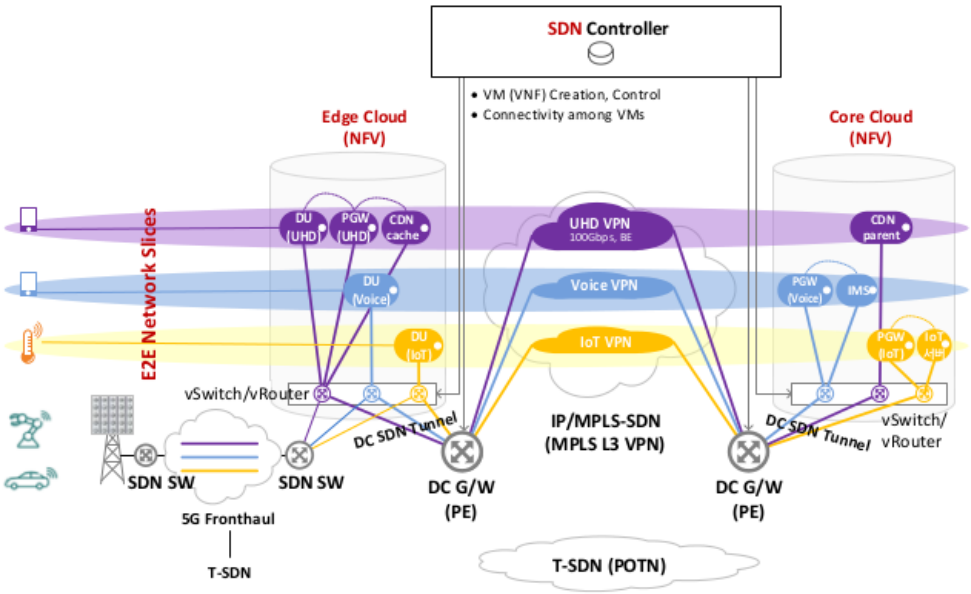


Figure A.10: Ejemplo Slicing

El el Core cloud existe un servidor virtualizado donde corre un built-in vRouter/vSwitxh. El controlador SDN realiza el provisionamiento de los servidores virtualizados y routers DC G/W, para poder crear túneles SDN entre cada VM, en el Core Cloud y el router DC G/W. El controlador SDN realiza el mapping entre esos túneles y el VPN MPLS L3. El proceso es similar si nos centramos en el Cloud limítrofe. Aquí se crean Slices IoT que se conectan del Cloud limítrofe al backbone IP/MPLS y de allí al Core Cloud.. Este último proceso puede ser implementado usando tecnologías estandard

El único punto pendiente existente, sería el Slice del fronthaul entre el Cloud limítrofe y el RU 5G. Primero se debe definir como debe ser el 5G fronthaul. Se han definido varias alternativas (p.e. introducir un nuevo fronthaul basado en paquetes mediante la redefinicion del DU y RU), pero sigue sin existir un estándar

A.2 IMS

A.2.1 Historia

IMS (IP Multimedia Subsystem) es un conjunto de especificaciones que describen la arquitectura de las redes de siguiente generación. IMS soporta telefonía y servicios multimedia a través de la conmutación de paquetes a direcciones IP. IMS define un marco de trabajo y arquitectura base para servicios e imágenes basado en redes IP. IMS utiliza el protocolo de sesión SIP para la señalización se sesiones

IMS fue definido por el congreso llamado 3G.IP en 1999. El objetivo era definir un framework que permitiera dotar de servicio multimedia IP a usuarios finales. IMS fue llevada a 3GPP como parte del trabajo de estandarización de sistemas 3G en la red UMTS. IMS apareció en la Release5 de UMTS (3GPP TS 22.228 Release5) cuando se incorporó el protocolo de sesión SIP (Session Initiation Protocol). En la Release6(3GPP TS 22.228 Release6) se añadieron nuevo requerimientos para soportar el acceso a redes diferentes a GPRS.

A.2.2 IMS

Los principales requisitos que se establecieron para IMS se describen a continuación

- Soporte para establecer sesión IP multimedia
- Soporte a mecanismos de negociación de QoS (Quality of Service)
- Soporte para la interrelación entre Internet y redes de circuitos interconectados (pe, PSTN)
- Soporte a Roaming
- Soporte para la creación rápida de servicios sin necesidad de estandarización
- Soporte al control rígido puesto por el operador en relación al servicio entregado al cliente final

Los protocolos en los que se basa IMS son los siguientes:

- Control de Sesión : SIP. El hecho que SIP permitiera crear nuevos servicios y que se basara en HTTTP, fue el determinante a la hora de escoger
- AAA: Diameter. Se escogió por si amplia utilización en Internet para AAA
- Otros Protocolos. H.248. Utilizado para el control de los nodos en el área multimedia

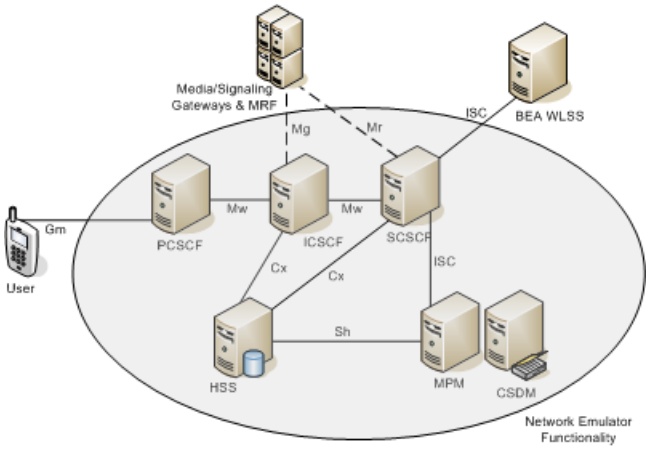


Figure A.11: Arquitectura IMS

Los elementos dentro de IMS

- **CSCF.Call Session Control Function**
  - ES un servidor SIP

  - Nodo esencial en la arquitectura IMS
  - Existen 3 tipos diferentes:
    * P-CSCF (Proxy-CSCF)
    * I-CSCF (Interrogating-CSCF)
    * S-CSCF (Serving-CSCF)

- **HSS. Home Subscriber Server**
- **SLF. Subscription Location Function**

El **P-CSCF (Proxy-CSCF)** es el primer punto de contacto entre el terminal de usuario (UE) y la red IMS. Actúa como un servidor proxy. Recibe todas las peticiones destinadas a la red IMS y las dirige en la dirección correcta. Incluye muchas funciones: seguridad, autenticación, validación de la integridad de mensajes SIP, compresión/descompresión de mensajes SIP. Genera información de tarificación para el nodo de recogida de datos. Generalmente, una red IMS incluye diferentes P-CSCF para asegurar la escalabilidad y redundancia.

El **I-CSCF (Interrogating-CSCF)** es un proxy SIP localizado en el borde del denominado, dominio administrativo. La dirección IP del I-CSCF esta dentro del DNS. Interconectada con el SLF y HSS. Esta interfaz esta basada en el protocolo Diameter. Obtiene información del perfil del usuario y lo enrute al servidor apropiado. Incorpora además interfaces contra AS (Applications Servers). Puede encriptar partes de los mensajes SIP que contienen información de usuario sensible. Generalmente, una red IMS incluye diferentes I-CSCF para asegurar la escalabilidad y redundancia.

El **S-CSCF (Serving-CSCF)** es el nodo central del área de señalización. El Servidor SIP que además realiza control de sesión. Incorpora una interfaz con el HSS con el protocolo Diameter

El **HSS (Home Subscriber Server)** es el repositorio central de información de usuario. Mantiene información de la suscripción de usuario para gestionar las sesiones multimedia del usuario. La red puede incorporar más de un HSS en caso que el número de suscriptores sea excesivo. Se implementa una configuración redundante para asegurar la gestión de la disponibilidad

El **SLF (Subscription Location Function)** es la base de datos que mapea direcciones de usuario contra HSS. Su función básica es en una red con múltiples HSS, es redirigir cada petición de usuario a su correspondiente HSS. En el caso de redes con un único HSS, no aparece. Implementa el protocolo Diameter en la interfaz con el HSS Las principales Interfaces involucradas en IMS son

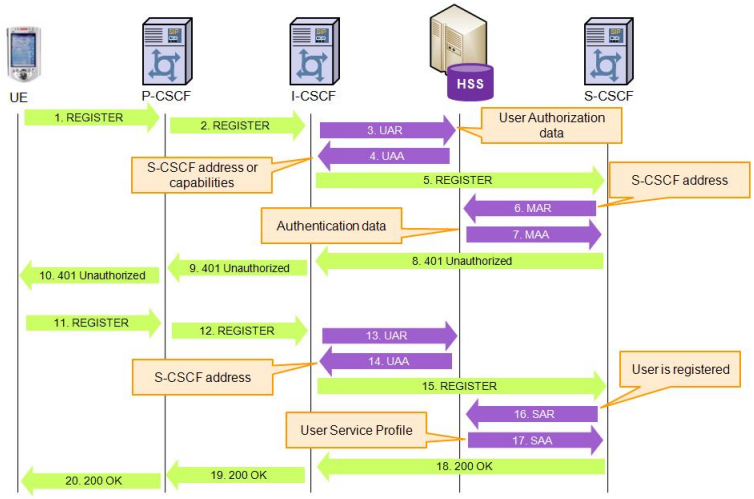


Figure A.12: Flujos IMS

- Interfaz Cx (I-CSCF/S-CSCF –> HSS) Protocolo Diameter Definido en TS29.229
- Interfaz Dx (I-CSCF/S-CSCF <-> SLF) Protocolo Diameter Definido en TS29.229
- Interfaz Gm (UE <-> P-CSCF) Protocolo SIP

- Interfaz Ma (I-CSCF <-> AS) Protocolo SIP

- Interfaz ISC (S-CSCF <-> AS) Protocolo SIP

A.2.3 VolTE

Es el acrónimo de Voice over LTE. Se basa en las redes IMS lo que implica que no existe dependencia en una red “circuit-switched”. Tiene hasta 3 veces más capacidad de voz y datos que 3G UMTS (y mas de 6 veces que 2g GSM). Es capaz de liberar más ancho de banda ya que las cabeceras de paquetes son mas pequeñas que las existentes en VoIP/LTE

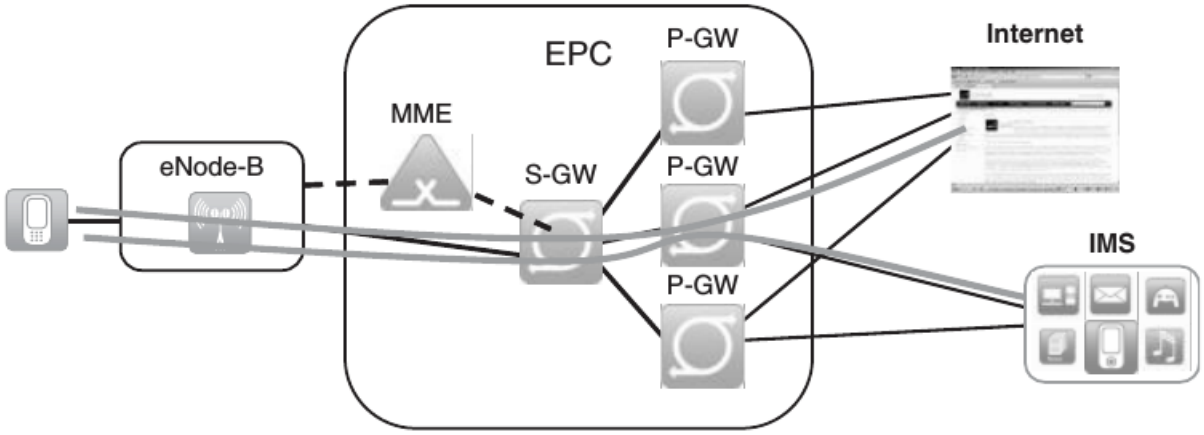


Figure A.13: Arquitectura VolTE

A.3 EMM

A.3.1 Liberación S1

En la siguiente Figura A.14 se describe el proceso de liberación del enlace S1 debido a la inactividad del usuario.

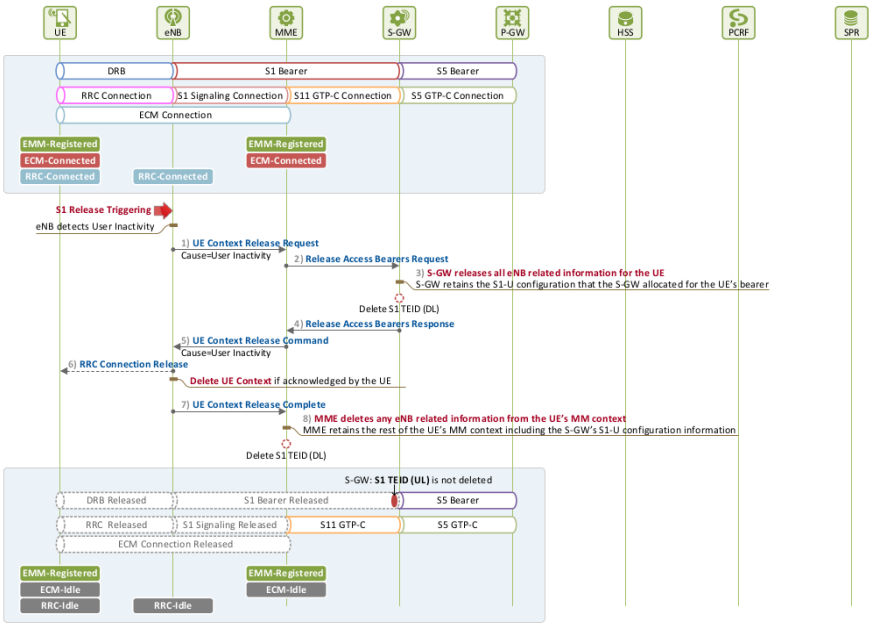


Figure A.14: Liberación S1 por inactividad Usuario

- **1) [eNB –> MME] Solicitando la liberación del contexto UE**. El eNB, una vez ha detectado la inactividad,envia al MME un mensaje **UE Context Release Request** para liberar el contexto UE
- **2) [MME –> S-GW] Solicitando la liberación del Bearer S1**. El MME solicita al S-GW la liberación de los recursos asociados al eNB enviando un mensaje **Release Access Bearers Request**. De esta forma informa al S-GW que no se debe entregar trafico de bajada al UE
- **3) [S-GW] Liberación del Bearer S1 de bajada**. El S-GW libera todos los recursos del bearer S1 de bajada asociados al UE, pero mantiene el enlace de subida sin liberar. De esta forma si llega trafico de subida, el eNB puede entregarlo utilizando el enlace de subida
- **4) [MME <– S-GW] Respondiendo a la petición de liberación del Bearer S1**. El S-GW informa que los recursos del Bearer S1 de bajada han sido liberados enviando un mensaje **Release Access Bearers Response**. Despues, si existe trafico de bajada destinado al UE, el S-GW lo almacena, y lo entrega solo en el caso que el enlace de bajada se volviera a establecer.
- **5) [eNB <– MME] Comando Liberación Contexto UE**. El MME envía al eNB un mensaje **UE Context Release Command** para liberar el contexto UE que ENB almacena
- **6) [UE <– eNB] Liberación Conexión RRC**. El eNB, una vez recibido el mensaje, elimina todo el contexto UE que mantenía. Si no se ha eliminadola conexión RRC aun, el ENB envía un mensaje **RRC Connection Release**. Una vez enviado, el eNB libera todos los recursos y bearers asociados al UE, y elimina el contexto UE
- **7) [eNB –> MME] Liberación contexto UE Completo**. El eNB envía un mensaje **UE Context Release Complete** como respuesta al mensaje enviado en el punto 5.
- **8) [MME] Liberación S1**. El MME elimina toda la información relacionada con eND a excepción del enlace de subida del bearer S1, en el contexto UE.

A.3.2 UE Inicia la Solicitud de Servicio

- **1 - Establecimiento conexión ECM**

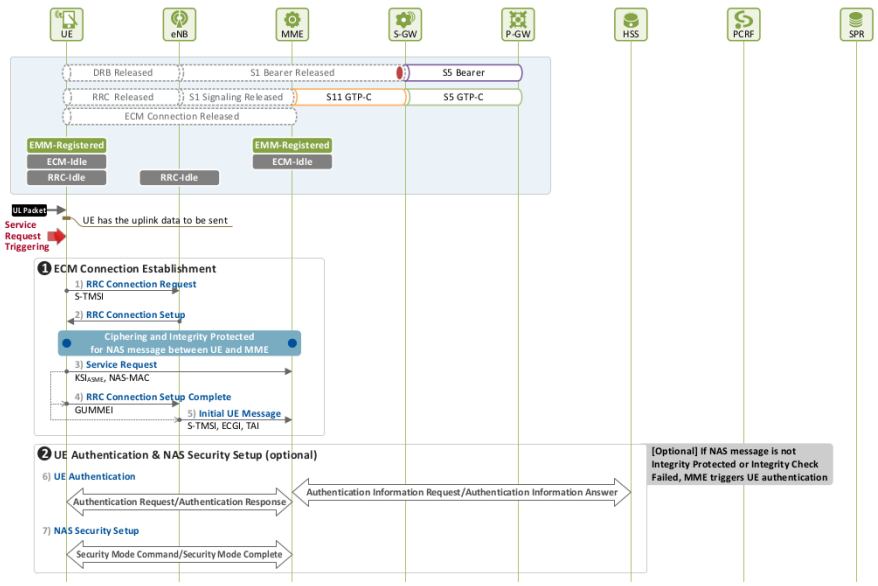
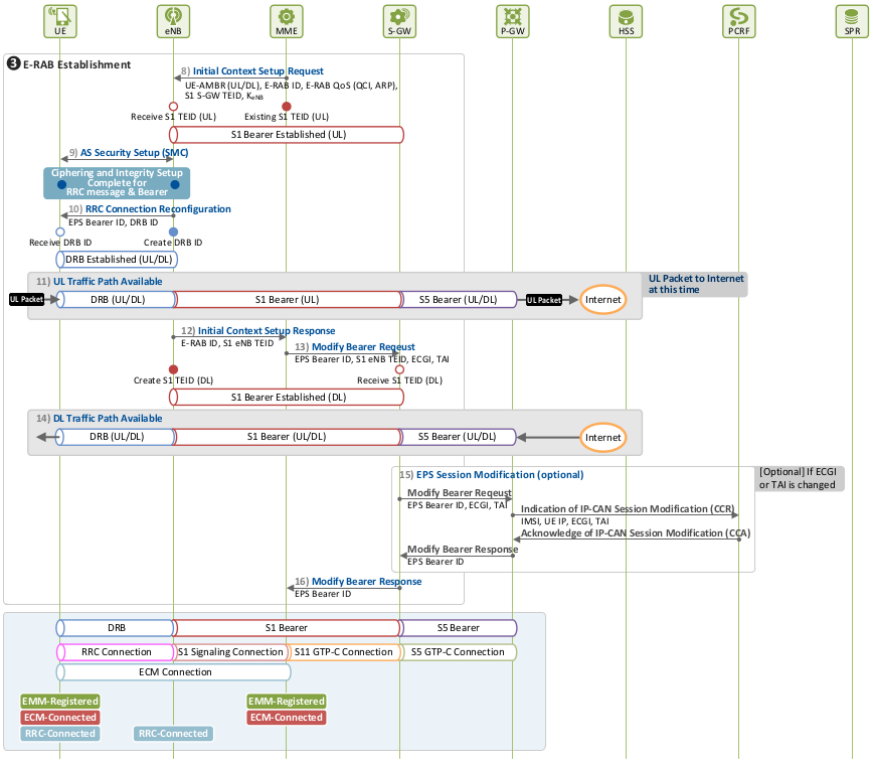


Figure A.15: UE Inicia la Solicitud de Servicio

- **1) 2) [UE - eNB] Configuración Conexión RRC**. La capa NAS en el UE provee la capa RRC con S-TMSI. La capa RRC envía un mensaje **RRC Connection Request** al eNB para configurar la conexión RRC. El eNB devuelve un mensaje **RRC Connection Setup** al UE
- **3) 4) 5) [UE –> MME] Solicitud Configuración Conexión ECM**. La capa NAS envía un mensaje **Service Request** al MME para configurar la conexión ECM. El contexto de seguridad NAS con el UE esta almacenado tanto en UE como MME. El mensaje incluye la identificador de clave base NAS (KSIasme)y esta encriptado con la clave de encriptación (KNASenc) y protegido con la clave de integridad (NASint). Este mensaje es entregado al eNB incluido dentro del mensaje **RRC Connection Setup Complete** sobre el enlace radio entre UE y eNB. Entonces es incluido en el mensaje S1AP **Initial UE MEssage** del eNB al MME.En este momento, el eNB asigna un eNB UE S1AP ID, y lo incluye en el mensaje **Initial UE Message** enviado al MME. Una vez recibido el mensaje, asigna un identificador MME S1AP UE ID, y establece una conexión de señalización S1 entre él y el eNB.

- **2 - Autenticacion UE y Configuración Seguridad NAS (Opcional**
  - **6) [UE - MME - HSS] Autentication UE**. Una vez recibido el mensaje **Service Request** del UE, el MME ejecuta una comprobación de integridad. Si pasa, el MME puede utilizar el contexto actual para enviar mensaje sin tener que volverse a autenticar. Si falla, el MME ejecuta los procesos de autenticación.
  - **7) [UE - MME] Configuración Seguridad NAS**. Cuando la autenticación esta completa, tanto EUE como MME generan las claves de seguridad NAS (KNASenc, KNASint)

- **3 - Establecimiento E-RAB**
  - **8) [eNB <– MME] Solicitando Establecimiento E-RAB**. Una vez recibido el mnesaje **Service REquest**, el MME se percata que se debe establecer un E-RAB. Por tanto, envía un mensaje **Initial Context Setup Request** al eNB para que vaya estableciendo un bearer S1 con S-GW, y un DRB con UE.
  - **9) [UE – eNB] Configuración Seguridad AS**. Despues de recibir el mensaje **Initial Context Setup Request** del MME, el eNB se percata que se debe realizar la configuracion tanto del bearer S1 como el DRB. Previamente, el eNB realiza la configuración de los procedimientos para establecer la seguridad en las comunicaciones. Tanto UE como eNB derivan las claves para gestionar la integridad y encriptacion.
  - **10) [UE <– eNB] Establecimiento DRB**. El eNB asigna un DRB ID para crear el DRB, un bearer EPS sobre enlace radio, y envía un mensaje **RRC Connection Reconfiguration**. El UE, una vez recibido el mensaje del eNB, genera un DRB y un SRB2



- **11) Disponibilidad path trafico subida UL**. Una vez el DRB se ha generado, un bearer EPS de subida es configurado desde el UE hasta el P-GW, permitiendo entregar trafico de subida.
- **12) 13) 16) [eNB –> S-GW] Configurando Bearer S1 bajada DL**.
  - 12) eNB asigna un S1 eNB TEID de bajada para el bearer S1 y lo envía al MME, incluyendolo en el mensaje **Initial Context Setup Response**
  - 13) El MME entrega un S1 eNB TEID incluido en el mensaje **Modify Bearer Request** al S-GW
  - 16) El S-GW informa al MME del establecimiento del bearer S1 de bajada a través de un mensaje **Modify Bearer Response**
- **14) Disponibilidad path trafico bajada DL**. Es creado un tunnel de bajada S1 GTP-U del S-GW al eNB, completando el establecimiento de un bearer EPS de bajada
- **15) Modificando Sesión EPS (Registro Localización UE)**. En el caso que la celda actual (ECGI) o el TA haya cambiado durante el proceso de petición de servicio, el S-GW informa al P-GW del cambio. Entonces, el P-GW hace lo propio con el PCRF

A.3.3 Red Inicia la Solicitud de Servicio

En la Figura A.16 de la [8] se describe el proceso en el que la red inicia la solicitud para establecer la conexión ECM

- **1 - Ejecución Petición Servicio**. Si el S-GW recibe paquetes de bajada del P-Gw pero no puede enviarlo al eNB porque el bearer S1 de bajada esta liberado, almacena los paquetes, y averigua en que MME se ha registrado el UE. Entonces, el S-GW envía un mensaje **Downlink Data Notificaction** al MME informando de las conexiones de señalización y bearers que se necesitan establecer con el UE
- **2 - Paging**. El MME conoce la localización del UE en uno de sus TA's pero no sabe en que celda. Entonces el MME envía un mensaje de Paging a todas las eNBs donde estuvo por el UE. El eNB hace broadcast del mensaje a través del PCH (Paging Channel), asi el UE puede recibirlos durante su conexión regular.
- **3 - Establecimiento Conexión ECM**. Una vez identifica que existe trafico para él, el UE envía un mensaje **Service Request** para establecer la conexión ECM. Los procesos para establecer la conexión ECM comienzan cuando el UE accede a la celda

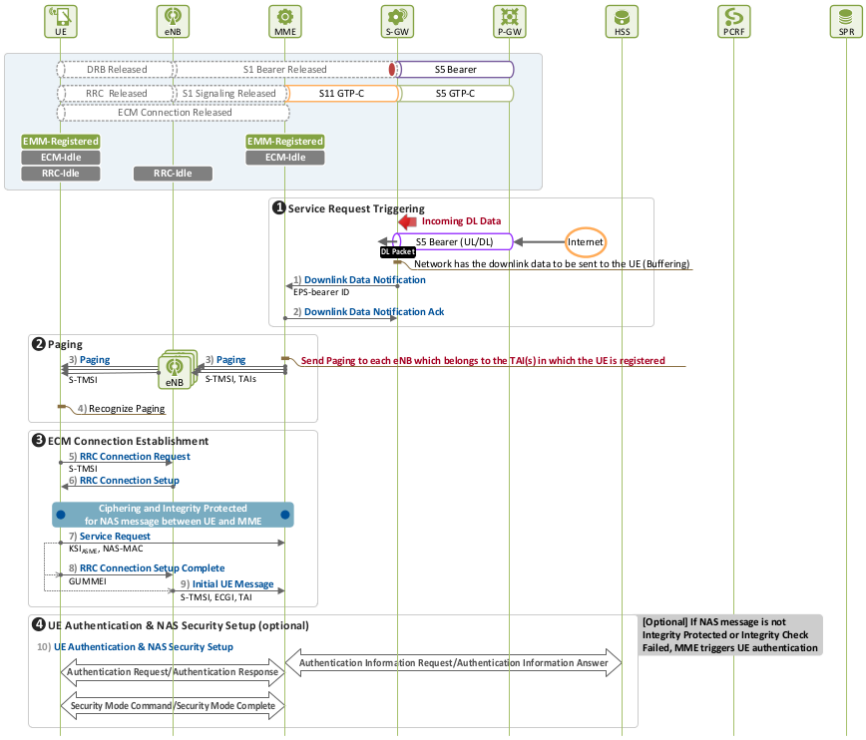


Figure A.16: Red Inicia la Solicitud de Servicio

a través del canal de enlace radio, y entonces, envía un mensaje **RRC Connection Request** para establecer la conexión RRC.

- **4 - Autenticación UE y Configuración Seguridad NAS**. El MME, una vez recibido el mensaje, ejecuta los procesos de autenticación.
- **5 - Establecimiento E-RAB**. Después de recibir el mensaje **Service Request** del UE, el MME establece un DRB y un bearer S1 de bajada

A.3.4 Proceso TAU Periódico

1 - Ejecutando TAU Periódico

- **1) [UE] Temporizador TAU expirado**. El UE en estado inactivo inicia un procedimiento de TAU periódico para reportar su localización una vez ha expirado su temporizador

2 - Establecimiento Conexión ECM y Reporte TA

- **2) 3) [UE - eNB] Establecimiento conexión RRC**. UE envía al eNB un mensaje **RRC Connection Request** solicitando recursos radio. El eNB asigna una conexión RRC y confirma enviando un mensaje **RRC Connection Setup**
- **4) 5) 6) [UE –> MME] Petición Establecimiento Conexión ECM y Reporte TA**.
  - El UE envía un mensaje **TAU Request** incluido en un mensaje **RRC Connection Setup Completed** del UE al MME y posteriormente incluido en el mensaje **Initial UE Message** del eNB al MME.
  - Como el contexto de seguridad NAS sigue siendo valido entre el UE y el MME, el mensaje esta protegido con la clave de integridad KNASint y encriptado con la clave KNASenc.
  - El mensaje **TAU Request** incluye la siguiente información (Update Type = Periodic Updating, Active Flag = 0, GUTI, Last Visited TAI, KSIasme, NAS-MAC).
  - eNB asigna un eNB S1AP UE ID al MME con el mensaje **Initial UE Message**

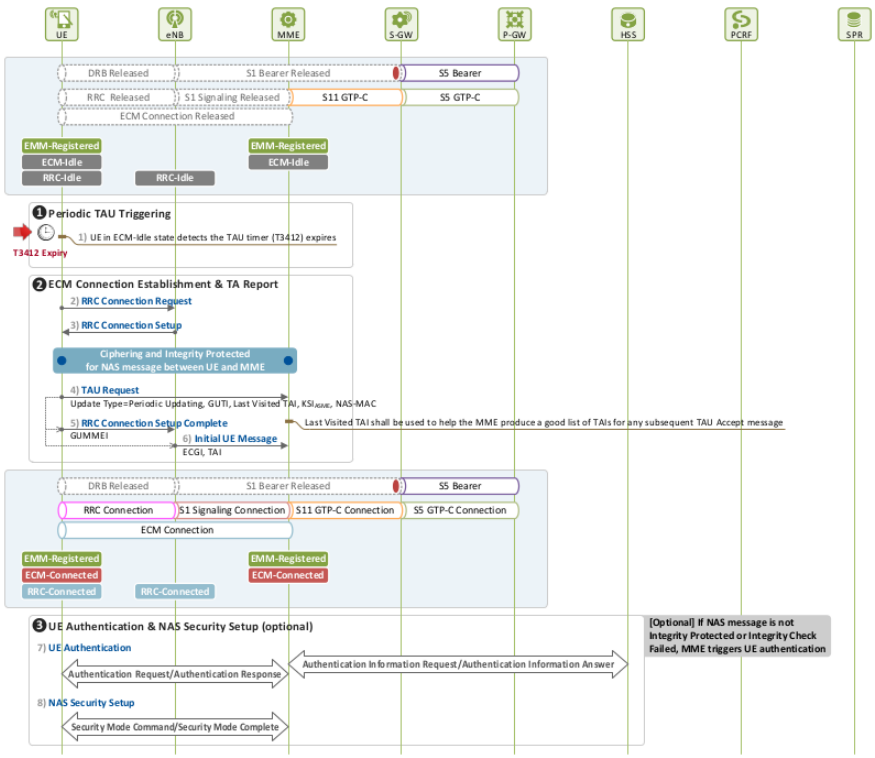


Figure A.17: Proceso en el TAU Periódico

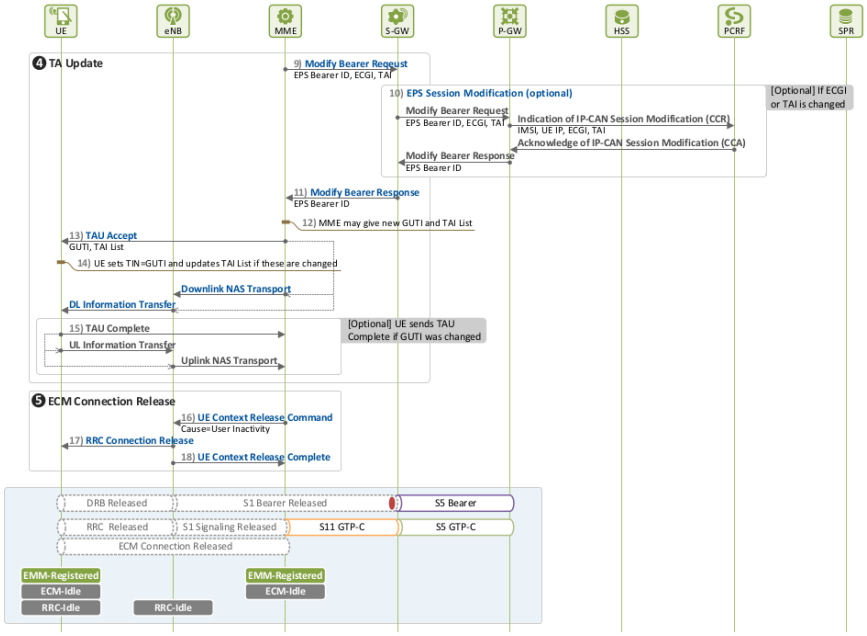
– MME asigna un MME S1AP UE ID estableciendo la conexión de señalización S1

3 - Autenticación UE y configuración seguridad NAS

- **7) [UE - MME - HSS] Autenticación UE**. El MME una vez recibido el mensaje **TAU Request** realiza una validación de integridad en el NAS-MAC. Si pasa, el MME obvia la autenticación UE y continua utilizando el contexto de seguridad NAS almacenado. Si no pasa, tiene que ejecutar la autenticación UE
- **8) [UE - MME] Configuración de seguridad NAS**. Una vez el UE ha sido autenticado, se generan las claves de seguridad NAS (KNASenc,KNASint) que serán utilizadas en los mensajes NAS

4 - Actualización TA

- **9) [MME –> S-GW] Actualización TA**. Cuando el MME recibe el mensaje **TAU Request**, resetea el temporizador TAU y envía al S-GW un mensaje **Modify Bearer Rquest**, actualización la localización del UE (ECGI, TAI)
- **10) Modificación Sesión EPS**. El S-GW una vez recibida la información de la localización del UE valida si ha cambiado la información de la celda del UE o la TA. Si ha cambiado, envía un mensaje **Modify Bearer Request** al P-GW para informar del cambio. Este a su vez, informa de lo mismo al PCRF a través de un procedimiento de modificación de sesión EPS
- **11) [MME <– S-GW] Respondiendo a una petición de actualización TA**. El S-GW envía un mensaje **Modify Bearer Response** al MME respondiendo a 9)
- **12) [MME] Preparando mensaje TAU Accept**. El MME puede configurar una nueva TAI list para reflejar los cambios en la localización UE
- **13) [UE <–MME] Enviando Mensaje TAU Accept**. El MME envía al UE un mensaje **TAU Accept**. Este mensaje se entrega a través de un mensaje **Downlink NAS Transport** del MME al eNB, y posteriormente en un mensaje **DL Information Transfer** del eNB al UE
- **14) [UE] Actualización TIN y TAI List**. Cuando el UE recibe un mensaje **TAU Accept** del MME, valida los valores GUTI y TAI List. Si estos han cambiado, actualiza el TIN y la TAI List. El TIN es un user ID a utilizar la próxima vez que el UE envie un mensaje **TAU Request** y es actualizado con el GUTI que había sido incluido en el mensaje **TAU Accept**



- **15) [UE] Puesta en conocimiento del Nuevo GUTI**. Si se ha asignado un nuevo GUTI, el UE envía un mensaje **TAU Complete** al MME, informando de la recepción del nuevo GUTI

5 - Liberación Conexión ECM

- **16) [eNB <–MME] Solicitando al E-UTRAN que libere el contexto UE**. Despues de actualizar la información de localización del UE, el MME envía un mensaje **UE Context Release Command** al eNB para liberar la conexión ECM, y para liberar el contexto UE
- **17) [UE <– eNB] Liberando la conexión RRC**. Una vez recibido el mensaje **UE Context Release Command** del MME, el eNB libera el contexto UE, y libera todos los recursos E-UTRAN. Por último envía un mensaje **RRC Connection Release** para liberar la conexión RRC
- **18) [eNB –> MME] Anuncio de la liberación del contexto UE del E-UTRAN**. El eNB envía un mensaje **UE Context Release Complete** al MME informándole que la conexión ha sido liberada. Por último,la conexión ECM que se había establecido con el mensaje **TAU Request** es liberada, y el UE transita otra vez a inactivo

A.3.5 Proceso Handover X2

- **Antes Handover**
  - eNB A da servicio al UE. El UE detecta el evento de medición y envía un mensaje **Measurement Report** al eNB A
- **Preparación Handover**
  - eNB origen (eNB A) elige un eNB destino para realizar el Handover basándose en la información del mensaje **Measurement Report**
  - eNB origen y destino, preparan el Handover X2 a través de la señalización X2
  - eNB destino asigna los recursos a priori para dar cobertura a los mismos servicios que el UE esta disfrutando con el eNB origen
  - Para acelerar el proceso, el eNB destino envía toda la información necesaria para realizar la conexión con la celda destino al eNB origen, que se la reenvía al UE, iniciando el proceso de Handover
  - Los pasos y recursos durante el proceso de preparación de Handover:
    * El eNB origen envía un mensaje **Handover Request** que incluye la información de contexto del UE
    * El eNB destino obtiene la información del bearer S1 (S1 S-GW TEID) para establecer el bearer S1 UL a través del cual enviar mensaje de subida (UL)

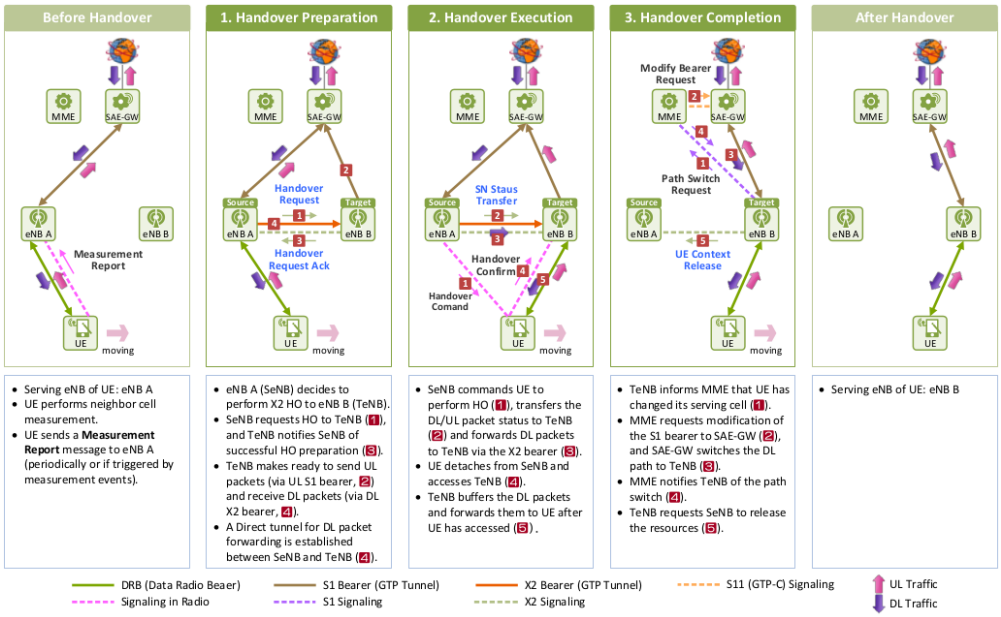
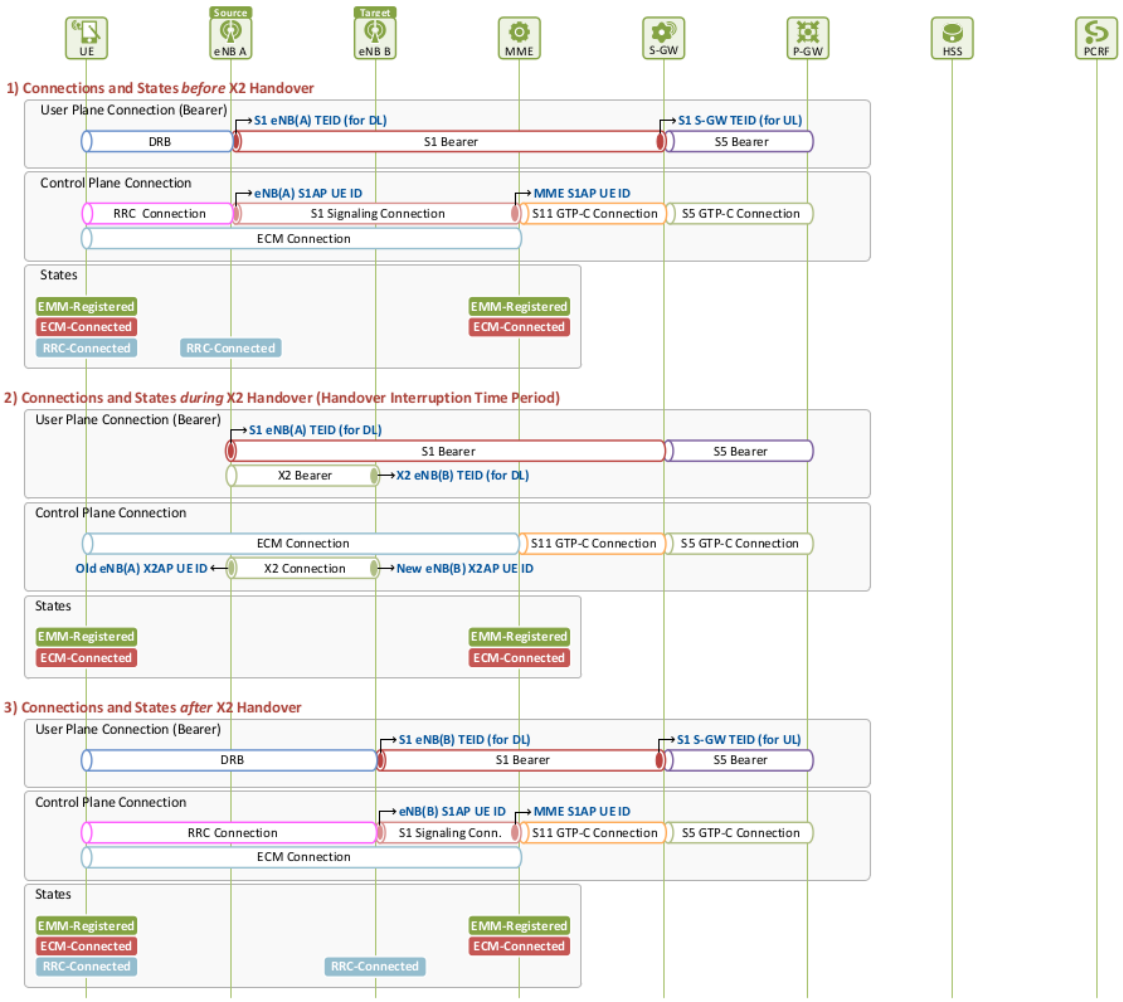


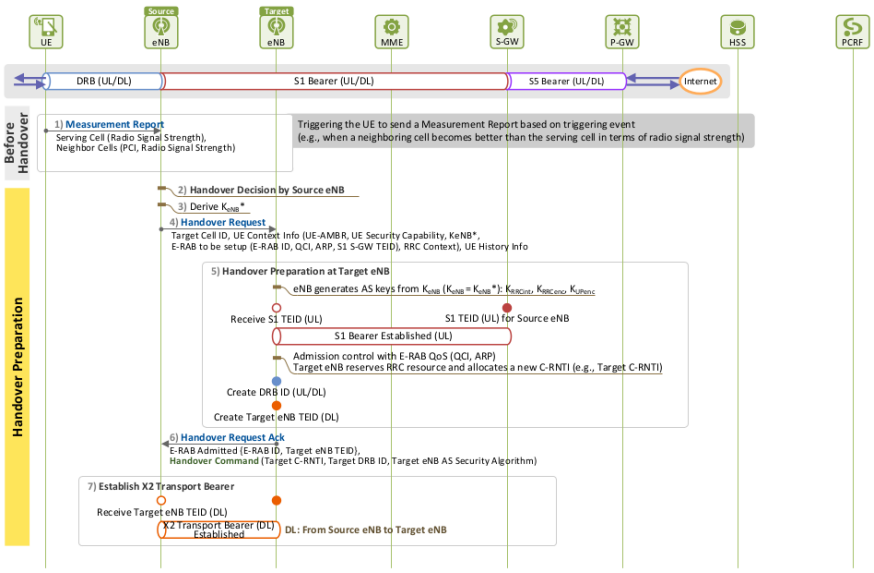
Figure A.18: Etapas del proceso de Handover X2

    - eNB destino asigna TEID para el bearer de transporte X2 a través del cual recibir mensaje de bajada (DL)
    - eNB destino asigna recursos DRB y C-RNTI para ser utilizados por el UE en la celda destino
    - eNB destino envía un mensaje **Handover Request Ack** a eNB origen
    - Una vez recibe el mensaje, el eNB origen establece un bearer de transporte X2 a través del que enviar paquetes de bajada DL

- **Ejecución Handover**
  - eNB origen informa al UE que ejecuta el Handover a la celda destino enviándole un mensaje **Handover Command**
  - eNB origen informa desde que paquete de UL/DL el eNB destino debe recibir o enviar cuando comunique cone el UE enviándole un mensaje **SN Status Transfer**
  - eNB origen reenvía los paquetes DL recibidos del S-GW al eNB destino a través del bearer de transporte X2 establecido entre él y el eNB destino
  - UE se desconecta del eNB origen y accede al eNB destino
  - eNB destino pasa a ser capaz de enviar y recibir paquetes una vez el UE se ha conectado con éxito
- **Finalización Handover**.
  - Una vez el UE ha accedió al eNB destino, el eNB informa al EPC y envía un mensaje **Path Switch Request** al MME, de forma que el bearer EPS sea establecido con el nuevo path correcto
  - Una vez recibido el mensaje, el MME conoce la nueva celda que da servicio al UE. MME solicita al S-GW la modificación del bearer S1
  - S-GW establece un bearer S1 DL (S1 Target eNB TEID) que conecta a eNB destino. Después, deja de enviar paquetes DL al eNB origen, y empieza a enviarlos al eNB destino a través del nuevo bearer DL establecido
  - MME informa al eNB destino que el path del bearer S1 ha sido modificado
  - eNB destino envía al eNB origen un mensaje **UE Context Release** permitiendo al eNB origen liberar el contexto de UE
- **Despues Handover**
  - eNB B es el que da ahora servicio al UE



- **Antes Handover X2**
  - El UE se mantiene en el estado **EMM-Registered** y **ECM/RRC-Connected** y mantiene todos los recursos asignados
- **Durante Handover X2**
  - Durante la fase de Handover, el UE no cambia de estado en la capa NAS, aun cuando no existe conexión radio
- **Despues Handover X2**
  - El UE se mantiene en **EMM-Registered** y **ECM/RRC-Connected**. El path E-RAB(DRB + Bearer S1) cambia al nuevo eNB en el panel de usuario y en el panel de control se establece una nueva conexión RRC y señalización S1
- **Antes Handover**
  - **1) [UE –> eNB] Reporte Medición**
    - Cuando se ejecuta el evento, el UE realiza una medición de la potencia de señal de las celdas vecinas y envía un mensaje **Mesaurement Report** a su eNB asociado
- **Preparación Handover**
  - **2) [eNB origen] Decisión de Handover**
    - El eNB origen selecciona un eNB destino basandose en la información incluida en el mensaje **Measurement Report**



- **3) [eNB origen] Derivación claves Seguridad para utilizar con el nuevo eNB destino**
  - Durante un Handover X2 se debe asegurar la entrega de paquetes de forma segura. En este tipo de Handover, no existe una involucración del MME, por lo que la derivación de las claves es realizada por el eNB que se encarga de proporcionarlas al eNB destino
- **4) [eNB origen –> eNB destino] Solicitando Handover X2**
  - El origen eNB solicita el Handover enviando un mensaje **Handover Request** al eNB destino. En este mensaje se entrega la información de contexto del UE.
- **5) [eNB destino] Preparando Handover X2**
  - Una vez recibido el mensaje de **Handover Request**, el eNB destino inicia la preparación del Handover
    i) Deriva las claves de seguridad AS (KRRCint, KRRCenc,KUPenc) de la clave KeNB. Utilizando estas claves, el eNB destino puede comunicarse de forma segura con el UE a través del enlace radio
    ii eNB valida que puede proveer la misma QoS que el eNB origen. Si puede, establece un Bearer S1 UL con el S-GW a partir de la información que posee del eNB origen (S1 S-GW TEID)
    iii Basándose en la información de QoS, el eNB destino reserva los recursos RRC a ser utilizados en el enlace radio, y asigna un C-RNTI
    iv) Mientras se ejecuta el Handover, los paquetes DL que llegan al eNB origen se reenvían al eNB destino. Para ello, el eNB destino asigna un X2 TEID para el eNB destino (DL TEID del túnel GTP X2) de forma que puede establecer un bearer X2 de transporte (túnel GTP)
- **6) [eNB origen <– eNB destino] Notificando la finalización de la preparación**
  - El eNB destino envía información de todos los recursos preparados al eNB origen incluidos en el mensaje **Handover Request Ack**
- **7) [eNB origen] Establecimiento Bearer X2 para entregar paquetes DL**
  - Una vez recibido el mensaje **Handover Request Ack**, el eNB origen sabe que el eNB destino puede dar servicio al UE. Entonces, utilizando su **X2 Target eNB TEID** empieza a establecer un bearer de transporte X2 de forma que puedan ser reenviados los paquetes DL al eNB destino
- **8) [UE <– eNB origen] Ordenando el Handover**
  - Una vez el eNB origen ha completado la preparación, ordena empezar el Handover enviando un mensaje **Handover Command**
- **9) [UE] Ejecutando el Handover**
  - El UE, del mensaje recibido, extrae el C-RNTI y el DRB ID a ser usado con el eNB destino, y se desconecta el eNB origen. Todo envío entre el eNB origen y el UE separa, y empieza el tiempo de interrupción del Handover.
- **10) [UE] Configuración Seguridad AS**
  - El UE deriva las claves de seguridad AS a ser utilizadas en el enlace radio con el eNB destino.
- **11) [eNB origen –> eNB destino] Notificando el número de paquetes a Enviar/Recibir**
  - El eNB origen informa al eNB destino a partir de que paquetes debe recibir (o enviar) del UE enviando un mensaje **SN Status Transfer**.

    - Se incluye en el mensaje, el DL Count (número de paquete a enviar primero al UE) y el UL Count (número de paquete a recibir del UE)
    - Después de enviar el mensaje **SN Status Transfer**, el eNB origen empieza a reenviar los mensajes DL que le llegan del S-GW, al eNB destino a través del bearer de transporte X2.
    - El eNB destino almacena los mensajes mientras espera que se complete el acceso del UE
- **12)-14) [UE,eNB destino] Acceso UE al eNB destino**
    - 12) El UE detecta la señal para ejecutar la sincronización con el eNB destino. Una vez sincronizado, el UE inicia el acceso
    - 13) El eNB destino envía al UE la información de alineamiento de tiempo y el acceso UL
    - 14) El UE envía el mensaje **Handover Confirm** al eNB destino incluido en el mensaje **RRC Connection Reconfiguration Complete**. Ahora el UE puede enviar/recibir paquetes a/del eNB destino, y finaliza el tiempo de interrupción
- **15) [UE - eNB destino] Comunicaciones seguras sobre el enlace radio**
    - Todos los mensajes de señalización RRC y paquetes de usuario ahora son enviados de forma segura utilizando las claves RRC. La señalización RRC esta protegida de integridad y encriptada, y los paquetes de usuario encriptados antes de ser enviado
- **16) [eNB destino] Continuando entrega de paquetes DL al UE**
    - Como el UE esta correctamente conectado al eNB destino, esté empieza a enviar los paquetes DL almacenados previamente al UE a través del nuevo path
    - En el caso de los paquetes enviados por el UE, el eNB destino revisa que esten en el orden correcto, y posteriormente, los reenvia al S-GW a través del nuevo path
- **17) [eNB destino –> MME] Solicitando el cambio de path del Bearer EPS**
    - El eNB destino notifica al MME que la celda de servicio del UE ha sido cambiada enviando un mensaje **Path Switch Request**, y solicita el cambio del path del bearer EPS
- **18)-23) Modificando el Bearer EPS**
    - El MME reenvia el S1 Target ENB TEID que fue asignado al eNB destino enviando un mensaje **Modify Bearer Request**. De esta forma, el S-GW informa que el bearer S1 DL ha sido modificado, y solicita el cambio del path de forma correspondiente.
    - S-GW establece el bearer S1 DL conectando con el eNB destino
    - El S-GW envía un mensaje **Modify Bearer Request** al P-GW informandole que la celda que da servicio al UE ha cambiado.
    - El P-GW se encarga de informar al PCRF
- **24) [S-GW] Modificando el path del Bearer EPS y enviando Paquetes EM**
    - S-GW modifica el path de entrega de paquetes DL al bearer S1 que esta conectado al eNB destino. Primero envía una marca de fin (EM) indicando que es el ultimo paquete al Bearer S1 que esta conectado al eNB origen. Luego envía paquetes DL al ENB destino a través del Bearer S1 DL
- **25) [eNB destino] Reordenamiento de paquetes**
    - Ahora el eNB destino recibe paquetes DL reenviados desde el eNB origen a través del Bearer de Transporte X2 además de los recibidos del S-GW del bearer S2 de bajada modificado.
    - El eNB destino debe ser capaz de reordenar todos los paquetes en el orden correcto
- **26) [eNB destino <– MME] Notificando la modificación del path Bearer**
    - El MME notifica al eNB destino que el S-GW ha cambiado el path del bearer EPS enviando un mensaje **Path Swith Request Ack**
    - El MME tambien envía el contexto de seguridad necesario para realizar un Handover NH Chaining Count(NN), Next Hop(NH) así el eNB destino puede usarlo en el próximo Handover del UE a otra celda
- **27) [eNB origen <– eNB destino] Notificando la liberación del contexto UE**
    - El eNB destino mantiene NCC,NH y envía al eNB origen un mensaje **UE Context Release** informado que el contexto UE puede ser liberado y que el path del bearer UE ha sido cambiado

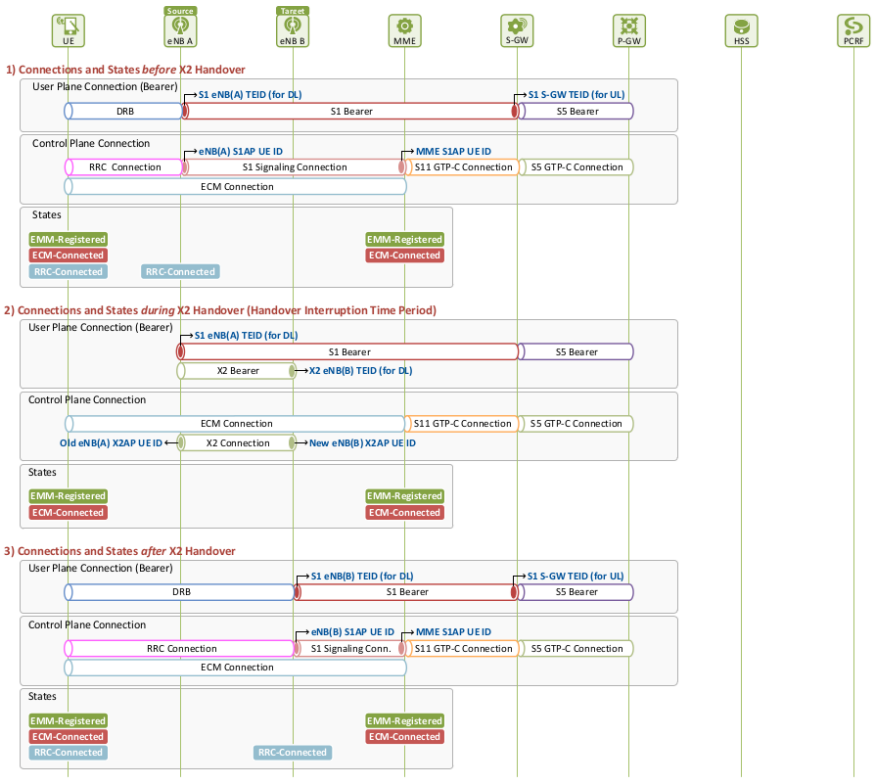
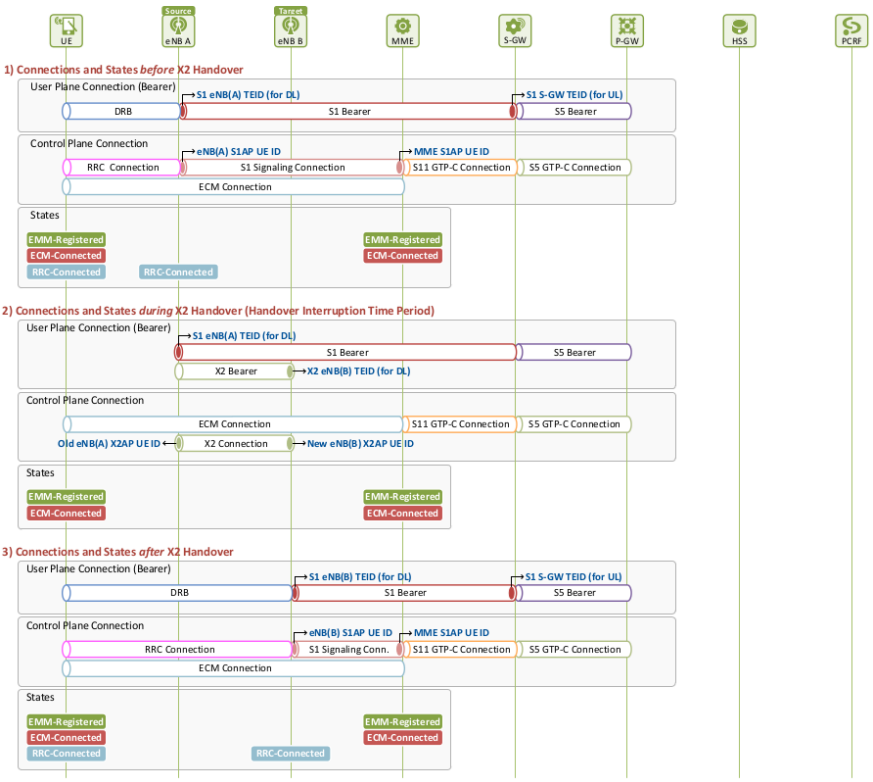


Figure A.19: Conexiones y estados durante el proceso de Handover S1

A.3.6 Proceso Handover S1

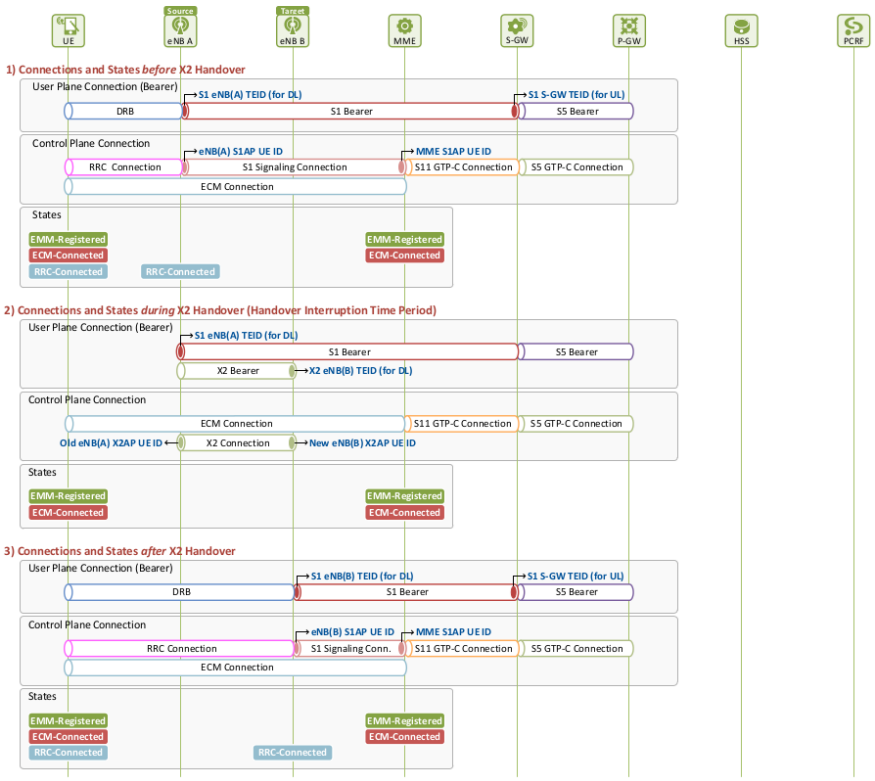
- **Antes Handover S1**
  - UE esta conectado a través del eNB A.
  - Cuando el UE detecta un evento de medición, envía un mensaje **Measurement Report** al eNB A
- **Preparación Handover S1**
  - El eNB A selecciona un eNB destino (eNB B) para ejecutar el Handover a través de la información del mensaje **Measurement Report**
  - Una vez identificado que el Handover X2 no es posible, se decide realizar un Handover S1 a través del MME
  - Ambos eNB, destino y origen, se comunican con el MME a través de la señalización S1AP
  - El eNB destino asigna recursos con antelación, para asegurar que dará la misma QoS al UE que tenía anteriormente
  - El MME facilita al eNB origen la información necesaria para que el UE se conecte a la celda destino
  - El eNB destino y el S-GW asignan los recursos necesarios para crear un túnel indirecto a través del cual, los paquetes DL que lleguen al eNB origen se reenvien al S-GW y posteriormente, al eNB destino mientras se completa el Handover
- **Ejecución Handover S1**
  - El eNB origen
    - Indica al UE que debe realizar un Handover a una celda destino
    - Informa al MME a partir de que paquetes UL/DL debe recibir/enviar del/al UE
    - Envía los mensajes DL recibidos por el S-GW al eNB destino a través del túnel indirecto creado anteriormente
  - MME informa al eNB destino a partir de que paquete UL/DL debe recibir/enviar del/al UE
  - UE se desconecta del eNB origen y se conecta al eNB destino

- **Finalización Handover S1**
  - El eNB destino, una vez el UE se ha conectado a él, informa al MME que el UE ha completado el Handover
  - El MME solicita al S-GW la modificación del bearer S1
  - El S-GW
    - Modifica el path del bearer DL S1 para que ahora indique la conexión al eNB destino
    - El S-GW deja de enviar mensajes DL al eNB origen, habiéndole informado previamente
    - El S-GW crea un bearer S1 DL que conecta al eNB destino y empieza a entregarle mensajes DL
  - El eNB destino envía paquetes al UE por el túnel indirecto hasta que el MME le informa, y comienza a utilizar el path nuevo asignado por el S-GW
  - El MME:
    - Solicita al eNB origen la liberación del contexto UE
    - Solicita al S-GW la liberación de los recursos asignados a túnel indirecto creado previamente
- **Después Handover S1**
  - El UE ahora recibe servicio del eNB destino al cual esta conectado



- **Antes Handover S1**. UE esta en **EMM-Registered** y **ECM/RRC-Connected** manteniendo todos los recursos asignados
- **Durante Handover S1**. No existe ningún cambio en el estado de UE. La única diferencia es que durante este periodo, la conexión radio no está activa pero el UE se mantiene conectado
- **Despues Handover S1**. El UE se mantiene **EMM-Registered** y **ECM/RRC-Connected**

- **Antes Handover S1**
  - **1) [UE –> eNB] Report Medición**. El UE realiza una medicion y envía el mensaje **Measurement Report**



- **Preparación Handover**
  - **2) [eNB origen] Decisión Handover**. El eNB origen escoge una eNB destino a partir de los resultados de la medición. Una vez se ha dado cuenta que no existe la posibilidad de realizar un Handover X2, decide ejecutar un Handover S1
  - **3) [eNB origen –> MME] Solicitando Handover**. El eNB envía un mensaje **Handover Required** al MME, solicitando el Handover
  - **4) [MME] Derivando el Contexto de Seguridad y reenviándolo al eNB destino**. El MME deriva la información contexto seguridad y asi comprueba que el eNB destino puede tambien derivarla
  - **5) [eNB destino <– MME] Solicitando al eNB destino el Handover**. El MME envía un mensaje **Handover Request** al eNB destino, solicitando el Handover en nombre del eNB origen.
  - **6) [eNB destino] Preparando Handover S1**. Una vez recibida la solicitud de Handover, el eNB destino empieza la preparación
    - **(i) Asignación recursos nuevo Bearer S1**. El eNB destino comprueba que puede dar servicio asegurando el mismo QoS que disfruta el UE actualmente. Si es así, establece un Bearer S1 UL con el S-GW. Asigna un eNB TEID para el Bearer S1
    - **(ii) Asignación recursos túnel indirecto**. Es necesario un túnel indirecto para enrutar los paquetes DL que le llegan al eNB origen al eNB destino a través del S-GW.
    - **(iii) Asignación recursos para ser usados por el UE en el enlace radio**. El eNB destino asigna recursos RRC a ser utilizados en el enlace radio y asigna un C-RNTI
    - **(iv) Derivación Kenb**. Deriva la clave Kenb utilizando la información de contexto que le habían facilitado. Además deriva la claves de seguridad AS con las que se podrá comunicar con el UE una vez conectado
  - **7) [eNB destino –> MME] Notificando al MME de la finalización de la preparación**. El eNB destino envía toda la información de los recursos asignados al MME mediante un mensaje **Handover Request Ack**
  - **8) [MME –> S-GW] Solicitando la creación del Bearer S1 para la entrega de paquetes DL**. El MME envía al S-GW un mensaje **Create Indirect Data Forwarding Tunnel Request** solicitando la creación de un túnel indirecto para entregar los paquetes DL mientras el UE ejecuta el Handover

- **9) [MME <– S-GW] Notificando al Bearer S1 la creación del Bearer S1**. El S-GW crea el túnel indirecto conectando con el eNB destino. Una vez asignado el S1 S-GW TEID lo reenvia al MME mediante un mensaje **Create Indirect Data Forwarding Tunnel Response**
- **10) [eNB origen <– MME] Notificando la finalización Handover**. El MME envía al eNB origen un mensaje **Handover Command** incluyendo el i) S1 S-GW TEID y ii) la información recibida en el mensaje **Handover Command** del eNB destino

- **Ejecución Handover S1**
  - **11) [UE <– eNB origen] Ordenando la ejecución del Handover**. El eNB origen ordena al UE la ejecución del Handover enviándole un mensaje **Handover Command**
  - **12) [UE] Ejecutando el Handover**. Una vez el UE obtiene del mensaje **Handover Command** el C-RNTI y el DRB ID, se desconecta del eNB origen. El intercambio de paquetes entre UE y eNB origen se detiene, dando por iniciado el periodo de interrupción del Handover
  - **13) [UE] Configurando Seguridad AS**. UE deriva las claves de seguridad para utilizar el enlace radio con el eNB destino
  - **14)-15) [eNB origen –> MME, MME –> eNB destino] Notificando el Num.Paquete a enviar/recibir**. El eNB origen envía un mensaje **eNB Status Transfer** al MME que incluye un contador DL y UL, el MME envía a su vez el mensaje **MME Status Transfer** al eNB destino. De esta forma, el eNB destino conoce a partir de que paquete debe enviar/recibir. Una vez enviado el mensaje, el eNB origen enviada a reenviar los paquetes DL que le llegan S-GW al eNB destino por el túnel indirecto.
  - **16)-18) [UE, eNB Destino] Acceso del UE al eNB destino**.
    - **16)** El UE detecta la señal de sincronización para realizar la sincronización con el eNB destino
    - **17)** El eNB destino envía al UE la información de alineamiento del tiempo y el permiso acceso UL
    - **18)** El UE envía al eNB destino un mensaje **Handover Confirm**.

    UE puede enviar/recibir paquetes a/de eNB destino, y finaliza el tiempo de interrupción de Handover
  - **19) [UE - eNB destino] Comunicaciones Seguras sobre el enlace radio**. Todos los mensajes de señalización y paquetes enviados sobre el enlace radio entre UE y eNB destino se entregan de forma segura con las claves de seguridad AS. Asimismo, los mensajes de señalización están encriptados y protegida su integridad
  - **20) [eNB destino] Continuando la entrega de paquetes DL al UE**. Una vez el UE está conectado, el eNB destino empieza a enviar los paquetes almacenes al UE a través del nuevo path
  - **21) [eNB destino –> MME] Solicitando el cambio path del Bearer S1**. El eNB destino notifica al MME que el UE ha finalizado con éxito el Handover S1 enviando un mensaje **Handover Notify**
  - **22)-27) Modificando el Bearer EPS**. El MME envía el S1 Target eNB TEID asignado al eNB destino al S-GW a través de un mensaje **Modify Bearer Request**. El S-GW establece un Bearer S1 DL conectando con el eNB destino. A su vez, elS-GW envía un mensaje **Modify Bearer Request** al P-Gw, que a su vez, notifica al PCRF
  - **28)-29) Modificando el path del Bearer EPS**. S-GW cambia el path de entrega de paquetes DL por el Bearer S1 DL que esta conectado al eNB destino. Primero envía un **EndMArker** para indicar que es el último paquete que se envía por el antiguo path. Desde entonces envía los paquetes por el Bearer S1 modificado
  - **30) [eNB destino] Reordenando paquetes**. El eNB destino recibe los paquetes reenviados del eNB origen y aquellos del S-GW a través del nuevo path. eNB destino debe asegurarse la entrega de los mensajes en el orden correcto. Primero entrega los paquetes recibidos del eNB origen, y posteriormente, los recibidos por el nuevo path modificado
  - **31)-32) [eNB destino <–> MME] Liberando Contexto UE y recursos asignados en el eNB origen**. MME informa al eNB origen que debe liberar los recursos asignados (Bearer S1 y túnel indirecto) enviando un mensaje **UE Context Release Commnand**. Finalmente, libera la información de contexto y los recursos S1, e informa al MME enviandole un mensaje **UE Context Release Complete**
  - **33)-34) [MME <–> S-GW] Liberando el túnel indirecto**. El MME envía al S-GW un mensaje **Delete Indirect Data Forwarding Tunnel Request** solicitando la liberación del tunel indirecto. Una vez liberado, el S-GW informa al MME a través de un mensaje **Delete Indirect Data Forwarding Tunnel Response**

Appendix B

Practicas

B.1 Practicas Diameter

B.1.1 FreeDiameter

FreeDiameter es un proyecto open source para la implementación del protocolo Diameter. FreeDiameter provee una plataforma extensible para instalar una red Diameter para cualquier necesidad de autenticación, autorización y/o accounting (AAA). En la pagina web del proyecto , *www.freediameter.net*, podréis obtener más información relacionada con el proyecto además de variado material para el estudio del protocolo Diameter.

El framework FreeDiameter se basa en diferentes archivos de configuración que podemos diferenciar en tres tipos:

- Configuración local
- Extensiones
- Conexiones Remotos

Configuración Local

La configuración local básica de un cliente Diameter se localiza dentro de un fichero llamado **freeDiameter.conf**. Este fichero es un fichero de texto plano que dispone de múltiples lineas de comandos donde realizar la configuración mínima de todos los parámetros de un cliente Diameter. Un cliente Diameter es un nodo Diameter que soporta Aplicaciones Diameter Clientes además del protocolo base. Un nodo Diameter pasa a llamarse peer cuando establece y comparte una conexión directa TCP (o SCTP) con otro nodo.

A continuación describiremos algunos de los atributos más importantes que podemos configurar en el fichero **freeDiameter.conf**. Debemos remarcar que en la pagina web del proyecto podemos encontrar ficheros de configuración de ejemplo con todos los parámetros posibles y una breve explicación de cada uno de ellos. Que existan este tipo de ficheros de ejemplo no significa que no podamos crear nosotros mismos desde cero un fichero de configuración con los pocos parámetros que queramos configurar.

Parámetros del protocolo Diameter

- **Identity** Identity es un parámetro que será utilizado para identificar al peer dentro de la red Diameter. El protocolo exige que el valor Identity utilizado sea un FQDN (fully qualified domain name) valido. Este valor podría ser omitido en cuyo caso, se intentaría utilizar el nombre del sistema por defecto
- **Realm** En Diameter, todos los peers pertenecen a un Realm. Si no se especifica, el framework utilizará la parte de Identity después del primer punto (p.e. Si Identity es nas1.example.org, el Realm sería example.org)
- **NoRelay** Por defecto, freeDiameter actúa como un Agente Relay reenviando todos aquellos mensajes que no puede gestionar localmente. Con este parámetro se desactivaría este comportamiento

Parámetros de red del protocolo

- **Port** El número de puerto en el que escuchará para conexiones entrantes
- **SecPort** Puerto utilizado para conexiones TLS

- **No_TCP** Por defecto se utiliza el protocolo TCP y SCTP, siendo siempre SCTP la primera opción, para las conexiones entrantes así como IPy IPv6. En el caso que se especifique esta optión, el peer nunca intentará realizar conexiones salientes con TCP
- **No_SCTP** Por defecto se utiliza el protocolo TCP y SCTP, siendo siempre SCTP la primera opción, para las conexiones entrantes así como IPy IPv6. En el caso que se especifique esta optión, el peer nunca intentará realizar conexiones salientes con SCTP
- **Prefer_TCP** Por defecto se utiliza el protocolo TCP y SCTP, siendo siempre SCTP la primera opción, para las conexiones entrantes así como IPy IPv6. En el caso que se especifique esta optión, el peer intentará realizar conexiones salientes con TCP
- **No_IP** Por defecto se utiliza el protocolo TCP y SCTP, siendo siempre SCTP la primera opción, para las conexiones entrantes así como IPy IPv6. En el caso que se especifique esta optión, el peer no utilizará IP
- **No_IPv6** Por defecto se utiliza el protocolo TCP y SCTP, siendo siempre SCTP la primera opción, para las conexiones entrantes así como IPy IPv6. En el caso que se especifique esta optión, el peer no utilizará IPv6
- **SCTP_streams** Sobrescribe el número de transmisiones SCTP

Parámetros TLS

- **TLS_Cred** Aún cuando se puede desactivar TLS para algunas conexiones, este parámetro es obligatorio. Debe contentar un certificado valido para el valor indicado en el parámetro Identity. Más adelante se describirá como obtener un certificado valido para realizar los escenarios de practicas

Extensiones

- **LoadExtensions** Especifica el path en el que se encuentra el fichero que deseas cargar con configuración adicional a la básica

Existen en este caso diferentes extensiones a utilizar. A continuación comentaremos algunas de ellas, las relacionadas con las practicas a continuación. Para obtener más información al respecto se puede consultar la pagina web del proyecto donde adicionalmente, podemos obtener ficheros de ejemplo de cada uno de ellos

- **acl_wl.fdx** Permite configurar la lista de peers desconocidos (es decir, que no están en la tabla de peers estática) autorizados a realizar la conexión con el sistema local.
- **rt_default.fdx** Permite configurar la tabla de rutas en el peer local
- **test_app.fdx** Permite realizar testeos en la aplicación de forma que envíe mensajes Diameters a otro peer.

Conexiones remotas

- **ConnectPeer** Defines otro nodo Diameter con el que establecerás una conexión y por tanto se convertirán en peers. Adicionalmente, para este peer se pueden establecer algunos parámetros específicos para esta conexión como hemos visto en la sección anterior de Parámetros Locales. Por ejemplo podríamos establecer que con ese peer la conexión especificada el protocolo prioritario sería TCP (con la linea de comando Prefer_TCP)

El siguiente podría ser un ejemplo de fichero de configuración freeDiameter.conf

```
# Uncomment if the framework cannot resolv it.
#Identity = "backend.localhost";

# TLS configuration (see previous section)
TLS_Cred = "cert.pem" , "privkey.pem";
TLS_CA = "ca.pem";

# Limit the number of SCTP streams
SCTP_streams = 3;

# -------- Peers ---------
ConnectPeer = "nas.localhost" { No_TLS; };
ConnectPeer = "relay.localhost" { ConnectTo = "2001:DB8:1234::5678"; };
```

En el vemos como no se ha configurado Identity por lo que se obtendrá del sistema local. Nos indica que los certificados y las claves se encuentran en los ficheros que se indican (al no tener ruta estarán alojados en el mismo path que el fichero freeDiameter.conf). Y por último que se establecerá conexión con el nodo "nas.localhost" sin utilizar TLS, mientras que con el nodo "relay.localhost" se conectará utilizando la dirección que indica.

Una vez realizada la configuración de los equipos (ya sean locales o virtuales) el fichero freeDiameter.conf debe situarse en la misma carpeta donde se haya instalado el cliente freeDiameter (por defecto es /etc/freeDiameter).

Ya por último se deberá arrancar el cliente freeDiameter en el equipo (localmente o mediante SimTools) con el comando

```
root@virt1:~# freeDiameterd -dddd
```

Donde las “d” indican el nivel de log que nos mostrará una vez activo el cliente.

B.1.2 Diameter Básico

Escenario

El objetivo de los siguientes ejercicios prácticos es la familiarización del alumno con el protocolo Diameter. Dicho protocolo esta presente en varias interfaces actuales dentro de las redes móviles 4G. Para ello, se realizará el envío de mensajes Diameter entre 2 terminales tal como muestra la Figura B.1. Se espera que una terminal origen pueda remitir una mensaje Diameter (CEA) a una terminal destino y a su vez sea capaz de recibir el mensaje Diameter de respuesta (CER).

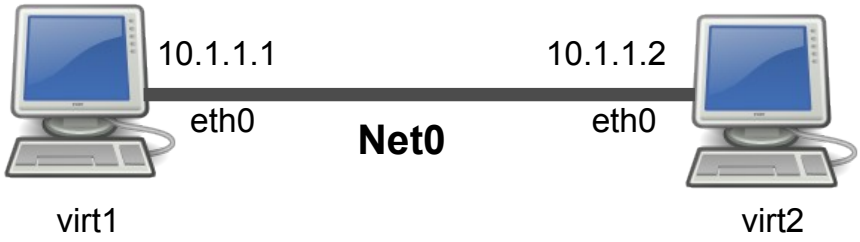


Figure B.1: Esquema de la red para el Escenario Básico

Configuración inicial

Para poder establecer una conexión entre dos entidades (clientes o servidores), a partir de ahora llamados peers, estos deben conocerse mutuamente, es decir, deben tener dentro de la lista de peers conocidos **Peer Table**. Para poder comunicarse por tanto, será necesario que sepamos el nombre del otro peer o la dirección IP en su defecto. Para poder establecer esta configuración básica en Diameter, existe una serie de ficheros que permiten ampliar las capacidades de los terminales.

Para poder arrancar el escenario anterior

```
simctl diameter-basic start
```

Con este comando se realizarán todas las acciones descritas en el fichero vnuml de configuración del escenario para cada uno de los equipos. Si entramos un poco más en el detalle del fichero de configuración diameter-basic.vnuml veremos

```
<vm name="virt1">
    <if id="0" net="Net0"></if>
    <filetree root="/etc/freeDiameter" seq="start">files/diameter-basic/virt1/etc.freeDiameter.testbasic</filetree>
    <exec seq="start" type="verbatim">ifconfig eth0 10.1.1.1/24</exec>
    <exec seq="init" type="verbatim">freeDiameterd &gt; /root/freediameter.log</exec>
    <exec seq="stop" type="verbatim">killall freeDiameterd</exec>
  </vm>
```

Como vemos al haber lanzado la sentencia start al iniciar el escenario, se habrán copiado los ficheros
../files/diameter-basic/virt1/etc.freeDiameter.testbasic en el directorio */etc/freeDiameter* del terminal remoto virt1

Conexión Directa entre terminales

Ejercicio 1.1. En este ejercicio se enviará un mensaje Diameter de forma directa entre las dos estaciones **virt1** y **virt2** utilizando el comando $kill - USR1$. Capturaremos el tráfico y analizaremos el flujo básico de una interfaz Diameter. Note que el usuario que envía el mensaje debe conocer, como mínimo, la dirección IP o nombre del equipo receptor. Si no se especifica nada más, los valores por defecto utilizados serán, el protocolo de transporte SCTP y el puerto 3868

Una vez arrancado el escenario, debe arrancar cada una de las máquinas involucradas en dicho escenario utilizando la instrucción *get* de SimTools. El comando a utilizar será **simctl diameter-basic get nombre-maquina** donde nombre-maquina identifica el nombre de la maquina identificado dentro del fichero de configuración de la aplicación SimTools *fichero.vnuml*

```
simctl diameter-basic get virt1
simctl diameter-basic get virt2
```

Inicie el cliente freeDiameter en virt1, que será quien envíe la señal USR1. Esta señal permite enviar un mensaje CEA Diameter para intercambiar las capacidades de cada peer. De esta forma sabremos si el terminal con el que queremos establecer la conexión

tiene las mismas capacidades que el terminal origen. Con la siguiente opción arrancamos el servicio freeDiameter en el terminal en cuestión

```
root@virt1:~# freeDiameterd -dddd
```

Cuando se arranca el cliente freeDiameterd, se realiza la configuración de sus parámetros a través de los diferentes ficheros de setup existentes (y que se copian a la maquina virtual a través de los comandos indicados en el fichero de configuración vnuml de SimTools). El fichero básico de configuración es el **freeDiameter.conf** que debe estar presente en cada uno de las maquinas que queramos que participen en el escenario práctico. Allí se indicarán varios puntos de su configuración como:

- Dirección IP
- Nombre maquina
- Protocolos que acepta (transporte,
- Realm al que pertenece
- Peers
- Extensiones. Esto son ficheros que permiten ampliar determinadas configuraciones como por ejemplo, enrutamiento, aceptación de peticiones de peers, etc...
- etc...

1. ¿ Cual es el nombre del comando para configurar un nuevo Peer?

2. ¿Cual es el comando que debemos habilitar para poder deshabilitar el uso de SCTP?

Si nos fijamos en la consola donde hemos iniciado el cliente freeDiameter veremos que constantemente nos está dando información del estado de la maquina.

3. ¿ Que esta intentando realizar el cliente freeDiameter en la maquina virt1?

4. ¿ De que estado a que estado transita cuando no puede establecer conexión?

5. ¿ Que crees que falta por iniciar para poder establecer la conexión?

Inicie el cliente freeDiameter en virt2, que será quien reciba la señal USR1, con la siguiente opción

```
root@virt2:~# freeDiameterd -dddd
```

6. ¿ Consigue establecer la conexión virt1 con virt2?

7. ¿Que información se transmite entre virt1 y virt2?

8. ¿Existen cambios en el estado de maquina de virt1?

Desde el terminal de virt2 pulsamos la combinación de teclas Ctrl+C terminando la ejecución del proceso freeDiameter en virt2.

9. ¿Que ha pasado con virt1? ¿En que estado se encuentre en estos momentos?

Volvemos a iniciar el cliente freeDiamerter en virt2. Una vez establecido el cliente freeDiameter, necesitaremos tener acceso a otro terminal conectado a virt1 para poder realizar el envío de la señal USR1. Por tanto, desde la consola principal volvemos a iniciar otra consola en virt1

```
 simctl diameter-basic get virt1 1
```

Para poder enviar una señal USR1 de virt1 a virt2, debemos conocer el número de proceso freeDiameter que se está ejecutando en nuestra maquina. Para conocerlo

```
root@virt1:~# ps -ux | grep -i USR1
```

Una vez obtenido el número de proceso enviaremos la señal mediante el comando kill

```
root@virt1:~# ps -ux | grep -i USR1
```

10. ¿ Que ha recibido virt2?

11. ¿ Que ha recibido virt1?

A continuación, iniciamos el analizador de protocolos wireshark con el que realizaremos las capturas de tráfico en SimNet0 para poder consultar el trafico generado entre las 2 maquinas virt1 y virt2. Una vez activo, iniciaremos la captura de trafico en la interfaz

Ahora volveremos a enviar una señal de USR1 de la maquina virt1 a virt2.

12. ¿Que trafico se ha capturado en Wirsehark?

13. ¿Aparece la misma información en Wirsehark que la que hemos recogido en el terminal de la maquina virtual virt1?

Conexión Indirecta entre terminales

Paramos el escenario

```
simctl diameter-basic start
```

Como hemos visto en el esquema de nuestra red, la configuración es muy sencilla, existiendo únicamente una conexión directa entre terminales. Si entramos y editamos el fichero de configuración del terminal destino virt2, veremos que tiene configurado en su tabla de peers (mediante la linea de configuración **ConnectPeer** la conexión con virt1

```
ConnectPeer = "virt1.example.com" { ConnectTo = "10.1.1.1"; No_TLS; } ;
```

Pero no solo tenemos el nombre de la maquina sino la dirección IP para poder realizar la conexión (al no disponer de DNS en el esquema)

Accede a la configuración del fichero freeDiameter.conf y comenta la línea donde se define el peer valido de virt2. De esta forma estamos estableciendo que virt2 no puede establecer una conexión valida con ningún otro peer de forma estática

```
# ConnectPeer = "virt1.example.com" { ConnectTo = "10.1.1.1"; No_TLS; } ;
```

14. ¿Podrá virt1 enviar un mensaje CEA y obtener un CER?

15. ¿Cual es el mensaje de error recibido por virt1?

16. ¿Que crees que pasaría si cambiáramos el comando anterior, y le eliminaramos la dirección IP? ¿Podría establecer la conexión con el peer virt1?

Conexión Directa entre terminales con TLS

Ejercicio 1.2. Hasta ahora habíamos visto conexiones entre terminales sin implementar ningún tipo de seguridad entre ellos. Este escenario en la vida real podría dar lugar a muchos problemas de integridad de datos al enviar la información sensible en plano por la red. Por lo tanto vamos a implementar la seguridad TLS en nuestro escenario. Lo más simple para hacer pruebas en un entorno no real es crear un certificado autofirmado que corresponda a la identidad de nuestro peer. Para ello es necesario tener una clave privada y un certificado publico.

En primer lugar, generaremos una clave privada de 1024 bits de forma aleatoria que este cifrada con Triple-Des y protegida con una contraseña

```
openssl genrsa -des3 -out privkey.pem 1024
```

Posteriormente, crearemos el certificado autofirmado utilizando la clave privada generada anteriormente para la identidad virt1.example.com

```
openssl req -new -batch -x509 -days 3650 -nodes -newkey rsa:1024 -out virt1.cert.pem
-keyout privkey.pem -subj /CN=virt1.example.com
```

Aunque no es obligatorio, se recomienda generar un fichero dh, de forma que no se genere uno de forma automática cada vez que se inicie un escenario nuevo. Utilizamos el siguiente código

```
openssl dhparam -out dh.pem 1024
```

Para poder tener el certificado autofirmado para nuestros 2 peers

```
cat virt1.cert.pem virt2.cert.pem > cert.pem
```

Ya por último, debemos configurarlo para que pueda ser utilizado en freeDiameter. Para ello, dentro del fichero de configuración freeDiameter.conf deberemos identificar los certificados y sus ubicaciones. Con anterioridad, nos deberemos haber asegurado que los certificados y claves, estén ubicaciones en las carpetas correspondientes

```
TLS_Cred = "/etc/freeDiameter/cert.pem", "/etc/freeDiameter/privkey.pem";
TLS_CA = "/etc/freeDiameter/cert.pem";
TLS_DH_File = "/etc/freeDiameter/dh.pem";
```

Para que ambos peers intenten establecer una conexión utilizando seguridad TLS se deberá modificar el fichero de configuración freeDiameter.conf de ambos peers. En este caso adicionalmente intentaremos establecer la conexión no utilizando STCP sino TCP

```
ConnectPeer = "virt2.example.com" { ConnectTo = "10.1.1.2"; No_SCTP; } ;
```

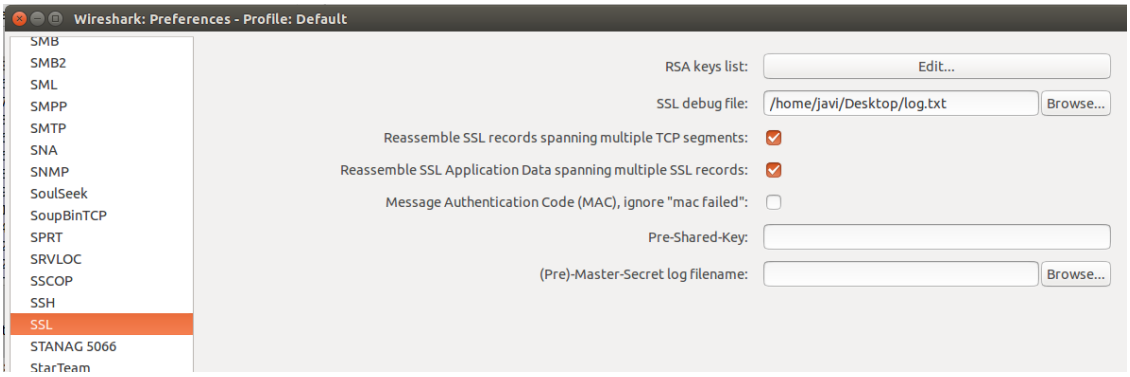
Iniciaremos la captura en WireShark para intentar analizar la información enviada entre virt1 y virt2.

17. ¿Se establece la conexión?

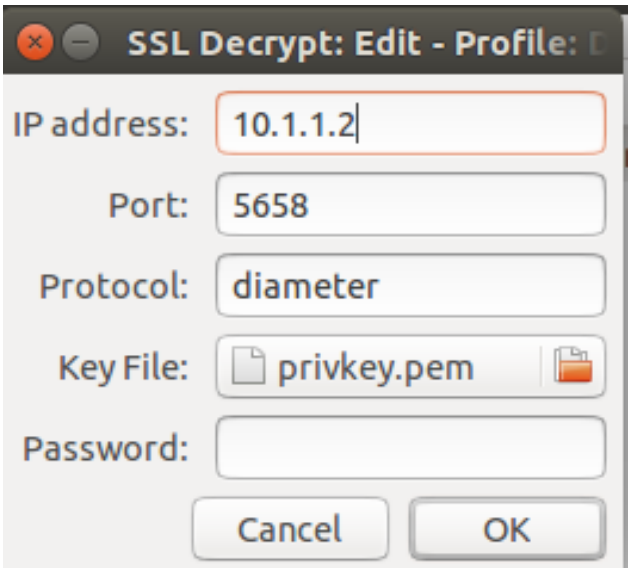
18. ¿Somos capaces de analizar la información recibida?

Dado que ahora se envía la información mediante TLS, toda la información esta cifrada y es imposible analizarla. En este caso, disponemos de otra opción mediante la configuración de Wireshark, ya que nos permite descifrar SSL si disponemos de la clave privado y los certificados. Para ello:

1. En *Wireshark* > *Edit* > *Preferences* > *Protocols* > *SSL*



2. Pulsamos sobre el botón *Edit* y añadimos la información a continuación



3. Aplicamos y salimos de la pantalla de preferencias

19. ¿Ha cambiado algo en la captura de Wireshark? ¿Podemos analizar el trafico?

B.1.3 Diameter: Escenario Router

Escenario

El objetivo de los siguientes ejercicios es iniciar al alumno en escenarios donde existen diferentes proxies y en los que el protocolo de comunicación será Diameter. En dicho escenario será necesaria la configuración de algunas rutas entre los diferentes terminales. En la figura B.4 podemos consultar el esquema que vamos a testear.

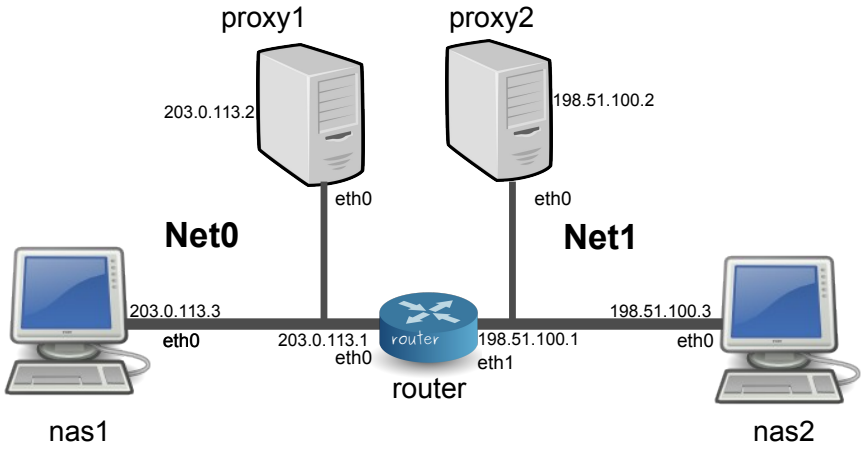


Figure B.2: Esquema de la red para el Escenario con Router y Proxies

Configuración inicial

Para poder establecer una conexión entre Peer según el RFC6733, se puede realizar de 2 formas, a través de la lista estática de

peers conocidos, o a través del descubrimiento de peers *(dynamic peer discovery)*. En el siguiente ejercicio desarrollaremos la idea de las listas estáticas de peers conocidos. Como ya hemos visto anteriormente, Diameter permite definir tantos peers como se desee y por tanto establecer una lista de peers estática, mediante la linea de configuración **ConnectPeer**. De esta forma podremos definir tantos peers como queramos, estableciendo adicionalmente, los parámetros de conexión entre ellos.

Arrancaremos el siguiente escenario diameter-proxy, asi como los nodos Diameter necesarios para realizar la practica

```
simctl diameter-proxy start
simctl diameter-proxy get nas1
```

Ejercicio 1.3. En el siguiente ejercicio tendremos un esquema de conexión como muestra la Figura B.4. En este esquema el objetivo será que el terminal nas1 sea capaz de enviar un mensaje Diameter CEA a nas2, y recibir de ella, una respuesta a la transmisión (CER). La expectativa es que la señal enviada realice el siguiente camino **nas1 > proxy1 > router > proxy2 > nas2 > proxy2 > router > proxy2 > nas1**

20. ¿ Si queremos que el mensaje siga esta ruta, que **ConnectPeer** deberíamos establecer en proxy2 si queremos utilizar una lista estática de peers ?¿Y en router?

21. ¿Que pasaría si arrancáramos el ejercicio pero no iniciáramos el proxy1?¿Que intentaría hacer nas1?¿Podría llegar el mensaje de nas1 a nas2?

Iniciamos todos los elementos del esquema y adicionalmente otro terminal para nas1 de forma que este pueda enviar un mensaje Diameter a nas2

```
simctl diameter-basic get virt1 1
root@virt1:~# ps -ux | grep -i USR1
root@virt1:~# kill -USR1 pid
```

22. ¿Es capaz ahora nas1 de enviar un mensaje a nas2 y recibirlo?

23. ¿Que pasaría si desconectáramos (Ctrl+K) el terminal proxy2? ¿Dejaría de recibir la información nas1? Y si lo hiciéramos con router?

B.1.4 Diameter: Escenario Esquema con respuesta a error

Escenario

El objetivo de los siguientes ejercicios es ver las capacidades de las redes Diameter para gestionar el control de errores y la retransmisión de las repuestas La siguiente red dispone de una ruta principal marcada en rojo que es por donde transitarán los mensajes de un terminal de usuario nas1 a un servidor nas2. Esta ruta implica que los mensajes se enviarán a través del proxy1. Adicionalmente existe una ruta secundario marcada en color negro que permitirá tener una linea de backup en caso de error en la primera.

Configuración inicial

Se establecerá la siguiente configuración para esta prueba. El terminal de usuario nas1 tendrá como ConnectPeer a proxy1 y como siguiente terminal al que retransmitir todos los mensajes. En cambio proxy1 no tendrá a nas1 dentro de su lista de peers estáticos. En este punto iniciamos la simulación

```
simctl diameter-failure start
simctl diameter-failure get nas1
simctl diameter-failure get proxy1
```

Ejercicio 1.4. Al iniciar los terminales, como hemos visto anteriormente, nas1 al tener como **ConnectPeer** a proxy1 intentará establecer una conexión Diameter. Esta conexión no se establece y aparece en nas1 el mensaje de DIAMETER_UNKNOWN_PEER. Si nos fijamos mas en detalle veremos que en el terminal proxy1 aparece la información como si estuviera recibiendo información de un terminal desconocido.

24. ¿Que fichero de configuración Diameter nos permitirá recibir mensajes de terminales desconocidos?

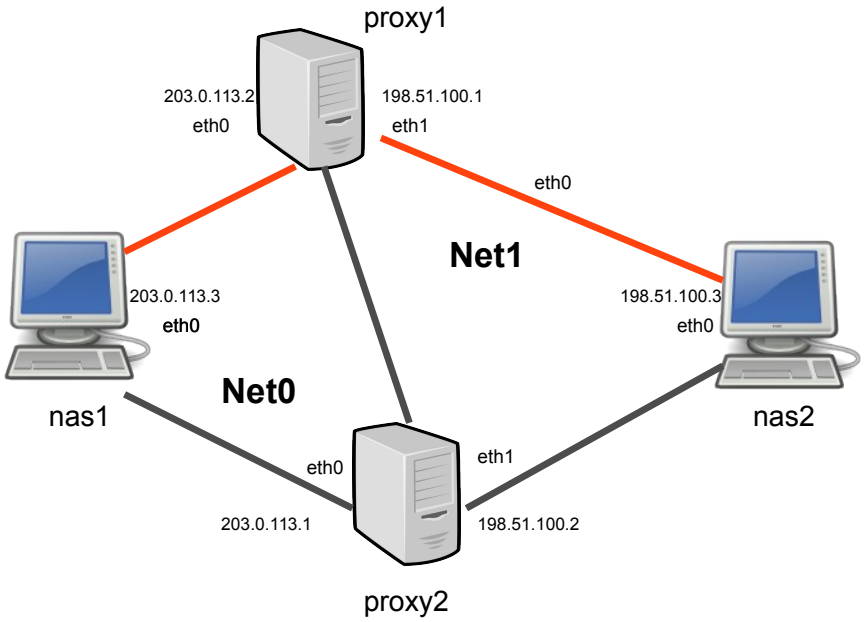


Figure B.3: Esquema de la red para el Escenario con Router y Proxies

25. ¿Que debemos incluir en la linea para que proxy1 permita recibir CER y responder un CEA para poder establecer la conexión?

El resto de elementos del esquema se conectan entre ellos mediantes tablas de peers dinámicos (ConnectPeer instrucción). Intentamos ahora enviar un mensaje Diameter desde nas1 a nas2

26. ¿Es capaz ahora nas1 de recibir respuesta de nas2?

27. ¿Por donde se envía la información?

Ahora simularemos una caída del terminal proxy1 que evitaría que la información se transmitiera por el canal primario.

28. ¿Transitaría la información por la ruta secundaria? ¿El mensaje que nos aparece nos es común, que es lo que debemos modificar?

29. ¿Que crees que pasaría en el caso que enviáramos múltiples señales Diameter de nas1 a nas2 y la conexión se ralentizará?

B.1.5 Diameter: Escenario Dynamic Peer Discovery

Escenario

El objetivo del siguiente ejercicio es iniciar al alumno en escenarios donde el protocolo de comunicación será Diameter y en los que se utilizará un método dinámico de descubrimiento de peers. Este método permite realizar un mantenimiento de la red más sencilla ya que no es necesario disponer de tablas estáticas de peers en cada nodo Diameter existente. En este caso, solo será necesario conocer el peer contra el que queramos establecer la conexión y de forma dinámica, se establecerá la ruta hasta llegar a él. Al contrario, si pensáramos en un método estático implicaría que cada vez que introdujéramos un nuevo nodo Diameter, se debería modificar todos los ficheros de configuración en cada uno de los nodos Diameter de la red existente. En la figura B.4 podemos consultar el esquema que vamos a testear.

Configuración inicial

Para poder establecer una conexión entre Peer según el RFC6733, se puede realizar de 2 formas, a través de la lista estática de

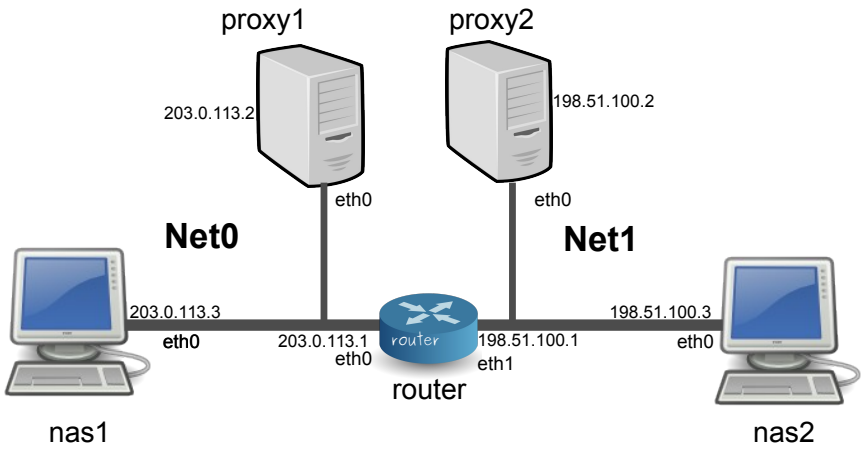


Figure B.4: Esquema de la red para el Escenario Dynamic Discovery

peers conocidos, o a través del descubrimiento de peers *(dynamic peer discovery)*. Tal como hemos comentado con anterioridad, en el siguiente ejercicio desarrollaremos la idea del descubrimiento dinámico de peers. En ejercicios previos habíamos visto que, de forma sencilla, se podía indicar en el fichero de configuración freeDiameter.conf, el nombre del peer con el que se deseaba establecer la conexión. En este caso, solo necesitaremos disponer del nombre del peer destino contra el que queremos establecer la conexión. Para ello utilizaremos las Extensiones que habíamos visto en el inicio del capitulo. La extensión **test_app.fdx** dispone de los parámetros **dest-host** y **dest-realm** con los que podemos indicar el nodo Diameter destino de nuestro mensajes y el realm al que pertenece. Así, en el momento que nas1 envíe la señal CEA indicará en ella que el destino es nas2 y esta información será la que nodo tras nodo se vaya consultando para saber el siguiente loop del camino.

Arrancaremos el siguiente escenario diameter-nai, así como los nodos Diameter necesarios para realizar la practica

```
simctl diameter-nai start
simctl diameter-nai get nas1
```

En este esquema adicionalmente, existe un router en el que se dispone de un servicio DNS (cliente bind) con parte de la configuración DNS. Este elemento es fundamental para realizar el descubrimiento dinámico de peers. Según indica el RFC 6733, la implementación dinámica ejecuta una query NAPTR para obtener un servidor Diameter en el realm destino. El uso de NAPTR sigue la aplicación S-NAPTR DDDS (mostrada en el RF3958) en las que el campo SERVICE incluye los tags para la aplicación deseada soportada en el protocolo. En el caso de Diameter la aplicación es 'aaa' y los tags de las aplicación deseada son

- 'diameter.tcp' –> TCP
- 'diameter.sctp' –> SCTP
- 'diameter.dtls' –> DTLS
- 'diameter.tls.tcp' –> TLS

El cliente seguirá el proceso de resolución definido en S-NAPTR para obtener un valor correspondiente en SRV, A o AAAA para un candidato a peer.

En el caso que no se obtuviera ningún valor NAPTR, el cliente seguiría haciendo consulta ahora para registros SRV. En este caso se utilizaría lo siguiente

- '_diameter_tcp.realm' –> TCP
- '_diameter_sctp.realm' –> SCTP
- '_diameters_sctp.realm' –> DTLS
- '_diameters_tcp.realm' –> TLS

De forma que obtuviera alguna resolución A o AAAA para un candidato a peer.

En el caso que no obtuviera ningún resultado, el cliente dejaría de intentarlo. En el caso que hubiera tenido éxito, el valor resuelto (FDQN valido) se insertaría en la lista de peers.

Ejercicio 1.5. En el siguiente ejercicio tendremos un esquema de conexión como muestra la Figura B.4. En este esquema el objetivo será que el terminal nas1 sea capaz de enviar un mensaje Diameter CEA a nas2, y recibir de ella, una respuesta a la transmisión (CER). La expectativa es que nas1 al no tener ningún peer estático establecido por configuración, realice una consulta NAPTR al DNS para conocer cual es el siguiente loop a realizar para que su mensaje Diameter llegue al destino. En este caso, para el resto de nodos Diameter deben estar configurados en modo Relay permitiendo pasar el mensaje CER al siguiente nodo hasta llegar a nas2. Para ello será necesario realizar la configuración de los equipos

- nas1 –> cliente Diameter
- nas2 –> Servidor Diameter
- resto –> Relay

30. ¿En que extensión indicaremos que un equipo es cliente o servidor? ¿Se deberá configurar para los equipos Realy esta extensión?

31. ¿En los equipos que hacen de Relay que extensión será necesario configurar para que acepten conexiones de equipos desconocidos?

32. ¿Que pasaría si nas1 no pudiera obtener una resolución a su petición para llegar a nas2?

Ejercicio 1.6. En el ejercicio anterior, hemos visto que nas1 ha recibido un mensaje de DIAMETER_UNABLE_TO_DELIVER. Este mensaje nos indica que nas1 no ha sido capaz de encontrar un peer valido para enviar su mensaje. Para comprobar la resolución en un terminal sobre nas1 validaremos

```
root@virt1:~# dig NAPTR example.com
root@virt1:~# dig SRV \_diameter\_tcp.example.com
```

33. ¿ Que esta resolviendo? ¿Es correcto?

34. ¿ Que cambios crees que se deberían hacer para que resuelva correctamente?

35. Edite el fichero de configuración del DNS y modifique las entradas erróneas. Para ello abra un terminal de router y en el path /etc/bind edite el fichero invalido. Modifique la entrada y vuelva a intentar enviar el mensaje desde nas1. ¿Funciona ahora?

Bibliography

[1] MMC Consulting Group. LTE Network Architecture: Basic, July 2013.

[2] MMC Consulting Group. LTE Identification I: UE and ME Identifiers, August 2013.

[3] MMC Consulting Group. LTE Security I: Concept and Authentication, July 2013.

[4] MMC Consulting Group. LTE Security II: NAS and AS Security, August 2013.

[5] MMC Consulting Group. LTE QoS: SDF and EPS Bearer QoS, September 2013.

[6] MMC Consulting Group. EMM Procedure 1. Initial Attach - Part 1. Cases of Initial Attach, December 2013.

[7] MMC Consulting Group. EMM Procedure 2. Detach, January 2014.

[8] MMC Consulting Group. Eleven EMM Cases in an EMM Scenario, October 2013.

[9] MMC Consulting Group. LTE Charging I: Offline, February 2015.

[10] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn. Diameter Base Protocol, October 2012.

[11] MMC Consulting Group. LTE Identification II: NE and Location Identifiers, August 2013.

[12] MMC Consulting Group. LTE Identification III: EPS Session/Bearer Identifiers, August 2013.

[13] MMC Consulting Group. Eleven EMM Cases in an EMM Scenario, October 2013.

[14] MMC Consulting Group. EMM Procedure 1. Initial Attach - Part 2. Call Flow of Initial Attach, January 2014.

[15] MMC Consulting Group. LTE Policy and Charging Control (PCC), August 2014.

[16] MMC Consulting Group. LTE IP Address Allocation Schemes I: Basic, August 2013.

[17] MMC Consulting Group. LTE IP Address Allocation Schemes II: A Case for Two Cities, February 2015.

[18] DMC RandD Center. 5G Vision, February 2015.