Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica

PROPUESTA DE TEMA
TRABAJO FINAL DE GRADUACIÓN
LICENCIATURA

Estrategia de Migración de Equipos CORE PS/EPC y APN a Dual-IPv4/IPv6 e IPv6

Por:
Jairo Alberto Roldán Morales

Ciudad Universitaria Rodrigo Facio
Agosto del 2021

Estrategia de Migración de Red CORE PS/EPC a IPv6

Por:

Ing. Jairo Alberto Roldán Morales

Sometido a la Escuela de Ingeniería Eléctrica

de la Facultad de Ingeniería

de la Universidad de Costa Rica

como requisito parcial para optar por el grado de:

LICENCIADO EN INGENIERÍA ELÉCTRICA

Aprobado por el Tribunal:

Firmado digitalmente por LUCKY LO CHI YU LO (FIRMA)
Fecha: 2021.08.21 10:14:39 -06'00'

Ing. Lochi Yu Lo, PhD.
Director, Escuela de Ingeniería Eléctrica

GUILLERMO RIVERO GONZALEZ (FIRMA)

Firmado digitalmente por GUILLERMO RIVERO GONZALEZ (FIRMA)
Fecha: 2021.08.16 17:32:18 -06'00'

Ing. Guillermo Rivero González, M.Sc.
Director, Comité Asesor

EDUARDO ANTONIO NAVAS CARRO (FIRMA)

Firmado digitalmente por EDUARDO ANTONIO NAVAS CARRO (FIRMA)
Fecha: 2021.08.20 18:38:44 -06'00'

Ing. Eduardo Navas Carro, M.Sc.
Miembro, Comité Asesor

OSVALDO FRANCISCO FERNANDEZ CASCANTE (FIRMA)

Firmado digitalmente por OSVALDO FRANCISCO FERNANDEZ CASCANTE (FIRMA)
Fecha: 2021.08.16 14:25:50 -06'00'

Ing. Osvaldo Fernández Cascante, M.Sc.
Miembro, Comité Asesor

GILBERTH ARCE MONTERO (FIRMA)

Firmado digitalmente por GILBERTH ARCE MONTERO (FIRMA)
Fecha: 2021.08.16 21:13:26 -06'00'

Ing. Gilberth Arce Montero, Lic.
Miembro, Comité Asesor

ARMANDO JOSE CAMPOS UREÑA (FIRMA)

Firmado digitalmente por ARMANDO JOSE CAMPOS UREÑA (FIRMA)
Fecha: 2021.08.16 14:12:58 -06'00'

Ing. Armando Campos Ureña, Lic.
Miembro, Comité Asesor

DEDICATORIA

Dedico este trabajo priemeramente a Dios, que me permite levantarme cada día con salud y fuerzas, que me ha permitido entrar a la universidad y aprender tantas cosas importantes para la vida profesional.

También, dedico este trabajo a mi esposa Keren Loáigica Fallas y mi hijo Samuel Roldán Loáiciga, es por ustedes que saqué fuerzas para retomar mi licenciatura, para que mi hijo pueda ver que las cosas cuando se inician se terminan.

Finalmente, dedico este trabajo a mi mamá y papá, que me motivaron a ser profesional, a estudiar en la mejor universidad del país, aunque ellos no hayan podido ir a la U, pero con una gran e invaluable herencia: una imensa cantidad de valores y principios que me definen como persona.

RECONOCIMIENTOS

En nuestras vidas, tenemos la oportunidad de compartir con muchas personas, muchas de las cuales nos han dejado una huella difícil de borrar, pues al final somos quienes somos por las personas con las que hemos tenido la oportunidad de compartir. Igual sucede en nuestra vida profesional, nuestros trabajos, nuestros jefes, nuestros colegas, nuestros otros compañeros de trabajo, las experiencias que vivimos nos forman como profesionales y con la experiencia que vivimos con ellos, aprendemos a ser mejores cada día.

Primeramente, agradezco profundamente a Dios, a mi esposa Keren y a mi hijo Samuel, que siempre han estado conmigo, me han acompañado, apoyado, guiado y motivado a sacar fuerzas para realizar este trabajo de la mejor manera que me ha sido posible. Son mi inspiración y felicidad cada día para dar lo mejor de mi.

También, quiero reconocer a dos grandes instituciones de Costa Rica, que han sido baluarte del país y en mi formación. Primero, la Universidad de Costa Rica, mi universidad, donde conocí tantos profesores y compañeros de los que pude aprender muchísimo, de quienes me acuerdo constantemente y a quienes aprecio mucho por todo lo que me han dado en mi etapa como estudiante. Segundo, el Instituto Costarricense de Electricidad, lugar donde me dieron la oportunidad de formarme como ingeniero en Telecomunicaciones, donde he podido aprender tantas cosas prácticas que han complementado el conocimiento que nos da la universidad, lugar donde he conocido tantos colegas valiosos, quienes amablemente han compartido conmigo su conocimiento y me han ayudado a crecer enormemente.

Muchas gracias también al Ing. Gerardo Blanco Méndez por la oportunidad y gran cantidad de conocimiento que me transmitió los años que fue mi jefe, de igual manera al Ing. Gilberth Arce Montero por toda la colaboración que me ha dado (en especial cuando apenas daba mis primeros pasos como ingeniero), al Ing. Armando Campos Ureña por todas las veces que tuvimos que “hacer yunta” para aprender juntos de cero cuando nos ponían un reto complicado, al Ing. Guillermo Rivero por la oportunidad de realizar este trabajo.

Muchas gracias a mis colegas Ing. Alejandro Bonilla Ramírez, Ing. Gabriela Porras Moreno, Ing. Vivian Valverde Argüello, Ing. Manfred Aglietti Acosta y al Ing. Alexander Fonseca Sequeira por toda la colaboración que me brindaron durante el desarrollo de este trabajo, sin su valioso conocimiento y ayuda este trabajo no hubiera sido posible.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

NOMENCLATURA

3GPP: Siglas de 3rd Generation Partnership Project

BSC: Siglas de Base Station Controller

BTS: Siglas de Base Station

CAPEX: Siglas de Capital Expenditure

CQI: Siglas de Channel Quality Indication

CSP: Siglas de Communications Service Provider

DSL: Siglas de Digital Subscriber Line

CQI: Siglas de Channel Quality Information

GB: Siglas de Gigabyte

Gb: Siglas de Gigabit

GE: Siglas de Gigabit Ethernet

GSM: Siglas de Global System for Mobile Communications

HLR: Siglas de Home Location Register. Es una base de datos que almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar). Es de carácter más bien permanente; cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.

HSDPA: Siglas de High Speed Downlink Packet Access

HSPA: Siglas de High Speed Packet Access

HSUPA: Siglas de High Speed Uplink Packet Access

IMSI: Siglas de International Mobile Subscriber Identity (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

LTE: Siglas de Long Term Evolution

MGW: Siglas de Media Gateway. El MGW es donde el tráfico entra o sale de la red IP desde o hacia la red telefónica convencional

MSC: Siglas de Mobile Switching Center. Es una sofisticada Central Telefónica la cual proporciona conmutación de llamadas, Administración de movilidad y Servicios de voz para los teléfonos móviles dentro de su área de servicio

MSISDN: Siglas de Mobile Station Integrated Services Digital Network. Identifica a una suscripción en la red GSM o UMTS. Es decir, identifica la suscripción y corresponde con el número de teléfono de la tarjeta SIM. Tiene una longitud máxima de 15 dígitos y se compone por el código de país y el número del abonado

Nodo B: Radiobase de telefonía móvil con tecnología 3G

OPEX: Siglas de Operational Expenditure

QoS: Siglas de Quality of Service

RNC: Siglas de Radio Network Controller. Es un elemento de red de alta jerarquía de la red de acceso de la tecnología UMTS, responsable del control de los nodos b que se conectan a ella. La RNC se encarga de la gestión de recursos radio y parte de la gestión de movilidad. Además es el punto en el que se realiza la encriptación de los datos, antes de que sean enviados desde o hacia el terminal móvil. La RNC se conecta a la red de núcleo de conmutación de circuitos (CS-CN, Circuit Switched Core Network) a través del Media Gateway (MGW) y del SGSN (Serving GPRS Support Node) en la red de núcleo de comunicación de paquetes (PS-CN, Packet Switched Core Network).

WCDMA: Siglas de Wideband Code Division Multiple Access

WLAN: Siglas de Wireless Local Area Network

RESUMEN

El trabajo para definir una estrategia de migración para los equipos de Red en el CORE PS/EPC y usuarios de una red móvil a IPv6 (puro/dual), es un reto útil de conocer para un operador de telecomunicaciones, pues es un paso que los operadores de servicios de Internet deben dar, dada las limitaciones en cantidad de direcciones IPv4 y gran demanda de nuevas conexiones, misma que impulsó el desarrollo de IPv6.

Se considera que la red móvil a migrar está operativa, en un mercado regulado y en competencia, por lo tanto, se debe minimizar el impacto al cliente final, ya que este puede representar pérdida de clientes, multas si no se realiza de manera correcta.

Durante la etapa de investigación, se encuentra que a nivel de regulación nacional existe un interés político para incluir IPv6 en Instituciones Públicas. Por otro lado, a nivel internacional, los sitios Web se han adaptado a IPv6, ofreciendo múltiples puntos de conexión para que los usuarios con este tipo de direccionamiento puedan alcanzar el contenido que ofrecen. A nivel de equipos de usuario, se estima que alrededor de un 90% soportan direccionamiento IPv6.

Durante la etapa de Diseño y Pruebas, se encontraron hallazgos que infieren directamente en una posible migración, como el hecho de que los equipos actuales del operador estudiado cuenten con limitaciones para integrarse a otros equipos utilizando IPv6. Por otro lado, se encuentran limitaciones en licencias que si bien permiten realizar pruebas, por ahora no permiten masificar una implemetación, por lo que en las recomendaciones se incluye la adquisición de estas licencias de software.

Con respecto a las pruebas de usuario, fue posible ejecutarlas para los escenarios IPv6 puro (con limitaciones a nivel de DNS64, equipo no disponible por el momento), IPv4 / IPv6 dual (con un funcionamiento 100% efectivo) así como pruebas de oferta comercial (la tasación en línea y fuera de línea, así como la aplicación de políticas dinámicas y predefinidas funcionaron 100% exitosas).

Finalmente, con la experiencia adquirida durante el desarrollo del trabajo, documentación oficial, respuestas del soporte técnico del fabricante, pruebas realizadas y considerando la reculación actual así como el mercado en competencia, fue posible determinar la mejor estrategia de migración desde IPv4 a IPv6 para equipos y usuarios (migrar por etapas, iniciando con un escenario Dual IPv4/IPv6).

Capítulo 1. Introducción

El trabajo propuesto, pretende hacer una investigación con fuentes confiables y ejemplos prácticos, de los efectos que conlleva migrar equipos y clientes, desde IPV4 (actual) a IPV6, todo esto evaluado en el CORE de datos PS/EPC de una red móvil. Esto para poder analizar, medir y proponer una estrategia que permita reducir el impacto de la migración, sobre el cliente final.

El otro punto importante que se abarca en este análisis, que es la estrategia de migración de clientes de datos a IPv6, en este estudio se considera que la mayoría de dispositivos del cliente son tipo Smartphone, lo que permite a los operadores facilitar la posible estrategia de migración a IPV6, ya que la gran mayoría de estos dispositivos del cliente soportan el direccionamiento IPV4, IPV6 y DUAL IPV4/IPV6.

La evolución tecnológica que los operadores de telecomunicaciones móviles tienen que dar, para dar el salto a IPV6 es algo que es ineludible, pues existe una tendencia de crecimiento en la cantidad de equipos y dispositivos móviles conectados a Internet, especialmente con el auge que ha experimentado el Internet de las Cosas IoT (siglas en inglés de Internet of Things), que incrementa la demanda de direcciones IP, cuya disponibilidad de IPv4 ha venido disminuyendo los últimos años. Adicional a esto, más sitios en Internet están utilizando IPV6 cada día, por lo que el impacto relacionados al NAT de IPV4 a IPV6 y viceversa irá disminuyendo paulatinamente en los próximos años.

1.1 Alcances

1. Determinar las diferentes etapas técnicas que se deben ejecutar para asignar IPV6 a los usuarios finales.

2. Determinar si es posible migrar a IPV6 los equipos del CORE de la red.

3. Medir el impacto técnico de la migración hacia IPV6 en un ambiente controlado, para usuarios y equipos en el CORE de red móvil PS/EPC.

4. Elaborar los procedimientos técnicos para una migración efectiva de IPV4 a IPV6 en el cliente final y en el CORE de una red móvil de datos PS/EPC.

1.2 Objetivos

1.2.1 Objetivo General

- ✓ Determinar la estrategia óptima para migrar los clientes y equipos del CORE PS/EPC de IPV4 a IPV6 en una red móvil.

1.2.2 Objetivos Específicos

- ✓ Analizar cuáles equipos de una red móvil PS/EPC son sujetos a migrar a IPV6.
- ✓ Elaborar el perfil de cliente que debe aprovisionarse a un cliente para migrarlo a IPV6.
- ✓ Realizar mediciones prácticas para evaluar el impacto técnico en equipos y clientes finales.
- ✓ Determinar el procedimiento que debe realizarse para una migración IPV4 a IPV6 de equipos y clientes finales.

1.3 Justificación

Cuando se desarrolló IPV4, no se esperaba el crecimiento en la demanda de direcciones IP, el incremento en la cantidad de plataformas red y terminales de cliente final, que generan alto consumo de servicios de red, por lo que fue necesario desarrollar y estandarizar lo que hoy conocemos como IPv6.

Las nuevas tendencias de la industria también impulsan una migración hacia IPv6 (por ejemplo, la evolución tecnológica hacia 5G). Hoy en día podemos ver como objetos que antes eran aislados de la red, hoy en día están permanentemente conectados (por ejemplo: refrigeradoras, cámaras de seguridad, flotillas vehiculares, brazaletes electrónicos, etc.).

El principal problema de IPv4, radica en la escasa cantidad de direcciones IPV4 públicas, que son particularmente útiles cuando se quiere alcanzar (desde cualquier sitio) un destino específico, sin tener que hacer traducción de direcciones IP o bien la reconversión de IP privada a pública.

Es importante considerar también la figura del regulador de telecomunicaciones (SUTEL), el cual tiene la tarea de velar por los intereses de los usuarios y por el cumplimiento del servicio a los clientes finales, lo cual puede desembocar en una multa económicas si existe incumplimiento de parte del operador.

Por lo mencionado anteriormente, se justifica la necesidad de tener una estrategia óptima de migración de IPv4 a IPv6.

1.4 Planteamiento del Problema

El principal problema que se encuentra, consiste en el reto de definir la estrategia para migrar con el menor impacto al cliente final, pues esto se traduce en menores pérdidas por salida de servicio (se captan menos recursos mientras se interrumpe el servicio), no afectar la imagen del operador de telefonía móvil y se optimiza el recurso del direccionamiento IP con que se dispone.

Otra dificultad que se presenta para este proyecto, es el hecho de que nunca se han hecho pruebas punto a punto con direccionamiento IPv6 en la red móvil, por lo que existen muchos retos que se desconocen, tales como capacidades reales de los equipos y sistemas, relación teoría / práctica, medición del impacto real en la red móvil, entre otros.

Adicionalmente, la regulación del país normado por SUTEL, establece multas y penalizaciones para los operadores de telefonía móvil cuando existe afectación o degradación del servicio, por lo que se debe contemplar la satisfacción de la necesidad técnica considerando una adecuada optimización de los aspectos comerciales y regulatorios.

1.5 Metodología

La siguiente lista resume la metodología que se pretende utilizar para la elaboración del proyecto:

- **Mapeo**: Determinar los equipos involucrados en el proceso de migración.
- **Estudio de Mejores Prácticas:** Encontrar el mejor ajuste en la configuración de los elementos y parámetros de red, a partir de las mejores prácticas y recomendaciones que se encuentren durante las pruebas.
- **Diseño y Ejecución**: Realizar propuestas de Diseño para implementación que permitan evaluar el impacto de la migración IPV4 a IPV6.
- **Definir Procesos**: A partir de los diseños elaborados y los resultados post implementación, se procede a plantear una estrategia de migración de clientes de datos móviles de IPv4 a IPv6.
- **Documentación:** Documentar los resultados y estrategia utilizada para obtener el resultado óptimo que responda al objetivo principal de este trabajo.
- **Reevaluación**: Repetir los pasos anteriores tantas veces como sea necesario hasta obtener resultados satisfactorios.

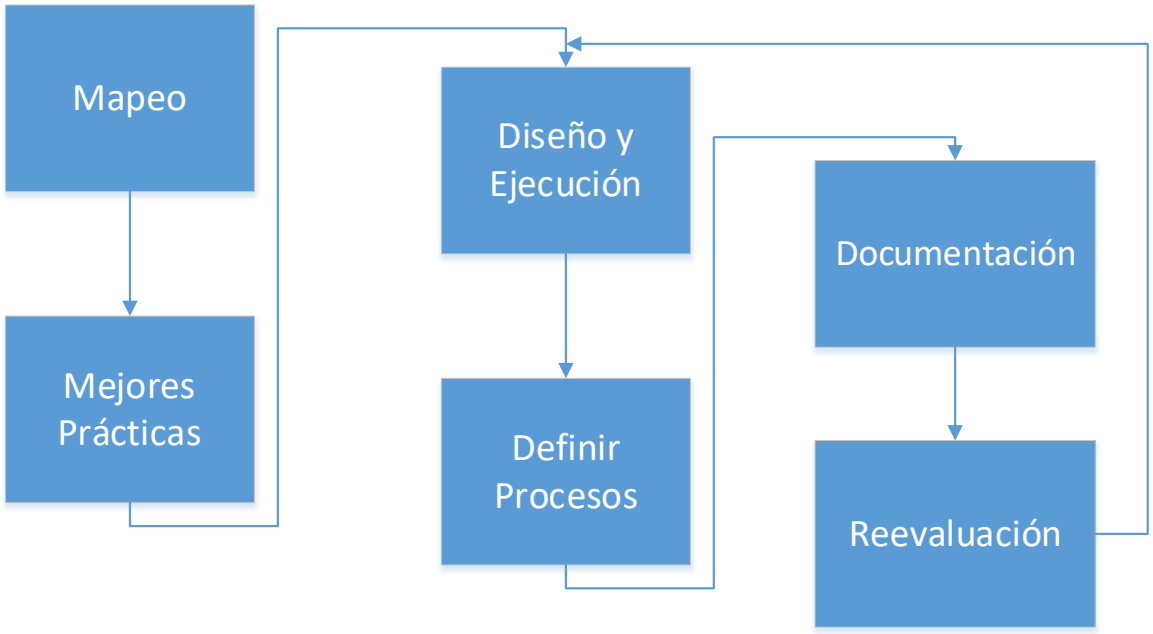


Figura 1: Diagrama de Flujos con la Metodología a utilizar en la elaboración del proyecto.

1.6 Procedimiento de Evaluación

La evaluación del proyecto se hace en 3 fases, siempre basada en el análisis de resultados obtenidos al ejecutar las posibles configuraciones que se deben realizar para migrar los equipos y clientes finales a IPV6. A partir del análisis de resultados obtenidos, se documentará la metodología utilizada para la propuesta de migración, así como las recomendaciones y conclusiones finales basadas en los mejores resultados.

1.6.1 Fase 1: Preparación.

- Análisis y procesamiento de la Información teórica relacionada con los conceptos incluidos en el Marco Teórico.
- Recopilación de información de los equipos del CORE PS/EPC y terminales Móviles (dispositivos)
- Correcta interpretación del entorno jurídico, legal y politico asociado a la estrategia de migración.

1.6.2 Fase 2: Implementación.

- Asignación y comunicación de etapas administrativas a los responsables, requeridas durante el proceso de implementación y pruebas.
- Asignación de direccionamiento para usuarios e interfaces involucradas en el proceso de Pruebas.
- Diseño a nivel de migración de equipos Móviles del CORE PS/EPC.
- Diseño a nivel de migración de usuarios finales (sesión de datos móvil).

- Implementación de los Diseños acorde a la mejor estrategia que se logre definir a partir de los hallazgos encontrados.
- Resultados obtenidos en la ejecución de Pruebas técnicas.

1.6.3 Fase 3: Documentación.

- Análisis de las Pruebas obtenidas.
- Elaboración de Estrategia
- Completación de informe y presentación.

Capítulo 2. Marco Teórico

2.1 Redes Móviles

2.1.1 CORE

El CORE es el núcleo de la red móvil. Consiste en una serie de equipos interconectados entre sí, de manera que permiten el control y establecimiento de llamadas, sesiones de datos. Es desde el CORE que la red móvil se interconecta con la red fija de telefonía (PSTN), la red de Internet, otros operadores móviles (PLMNs), Servicios de Valor Agregado (VAS) entre otros.

Existen varios elementos del CORE de la red móvil que son los responsables del adecuado funcionamiento de la red, entre ellos se pueden mencionar:

2.1.1.1 HLR (Home Local Registry)

Es el registro de abonados de la red móvil local. Consiste en una base de datos, en la que se asocian varios campos a cada usuario específico, con la lista de servicios y funcionalidades que el abonado tiene activos, como por ejemplo datos móviles, mensajería multimedia, entre otros. El HLR se comunica con el AuC para la autenticación del usuario a través del IMSI, MSISDN y algunas llaves de seguridad que el teléfono móvil le envía a la red cuando hace una solicitud de autenticación en la red.

2.1.1.2 HSS (Home Subscriber Server)

Es la evolución del HLR, en el sentido que también es un registro de abonados de la red móvil. Al igual que el HLR, consiste en una base de datos, en la que se asocian varios campos a cada usuario específico. La diferencia con el HLR, consiste en que el HSS es utilizado para redes móviles LTE (HSS-SAE) y también para servicios de IMS (HSS-IMS).

2.1.1.3 MSC (Mobile Switching Centre)

Es una sofisticada Central Telefónica la cual proporciona conmutación de llamadas, Administración de movilidad y Servicios de voz para los teléfonos móviles

dentro de su área de servicio. La MSC está integrada a los otros equipos de red por conexiones IP y SS7, además de permitir el establecimiento de llamadas mediante señalización ss7 y SIP (IP).

2.1.1.4 SGSN (Serving GPRS Support Node)

Dentro de un sistema de datos móviles GPRS; EDGE o UMTS, el SGSN es el responsable de enviar o recibir datos (WAP, Internet, MMS) hacia o desde los teléfonos móviles. El enviar o recibir datos requiere de algunas tareas tales como enrutar y transferir paquetes, manejo de movilidad (attach/detach y manejo de localización) y manejo de enlace lógico.

La información de los usuarios es almacenada, de modo a tener un concepto claro de la identidad del usuario. Por tanto el registro de localización del SGSN almacena información de localización (ej: en que celda esta el usuario, de que HLR/VLR esté caído) y perfiles de usuario de todos los usuarios GPRS registrados dentro del SGSN (ej: IMSI utilizado en la red de radio). También se lleva a cabo la autenticación, que es un proceso por el cual se cuida no revelar el IMSI (numero que identifica al móvil). También es el encargado de llevar la facturación.

Un poco más resumido sería que el SGSN recibe y enviar paquetes, identificando al usuario de modo a verificar si puede utilizar el servicio, manejar la facturación, cuidando siempre su identidad.

Cada SGSN funciona dentro de un área geográfica que varía, depende en muchos aspectos de la cantidad de usuarios de la zona, los equipos los cuales tiene asignado y el uso de WAP, Internet y MMS de la zona[1].

2.1.1.5 GGSN (Gateway GPRS Support Node)

El GGSN es la puerta de enlace o punto central de conexión hacia el exterior o la PDN (Packet Data Network) de una red celular (red móvil), estas redes externas pueden ser Internet o una red corporativa. El GGSN también es el punto de acceso para múltiples puntos de accesos llamados APN (Access Point Network). Una de las principales funciones del GGSN, es realizar la asignación de la IP para uso del terminal dependiendo del APN solicitada.

Dependiendo de la configuración, el GGSN puede manejar una parte de autentificación o autorización de navegación llamada Radius/Diameter, esto se puede realizar por APN. En la parte de configuración de las APN se puede configurar de tal forma que se pueden especificar el tipo de esquema de facturación que puede ser, pre-pago o pos-pago

En parte se encarga del QoS aunque el SGSN es el principal encargado, además de aplicar políticas y reglas de navegación en base a los datos transmitidos/recibidos por los celulares[2].

2.1.1.6 MME (Mobile Management Entity)

Elemento del CORE EPC encargado de la administración del plano de control en redes móviles LTE, específicamente para la gestión de movilidad, autenticación y roaming. Desde el MME se intercambian mensajes de señalización con la red de acceso (eNode-B) utilizando la interfaz S1-MME y el protocolo estándar S1-AP. De igual manera, este elemento intercambia mensajes de señalización con la base de datos de abonados (HSS) utilizando la interfaz estándar S6a (red local) o s6d (red visitada o roaming) a través del protocolo estándar DIAMETER. Finalmente, el MME también tiene comunicación con el elemento SGW a través de la interfaz S11, que utiliza el protocolo estándar GTPC v2.

2.1.1.7 SGW (Serving Gateway)

Elemento del CORE EPC utilizado como punto de anclaje para recibir el plano de control del MME necesario para poder gestionar el plano de usuario que proviene de los diferentes eNodeB que está compuesta la red, lo cual se hace utilizando el protocolo estándar GTPU v1. Es un elemento que necesariamente forma parte de la conectividad del cliente en la red visitada cuando un usuario hace roaming de datos LTE, ya que es desde este nodo que se hacen las consultas DNS - APN que permitan conocer el destino del plano de usuario que proviene de los eNodeB.

2.1.1.8 PDN-GW (Packet Data Network Gateway)

Elemento del CORE EPC que es el Gateway final de datos móviles. Recibe el plano de usuario del SGW a través de las interfaces estándar S5 (red local) o S8 (red visitada o roaming). Este elemento es de mucha importancia, pues es acá donde se dan las asignaciones de direcciones IP del operador nativo del cliente local o roaming. Esto es, el tráfico de datos de los clientes de un operador móvil LTE siempre tendrán salida a internet por este elemento, sea que se encuentren o no en la red local. Desde este elemento también se pueden establecer conexiones VPN con redes privadas (por ejemplo una intranet empresarial) si es que se desea una salida a datos móviles distinta a la internet. La interfaz de salida a datos de este elemento se denomina SGi.

2.1.1.9 DNS (Domain Name System)

El servicio de DNS es el que le permite a la computadora traducir los nombres de dominio a direcciones IP, ese valor de cuatro números que sirve para identificar a una computadora en una red, y por lo tanto también en Internet. Generalmente, es el proveedor de Internet quien provee los servidores DNS, como así también en las redes suelen contar con servidores propios[3].

2.1.1.10 OCS (Online Charging system)

El OCS es el sistema que permite al proveedor de servicios de telecomunicaciones el cobro a los usuarios en tiempo real, basado en el uso del

servicio. Por otra parte, el sistema de carga en tiempo real ofrece a los usuarios la capacidad de manejar su crédito y disfrutar de un valor agregado en términos de ventajas y descuentos.

2.1.1.11 PCRF (Policy and Charging Rules Function)

El servidor de políticas PCRF ofrece a los proveedores un método avanzado para ofrecer productos con calidad de servicio (QoS), manteniendo la integridad de la red y asegurando otros cambios de políticas en tiempo real a través de servicios.

2.1.1.12 PCEF (Policy and Charging Enforcement Function)

El servidor PCEF (Función de Políticas y Cumplimiento de Tarifas) es el encargado de obtener las reglas y políticas del PCRF y aplicarlas a los usuarios de la red móvil.

2.1.1.13 CDR (Charging Data Record)

Registro de datos para cobro, estos registros son automáticamente generados y pueden ser bajados a la computadora en distintos formatos. Estos reportes contienen información como el número de llamadas realizadas, la duración de las llamadas, el origen y destino de las llamadas y el gasto de las mismas.

Otros servicios como mensajería de texto, internet móvil, RBT, PTT, entre otros, también generan CDRs, los cuales son utilizados por los sistemas de tarificación para aplicar el cobro respectivo a los usuarios.

2.1.2 VAS (Value Added Services)

Los VAS son Servicios de Valor Agregado, corresponden a servicios no contemplados en la telefonía básica, que complementan a los servicios básicos (llamadas de voz) para hacer más atractiva la oferta de servicios al cliente. Por ejemplo, un VAS seria el envío de mensaje de contenido diariamente a usuarios, lo que corresponde que este servidor de contenido se conecte al Centro de Mensajes o una plataforma con conexión al SMSC para realizar la tarea. En sí, es envió de mensajes, pero que tienen una lógica más compleja que un simple envió de mensajes.

Unos ejemplos comunes de VAS serian:

- LBS (Location Based Services): Localización de los usuarios por triangulación de celdas o conexión GPRS con terminales con GPS.
- OTA (Over The Air): Plataforma utilizada para gestionar remotamente los aplicativos y configuraciones de las tarjetas SIM/USIM/eSIM.
- DM (Device Manager): Elemento utilizado para gestionar remotamente las configuraciones de los dispositivos móviles registrados en una red móvil.
- SMSC (Short Messages Service Centre): Elemento utilizado para el envío de mensajería corta de texto.

2.1.3 OSS/BSS (Operations Support Systems / Business Support Systems)

Las operaciones de una compañía requieren flujo de información y datos gratuitos para permitir a los procesos de negocio terminar una tarea o alcanzar una meta. Tradicionalmente las compañías de telecomunicaciones han utilizado la abreviatura OSS/BSS del inglés "operations support systems, business support systems" para identificar una serie de aplicaciones de software que automatizan la operación y la administración de servicios de telecomunicaciones.

Las definiciones de BSS se refieren en gran parte a las interacciones y procesos de sistemas de soporte de facturación o gestión de relación con el cliente. La definición de los OSS interactúa con las operaciones de las unidades de negocio o empresariales para permitir o admitir los servicios y el mecanismo de entrega.

Dentro de estos sistemas, se pueden mencionar:

- **Sistemas de aprovisionamiento**: Encargados de dar de alta los servicios al abonado.
- **Sistemas de Facturación**: encargados de recibir los CDRs desde las centrales, convertirlos a un formato conocido y posteriormente facturar al cliente.
- **Sistemas de Gestión**: sistemas encargados del control y vigilancia de recursos de telecomunicaciones. Su principal objetivo es garantizar un nivel de servicio en los recursos gestionados con el mínimo coste
- **Sistemas de Inteligencia de Negocio**: Encargados de hacer minería de datos, para darle forma, valor a la información y luego poder monetirzar la red.

2.1.4 Red de Transporte

Las redes de transporte juegan un papel muy importante en las telecomunicaciones de la actualidad, son las encargadas del envío y multicanalización de diversos tipos de información en diferentes formatos tanto analógicos como digitales[4].

Gracias a la red de transporte, es posible la comunicación entre los diferentes equipos y subsistemas de red, lo que permite el establecimiento de sesiones y conectividad entre todos los elementos que sí se determine.

En este subsistema de red, toma especial importancia las 7 capas del modelo OSI, las cuales se mencionan a continuación (basados en el objetivo de este trabajo):

2.1.4.1 Capa 1 - Capa física.

Existen diferentes materiales utilizados en la capa física a nivel de transporte, entre los cuales podemos encontrar "el cobre" (par telefónico, coaxial, UTP) y la fibra óptica. Todos son útiles dependiendo de la demanda de ancho de banda y tolerancia al retardo de paquetes que requiera la conexión, por lo que es muy normal que encontremos conexiones híbridas a nivel de transporte.

2.1.4.2 Capa 2 - Capa de enlace de datos

Con respecto a la capa de enlace de datos, es normal escuchar el concepto DWDM (acrónimo, en inglés, de Dense Wavelength Division Multiplexing) que significa multiplexado denso por división en longitudes de onda. DWDM es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550 nm). Es particularmente utilizado en distancias grandes que requieren establecer comunicación entre 2 localidades sin que exista análisis a nivel de red (no existe NAT ni otro análisis a nivel de IP para enrutamiento).

2.1.4.3 Capa 3 - Capa de red

A nivel de Capa 3, podemos encontrar los enrutadores y switches, que permiten establecer la Comunicación entre equipos basados en reglas, prioridades, conversion (NAT) y otros análisis, que permiten un control inteligente en el flujo de datos. Esto con el fin de establecer las rutas óptimas para minimizar los tiempos de retardo y evitar la congestion de rutas.

En esta capa es común escuchar de diferentes protocolos de enrutamiento que utiliza el diseñador, como por ejemplo RIP, IGRP, OSPF, BGP, entre otros. Cada uno con sus particularidades y utilidad según el requerimiento de conexión.

2.1.4.4 Capa 4 - Capa de transporte

En la capa de transporte, es donde se efectúa el transporte de los datos. Se encuentran contenidos en unidades de información, empaquetados en los protocolos UDP (sin retransmisión) y TCP (permite retransmisión). A nivel de esta capa, no existe dependencia de la capa física utilizada.

2.1.4.5 Capa 5 - Capa de sesión

La capa de sesión permite el inicio de la Comunicación efectiva entre dos equipos. En esta etapa, los equipos intercambian información de sesión, que permite el inicio y monitoreo de la Comunicación entre ambos. Es común en esta etapa escuchar conceptos como "*keep alive*" (mantener activa), "*Hearth Bit*" (latido de corazón, refiriéndose a la confirmación activa, periódica y sin interrupción).

2.1.4.6 Capa 6 - Capa de presentación

En esta etapa, el objetivo principal es el intercambio reconocible de información, por lo cual, ambos extremos pueden decodificar correctamente la información que envían y reciben desde y hacia el otro extremo. En esta etapa, es donde se da el cifrado y compresión de la información (cuando así se requiere).

2.1.4.7 Capa 7 - Capa de aplicación

La capa de aplicación es la última de este modelo, que se encuentra en el nivel más alto y más cercano al usuario final. En esta capa, podemos encontrar los protocolos que utiliza el software o aplicación final, como por ejemplo, FTP (para transferencia de archivos), SMTP (para correo electrónico) o bien protocolos de red

como SIP (Telefonía IP), DIAMETER (plano de control en tiempo real), GTPc (control de sesión de datos), entre otros.

Ya conocidas las 7 capas del modelo OSI, es posible mencionar el protocolo DNS (por sus siglas en inglés para *Domain Name System*), sistema encargado de la resolución de los nombres de dominio. A continuación, se describe el DNS como protocolo de transporte perteneciente a las capas 4, 5 y 6 del modelo descrito anteriormente.

2.1.4.8 Protocolo DNS

El protocol DNS es un protocolo encargado de transportar las solicitudes/respuestas entre el cliente y servidor. Su principal función es traducir los nombres de dominio en direcciones IP. Esto permite localizar donde exactamente se ubica hospedado el servidor de un sitio alrededor del mundo, lo que permite desplegar el contenido al usuario que ha intentado accederlo ingresando un URL conocido.

Al día de hoy, existen equipos encargados de interpreter este protocolo y responder en el menor tiempo posible (a estos equipos por lo general se les llama igual que las siglas del protocol: “DNS”).

En la actualidad, existen equipos DNS adaptados a los diferentes tipos dedireccionamiento que existen a nivel mundial, los más importantes:

- **DNS IPv4**: Equipo DNS encargado de la resolución de nombres de dominio y traducirlo a direcciones IPv4.
- **DNS IPv6**: Equipo DNS encargado de la resolución de nombres de dominio y traducirlo a direcciones IPv6.
- **DNS64**: Equipo DNS encargado de la traducción entre direcciones IPv4 e IPv6, según el tipo de direccionamiento asignado al equipo terminal del usuario y el tipo de direccionamiento del servidor. Este equipo es indispensable para la convivencia entre ambos tipos de direccionamiento en una red de datos.

2.1.5 Red de Acceso

La red de acceso radio proporciona la conexión entre los terminales móviles y el Core Network. Está compuesta por varios elementos, entre los que se pueden mencionar: Radiobases, controladoras de radiobases, antenas, cables, interfaz de aire, entre otros.

En sistemas móviles GSM, la red de acceso recibe el nombre de GERAN (GSM EDGE Radio Access Network), mientras que es sistemas móviles UMTS recibe el

nombre de UTRAN (por sus siglas en inglés para Acceso Universal Radioeléctrico Terrestre). Finalmente, en las redes 4G LTE la red de Acceso suele llamarse EUTRAN (por sus siglas en inglés para Acceso Universal Radioeléctrico Terrestre Evolucionado).

Figura 2: Radiobase de telefonía celular

2.2 Sistemas GSM (2G)

Se define la Red del Sistema Global de Telefonía GSM como aquel servicio portador constituido por todos los medios de transmisión y conmutación necesarios que permiten enlazar a voluntad dos equipos terminales móviles mediante un canal digital que se establece específicamente para la comunicación y que desaparece una vez que se ha completado la misma.

Los sistemas de telefonía móvil automática necesitan conseguir una amplia cobertura y una gran capacidad de tráfico con un limitado número de frecuencias. Ello es posible gracias a la reutilización sistemática de las frecuencias, lo que se logra mediante las estructuras celulares[5].

Las redes móviles GSM, según el estándar del ITU 3GPP presentan la siguiente topología:

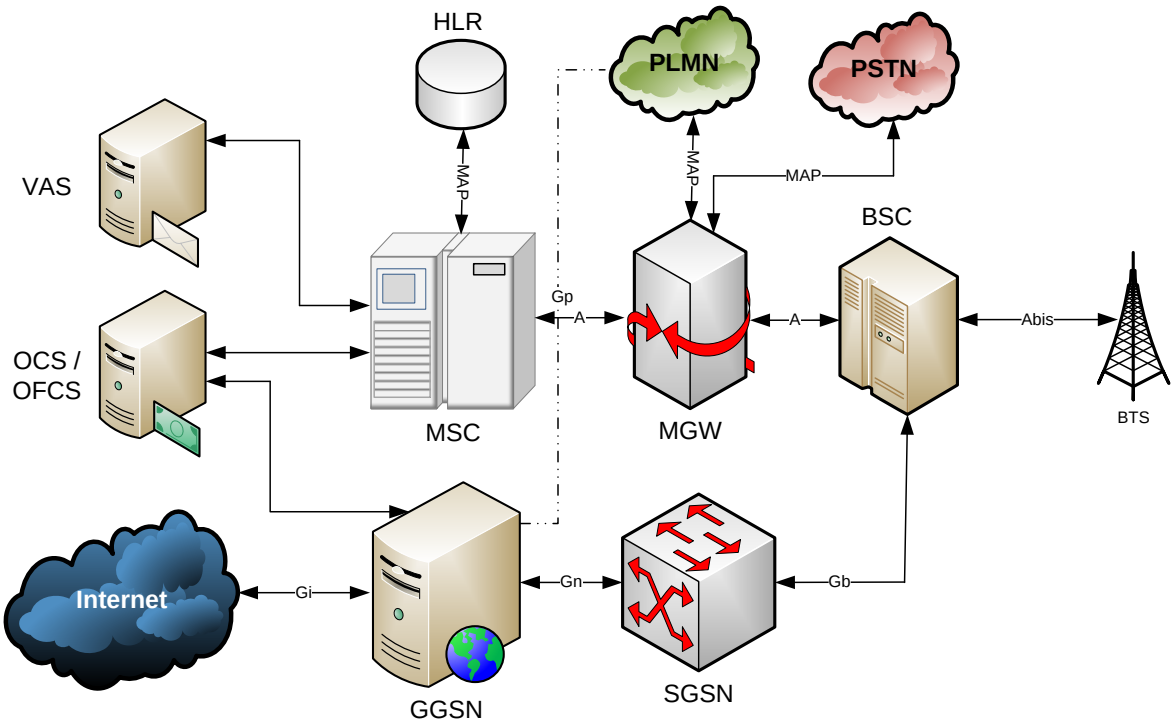


Figura 3: Topología de una red GSM

El sistema GSM es de acceso global, ya que permite dar cobertura internacional con un gran número de abonados. Además, permite el acceso a redes de comunicación avanzadas como la RDSI. Las directrices que orientaron el desarrollo de las especificaciones fueron:

Utilización de una banda común, reservada al GSM en el ámbito internacional

- Estructura celular digital
- Sistema de acceso múltiple AMDT de banda estrecha
- Algoritmo de codificación de fuente de pequeña velocidad binaria
- Control de potencia y de transmisión/recepción
- Arquitectura OSI
- Señalización avanzada (CCITT nº 7)

En cuanto a la arquitectura funcional de un sistema de comunicaciones móviles celular, GSM añade una función de autentificación en base a un registro de identificación de equipo (EIR) y la información de la identidad del abonado en el centro de identificación de usuario (AuC).

La siguiente figura muestra los protocolos de señalización y usuario de una red GSM (los números en paréntesis corresponden a la recomendación ETSI-GSM):

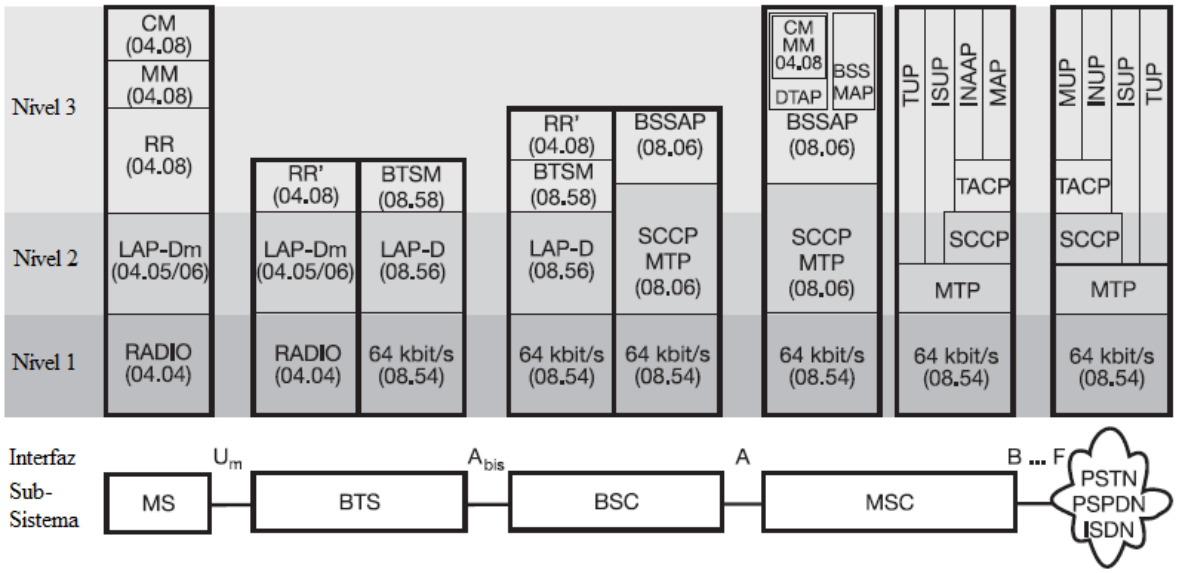


Figura 4: Interfaces y protocolos de una red GSM[6]

2.3 Sistemas UMTS (3G)

UMTS es el estándar que se emplea en la llamada tercera generación de telefonía móvil, que permite disponer de banda ancha en telefonía móvil y transmitir un volumen de datos importante por la red. Con la tercera generación es posible la videoconferencia, descargar vídeos, el intercambio de postales electrónicas, paseos virtuales por casas en venta, etc.

UMTS introduce más capacidad para las comunicaciones, lo que se traduce para el cliente en nuevos servicios, que antes no eran posibles con la capacidad de los sistemas actuales, y mejora de todos los servicios existentes[7].

Una red UMTS por lo general tiene la siguiente topología:

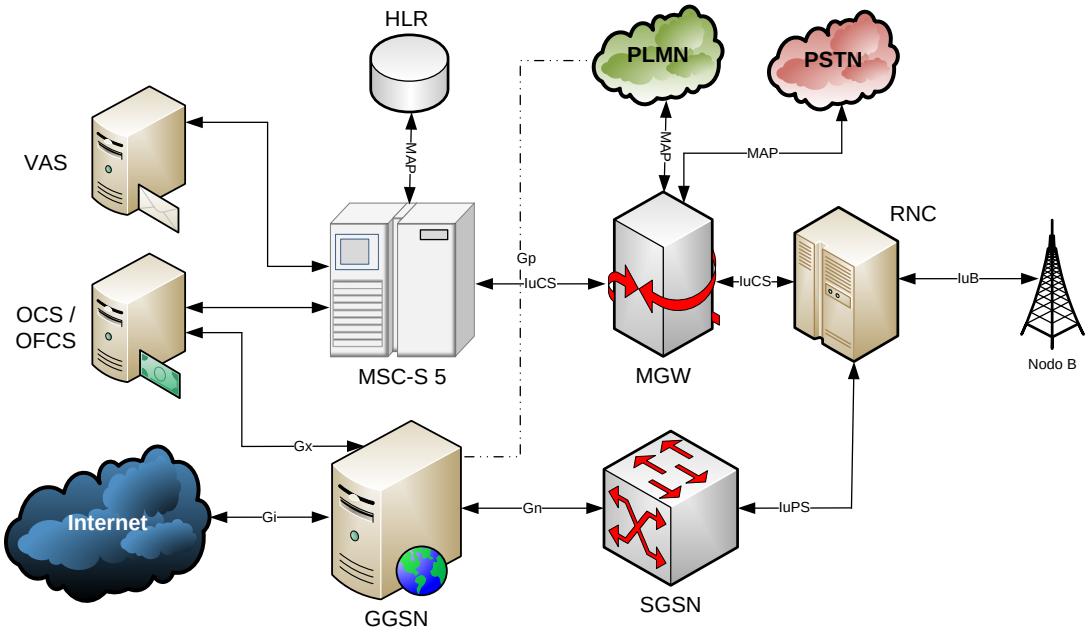


Figura 5: Topología de una red 3G

En particular, con la cobertura UMTS puede disponer de los siguientes servicios, tanto para particulares como para empresas:

- Comunicaciones personales. Además de todas las posibilidades actuales que ofrecen los servicios de voz y mensajería, que se enriquecerán con nuevas facilidades de uso gracias a la incorporación del vídeo, los usuarios de UMTS podrán realizar llamadas de videotelefonía y videoconferencia.
- Acceso a Internet a alta velocidad, con prestaciones más avanzadas para la navegación en movilidad. Es decir, seis veces más rápido que con los terminales GPRS anteriores.
- Para los usuarios de empresa, acceso a la intranet y a las distintas aplicaciones y sistemas corporativos a alta velocidad desde el móvil, sin limitaciones de lugar y con la misma riqueza de información que puede disfrutarse desde la oficina, pero con la mayor seguridad en las conexiones gracias a UMTS.
- Acceso a contenidos multimedia de información y entretenimiento: juegos, vídeos y música, noticias, alertas y otros servicios de comercio electrónico, información y ocio.

La tecnología UMTS es soportada por los terminales llamados 'móviles de tercera generación (3G)', los cuales ya se encuentran en el mercado desde hace tiempo. A continuación, mostramos algunas de las características que un terminal de este tipo puede tener:

- Más capacidad de memoria: para el almacenamiento de contenidos y aplicaciones adicionales.

- Capacidad de transmisión de datos de alta velocidad. Con esta rapidez, el terminal puede convertirse en multitarea, con funciones simultáneas como hacer fotos y enviarlas o recibir el correo electrónico mientras se habla.
- Combinación de vídeo, imagen, texto y voz al unísono en los mensajes multimedia.
- Navegador XHTML avanzado que, unido al ancho de banda de la UMTS, facilita la navegación por Internet. Posibilita la descarga de secuencias de vídeo de hasta 1,4 MB.
- Cámara fotográfica con temporizador y modo nocturno. También de vídeo, que permite la transmisión con sonido. Resolución de 640x480/128x96. Captura de vídeo de hasta 15 fotogramas por segundo. Uso de la pantalla como visor.
- Manos libres incorporado, para que las comunicaciones de audio y vídeo sean idénticas a las de una videoconferencia fija actual. El terminal UMTS está siempre conectado a esta red, lo que hace que la transmisión se produzca sin saltos, aunque nos estemos moviendo.
- Software PC, para la edición básica de secuencias de vídeo antes de enviarlas.
- Aplicaciones personales Java descargables.
- Reproductor de música MP3 y AAC. Puede descargar archivos musicales, reproducirlos y escucharlos con el kit manos libres estéreo, o por altavoz interno. Esa música se puede usar como tono del propio terminal[8].

Las redes UMTS 3G, presentan "evoluciones" tecnológicas que combinan técnicas de radiofrecuencia y multiplexación, que permiten incrementar los anchos de banda disponibles para el usuario. Por lo general, a nivel comercial se suele llamar "3.5G" a esta evolución, que técnicamente recibe el nombre de HSPA y HSPA+ (por sus siglas en inglés para *High Speed Packet Access*). En Costa Rica, esta evolución tecnológica ha permitido alcanzar anchos de banda por usuario de hasta 30Mbps en los canales de bajada y subida.

2.4 Sistemas LTE (4G)

LTE son las siglas en inglés de *Long Term Evolution*. Hace referencia a la tecnología de banda ancha inalámbrica basada completamente en IP (a diferencia de GSM y 3G que pueden incluir tecnología SS7) y como tal, sirve exclusivamente para la transmisión de datos a alta velocidad.

La principal evolución con respecto a las redes GSM y 3G, es el incremento de ancho de banda disponible, que permite alcanzar 150Mbps y hasta 300Mbps con multiplexación cuádruple de antenas.

Su principal rasgo, como hemos explicado en líneas anteriores, es su rápida velocidad para la bajada y subida de datos. No obstante, la tecnología LTE también posee otras características determinantes:

- Desarrollo y despliegue fácil y barato por parte de los operadores, ya que utiliza un protocolo de arquitectura simple, basado en el IP.
- Uso flexible del espectro radioeléctrico, pues es capaz de operar, por el tipo de duplexación, en FDD (bandas pareadas) y en TDD (bandas no pareadas).
- Baja latencia y compatibilidad con otras tecnologías 3GPP[9].

Como todo estándar tecnológico, desde su creación ha sido evolucionado y mejorado, con el objetivo de incrementar el ancho de banda por usuario. La evolución de LTE se conoce como LTE-Advanced (comercialmente, se suele mencionar como 4.5 G). Esta evolución de LTE, unifica y suma el ancho de banda de la señal de radio de múltiples antenas y portadoras de manera simultánea, lo que permite alcanzar anchos de banda de hasta 1Gbps (teórico).

A nivel estándar, las redes LTE presentan las siguiente topología:

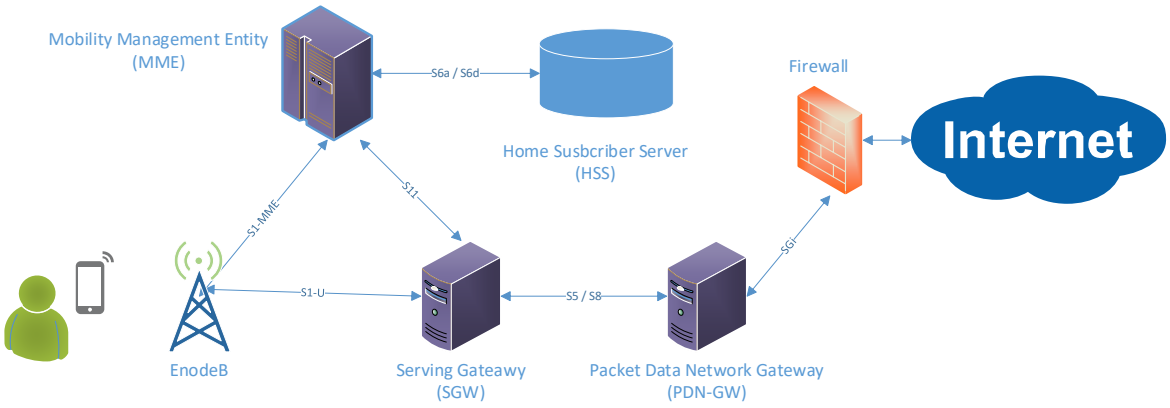


Figura 6: Topología de una red LTE

2.5 Estudio Situación Actual IPv6 en Costa Rica

2.5.1 Regulación IPv6 en Costa Rica

Con respecto al registro, orden y direccionamiento IPv6 en Costa Rica, se han identificado 2 instituciones que guardan algún tipo de relación en remas regulatorios para nuestro país. Estas son: LACNIC, MICITT y SUTEL.

2.5.1.1 LACNIC

Tal como se define en su propio sitio Web, LACNIC es el Registro de Direcciones de Internet de América Latina y Caribe que administra los números IP (IPv4, IPv6) y ASN a través del proceso de desarrollo de políticas. El Registro de Direcciones de Internet de América Latina y Caribe es una organización no gubernamental internacional, establecida en Uruguay en el año 2002. Su función es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región.[10]

Actualmente, para un Proveedor de Servicios de Internet o ISP (por sus siglas en inglés de *Internet Service Provider*), es indispensable ser un miembro activo para ser acreedor a los bloques de direcciones IP que otorga LACNIC directamente. Posteriormente, también es necesario estar registrado como ISP para poder ser catalogado como tal (un proveedor de internet que posteriormente asigna direcciones IPv4 e IPv6 a sus clientes). Los costos de esta membresía están definidos por LACNIC y tanto la cuota inicial como el pago anual dependerán de la categoría en que se ubique la empresa (definida por la cantidad de direcciones IP que requiera).

2.5.1.2 MICITT

El Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica fue el organismo designado por el poder ejecutivo para el Fortalecimiento, Planeamiento, así como la Implementación de IPv6 en las redes de Telecomunicaciones de los ministerios del Gobierno Central.

La Meta propuesta por el gobierno de Costa Rica en 2016, era tener 18 Ministerios utilizando direccionamiento IPv6, para lo cual por parte del MICITT se realizaron evaluaciones anuales en las metas de cumplimiento a finales de cada año a partir del 2017. Se obtuvieron los siguientes resultados:

- 5% de cumplimiento para diciembre del 2017
- 20% de cumplimiento para diciembre 2018
- 100% de cumplimiento para diciembre del 2019.[11]

2.5.1.3 SUTEL

La Superintendencia de Telecomunicaciones SUTEL, es el órgano responsable de la aplicación de la regulación al sector Telecomunicaciones, que debe velar por la protección de los derechos de los usuarios y universalización de los Servicios.

Por lo tanto, se ha encontrado referencias de la medición del desempeño, estándares de medición y normas de aplicación para que los proveedores de Servicios de internet (ISP) brinden un Servicio de Calidad conforme a las mejores practicas existentes, que garanticen un buen Servicio final al cliente.

Entre los estándares de medición que podemos encontrar en la documentación y resoluciones de SUTEL, se encuentra el RFC 2428 "*FTP Extensions for IPv6 and NATs*", definido así en la resolución RCS-019-2018 "RESOLUCIÓN SOBRE METODOLOGÍAS DE MEDICIÓN APLICABLES AL REGLAMENTO DE PRESTACIÓN Y CALIDAD DE LOS SERVICIOS" EXPEDIENTE GCO-NRE-REG-01209-2016.

Con respecto al RFC 2428 mencionado en la resolución de SUTEL en cuestión, se pueden mencionar los siguientes aspectos relevantes:

- El formato del EPRT debe respetar la siguiente estructura:
  - EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>
- Se utilizará la notación de dos puntos ":" para la representación de las familias de direcciones IPv6 (a diferencia de IPv4 que se usa el separador punto "."). Por ejemplo:
  - 1080::8:800:200C:417A es la notación utilizada en IPv6
  - 132.235.1.2 es la notación utilizada en IPv4
- El formato a utilizar para referirse al argumento "puerto" será la barra vertical, de la siguiente manera (por ejemplo, para IPv4 e IPv6 utilizando el Puerto 6275):
  - 1080::8:800:200C:417A|6275| es la notación utilizada en IPv6
  - 132.235.1.2|6275| es la notación utilizada en IPv4.[12]

2.6 Investigación Técnica sobre Equipos Terminales de Usuario

Mediante una búsqueda generalizada en internet, se ha confirmado que la mayoría de dispositivos Móviles soportan el direccionamiento IPv6, ya sea de manera exclusiva o dual. Se ha considerado como requisite indispensable que se Soporte la asignación dinámica de direccionamiento IPv6 (DHCPv6) como requisito mandatorio, pues sería indispensable para el operador de telefonía móvil poder asignar el direccionamiento de manera dinámica[13].

De acuerdo a la información suministrada por los principales manufacturadores de sistemas operativos Móviles, se tiene que las siguientes versiones ya incluyen el direccionamiento IPv6 con Soporte de DHCPv6:

- **Microsoft Windows Phone**: Versión 6.0 o superior (año 2012) [14].
- **Apple iOS**: iOS 4.0 o superior (año 2010) [15].
- **Google Android**: version 5.0 o superior (año 2014) [16].

Tomando en cuenta las cuotas de Mercado que existen a nivel global y en nuestro país, solamente se tomarán en cuenta las proporciones correspondientes a Google Android y Apple iOS, pues la proporcion de dispositivos que utilizan Windows Mobile representa menos del 0,1% de la cuota de Mercado (según estadísticas internas).

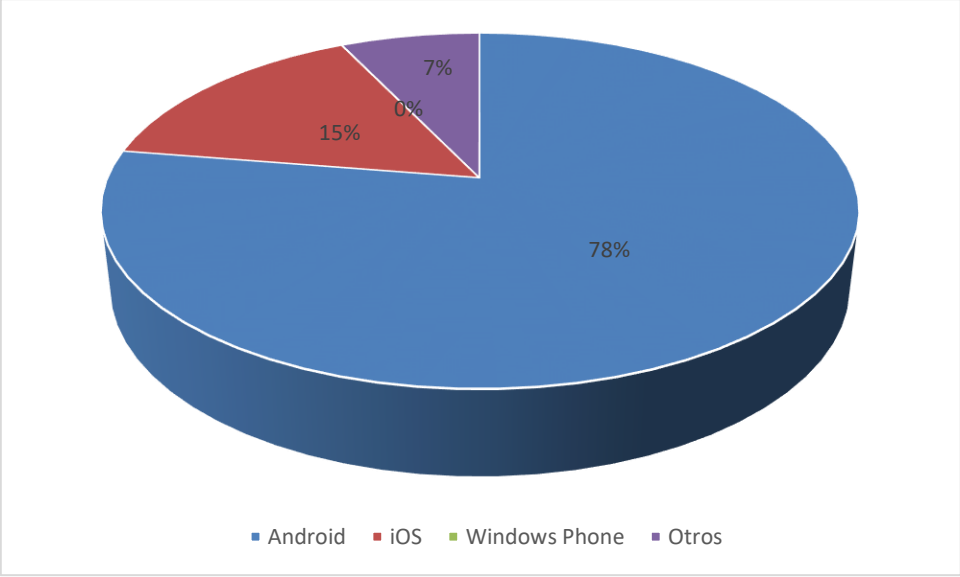


Figura 7: Penetración de Dispositivos Móviles por Sistema Operativo

Considerando estas versiones, se obtiene la siguiente información sobre la cantidad relativa de dispositivos que soportan IPv6, que existen a nivel global (por Sistema Operativo):

- **Android 5.0 o Superior**: 93% de los dispositivos que usan Android[17].
- **Apple iOS 4.0 o Superior**: 98% de los dispositivos utilizan iOS 4 o superior[18].

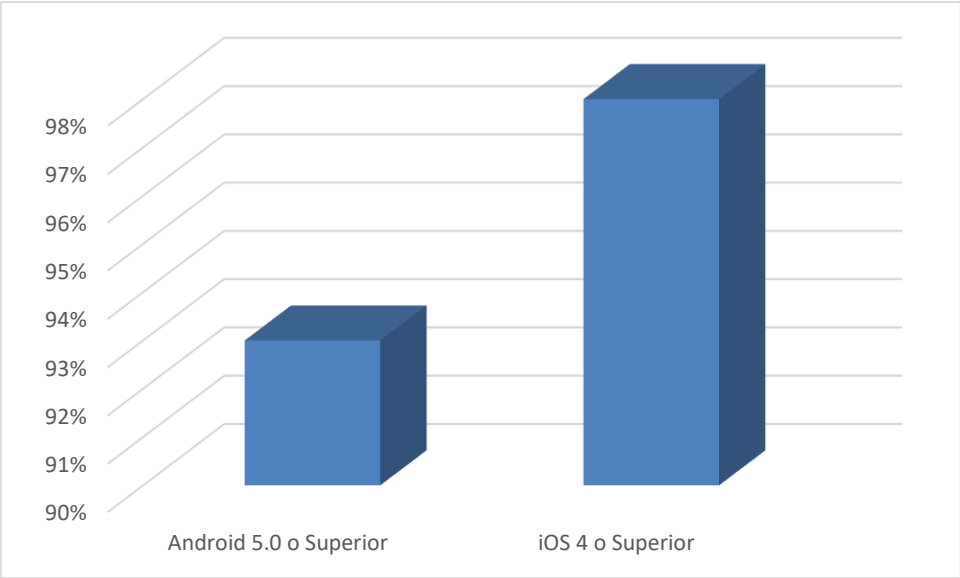


Figura 8: Porcentaje de Dispositivos con versiones que soportan IPv6 por Sistema Operativo

2.7 Investigación Sobre Enrutamiento y Resolución de direcciones IPv6

2.7.1 Resolución DNS64

La resolución DNS64 es indispensable para la convivencia de los direccionamientos IPv4 e IPv6, pues al día de hoy, no el 100% de los sitios y portales Web utilizan IPv4 y no el 100% de los sitios utilizan IPv6, por lo que los usuarios deben disponer de ambos tipos de conversion (NAT) para la resolución de búsquedas por URL.

Las redes *dual-stack* con conectividad IPv6 e IPv4 son ahora muy comunes, pero aún están lejos de ser universales. Para dar el siguiente paso de la transición a IPv6 e implementar redes solo IPv6, los operadores de red aún deben preservar el acceso a redes y servicios solo IPv4. Existen varios mecanismos de transición para proporcionar acceso IPv6 a IPv4; una opción cada vez más popular entre muchos operadores de red es NAT64. El uso de una puerta de enlace NAT64 con capacidad de traducción de IPv4-IPv6 permite que los clientes solo de IPv6 se conecten a servicios solo de IPv4 a través de direcciones IPv6 sintéticas que comienzan con un prefijo que las enruta a la puerta de enlace NAT64.

DNS64 es un servicio DNS que devuelve registros AAAA con estas direcciones IPv6 sintéticas para destinos solo de IPv4 (con registros A pero no AAAA en el DNS). Esto permite que los clientes de solo IPv6 usen puertas de enlace NAT64 sin ninguna otra configuración. Google Public DNS64 proporciona DNS64 como un servicio global utilizando el prefijo reservado NAT64 64: ff9b:: / 96. Google proporciona dos DNS64 públicos para que los usuarios puedan hacer búsquedas de este tipo, para lo cual se tienen las siguientes restricciones:

- Google Public DNS64 está diseñado para su uso solo en redes con acceso a una puerta de enlace NAT64 utilizando el prefijo NAT64 reservado 64:ff9b::/96. No lo use en redes que no puedan alcanzar tal puerta de enlace NAT64.
- Google Public DNS64 no proporciona acceso a dominios privados que no se pueden resolver desde la Internet pública, aunque puede devolver registros AAAA para direcciones IPv4 privadas (RFC 1918) devueltas en respuestas DNS públicas.
- Google Public DNS64 no es necesario para redes o hosts *dual-stack*, pero funciona y devuelve registros AAAA sintetizados y A originales (esto puede provocar que el tráfico a hosts solo IPv4 pase a través de NAT64 en lugar de directamente a través de IPv4, pero generalmente solo cuando la conexión NAT64 es más rápida)[19]

Para poder realizar Pruebas utilizando estos DNS64, es necesario configurar manualmente la dirección IP de los DNS, que se enuncian a continuación:

- 2001:4860:4860::6464 (que es lo mismo que decir 2001:4860:4860:0:0:0:0:6464)
- 2001:4860:4860::64 (que es lo mismo que decir 2001:4860:4860:0:0:0:0:64)

2.7.2 Sitios Web con IPv6

Por definición, en IPv4 se tienen 4 octetos de 8 bits cada uno, lo que nos da un total de 2^{32} = 4,294,967,296 direcciones IP en total. Para el caso de IPv6, por definición, se tienen 8 grupos de 16 bits cada uno, lo que nos da un total de 2^{128} = 3,4 x 10^{38} direcciones IP, suficiente para cubrir 6,67 x 10^{23} direcciones IP por m^2 sobre la Tierra (incluyendo océanos), suficiente para soportar un incremento importante en la asignación de direccionamiento para prácticamente todos los dispositivos que así lo requieran.

Se ha encontrado, que prácticamente todos los sitios Web más importantes soportan IPv6 (esto es por ejemplo: Google, YouTube, Facebook, Instagram, entre otros), por lo que bastaría con intentar acceder a cualquiera de estos sitios usando una dirección IPv6 para ejecutar las Pruebas que correspondan. Se ha encontrado que el navegador Firefox cuenta con un complemento llamado “SixOrNot” que facilita visualizar las direcciones IP y dominios que está utilizando un sitio Web.

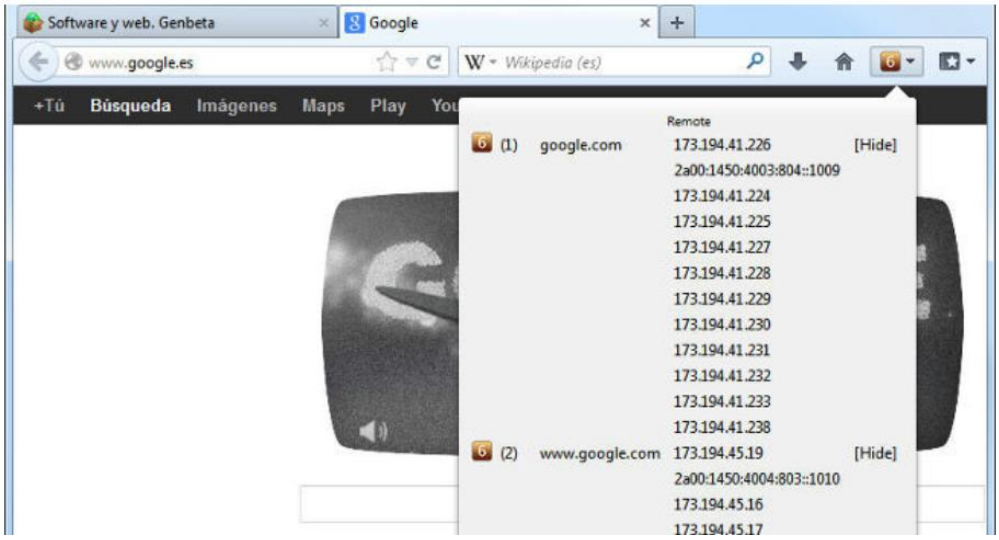


Figura 9: Captura de pantalla de complemento Firefox "SixOrNot"

Adicionalmente, se ha encontrado el sitio https://test-ipv6.com/ que muestra el diagnóstico completo a nivel de direccionamiento, DNS, ISP, protocolo, entre otros, útil para confirmar que el dispositivo esté utilizando el direccionamiento correcto.

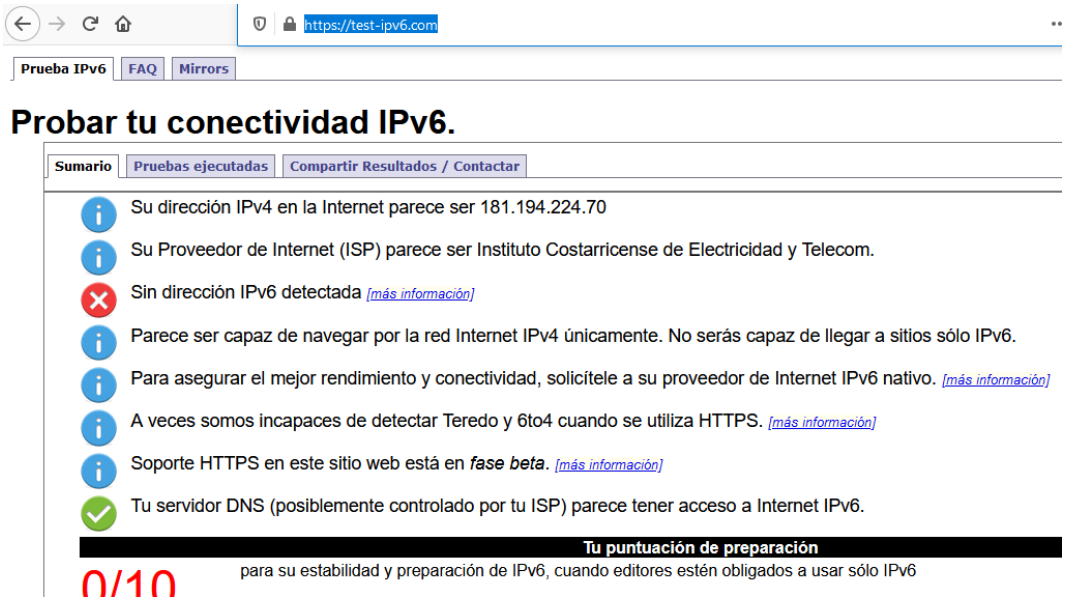


Figura 10: Prueba de IPv6 del sitio https://test-ipv6.com/ usando IPv4

Finalmente, según estadísticas actualizadas que se obtuvieron del Centro de Recolección de Estadísticas de Google[20], se visualiza un crecimiento constante en los últimos años, en la tasa de disponibilidad de usuarios que accesan a Google utilizando IPv6.

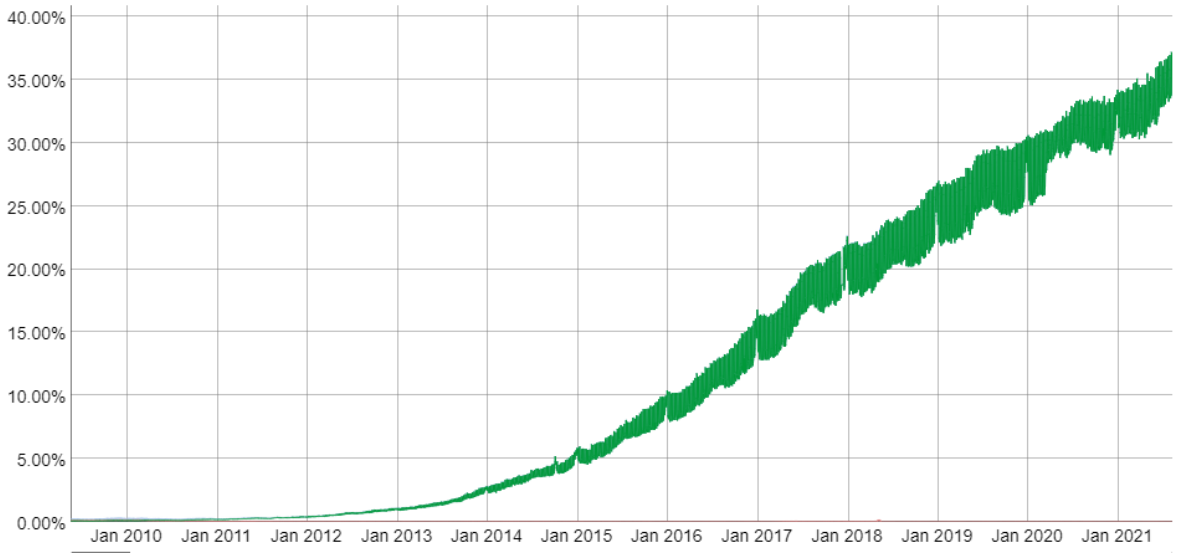


Figura 11: Porcentaje de Disponibilidad de usuarios que accesan a Google utilizando IPv6

2.7.3 Investigación sobre Capacidades de Equipos red móvil de ISP

De acuerdo a investigaciones internas realizadas, el ISP Kolbi soporta el direccionamiento IPv6 en la mayoría de sus equipos y plataformas, suficiente para realizar Pruebas de Servicio iniciales que permitan cumplir los objetivos de este trabajo.

Sin embargo, según LACNIC, en América Latina y específicamente para el caso de nuestro país Costa Rica, hacia finales del 2016 e inicios del 2017, se había retardado el despliegue de IPv6 por multiples dificulatades, entre las que figuran que el equipamiento de red no totalmente compatible con IPv6, aplicaciones no compatibles, conocimiento del personal, falta de soporte entre otros que se pueden visualizar en la siguiente figura:

PAÍS	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Equipamiento de red no totalmente compatible IPv6	66%	46%	-	50%	-	74%	67%	67%	60%	100%	-	33%	50%	20%	100%	-	-	43%	33%	50%	-	-	100%	-	-	-	100%	100%
Terminales no totalmente compatibles IPv6	65%	36%	-	50%	-	71%	67%	67%	80%	-	-	67%	50%	60%	-	-	-	43%	100%	50%	100%	-	-	-	-	-	100%	50%
Curva de aprendizaje del personal	63%	73%	-	-	-	64%	33%	67%	60%	-	-	100%	100%	40%	-	-	100%	0%	67%	100%	100%	-	100%	-	-	-	100%	100%
Aplicaciones que no soportan direccionamiento IPv6	52%	36%	-	50%	-	59%	67%	-	60%	-	-	67%	50%	40%	-	-	-	57%	33%	50%	-	-	-	-	-	-	-	50%
Falta de soporte de los proveedores	44%	55%	-	50%	-	48%	33%	17%	20%	100%	-	33%	50%	20%	100%	-	33%	14%	-	100%	-	-	100%	-	-	-	50%	-
Costos mayores a los estimados	22%	9%	-	-	-	26%	67%	33%	-	-	-	33%	50%	-	-	-	-	-	-	50%	-	-	-	-	-	-	-	-
Dificultades con los sistemas BSS - OSS	20%	27%	-	-	-	23%	-	17%	20%	-	-	-	50%	-	-	-	-	14%	-	50%	-	-	-	-	-	-	-	-
Otra	14%	-	-	-	-	12%	-	33%	20%	-	-	-	-	40%	100%	-	-	29%	33%	-	-	-	100%	-	-	-	-	50%
Base	193	11	-	2	-	133	3	6	5	1	-	3	2	5	1	-	3	7	3	2	1	-	1	-	-	-	2	2

Figura 12: LACNIC, principales dificultades encontradas en el despliegue de IPv6[21]

Entre las principales causas de estas dificultades que se mencionaron para la región, Costa Rica determinó que el principal motivo que ha retrasado el despliegue ha sido el hecho de temer dificultades de despliegue y operación, según se puede observar en la imagen a continuación:

PAÍS	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	Mexico	Nicaragua	Panamá	Paraguay	Perú	Rep. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Teme dificultades de despliegue y operación	35%	31%	-	33%	-	39%	10%	27%	100%	-	-	75%	50%	100%	-	-	60%	21%	40%	60%	-	-	-	-	-	-	-	67%
No lo ha considerado aún	34%	36%	-	-	-	31%	40%	27%	-	-	-	25%	50%	-	-	-	40%	50%	20%	60%	50%	-	50%	-	100%	-	100%	33%
La infraestructura actual presenta problemas para la transición a IPv6	29%	19%	-	33%	100%	35%	10%	27%	-	100%	-	50%	25%	50%	-	-	20%	21%	40%	20%	25%	-	-	-	-	50%	-	-
Inversión no justificada por las necesidades de la organización	17%	14%	-	-	-	18%	30%	27%	-	-	-	25%	25%	-	-	-	-	25%	-	-	25%	-	-	-	-	-	-	-
El ISP no soporta IPv6	16%	17%	-	100%	-	11%	40%	9%	-	100%	-	-	-	50%	-	-	20%	4%	20%	40%	25%	100%	50%	-	-	-	-	67%
Otra	20%	28%	-	-	-	16%	30%	55%	50%	-	100%	-	50%	-	-	-	40%	11%	20%	-	25%	-	-	-	-	50%	-	-
Base	252	36	-	3	1	120	10	11	2	1	1	4	4	2	-	-	5	28	5	5	4	1	2	-	1	2	1	3

Figura 13: LACNIC, Causas del retraso en el despliegue de IPv6[22]

Para cumplir el objetivo de este trabajo, se han considerado los siguientes equipos estádar que están involucrados en la asignación de direccionamiento IP en los equipos a utilizar para Pruebas:

Tabla 1: Soporte de direccionamiento IPv6 en equipos de CORE Red Móvil

EQUIPO	FUNCIONALIDAD REQUERIDA	SOPORTE DE IPV6
PDN-GW	Asignación direccionamento IP en LTE (DHCP Stateless)	✓
SGW	Enrutamiento tráfico CORE-Acceso en LTE	✓
GGSN	Asignación direccionamento IP en 3G (DHCP Stateless)	✓
SGSN	Enrutamiento tráfico CORE-Acceso en 3G	✓
MME	Gestión de movilidad y plano de control en LTE	✓
PCRF	Creación de políticas de QoS y control del tráfico	✓
HLR / HSS-SAE	Aprovisionamiento APN (para pruebas solamente)	⚠

De manera responsable, se han identificado también algunos licenciamientos que no se tienen disponibles, con el fin de poder adaptarse a estas limitaciones durante el desarrollo de Pruebas:

Tabla 2: Funcionalidades no soportadas en equipos CORE Red Móvil

EQUIPO	FUNCIONALIDAD REQUERIDA	SOPORTE DE IPV6
PDN-GW	DHCP Statefull iPv6 en LTE	X
GGSN	DHCP Statefull iPv6 en 3G	X

Capítulo 3. Diseño, Pruebas, Resultados y Estrategia

3.1 Diseño

Para la elaboración del Diseño, se determina que la ubicación del sitio CORE conocido como "La Guácima" era el ideal, pues cuenta con las mismas capacidades que la red comercial, está integrada 100% con la red móvil y red IP del ICE, con la ventaja de que por evolución de equipos, los clientes comerciales que estaban siendo atendidos por este CORE han sido migrados a otras localidades (pasó de attender hasta 600mil usuarios a menos de 50mil).

A nivel de Nombre del Punto de Acceso (APN), se definió que se iba a utilizer el APN "iceipv6", el cual contenía las siguientes características:

- APN se define de manera Dual, lo que permite usarlo como IPv4, IPv6 o Dual. A pesar de esto, se define en el APN que el direccionamiento IPv6 debe tener prioridad sobre el direccoinamiento IPv4.
- La asignación de la dirección IP se hará de manera dinámica y no de manera estática o fija (similar a como se hace comercialmente).
- Se gestionan y se determinan los bloques de direccionamiento (ip pool) para usuario, tanto en IPv4 como en IPv6. Se utiliza el siguiente direccionamiento para el desarrollo de Pruebas:
  - Primera dirección IPv6 de usuario: 2001:1335:1:0:0:0:0:0
  - Úlitma dirección IPv6 de usuario: 2001:1335:1:ffff:ffff:ffff:ffff:ffff
  - Primera dirección IPv4 de usuario: 192.168.200.1
  - Úlitma dirección IPv4 de usuario: 192.168.200.250
- Se utilizan los DNS del ICE, tanto para IPv4 (200.91.75.205 y 200.91.75.206) como para IPv6 (2001:1330:1:3002:aaaa:0:0:2). Adicionalmente, se utilizan los DNS64 de Google para pruebas de traducción por tipo de direccionamiento en sitios que así lo requieran (2001:4860:4860:0:0:0:0:6464 y 2001:4860:4860:0:0:0:0:64).
- Se determina la instancia VPN para enrutar el tráfico de usuario, la cual se identifica como "IPV6", que es de tipo dual (permite ambos tipos de direccionamiento).
- Con respecto a las interfaces estándar Gx (entre el GGSN/PDN-GW y el PCRF), Gy (entre el GGSN/PDN-GW y la OCS), se replicaron las configuraciones utilizadas en la red comercial, con el fin de poder experimentar si el manejo de políticas (PCRF) y la tasación en línea (OCS) se ven o no afectados por el tipo de direccionamiento.
- Los otros parámetros de configuración del APN, como por ejemplo temporizadores, umbrales de volumen/tiempo, manejo de errores, parámetros de sesión, entre otros, se replicaron de los valores utilizados en el APN comercial del ICE.
- A nivel de DNS de APN, se decide aprovechar las resoluciones existentes para los APN comerciales, con interfaces existentes (soportadas bajo IPv4), ya que no afectan el desarrollo de la prueba y permiten enrutar el APN sin problemas para que sea resuelto por el GGSN/PDN-GW del sitio CORE La Guácima.

- A nivel de HSS-SAE y HLR, se le asigna el identificador de plantilla de APN “111” (APNTPLID). Esto para poder ser aprovisionado correctamente en la base de datos de clientes (el equipo soporta valores de hasta 65534, pero ya estaban en uso los primeros 110 valores).
- Por cuestiones de orden, se define utilizar el identificador de contexto “20” (CNTXID) para aprovisionar el APNTPLID 111 (el equipo soporta valores entre 1 y 50, por lo general se utilizan los valores por encima de 10 para pruebas).
- Numeros de prueba a utilizar. Siendo el principal 87000105, pero se utilizaron hasta 4 más durante el desarrollo de las Pruebas (de diferentes colaboradores, que participaron durante la ejecución de pruebas).

La siguiente figura muestra la topología de la prueba, así como los equipos de red CORE y transporte involucrados durante el desarrollo de la prueba:

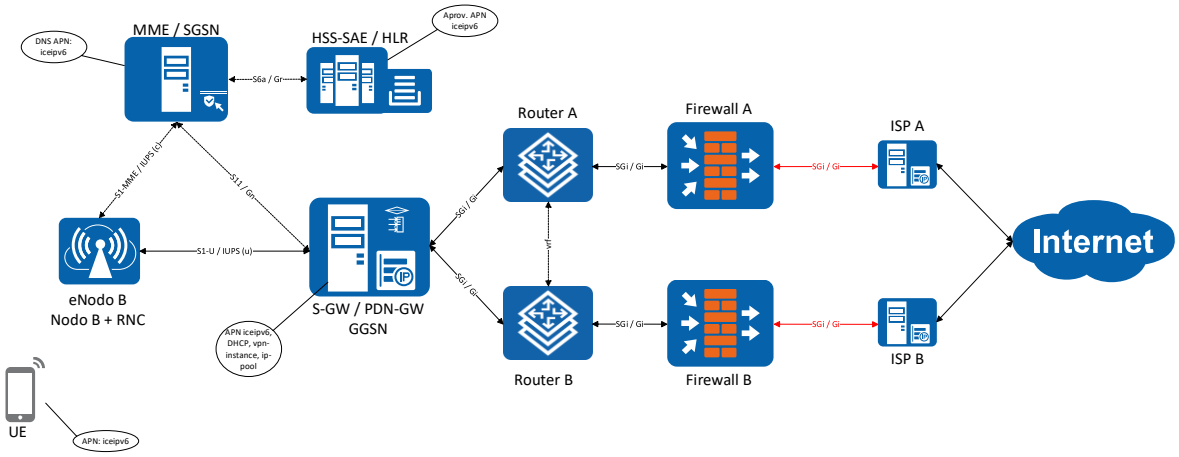


Figura 14: Diagrama Diseño Red Móvil

Tal como se observa en la figura 13, fue necesario configurar nuevas interfaces de salida a internet (Gi / SGi), para no mezclar el tráfico con el que opera la red comercial (pocos usuarios, pero usuarios comerciales que se decidieron proteger de cualquier eventualidad).

Para esta definición de interfaz Gi / SGi, se utilizó direccionamiento IPv6 a nivel de interfaz, de manera que tanto en el equipo GGSN/PDNGW como en los enrutadores NE40 (del fabricante Huawei), así como en los cortafuegos (Firewall E8000) fue necesario asignar direccionamiento, crear instancias VPN y enrutar el tráfico de esta interfaz de salida a internet.

Finalmente, fue necesario publicar los bloques de direcciones IPv4 e IPv6 en los DNS de la red IP, para que estos equipos pudieran atender las solicitudes de resolución de URL y la correspondiente conversión a dirección IP.

La siguiente figura muestra cómo finalmente quedó integrado la conectividad de interfaces de salida a internet en los equipos de la red de transporte.

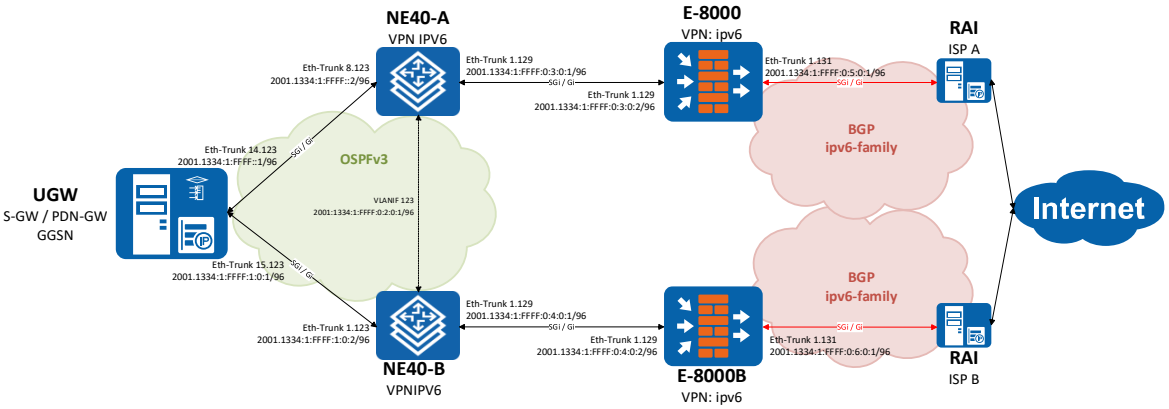
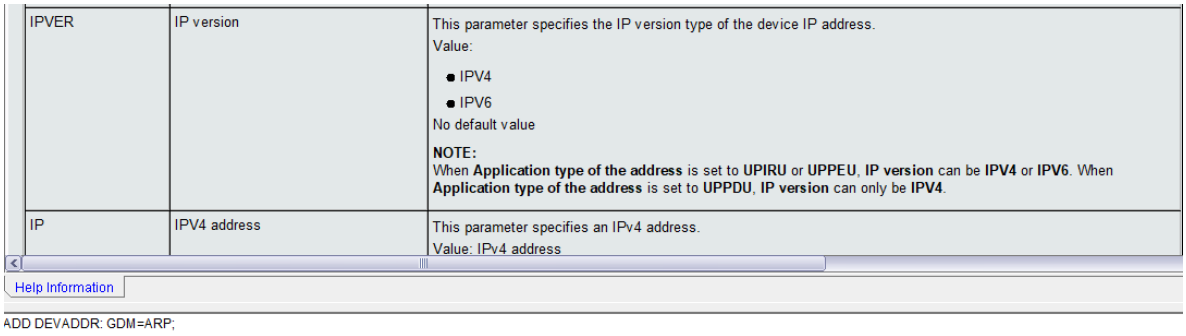


Figura 15: Diagrama Diseño Interfaces Transporte

Con respecto a la posibilidad de crear interfaces de red estándar (adicionales a la Gi / SGi), se ha realizado una investigación a nivel de equipos y documentación, respaldadas con consultas al fabricante del equipo. Se han encontrado los siguientes hallazgos.

Equipo HSS-SAE + HLR + PCRF (conocido como SDB). Soporta la creación de interfaces utilizando direccionamiento IPv6. Sin embargo, presenta la siguiente lista de restricciones y particularidades para la creación de interfaces de red estándar:

- Para conexiones con elementos externos al equipo que utilicen tarjetas de tipo UPPDU (como por ejemplo las interfaces que se deseaban crear) el equipo solamente soporta IPv4. Solamente se permite la creación de interfaces IPv6 para enlaces internos del equipo (como por ejemplo la interfaz Sp entre el PCRF y el SPR, que es una interfaz interna del mismo equipo). Abajo captura del comando ADD DEVADDR, primer paso de asignación de tarjeta / puerto / Dirección IP para enlaces externos en PCRF.



IPVER	IP version	This parameter specifies the IP version type of the device IP address. Value: • IPV4 • IPV6 No default value **NOTE:** When **Application type of the address** is set to **UPIRU** or **UPPEU**, **IP version** can be **IPV4** or **IPV6**. When **Application type of the address** is set to **UPPDU**, **IP version** can only be **IPV4**.
IP	IPV4 address	This parameter specifies an IPv4 address. Value: IPv4 address

Help Information

ADD DEVADDR: GDM=ARP;

Figura 16: Captura de pantalla con restricción de creación de interfaces externas con IPv6

- Para conexiones en general, se debe utilizar el mismo tipo de direccionamiento en ambos extremos a integrar, esto es, el nodo local y el nodo remoto. En la captura abajo se observa la documentación en donde se indica esta restricción:

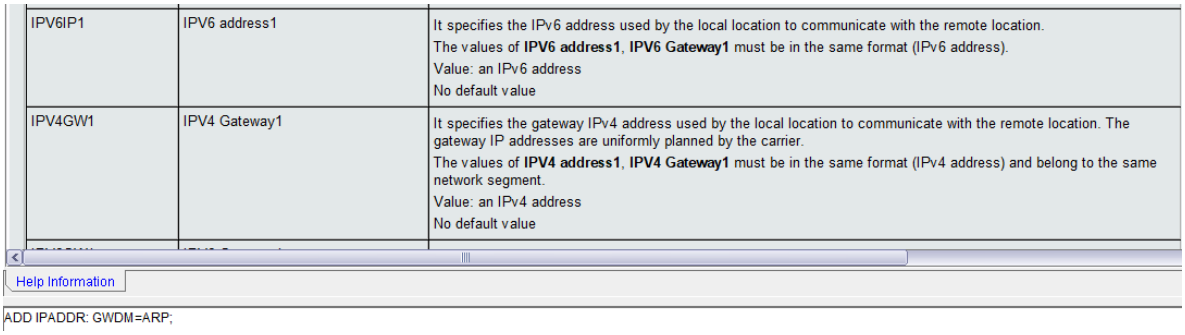


Figura 17: Captura de pantalla restricción tipo de direccionamiento en equipo local y remoto

Equipo SGSN + MME (conocido como USN en el ICE), se tiene como gran limitación, el hecho de que no soporta la creación de interfaces utilizando direccionamiento IPv6, tal como se muestra en la siguiente captura de pantalla (tomada del comando ADD DMLNK):

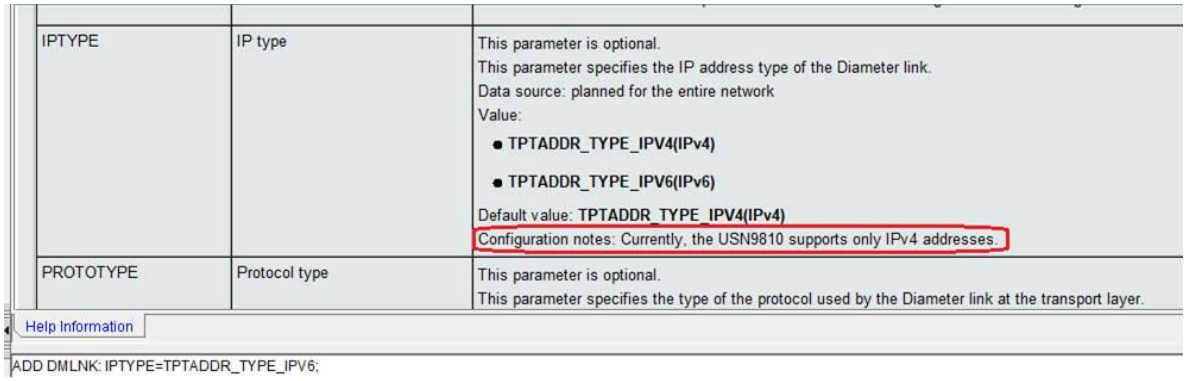


Figura 18: Captura de pantalla de Documentación con restricción de interfaces usando IPv6

Debido a estas limitaciones importantes encontradas en la fase de diseño, se observa que no es técnicamente viable crear un ambiente de pruebas de interfaces adicionales a la Gi / SGi. Esto implica, que bajo los equipos y versiones actuales, no es posible migrar plataformas o equipos a conexiones con IPv6, por lo que las pruebas se concentrarán en migrar a los usuarios, además de crear interfaces estándar Gi / SGi, necesarias para las pruebas de usuario final.

3.2 Pruebas Técnicas

3.2.1 Configuración General

Se inició la ejecución de Pruebas de campo creando las instancias y pool de IP que requiere el APN para su creación. Esto se hizo en los equipos GGSN/PDG-GW (que en el caso de la red ICE es el mismo equipo, del manufacturador Huawei, conocido como UGW9811).

Las capturas abajo muestran la configuración creada:

```
<GUAUGW01>display ip pool poolname ipv6
Pool Information
----------------
                Pool Name  =  ipv6
                Pool Type  =  Local
                Pool Lock  =  Unlock
       Pool Alarm Report   =  Disable
    single-ip-allocation   =  Disable
            Pool IP Type   =  IPv6
            VPN Instance   =  IPV6
      IP Release Time(s)   =  0
           Pool IP Lease   =  Disable
IMS Session Pool IP Lease  =  Disable
   Wait Release IP Number  =  0
           Section Count   =  1
     Prefix Total Number   =  65536
      Prefix Used Number   =  1
            Prefix Usage   =  0

          Section Number   =  0
            Section Type   =  Dynamic
             Prefix Lock   =  Unlock
        Section Start IP   =  2001:1335:1:0:0:0:0:0
          Section End IP   =  2001:1335:1:ffff:ffff:ffff:ffff:ffff
           Prefix Length   =  64
      Total Prefix Count   =  65536
       Used Prefix Count   =  1

           Bind APN Name   =  iceipv6

--------------------------
2021-07-28 13:41:21-06:00
```

Figura 19: IP Pool de IPv6 para APN de Pruebas

Tal como se observa en la consulta al equipo, se definieron instancias VPN, pool de IP y secciones de tipo IPv6. La siguiente captura de pantalla muestra la configuración de la instancia VPN para IPv6:

```
<GUAUGW01>display ip vpn-instance IPV6
  VPN-Instance Name               RD                    Address-family
  IPV6                            201:1                 IPv4
  IPV6                            201:1                 IPv6

-------------------------
2021-07-28 13:46:50-06:00
```

Figura 20: Configuración de la Instancia VPN "IPV6"

Tal como se observa, se crearon familias de direcciones IP para ambos tipos de direccionamiento (IPv4 e IPv6). Esto por cuanto se ejecutaron Pruebas bajo el escenario IPv6 puro y luego el escenario dual IPv4/IPv6. La diferenciación en la prueba se hizo a nivel de dispositivo del cliente, ya que en la configuración propia del APN en los terminales de pruebas, se puede definir el punto de acceso como solamente IPv6 o bien Dual IPv4/IPv6.

La contraparte de esta instancia VPN en el GGSN/PDNGW se encuentra en el enrutador NE-40, en el que se definen parámetros similares a los utilizados en el GGSN/PDNG, (por ejemplo: prioridad de la ruta, protocolo de transporte y enrutamiento, entre otros).

```
#
interface Eth-Trunk8.123
 vlan-type dot1q 123
 description TEST_IPV6
 ip binding vpn-instance IPV6
 ipv6 enable
 ipv6 address 2001:1334:1:FFFF::2/96
 ospfv3 123 area 0.0.0.0
 statistic enable
#
return
<GUANE40E-X16-A>display current-configuration interface vla123
#
interface Vlanif123
 description TEST_IPV6
 ip binding vpn-instance IPV6
 ipv6 enable
 ipv6 address 2001:1334:1:FFFF:0:2:0:1/96
 ospfv3 123 area 0.0.0.0
#
```

Figura 21: Consulta Router NE40 (Eth-Trunk8.123 y Vlanif123)

Mismo procedimiento se utilizó en el cortafuegos de salida a la red IP (E8000), en donde se definieron los bloques de direcciones, parámetros de prioridad, protocolo de transporte y enrutamiento ospf en la instancia VPN a utilizar para la salida del tráfico de internet con IPv6 y dual, tal como se puede observar en la siguiente consulta:

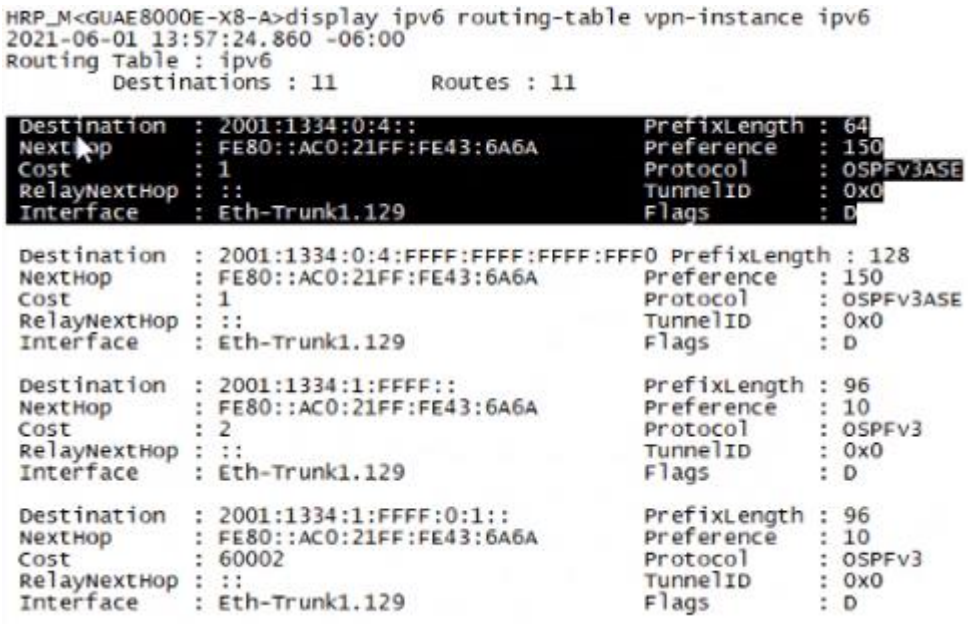


Figura 22: Consulta Firewall E8000 vpn ipv6

Finalmente, con las rutas creadas a nivel de instancias VPN, pool de IP así como la publicación de rutas en los equipos de transporte, se procede a ejecutar la configuración del Punto de Acceso en el GGSN/PDNGW (UGW), tal como se muestra a continuación (según los parámetros indicados en el Diseño):

```
<GUAUGW01>display apn iceipv6
APN information
---------------
                                    APN  =  iceipv6
                      IPV4 Vpn Instance  =  IPV6
                      IPV6 Vpn Instance  =  IPV6
                      content-awareness  =  DISABLE
                            access-mode  =  transparent-non-authentication
                ipv4 address-allocate  =  LOCAL
                    ipv4 radius-prior  =  DISABLE
                ipv6 address-allocate  =  LOCAL
                    ipv6 radius-prior  =  DISABLE
                 ipv4 address-support  =  ENABLE
                 ipv6 address-support  =  ENABLE
               address-support-preference  =  IPV6 PRIORITY
                           dual-address  =  IPV4V6
             address-allocate-withoutpco  =  DISABLE
                           virtual-apn  =  DISABLE
                           Second auth  =  DISABLE
```

```
                          address-inherit  =  ENABLE
                        perf used APN Type  =  SERVICE
                    AAA ACCT Msg used APN Type  =  SERVICE
                    AAA AUTH Msg used APN Type  =  SERVICE
                         OCS Msg used APN Type  =  SERVICE
                           CG used APN Type  =  SERVICE
                        PCRF Msg used APN Type  =  SERVICE
                  Header Enrichment used APN Type  =  SERVICE
                    Service Report used APN Type  =  SERVICE
                  S6b Interface Msg used APN Type  =  REQUESTED
                   remove-domain-name(radius)  =  DISABLE
                   append-domain-name(radius)  =  DISABLE
                     remove-domain-name(lns)  =  DISABLE
                     append-domain-name(lns)  =  DISABLE
                    roaming-user-access(SGW)  =  ENABLE
                   visiting-user-access(SGW)  =  ENABLE
                roaming-user-access(GGSN PGW)  =  ENABLE
               visiting-user-access(GGSN PGW)  =  ENABLE
                          session-timeout  =  DISABLE
                            idle-timeout  =  DISABLE
                         hlr-hss-provided  =  ENABLE
                          radius-conflict  =  ignore
                      radius-hlr-redundancy  =  DISABLE
                            static-ip route  =  DISABLE
                       binding-gn-interface  =  NULL
                          select-mode-check  =  DISABLE
                                       lock  =  DISABLE
                             deactive-user  =  DISABLE
                   ppp-access authentication  =  DISABLE
                        ppp-address-allocate  =  LOCAL
          ppp-address-allocate radius-prior  =  DISABLE
                                       l2tp  =  DISABLE
                          address-pool-name  =  ipv6
                          address-pool-name  =  ipv4
     IPv4 address assigned by pool priority  =  DISABLE
     IPv6 address assigned by pool priority  =  DISABLE
                    radius server group name  =  NULL
                  diameter server group name  =  NULL
                         QoS-Profile name  =  NULL
                       uplink qos-car flag  =  inherit
                     downlink qos-car flag  =  inherit
                       uplink qos-shape flag  =  inherit
                     downlink qos-shape flag  =  inherit
                       uplink qos-enforcement  =  none
                     downlink qos-enforcement  =  none
                                dns primary-ip  =  200.91.75.205
                              dns secondary-ip  =  200.91.75.206
                    IPV4 DNS first priority  =  dhcp
                   IPV4 DNS second priority  =  radius
                    IPV4 DNS third priority  =  local
                   IPV4 DNS fourth priority  =  pcrf
                    IPV6 DNS first priority  =  dhcp
                   IPV6 DNS second priority  =  radius
                    IPV6 DNS third priority  =  local
                   IPV6 DNS fourth priority  =  pcrf
                        ipv6 dns primary-ip  =  2001:1330:1:3002:aaaa:0:0:2
                     volume-statistic-mode  =  layer-all
                      G-CDR-field-template  =  inherit
                     PGW-CDR-field-template  =  inherit
                     SGW-CDR-field-template  =  inherit
```

GGSN-offline-charge-template	=	inherit
PGW-offline-charge-template	=	inherit
SGW-offline-charge-template	=	inherit
Serving-Node mapping PLMN ID	=	ENABLE
SGSN-SGW-IP mapping RAT type	=	ENABLE
radius-disconnect handle	=	ENABLE
apn-restriction	=	DISABLE
cbr/ubr temporarily-reject-retransmit	=	INHERIT
dbr temporarily-reject-retransmit	=	INHERIT
Soft bit	=	00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Soft byte	=	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Soft string1	=	<NULL>
Soft string2	=	<NULL>
Soft string3	=	<NULL>
Soft string4	=	<NULL>
Soft string5	=	<NULL>
apn binding home-zone-server group	=	NULL
multiple Service Mode	=	RADIUS
charge characteristic name	=	NULL
tariff group name	=	NULL
UserProfile Group name	=	upg_oracle
five-tuple-max	=	inherit
service-trigger	=	DISABLE
wait-accounting-response	=	DISABLE
acct response-timeout	=	DEACTIVE
data-before-response	=	PROHIBIT
accounting-update	=	ENABLE
rat-trigger	=	ENABLE
uli-trigger	=	ENABLE
sgsn-trigger	=	ENABLE
qos-trigger	=	ENABLE
ip-release	=	DISABLE
accounting-bearer	=	ALL
cache-acct-stop-msg	=	DISABLE
radius-server time threshold	=	0
radius-server volume threshold	=	0
dcc-template-name	=	dcc_oracle
charge-method online	=	inherit
charge-method offline	=	inherit
charge-method tight-interworking	=	inherit
sgw charge-method offline	=	inherit
home pcc-switch flag	=	ENABLE
roaming pcc-switch flag	=	ENABLE
visit pcc-switch flag	=	ENABLE
metering method	=	volume
reporting level	=	rg
ims-switch flag	=	inherit
signaling-radio-preference flag	=	inherit
primary p-cscf-group	=	NULL
pcrf-group-name(default)	=	pcrf_group
dhcp server expired time (day)	=	1
dhcp server expired time (hour)	=	0
dhcp server expired time (minute)	=	0
backoff-time overload-switch	=	disable
backoff-time apn-congestion	=	disable
backoff-time timer-length	=	600
dedicated-bearer-activation eutran-nb-iot	=	disable
support anti-spoofing for updata	=	ENABLE

support anti-spoofing for downdata	=	ENABLE
support coa(change-of-authorization)	=	DISABLE
qchat-switch	=	DISABLE
cf-switch	=	inherit
sponsor-switch	=	inherit
Null-MSISDN Flag	=	ENABLE
af-switch	=	DISABLE
TETHERING-SWITCH	=	DISABLE
service-statistic-switch	=	DISABLE
Emergency APN Flag	=	DISABLE
ipv6 max-retrans-adv-interval	=	14400
ipv6 ra-oflag	=	ENABLE
APN Max PDP Context Number	=	NULL
Framed Route Mode	=	DISABLE
access control degree	=	1
charge-profile	=	NULL
congestion-report-switch flag	=	DISABLE
intelligent-select-switch	=	DISABLE
location-report-rpt	=	DISABLE
icha-switch	=	inherit
binding User-Group	=	NULL
mse-profile-group name	=	NULL
IPv4 MSS Value	=	1400
IPv6 MSS Value	=	1400
single-pass-switch	=	ENABLE
uplink gi-defend-switch	=	inherit
downlink gi-defend-switch	=	inherit
UE heartbeat detect	=	DISABLE
gateway-proxy	=	INHERIT
pap-bypass(active-failure)	=	bypass
pap-bypass(slot-failure)	=	bypass
reactivation requested delete	=	DISABLE
reactivation requested transparent	=	ENABLE
Pseudo Active Function Switch	=	INHERIT
Pseudo Active Upper Limit	=	200
volte-monitor-switch	=	DISABLE
auth response-timeout	=	DEACTIVE
http2-degradation	=	INHERIT
ptt-switch	=	INHERIT
lbo-switch	=	INHERIT
ppd-switch	=	INHERIT
non-ip-switch	=	INHERIT
user-port	=	5683
binding M2M-Server-Group	=	NULL
ue-mutual-access forbidden inner-apn switch	=	INHERIT
ue-mutual-access forbidden inter-apn switch	=	INHERIT
Serving PLMN rate control function	=	INHERIT
APN rate control function	=	INHERIT
normal-user time length	=	6
nbiot-user time length	=	6
scef-switch	=	INHERIT
scef-group name	=	NULL

2021-07-28 13:40:30-06:00		

Tabla 3: Consulta Parámetros en Tabla DNS para APN iceipv6 (MME)

Con esta creación, se procede a crear los enrutamientos del APN en los DNS de APN (MME y SGSN). Estos son necesarios para que los equipos de red, al momento de iniciar una sesión de datos, sepan dar el tratamiento al PDP / Bearer y puedan encaminarlo por el GGSN / PDNGW del sitio CORE La Guácima, que contiene las configuraciones mostradas anteriormente. Esto se ejecutó en dos tablas, las tablas IPV4DNS y DNSH, responsables de la traducción del APN y enrutamiento hacia el GGSN (3G) y PDNGW (LTE) respectivamente.

Tabla 4: Consulta parámetros tabla IPV4DNS para APN iceipv6 (SGW-PGW)

```
The result is as follows:
-------------------------
 FQDN                                          Host Name Index  Entity  Interface Type  S5 Protocol  S8 Protocol  Priority  Weight

 ICEIPV6.APN.EPC.MNC001.MCC712.3GPPNETWORK.ORG  27               PGW     S5              GTP          GTP          0         100
 ICEIPV6.APN.EPC.MNC001.MCC712.3GPPNETWORK.ORG  30               PGW     S5              GTP          GTP          0         100
(Number of results = 2)

---    END
```

Tabla 5:Consulta Parámetros en Tabla DNS para APN iceipv6 (SGSN)

```
The result is as follows
------------------------
 Host Name Index  Host Name                      Address Section  IP Type  IP Address1      Priority1  Weight1  IP Address2      Priority2  Weight2  IP Address3      Priority3  Weight3

 256              ICEIPV6.ICE.MNC001.MCC712.GPRS  SECTION1         IPV4     201.191.199.129  127        127      201.191.199.130  127        127      201.191.199.131  127        127
 256              ICEIPV6.ICE.MNC001.MCC712.GPRS  SECTION2         IPV4     201.191.199.133  127        127      201.191.199.134  127        127      201.191.199.135  127        127
(Number of results = 2)
```

Ya con todas estas configuraciones, se procede a preparar el aprovisionamiento a nivel de HSS-SAE / HLR. Lo primero, crear la plantilla de APN en la table APNTPL, con el ID definido en el Diseño (111):

```
+++    USCDB        2021-06-02 14:49:14
PGW    #017370
%%LST APNTPL: HLRSN=1, TPLID=111;%%
RETCODE = 0 SUCCESS0001:Operation is successful

                        HLRSN = 1
                        TPLID = 111
                      TPLNAME = APNTPL_iceipv6
                          APN = iceipv6
                PDNGWALLOCTYPE = DYNAMIC
              NONIPDATADELMECH = SGi_BASED_DATA_DELIVERY

Total count = 6

There is together 1 report

---    END
```

Figura 23: Consulta SDB para APNTPL iceipv6

Con este valor, se procede a agregar el APN de tipo dual IPv4/IPv6 en las partes de suscripción de LTE (Tabla OPTGPRS -> EPS APN) y 3G (Tabla GPRS) del número de Pruebas 87000105, tal como se muestra a continuación.

```
                CNTXID = 20
              APNTPLID = 111
            DEFAULTAPN = FALSE
           WILDCARDAPN = FALSE
           EPSQOSTPLID = 200
               PDPTYPE = IPV4IPV6
                ADDIND = DYNAMIC ADDRESS
               ADD2IND = DYNAMIC ADDRESS
          VPLMNALLOWED = FALSE
                CHARGE = NORMAL
```

Figura 24: Consulta parámetros aprovisionamiento APN 4G LTE

```
                CNTXID = 20
               PDPTYPE = IPV4IPV6
                ADDIND = DYNAMIC ADDRESS
               ADD2IND = DYNAMIC ADDRESS
                RELCLS = ACKRLCPRODT
              DELAYCLS = DELAY1
                PRECLS = NORMAL
               PEAKTHR = 256000 OCT
              MEANTHR = BEST_EFFORT
           ARPRIORITY = NORMAL
               ERRSDU = NO
             DELIVERY = NO
           TRAFFICCLS = INTERACT
           MAXSDUSIZE = 1500 OCT
             MAXBRUPL = 8640K
             MAXBRDWL = 8640K
               RESBER = 0.00001
               SDUERR = 0.0001
          TRANSFERDEL = 10MS
           TRAFFICPRI = PRIORITY1
            MAXGBRUPL = 0K
            MAXGBRDWL = 0K
                  APN = iceipv6
                VPLMN = FALSE
               CHARGE = NORMAL
```

Figura 25: Consulta parámetros aprovisionamiento APN 3G

Con la información depurada, se realizan intentos de navegación para verificar el correcto establecimiento de la sesión de datos, en donde todos los equipos involucrados intervienen de manera correcta asignando una dirección de tipo IPv6, tal como se muestra en la siguiente captura de pantalla, tomada sobre la interfaz estándar S5/S8, que utiliza el protocolo de red GTP y se observa la asignación de la dirección IPv6:

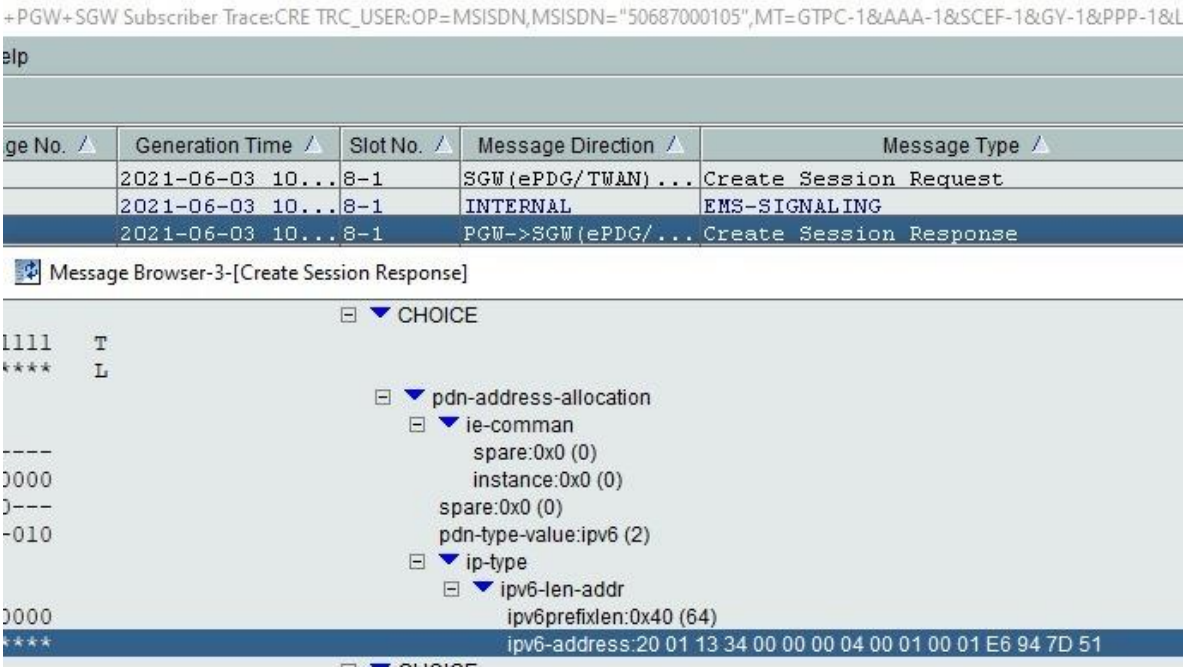


Figura 26: Captura Traza de asignación de IPv6 a usuario en creación de PDP

3.2.2 Pruebas y Análisis IPv6 (Puro)

Con las configuraciones listas a nivel de red CORE, transporte y aprovisionamiento, se procedió a configurar el APN “iceipv6” en el dispositivo terminal. Para esta primera prueba, se utiliza la configuración de APN ipv6 puro, tal como se muestra a continuación:

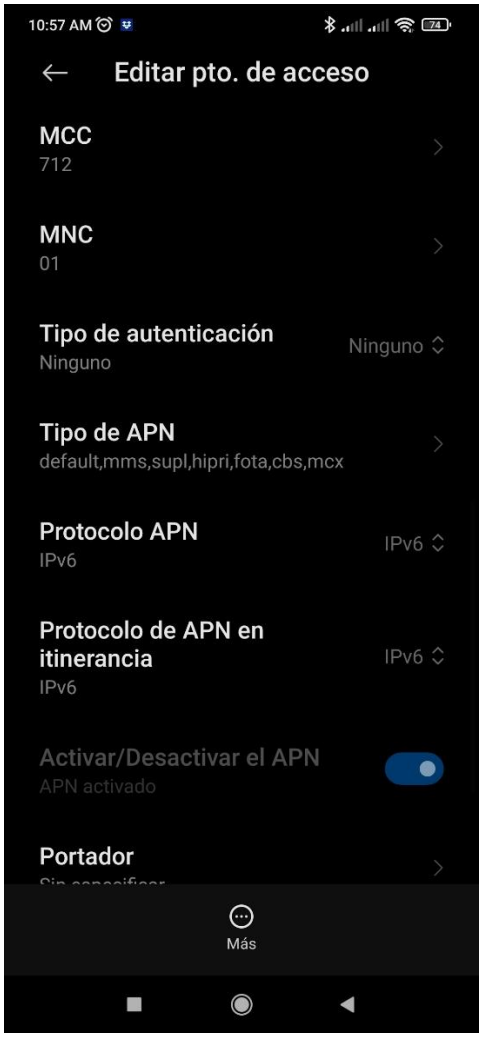


Figura 27: Configuración del APN en el dispositivo del cliente, IPv6 puro

Se inician las pruebas de navegación en sitios populares de internet, algunos internacionales (como YouTube, WhatsApp, Facebook) y otros destinos nacionales (como el sitio Web del T.S.E., sitio Web de Kolbi, entre otros).

Para facilidad de comprensión y visualización del comportamiento del dispositivo en Internet, también se utiliza el sitio https://ipv6-test.com/ que muestra la asignación de dirección IP, conectividad y el ISP (en este caso el ICE).

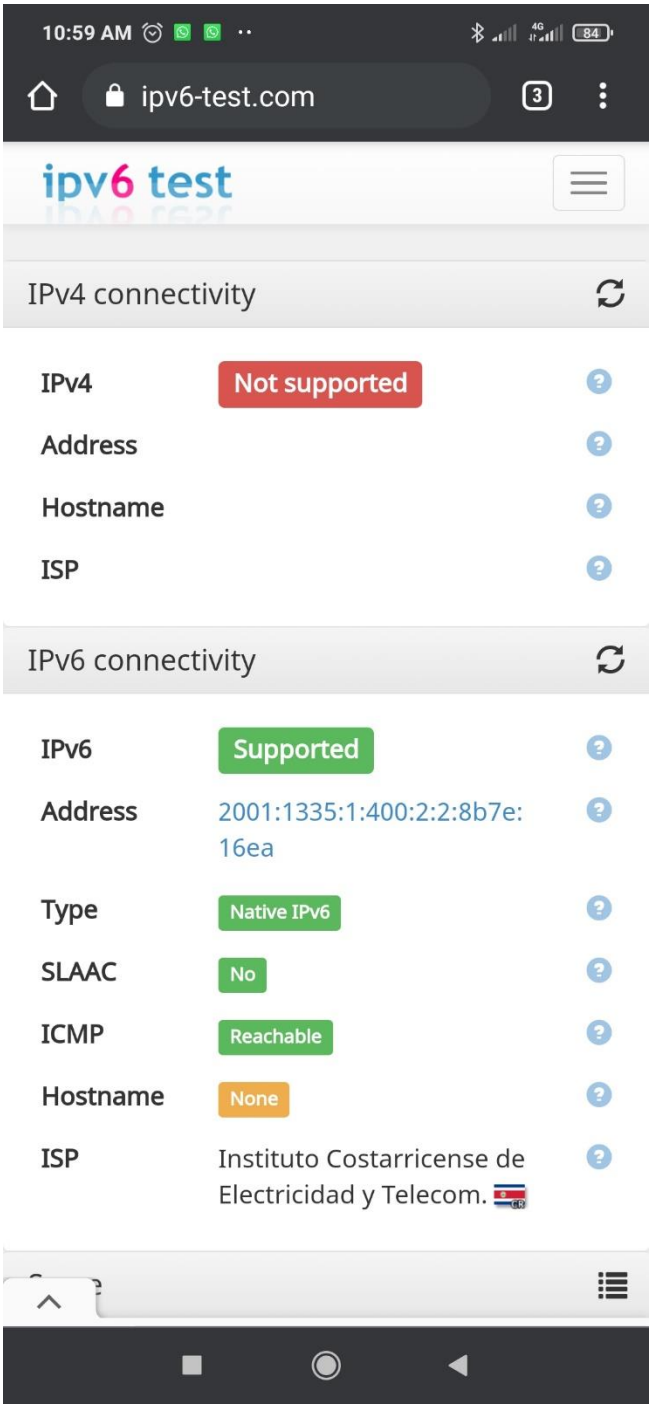


Figura 28: Prueba en sitio Web https://ipv6-test.com/ usando IPv6 puro

A nivel de aplicaciones móviles, se ha utilizado la herramienta “PingTools” para verificar la conectividad y asignación de direcciones IP:

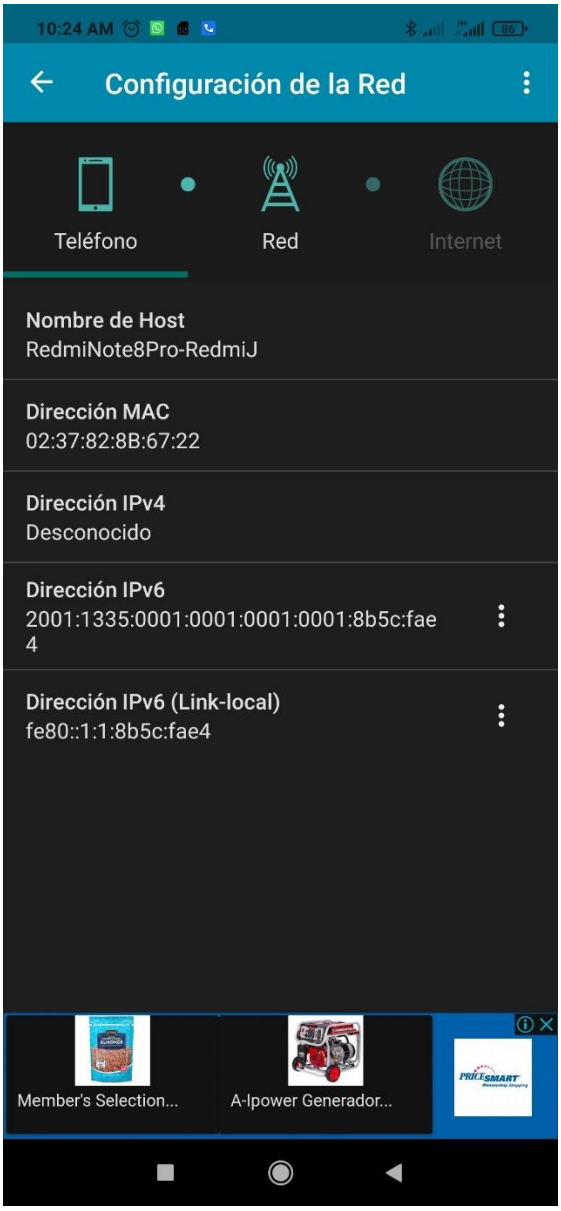


Figura 29: Estado conexión desde herramienta PingTools de Android. Caso IPv6 puro.

Desde el CORE de la red móvil, específicamente desde el equipo UGW (que contiene el GGSN/PDNGW) también se verifica el estado de la conexión, el cual se visualiza a continuación:

Tabla 6: Consulta PDP/Bearer confogurado como IPv6 puro

<GUAUGW01>display pdpcontext msisdn 50687000105
The PDP context on board 5

IMSI = 712012007529802
IMEI = 868909043593530
UGW Role = S+PGW

EPS Bearer ID	=	5
Default Bearer	=	Yes
PDP type	=	IPv6
IPv6 Address type	=	UGW ALLOC IP ADDRESS
IPv6 PDP address	=	2001:1335:1:400:1:1:c54:5c1b
MSISDN	=	50687000105
APN name	=	iceipv6
Requested Charging Characteristic	=	0X0800
Negotiated Charging Characteristic	=	0X0800
GTP Version	=	V2
Charging ID	=	42265344
Tunnel mode	=	direct tunnel mode
Left Local Teidc	=	0X01a09a21
Left Local Teidu	=	0X01a09a21
Left Peer Teidc	=	0X074c6104
Left Peer Teidu	=	0Xc10ad025
Left Local Signal Port	=	2123
Left Peer Signal Port	=	2123
Left Local Signal IP	=	201.191.199.151
Left Peer Signal IP	=	201.191.194.107
Left Local Data IP	=	10.178.122.247
Left Peer Data IP	=	10.204.18.82
Right Local Signal IP	=	NULL
Right Peer Signal IP	=	NULL
Right Local Data IP	=	NULL
Right Peer Data IP	=	NULL
APN AmbrUp	=	4294967kbps
APN AmbrDown	=	160000kbps
Requested QoS	=	2d840800,00000000,00000000,00000000,00000000,00000000
Request Qos Class Identifier	=	8
Request Allocation/Retention PRI	=	11
Request Allocation/Retention PRI PCI	=	0
Request Allocation/Retention PRI PVI	=	1
Request Max Bit Rate for Uplink	=	NULL
Request Max Bit Rate for Downlink	=	NULL
Request Gua Bit Rate for Uplink	=	NULL
Request Gua Bit Rate for Downlink	=	NULL
Negotiated QoS	=	2d840800,00000000,00000000,00000000,00000000,00000000
Qos Class Identifier	=	8
Allocation/Retention PRI	=	11
Allocation/Retention PRI PCI	=	0
Allocation/Retention PRI PVI	=	1
Max Bit Rate for Uplink	=	NULL
Max Bit Rate for Downlink	=	NULL
Gua Bit Rate for Uplink	=	NULL
Gua Bit Rate for Downlink	=	NULL
L2TP Flag	=	false
User Type	=	home
RAT Type	=	EUTRAN
PCC Type	=	true
Charge Rule Base Name	=	up_oracle
Mse Profile Match List Name	=	NULL
Online Charging Flag	=	No
Offline Charging Flag	=	No
SGW Offline Charging Flag	=	Yes
Content Charging Flag	=	Yes
Tight Interworking	=	No
Primary Charge Function	=	NULL
Secondary Charge Function	=	NULL
URL Filtering Flag	=	false
Sponsor Data Flag	=	false
ADC Type	=	false
MSE Type	=	false
NAT Switch	=	DISABLE
PAP Switch	=	DISABLE
IMS Signalling Context Flag	=	false

STE Flag	=	false
IPv6 VPN instance	=	IPV6
Primary IPv6 DNS Server IP	=	2001:1330:1:3002:aaaa:0:0:2
Session Activation Timestamp	=	11:21:18 07/30/2021(MM/DD/YYYY)
Lifetime(seconds)	=	8
No Service Time(seconds)	=	8
DSCP	=	10
Uplink Packets	=	0
Downlink Packets	=	0
Uplink Bytes	=	0
Downlink Bytes	=	0
Tethering Switch	=	DISABLE
User Location Information	=	Type:ECGI;MCC:712;MNC:01;ECI:344321
User Location Information	=	Type:TAI;MCC:712;MNC:01;TAC:3105
BCM Flag	=	UE_NW
Suspend Flag	=	false
Maintained Flag	=	false
Af Switch	=	DISABLE
PCC User Type	=	dynamic-pcc
MME/S4SGSN Identifier IP	=	NULL
DDN ACK Timeout Delay Delete	=	No
Anonymous Apn Type	=	false
Non-IP User	=	No
PRA FLAG	=	false
ToolBar Radius Status	=	disable
Serving PLMN Uplink Rate Limit	=	0
Serving PLMN Downlink Rate Limit	=	0
(Number of Results = 1)		

2021-07-30 11:21:30-06:00		

Si bien es cierto la experiencia de navegación en sitios internacionales (YouTube, Dropbox, Facebook, WhatsApp) resulta completamente funcional, se han experimentado problemas de navegación en sitios IPv4 puros. Esto debido a la inexistencia de un DNS64 en la red del ICE. Como plan de contingencia, se había investigado la existencia de un DNS64 de Google para poder utilizar en esta prueba, sin embargo, los DNS64 de Google al parecer no están disponibles el 100% del tiempo para traducciones entre sitios IPv4 e IPv6, por lo que en términos generales, para clientes masivos, de momento no se recomienda migrar a los clientes a un escenario de este tipo (con IPv6 puro).

Las capturas abajo muestran los resultados obtenidos desde el punto de vista del cliente, para los sitios de YouTube y www.tse.go.cr.

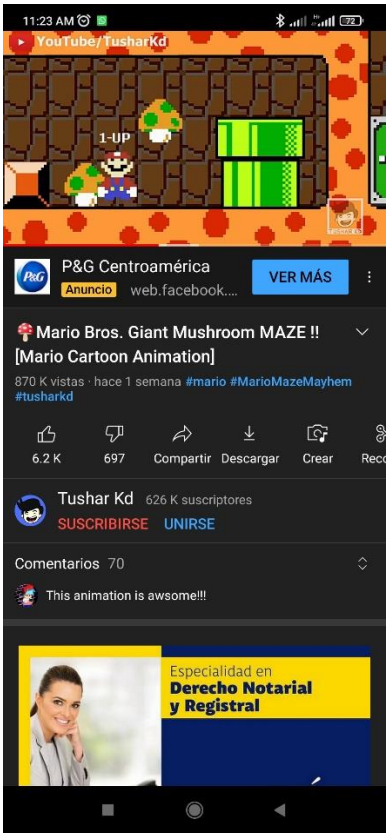


Figura 30: Prueba de Navegación en YouTube con IPv6 puro

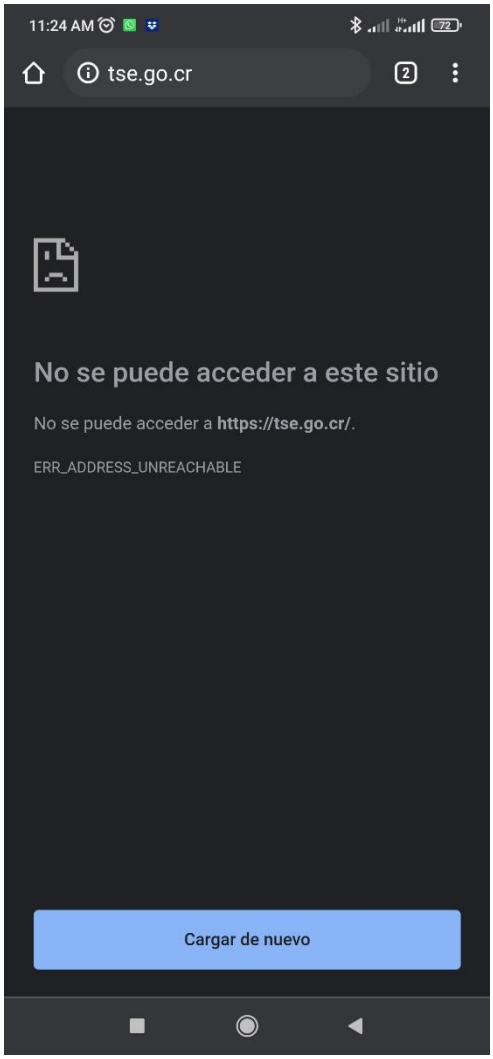


Figura 31: Prueba de Navegación a sitio Web IPv4 usando configuración IPv6 Puro

3.2.3 Pruebas y Análisis IPv4 / IPv6 (Dual)

El siguiente escenario a probar, fue el de una configuración dual, que permita tener al dispositivo ambos tipos de direccionamiento activos IPv4 e IPv6 de manera simultánea. Es importante mencionar que previo a la ejecución de esta prueba, fue necesario habilitar el licenciamiento de IPv4/IPv6 Dual a nivel del SGSN/MME, el cual permite al cliente la asignación dinámica de ambos tipos de direcciones IP en el mismo PDP / Bearer sin consumir otros licenciamientos (como por ejemplo el de cantidad de sesiones IP, o utilización de otras interfaces de red estándar como la Gx, Gy, SGs, entre otras).

La captura abajo muestra la configuración del APN en el dispositivo utilizado, con configuración dual:

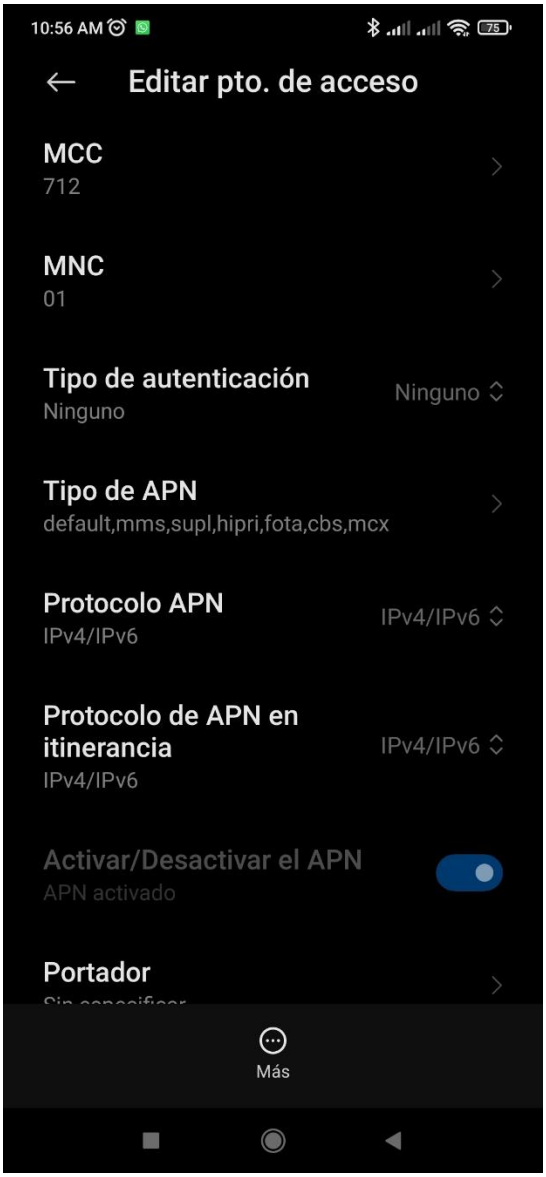


Figura 32: Configuración del APN en el dispositivo. IPv4/IPv6 Dual

Se procede a iniciar las Pruebas de navegación y usuario, con resultados satisfactorios para el 100% de los intentos y sitios que se probaron. A partir de los resultados obtenidos, se puede indicar que esta configuración es completamente functional y transparente para el cliente.

Al igual que para el escenario anterior, se verifica en aplicaciones, sitios Web internacionales y nacionales, aplicación PingTools y sitio Web http://ipv6-test.com de los cuales se muestran los resultados a continuación.

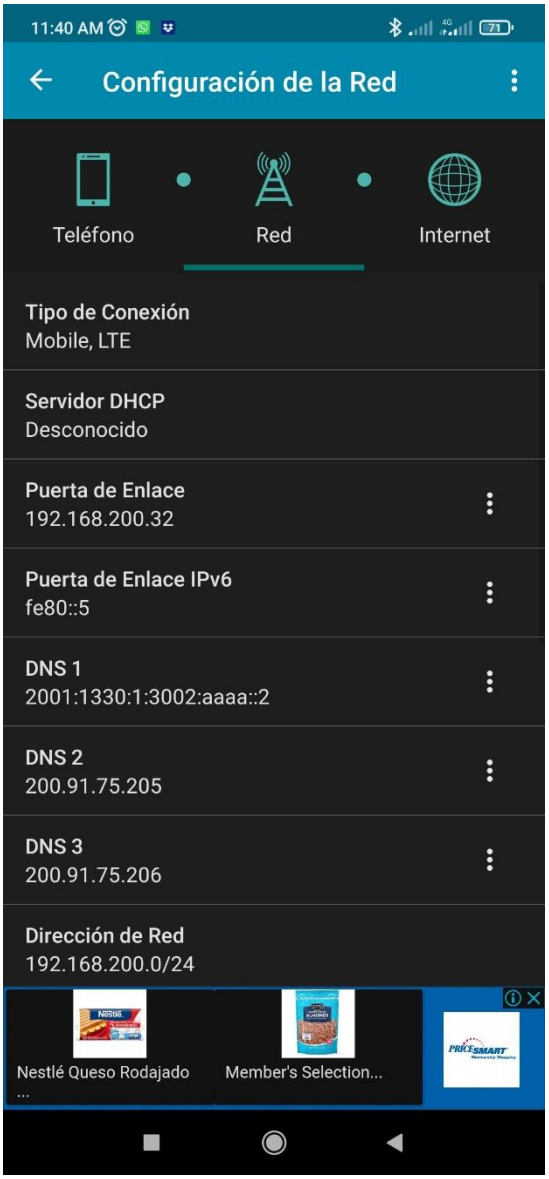


Figura 33: Estado conexión desde herramienta PingTools de Android. Caso IPv4 / IPv6 Dual.

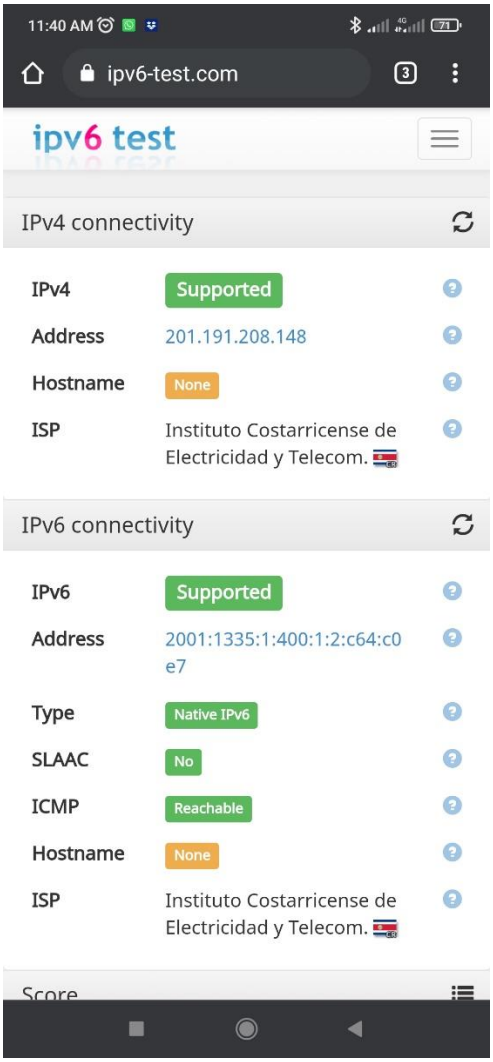


Figura 34: Estado conexión desde sitio Web ipv6-test.com. Caso IPv4 / IPv6 Dual.

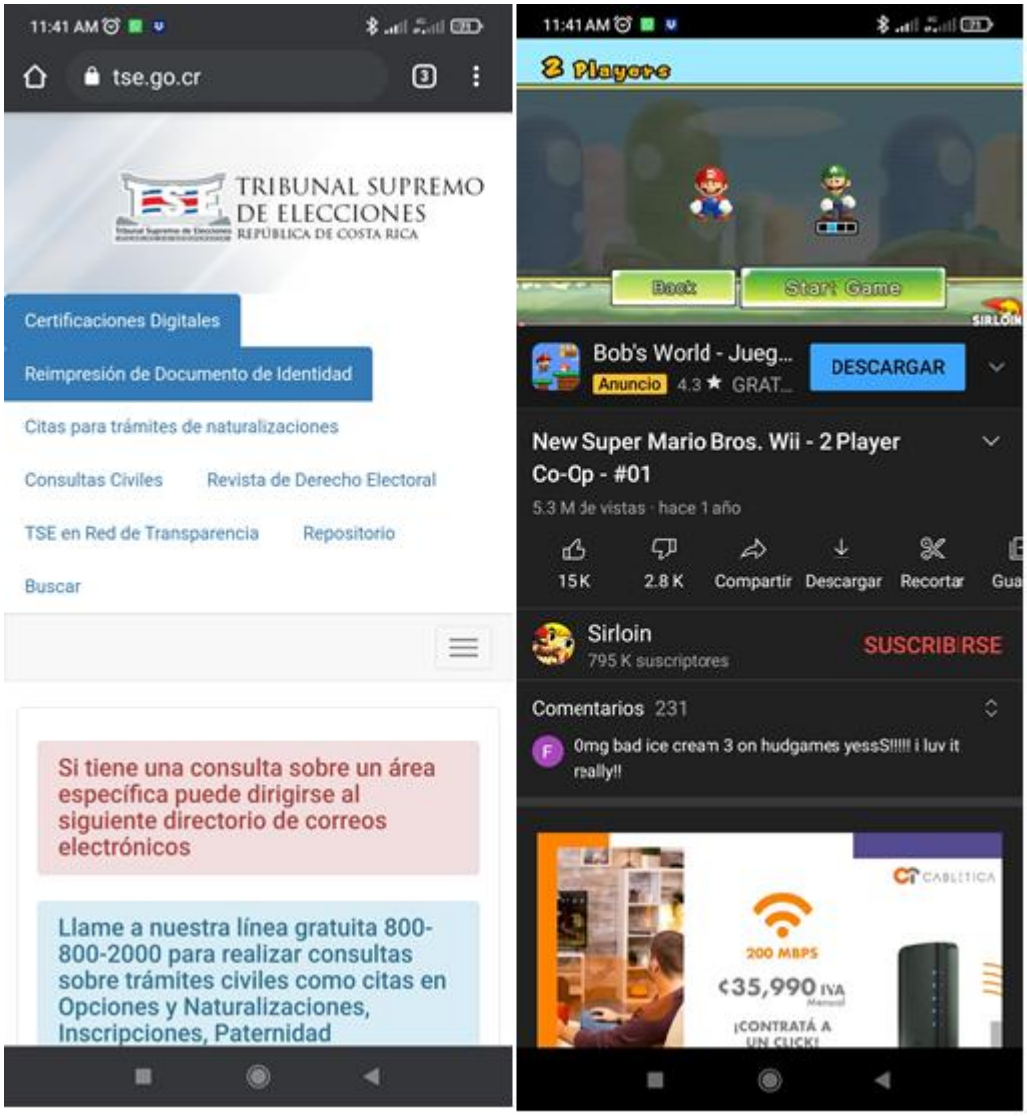


Figura 35: Pruebas de Navegación en Internet, usando configuración IPv4 / IPv6 Dual

Tal como se menciona arriba, se verifica que para el mismo PDP/Bearer se tienen dos direcciones IP: una de tipo IPv4 y otra de tipo IPv6, ambas para el mismo ID de contexto aprovisionado (el 20, que es el asignado al ID de la plantilla de APN asignada a nivel de HSS-SAE/HLR).

```
IPv4 address in use    IPv6 address in use            Link subscribed context ID

255.255.255.255        2001:1335:1:5:1:4:9195:5179    20
192.168.200.1          ::                             20
```

Figura 36: Consulta Sesión IP en SGSN/MME para una conexión Dual IPv4/IPv6

Posteriormente, se hacen las verificaciones del lado del CORE de datos móvil, en donde se verifica la sesión de datos IP desde el UGW (GGSN/PDNGW):

Tabla 7: Consulta en GGSN/PDNGW del PDP/Bearer utilizando configuración dual IPv4/IPv6

<GUAUGW01>display pdpcontext msisdn 50687000105
The PDP context on board 6

IMSI = 712012007529802
IMEI = 868909043593530
UGW Role = S+PGW
EPS Bearer ID = 5
Default Bearer = Yes
PDP type = IPv4v6
IPv4 Address type = UGW ALLOC IP ADDRESS
IPv6 Address type = UGW ALLOC IP ADDRESS
IPv4 PDP address = 192.168.200.32
IPv6 PDP address = 2001:1335:1:400:1:2:c64:c0e7
MSISDN = 50687000105
APN name = iceipv6
Requested Charging Characteristic = 0X0800
Negotiated Charging Characteristic = 0X0800
GTP Version = V2
Charging ID = 1384475671
Tunnel mode = direct tunnel mode
Left Local Teidc = 0X05f9c4b2
Left Local Teidu = 0X05f9c4b2
Left Peer Teidc = 0X197e0f04
Left Peer Teidu = 0Xcebc8c72
Left Local Signal Port = 2123
Left Peer Signal Port = 2123
Left Local Signal IP = 201.191.199.151
Left Peer Signal IP = 201.191.194.100
Left Local Data IP = 10.178.122.248
Left Peer Data IP = 10.204.18.42
Right Local Signal IP = NULL
Right Peer Signal IP = NULL
Right Local Data IP = NULL
Right Peer Data IP = NULL
APN AmbrUp = 4294967kbps
APN AmbrDown = 160000kbps
Requested QoS = 2d840800,00000000,00000000,00000000,00000000,00000000
Request Qos Class Identifier = 8
Request Allocation/Retention PRI = 11
Request Allocation/Retention PRI PCI = 0
Request Allocation/Retention PRI PVI = 1
Request Max Bit Rate for Uplink = NULL
Request Max Bit Rate for Downlink = NULL
Request Gua Bit Rate for Uplink = NULL
Request Gua Bit Rate for Downlink = NULL
Negotiated QoS = 2d840800,00000000,00000000,00000000,00000000,00000000
Qos Class Identifier = 8
Allocation/Retention PRI = 11
Allocation/Retention PRI PCI = 0
Allocation/Retention PRI PVI = 1
Max Bit Rate for Uplink = NULL
Max Bit Rate for Downlink = NULL
Gua Bit Rate for Uplink = NULL
Gua Bit Rate for Downlink = NULL
L2TP Flag = false
User Type = home
RAT Type = EUTRAN
PCC Type = true
Charge Rule Base Name = up_oracle

```
            Mse Profile Match List Name  =  NULL
                    Online Charging Flag  =  No
                   Offline Charging Flag  =  No
                SGW Offline Charging Flag  =  Yes
                   Content Charging Flag  =  Yes
                     Tight Interworking  =  No
                 Primary Charge Function  =  NULL
               Secondary Charge Function  =  NULL
                    URL Filtering Flag  =  false
                   Sponsor Data Flag  =  false
                              ADC Type  =  false
                              MSE Type  =  false
                            NAT Switch  =  DISABLE
                            PAP Switch  =  DISABLE
             IMS Signalling Context Flag  =  false
                              STE Flag  =  false
                    IPv4 VPN instance  =  IPV6
                    IPv6 VPN instance  =  IPV6
              Primary IPv4 DNS Server IP  =  200.91.75.205
            Secondary IPv4 DNS Server IP  =  200.91.75.206
              Primary IPv6 DNS Server IP  =  2001:1330:1:3002:aaaa:0:0:2
            Session Activation Timestamp  =  11:39:13 07/30/2021(MM/DD/YYYY)
                    Lifetime(seconds)  =  207
                No Service Time(seconds)  =  5
                                   DSCP  =  10
                         Uplink Packets  =  7861
                       Downlink Packets  =  10457
                          Uplink Bytes  =  3607880
                        Downlink Bytes  =  9827127
                      Tethering Switch  =  DISABLE
              User Location Information  =  Type:ECGI;MCC:712;MNC:01;ECI:296200
              User Location Information  =  Type:TAI;MCC:712;MNC:01;TAC:3105
                               BCM Flag  =  UE NW
                          Suspend Flag  =  false
                       Maintained Flag  =  false
                             Af Switch  =  DISABLE
                        PCC User Type  =  dynamic-pcc
              MME/S4SGSN Identifier IP  =  NULL
           DDN ACK Timeout Delay Delete  =  No
                    Anonymous Apn Type  =  false
                            Non-IP User  =  No
                               PRA FLAG  =  false
                  ToolBar Radius Status  =  disable
        Serving PLMN Uplink Rate Limit  =  0
      Serving PLMN Downlink Rate Limit  =  0
(Number of Results = 1)

------------------------
2021-07-30 11:42:42-06:00

<GUAUGW01>
```

Tal como se observa en la table anterior, los parámetros lucen consistentes con una sesión de datos adecuada para navegación y Buena percepción del cliente, sin impactos adicionales a nivel de equipos (licencias, alarmas u otros).

A partir de la evidencia recolectada durante el desarrollo de esta prueba, se valida que este escenario es 100% funcional para el Proveedor de Servicios de Internet así como para el cliente final.

3.2.4 Pruebas y Análisis Oferta Comercial con IPv6

Para el desarrollo de las Pruebas a nivel de oferta commercial, se validó a nivel de señalización, capturando y analizando trazas de usuario sobre las interfaces de red estándar Gx (DIAMETER, entre el GGSN y el PCRF para instalación de políticas), Gy (entre el GGSN y la OCS, para tasación en línea) así como Gz (para tasación fuera de línea, esto es CDRs). Esto por cuanto las Pruebas de navegación, usuario y parámetros del CORE ya han sido validados en los puntos anteriores.

Inicialmente, al abrir la sesión de datos, se observa cómo el flujo de señalización GTP y DIAMETER transcurre con normalidad. Esto es:

- Se hace la solicitud para la creación de la sesión de datos IP (GTP).
- Se hace la consulta (Request) hacia el PCRF sobre la interfaz Gx (DIAMETER).
- El PCRF contesta la consulta (Answer) sobre la interfaz Gx.
- Se hace la consulta (Request) hacia la OCS sobre la interfaz Gy (DIAMETER).
- La OCS contesta la consulta (Answer) sobre la interfaz Gy.
- Se responde la solicitud para la creación de la sesión de datos IP exitosamente (GTP).

El flujo completo se puede observar en la siguiente captura de pantalla:

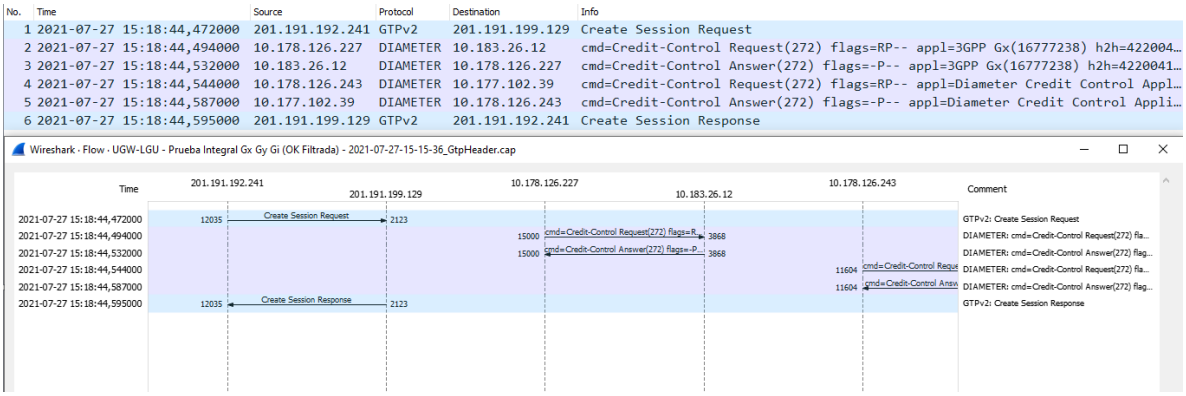


Figura 37: Flujo de señalización para el establecimiento de una sesión de datos con IPv6.

A continuación se verifican los mensajes individualmente con mayor detalle. Primero, se verifica la solicitud de apertura de sesión de datos IP, mensaje GTP “Create Session Request”, que contiene el APN en configuración dual:

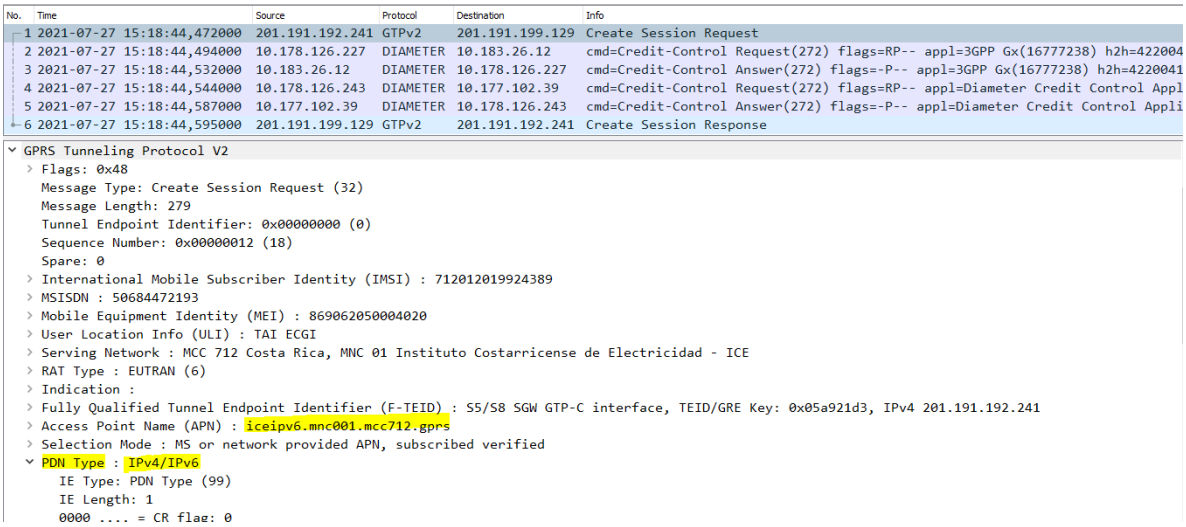


Figura 38: Consulta mensaje GTP Create Session Request, con configuración IPv4/IPv6 dual

La siguiente dupla de mensajes DIAMETER sobre la interfaz Gx, muestra que en efecto en la solicitud (Credit Control– Initial Request) se indica que el direccionamiento es de tipo IPv6. Por su parte, en la respuesta se observa correctamente la instalación de las reglas y el código de éxito 2001 “DIAMETER SUCCESS”:

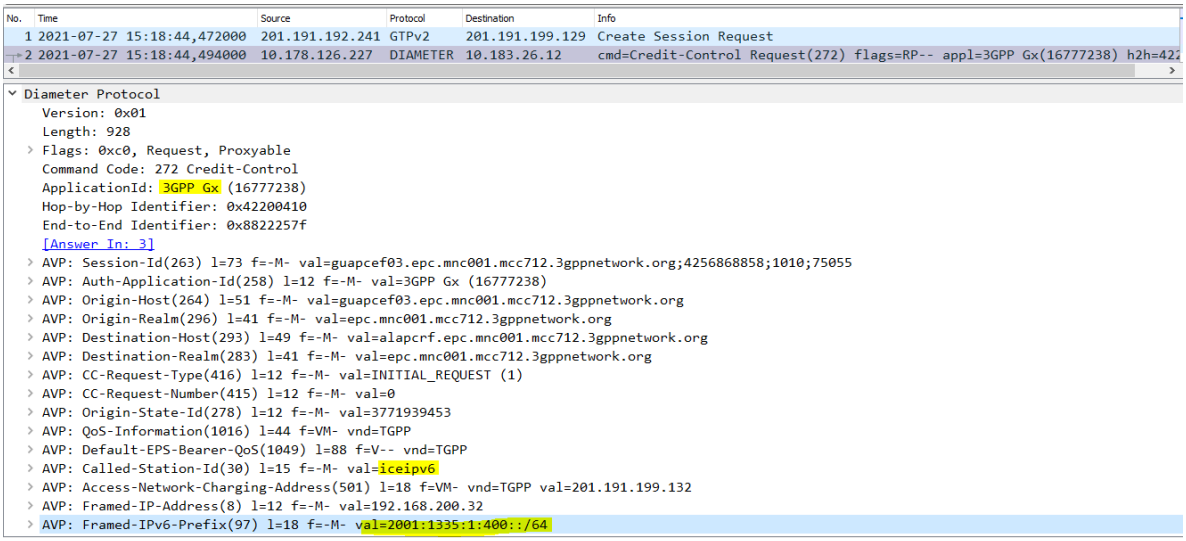


Figura 39: Mensaje DIAMETER Credit Control - Initial Request con IPv6

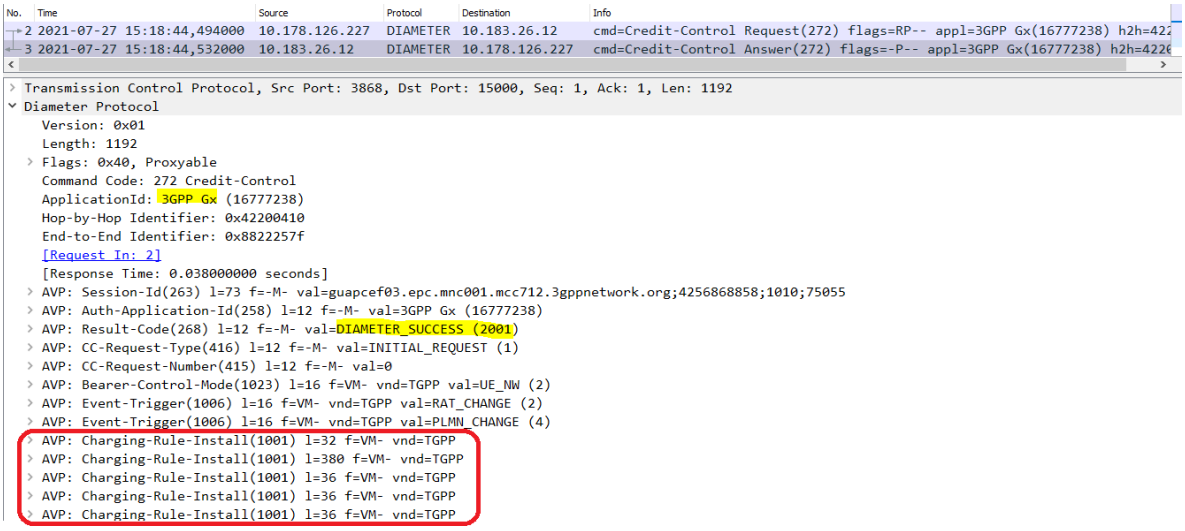


Figura 40: Mensaje DIAMETER Credit Control Answer – Initial con resultado exitoso

Se prosigue con los siguientes mensajes, que son la dupla de mensajes DIAMETER Credit Control hacia/desde la plataforma de cobro en línea OCS. Tal como se observa, se observan correctos la respuesta general del mensaje (bien construido) y también los parámetros de tasación (en este caso, para el Rating Group se obtiene un 2001 DIAMETER SUCCESS), los cuales no se han visto afectados por el tipo de direccionamiento utilizado en esta prueba:

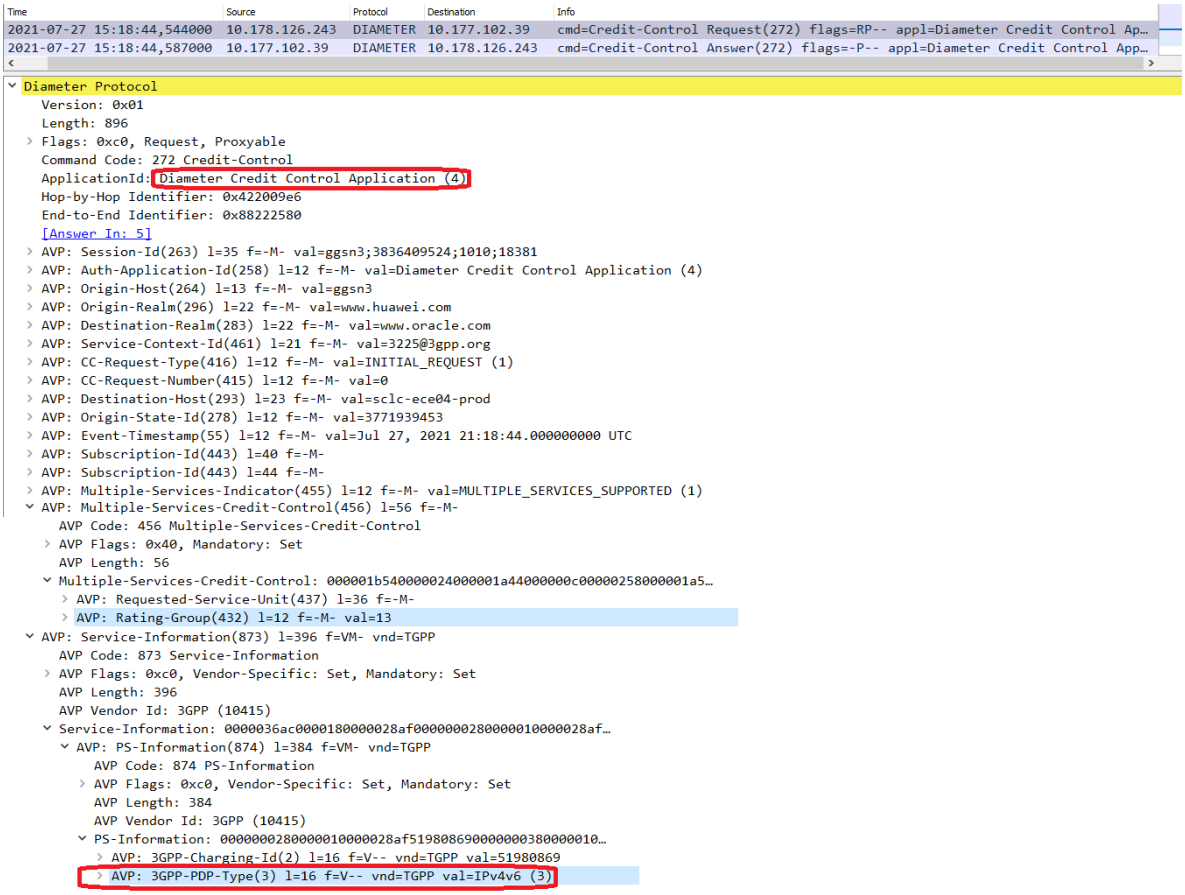


Figura 41: Mensaje DIAMETER Credit Control Request hacia OCS (Gy) con IPv4 / IPv6 Dual

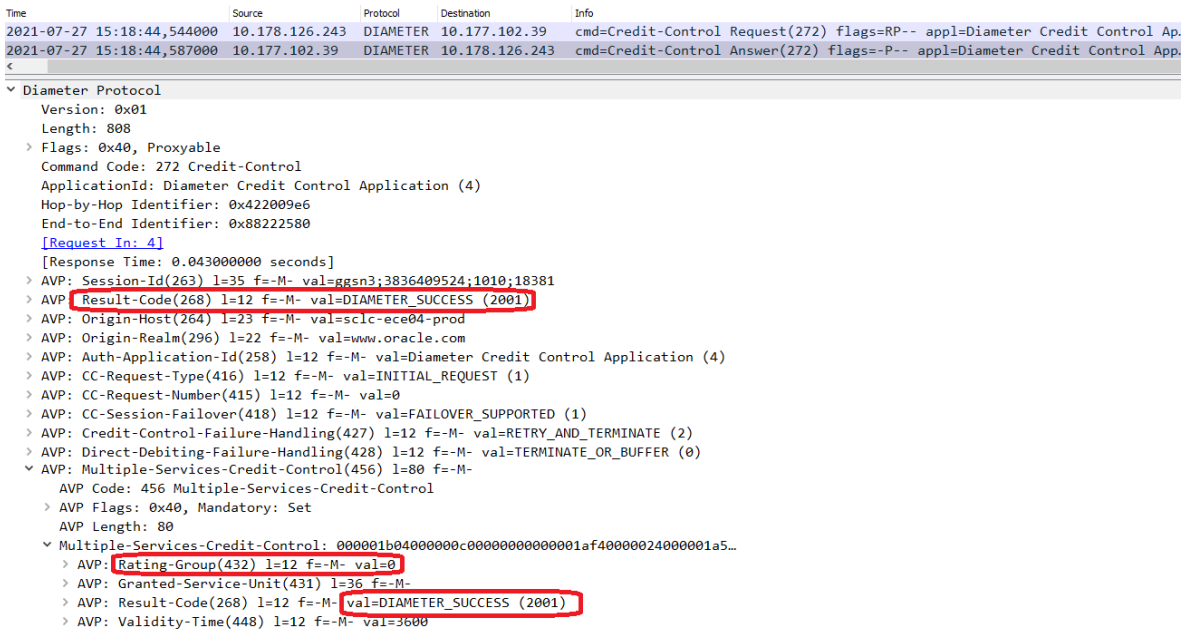


Figura 42: Mensaje DIAMETER Credit Control Answer desde OCS (Gy) con IPv4 / IPv6 Dual

Se consulta en el equipo UGW (GGSN/PDNGW) y se observa que en efecto se hizo la instalación de reglas (políticas) dinámicas y predefinidas según lo esperado:

```
<GUAUGW01>display pcc-session-info msisdn 50687000105
Pcc Session Information for MSISDN 50687000105 on board 6
------------------------------------------------------------

Rule information of bearer [NSAPI/EBI:5]
----------------------------------------
No    State     Priority    Type             Name                 CRBN
1     Active    0           Dynamic Rule     r-unlimited0cd645dc  NA
2     Active    65530       Predefined Rule  rule_any             NA


-------------------------
```

Figura 43: Consulta instalación reglas dinámicas y predefinidas en el UGW (GGSN/PDNGW)

Para confirmer que los reportes de uso también se hicieron correctamente, se verifica en el tasador antes y después de la navegación, desde donde se confirma que hubo una rebaja en el saldo del cliente (correcto) según lo esperado. Para este caso, el saldo antes de la navegación es de 3804.77816, y el saldo final (después de la navegación con IPv6 dual) era de 3654.48078.

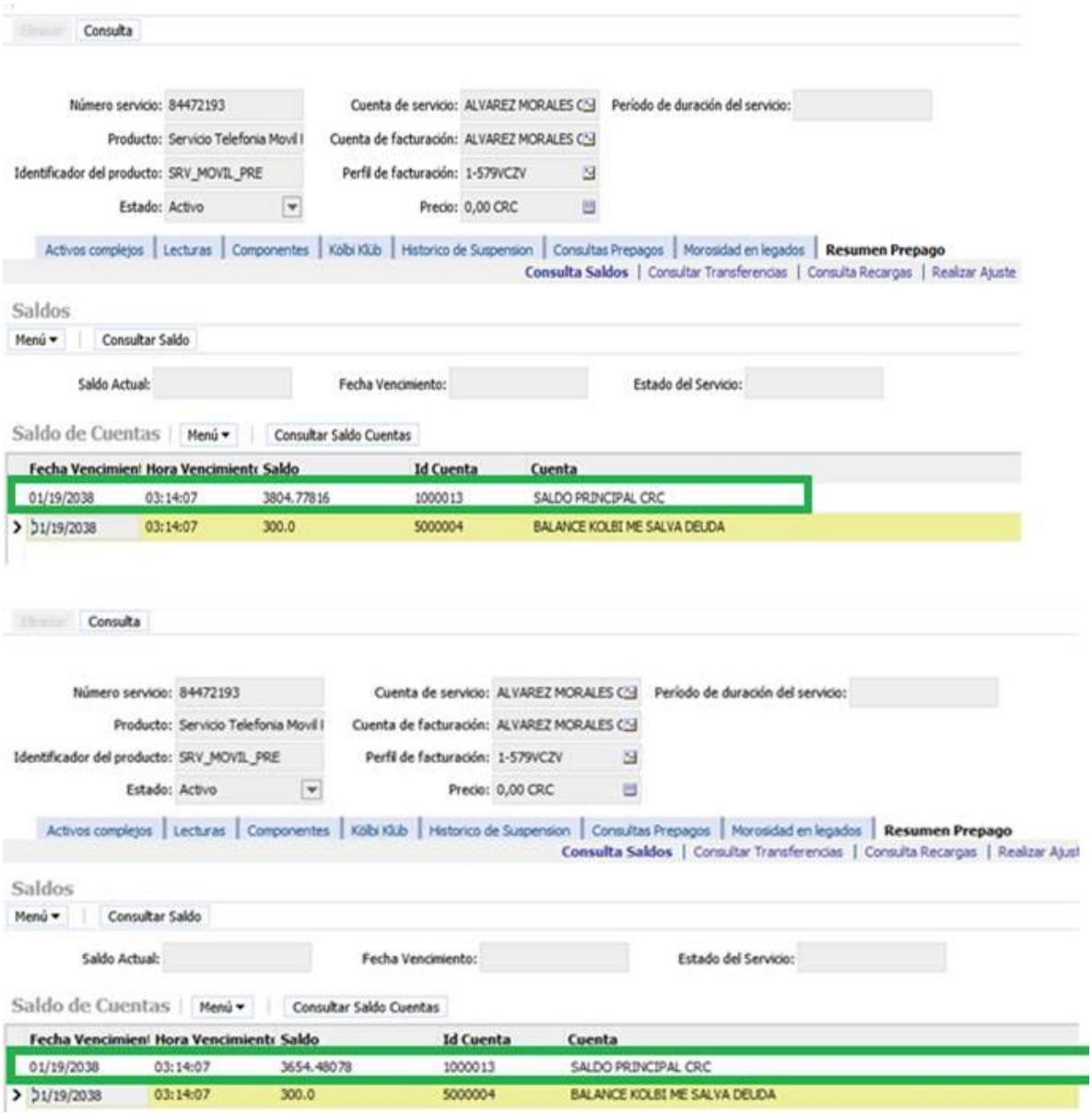


Figura 44: Resultados prueba de verificación de rebaja de saldo utilizando IPv4 / IPv6 dual

Finalmente, se verifica la construcción de los registros de cobro CDR (Interfaz Gx para tasación fuera de línea). Se procede a extraer los CDR de los equipos correspondientes (Charging Gateway), los cuales son verificados con los CDR extraidos en las plataformas de mediación, que pudieron ser correctamente interpretados.

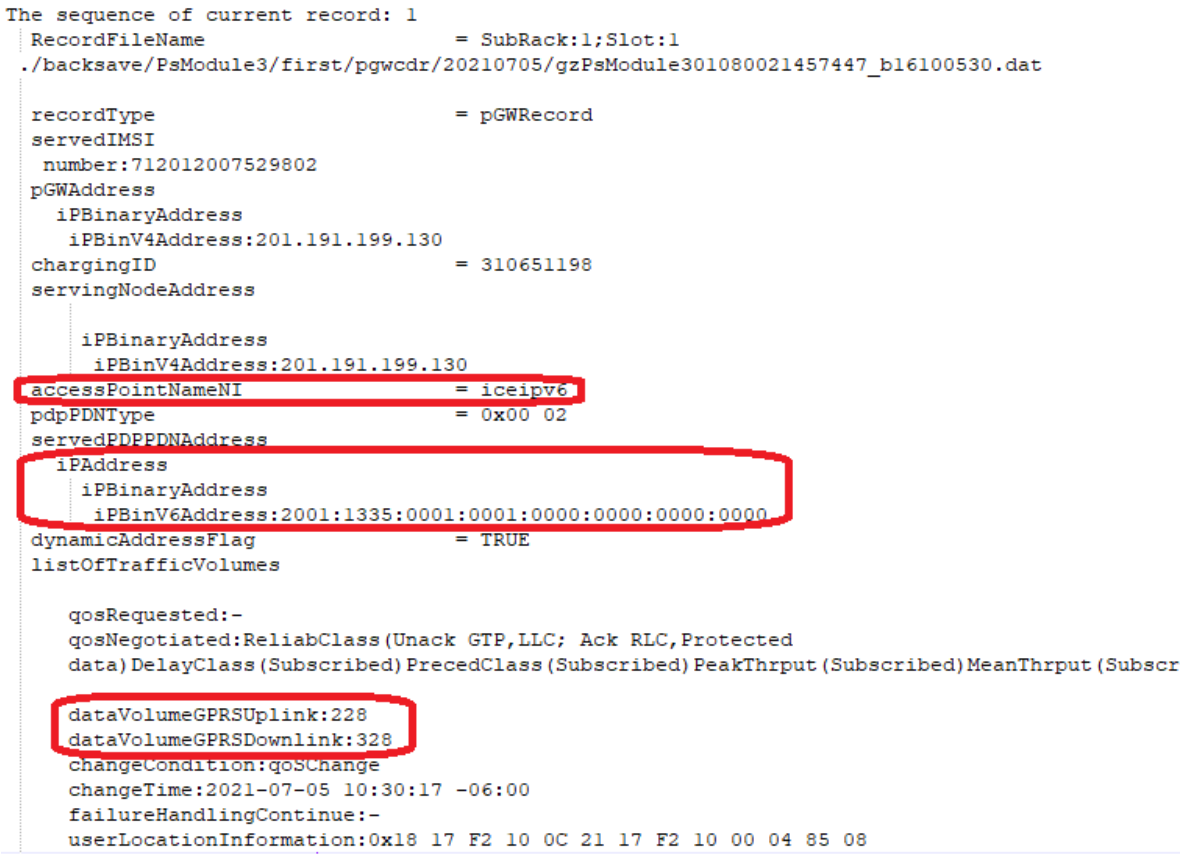


Figura 45: Registro de cobro (CDR) para navegación con IPv6

3.2.5 Impacto en la Red Móvil PS/EPC y Usuarios Finales

Finalmente, a partir de las pruebas, y considerando que se debe minimizar el impacto en los equipos del CORE PS/EPC y clientes finales, es posible determinar cuáles equipos, interfaces, configuraciones u otros, son indispensables y opcionales para una migración hacia IPv6. Los resultados se muestran en la siguiente tabla:

Tabla 8: Resumen de Impacto en Configuración en Equipos

Elemento	Nivel Impacto	Detalle
GGSN + SGW/PDNGW	Alto	APN, VPN, Pool IP
SGSN / MME	Bajo	DNS APN
HSS-SAE / HLR	Medio	APN, Aprovisionamiento
PCRF, OCS, OFCS	Ninguno	No impacta Oferta
Interfaces DIAMETER (Gx, Gx, S6a**)**	Ninguno	No impacta interfaces.
Interfaces GTP/SS7 (S5/S8, S11, S1-MME, S1-U, IuPS, Gn/Gp, Gr**)**	Ninguno	Se pueden reutilizar interfaces existentes.
Interfaces de salida a Internet en Red Móvil (Gi/SGi**)**	Alto	Creación Nueva Interfaz
Equipos de Transporte (Enrutadores, Firewall**)**	Alto	Listas Acceso, Interfaces
Equipos DNS y Salidas Internacionales	Medio	DNS64, Habilitación IPs
Equipo Terminal del cliente	Bajo	Configuración APN

3.3 Estrategia de Migración

Partiendo de la investigación realizada a nivel de documentación, así como de los resultados obtenidos durante el desarrollo de Pruebas, se determina que existen equipos e interfaces que no requieren ajustes o configuraciones, por lo cual, se recomienda aprovechar esta ventaja para optimizar tiempo, recurso humano y minimizar riesgos.

Con respecto a la migración de equipos y clientes a IPv6, se recomienda seguir la siguiente estrategia (dividida en 3 partes para mayor facilidad de comprensión):

3.3.1 Definiciones y Asignaciones

- Se deben definir segmentos de direcciones IP para las nuevas interfaces de salida a internet (esto es Gi y SGi). Para este caso, se deben asegurar direcciones para los equipos de CORE de red móvil (GGSN + PDNGW), así como para los enrutadores y Firewall de red. Esto es, al menos un segmento /64 para IPv6 por cada localidad.
- Para los clientes finales, se deben definir y asegurar tantas direcciones IP como usuarios se tengan en la red móvil al momento de realizar la migración. Al menos, 1 dirección IPv6 por cada usuario que el CORE de la red móvil esté en capacidad de gestionar.
- Se deben definir números de prueba para utilizar durante el desarrollo de Pruebas previas a la migración (con el fin de garantizar que los escenarios se encuentran 100% funcionales).
- Se deben definir las fechas en las que se ejecutarán las diferentes etapas de cada trabajo, con el fin de comunicarlos al regulador y a los clientes, para prevenir multas o penalizaciones en caso de que se presente algún tipo de afectación.

3.3.2 Equipos de transporte y enrutamiento.

- Se deben publicar en las salidas internacionales a Internet (enlaces internacionales), los segmentos de direcciones IPv6 definidos en el punto anterior “Definiciones y Asignaciones”.
- Se deben permitir alcanzar y resolver los DNS desde los segmentos de IP definidos para utilización de clientes (red IP del operador).
- Se deben realizar Pruebas de conectividad punto a punto, que permitan garantizar que el tráfico desde los GGSN / PDNGW tiene acceso a los DNS y salidas internacionales, además de garantizar que no existan bloqueos de Seguridad u otros que puedan interferir en la navegación del cliente.

3.3.3 Equipos del CORE de la red móvil

- Se debe habilitar los segmentos de direcciones IPv6 para usuario en los pooles de direcciones IP que actualmente está utilizando el APN comercial del ICE.
- Se recomienda validar los parámetros de activación de licencias y partes en los equipos de la red móvil, con el fin de garantizar que están correctamente habilitados y disponibles para ser utilizados (después de este Proyecto, se encuentran habilitados en los equipos actuales).
- Se recomienda utilizar un APN de Pruebas que replique la configuración comercial, tanto a nivel de parámetros como de enrutamiento. Al final de las Pruebas, se debe replica la configuración del APN de Pruebas en el APN comercial.
- Se debe proceder a aprovisionar a los suscriptores candidatos a migrar a IPv6 (dual) en las partes para 3G y LTE. Se recomienda hacerlo bajo la modalidad dual.
- Al momento de la migración, se debe modificar la configuración del APN en los GGSN/PDNGW para que permitan la asignación de direcciones de tipo IPv6, actualmente definidos como IPv4 solamente. Se recomienda migrar las localidades una por una diferentes días, con el fin de medir el impacto poco a poco, por si surgeran inconvenientes y hubiese que revertir configuraciones, minimizer el impacto.
- Se recomienda realizar una comunicación masiva a los clientes indicando que está disponible el direccionamiento IPv6, con el fin de que quienes lo deseen, puedan hacer la migración voluntaria a IPv6 dual. De esta manera, la migración a IPv6 se dará naturalmente de manera gradual (poco a poco).
- Se pueden gestionar campañas de modificación de perfiles de configuración de dispositivos (plataforma OTA o Device Manager) para automatizar la configuración en los dispositivos que aún no hayan sido configurados con el APN en modo dual.
- Para clientes que requieran servicios con IPv6 (por ejemplo, IoT), se puede configurar plantillas o perfiles de usuarios que ya tengan la configuración de IPv6 de manera preestablecida y probada.

Capítulo 4. Conclusiones y Recomendaciones

4.1 Conclusiones

- Se determina que existe una estrategia óptima de migración de clientes finales a IPv6 dual, que debe realizarse con etapas previamente validadas a nivel de red de transporte, red CORE y usuario.
- Se encuentra que para los equipos y versiones actuales, no es técnicamente factible migrar las integracions de equipos y plataformas de la red móvil a IPv6, debido a las limitaciones en las capacidades de los equipos que indica el fabricante.
- Se determina que el cliente final debe poseer un teléfono con capacidad de configuración en la modalidad IPv4 / IPv6 Dual. Adicionalmente, se determina que se debe modificar en HSS-SAE/HLR el aprovisionamiento del APN de navegación a internet con los parámetros de IPv4/IPv6 Dual a nivel de 3G y LTE.
- Se realizaron mediciones que permitieron evaluar el impacto en los equipos y clientes finales, de donde se concluye que en caso de ejecutar la migración, es recomendable hacerlo para la modalidad dual IPv4 / Ipv6. Se determina que no existe un impacto a nivel de oferta commercial para esta modaidad.
- Para migrar a un escenario IPv6 puro, es indispensable disponer de un equipo DNS64 propio del Operador.

4.2 Recomendaciones

- Se recomienda utilizar la modalidad IPv4 / IPv6 dual, que es la que presenta una compatibilidad del 100% en los equipos de red y es transparente para el usuario final. La modalidad de IPv6 puro está condicionada a la disponibilidad de un equipo NAT64 propio.
- Se recomienda realizar una migración paulatina de direccionamiento IPv6 (dual) por cada localidad (una a la vez), que permita medir el impacto de cada migración sin comprometer el 100% de los usuarios (en caso de que se presenten eventualidades).
- Se deben asegurar los licenciamientos en el HLR + HSS-SAE que permitan aprovisionar a cada usuario con capacidad de soportar IPv6.
- Se deben asegurar los licenciamientos en el GGSN/PDNGW (UGW) que permitan la asignación dinámica de direcciones IPv6 desde el UGW (Hacer DHCP desde el UGW sin otro equipo externo).

ANEXOS

Anexo 1: Resultados Pruebas Ping (DNS64 Google Primario)

```
<GUAUGW01>ping ipv6 vpn-instance IPV6 -a 2001:1334:1:FFFF::1 2001:4860:4860:0:0:0:0:6464
  PING 2001:4860:4860:0:0:0:0:6464 : 56  data bytes, press CTRL_C to break
    Reply from 2001:4860:4860::6464
    bytes=56 Sequence=1 hop limit=119  time = 44 ms
    Reply from 2001:4860:4860::6464
    bytes=56 Sequence=2 hop limit=119  time = 43 ms
    Reply from 2001:4860:4860::6464
    bytes=56 Sequence=3 hop limit=119  time = 46 ms
    Reply from 2001:4860:4860::6464
    bytes=56 Sequence=4 hop limit=119  time = 43 ms
    Reply from 2001:4860:4860::6464
    bytes=56 Sequence=5 hop limit=119  time = 43 ms

  --- 2001:4860:4860:0:0:0:0:6464 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 43/43/46 ms
```

Figura 46: Pruebas de ping hacia DNS64 Primario de Google

Anexo 2: Resultados Pruebas Ping (DNS64 Google Secundario)

```
<GUAUGW01>ping ipv6 vpn-instance IPV6 -a 2001:1334:1:FFFF::1 2001:4860:4860:0:0:0:0:64
  PING 2001:4860:4860:0:0:0:0:64 : 56  data bytes, press CTRL_C to break
    Reply from 2001:4860:4860::64
    bytes=56 Sequence=1 hop limit=119  time = 51 ms
    Reply from 2001:4860:4860::64
    bytes=56 Sequence=2 hop limit=119  time = 51 ms
    Reply from 2001:4860:4860::64
    bytes=56 Sequence=3 hop limit=119  time = 51 ms
    Reply from 2001:4860:4860::64
    bytes=56 Sequence=4 hop limit=119  time = 51 ms
    Reply from 2001:4860:4860::64
    bytes=56 Sequence=5 hop limit=119  time = 51 ms

  --- 2001:4860:4860:0:0:0:0:64 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 51/51/51 ms
```

Figura 47: Pruebas de Ping hacia DNS64 Secundario de Google

APÉNDICE

Artículo Universidad de Costa Rica: "IPv6: más direcciones en la UCR para conectarnos con el mundo"[23].

IPV6: MÁS DIRECCIONES EN LA UCR PARA CONECTARNOS CON EL MUNDO

Tecnología permite mejorar y ampliar la transmisión de datos

14 MAY 2019 Ciencia y Tecnología

La UCR actualiza las conexiones a Internet con el fin de brindar las condiciones idóneas para el desarrollo de la investigación y la docencia. Foto: Archivo ODI.

Con el fin de mantenerse a la vanguardia tecnológica, a inicios del 2018 la Universidad de Costa Rica (UCR), a través del Centro de Informática (CI), inició un **plan piloto para la implementación del Internet Protocol version 6 (IPv6).**

Para adentrarse en el mundo del IPv6, la Institución requirió de una inversión, tanto económica como de tiempo y recurso humano, para la renovación y configuración de la plataforma tecnológica requerida para trasegar a dicho protocolo.

De la mano de **Lacnic** (Latin America & Caribbean Network Information Center), ente encargado del registro regional de Internet para América Latina y el Caribe, se **realizó una revisión del inventario tecnológico, con el fin de identificar los equipos obsoletos o incompatibles con IPv6 en todas las sedes de la Universidad.**

Rebeca Esquivel Flores, coordinadora del Área de Gestión de Comunicaciones (AGC) del CI, comenta que **durante los últimos años se ha realizado el reemplazo de los equipos de comunicaciones que no soportan IPV6, con el objetivo de que toda la plataforma sea compatible.**

"Tras la renovación de infraestructura vino la parte lógica o de configuración en la inclusión del protocolo IPv6, reemplazando el prefijo /48 con el que contaba la UCR por un prefijo /44; esto significa que cuanto menor sea el tamaño de prefijo de red, mayor es el grupo de direcciones IP que tendremos disponibles", añadió Esquivel.

¿Qué es una IPv6?

Con la finalidad de entender lo trascendental que significa para Costa Rica que la UCR tome la iniciativa de formar parte de esta transición tecnológica, se puede explicar lo que es el IPv6 mediante la siguiente analogía: una **dirección IP (Internet Protocol) es una serie de números que identifica a cada dispositivo que se conecta a Internet**, o sea, podría decirse que es como el número de teléfono de cada aparato.

Siguiendo con la analogía, las direcciones IPv4 serían similares a los números de teléfonos de seis dígitos, que permiten hacer conexiones a una población de cinco millones de personas sin problemas, o sea, en tiempos en los que se esperaba que cada persona tuviera una computadora para su uso personal. Pero en nuestros días, **con las interconexiones por medio del Internet de las Cosas (IoT), existen computadoras, celulares, teléfonos, automóviles y hasta electrodomésticos con**

la capacidad de conectarse a la red, por lo que el alcance de IPv4 llegó a su límite.

IPv6 permitirá el desarrollo de IoT de forma exitosa a través de más accesos y conexiones, ya que pasa de 4 300 millones de direcciones IP únicas en IPv4 a y 340 sextillones de direcciones.

UCR a la vanguardia tecnológica

Gracias a este trabajo y a la implementación del plan piloto, se identificó una mejora en el acceso a través de la RedUCR a diferentes servicios de Internet a nivel mundial que ya se encuentran trasegando en IPv6.

Tras el agotamiento de direcciones IPv4 a finales de los años 90, nace IPv6 con direcciones de 128 bits que permiten generar más de 300 sextillones de direcciones únicas. Imagen: CI-UCR.

"Ahora los **investigadores cuentan con mejor comunicación hacia contenidos académicos de servicios como Google y Akamai, ya que el trasiego en IPv6 sumado al enlace para investigación con RedCLARA, permiten un acceso más rápido y directo a la información**", indica Esquivel.

Por ejemplo, la experta explica que **si efectuamos una consulta a Google desde nuestra computadora usando IPv4, dicha consulta podría requerir de hasta 23 saltos para llegar a su destino**, empezando desde nuestro dispositivo hasta llegar a la información que queremos consultar; mientras que **con IPv6, la misma consulta se completa en nueve saltos, lo que ayuda a disminuir los tiempos de respuesta en el acceso a la información**.

Por otro lado, el plan piloto permitió corroborar el método idóneo de transición hacia el nuevo protocolo, utilizando "Doble Pila o Dual Stack"; es decir, utilizando ambos protocolos (IPV4 e IPV6) de forma simultánea. Esta transición es la más recomendada ya que en el país el proceso de migración se encuentra en una etapa incipiente y son pocas las instituciones que usan IPV6 para el envío y recepción de información.

A lo largo del **2019 se continuará con el proceso de implementación de IPv6, para que todas las sedes y recintos puedan trasegar datos a través de dicho protocolo y mejorar su acceso a la consulta de información académica**. "Próximamente se comenzará la implementación en la Sede de Occidente, Sede del Atlántico y Sede de Guanacaste, y en los recintos de Tacares, Santa Cruz, Guápiles y Siquirres", indica Esquivel.

Finalmente, en conjunto con los usuarios administradores de las diferentes plataformas web de la Universidad, **se iniciará el proceso de migración de los diversos servicios institucionales a IPv6**.

Un impulso para la conectividad de América Latina

Alejandro Acosta, presidente de LAC-TF (IPv6 Task Force) e ingeniero de Innovación y Desarrollo en Lacnic, comenta que la incursión de la UCR en el IPv6 es de suma relevancia, no solo para el avance del país, sino de la región.

"Creo que es sumamente importante el hecho de que la **implementación del IPv6 comience por una universidad, podría ser un factor multiplicador porque los estudiantes van a poder utilizar IPv6 dentro de sus redes universitarias y posteriormente va a ser usadas en casas, oficinas, empresas y otros servicios**. Además, puede fomentar a otras universidades a realizar el cambio", indica Acosta.

Acosta destaca que esta iniciativa permitiría generar información de consulta que puede ser distribuida a través de medios de comunicación, de manera que más instituciones a nivel nacional e internacional conozcan y se interesen en la implementación del IPv6.

“En Latinoamérica existe aproximadamente un 45 % de personas que no están conectadas a Internet. Conectarlos con IPv4 significaría reutilizar en exceso las direcciones IP disponibles, lo que significa mayor NAT (Network Address Translation) y por ende, mayor número de fallas; no traería el Internet que queremos. Por esto, creemos importante que la iniciativa de IPv6 surja en todos los países de la región”, finaliza Acosta.

Bibliografía

[1] Ibíd.
[2] Sitio Web https://supportforums.cisco.com/thread/2119051, al 11 de octubre del 2012
[3] 3GPP, TS 23.002, v5.0.1, Network Architecture, Junio 2007.
[4] Sitio Web http://www.eveliux.com/mx/red-de-transporte.php, al 6 de noviembre del 2012
[5] 3GPP, TS 25.301, v7.3.0, Radio Interfaz Protocol Architecture, Octubre 2007.
[6] Wandel & Goltermann, "GSM Pocket Guide" Volumen 2, Página 11. Communications Test Solutions
[7] 3GPP, TS 23.107, v7.0.0, QoS Concept and Architecture, Junio 2007.
[8] Ibíd.
[9] Sitio Web https://softwarelab.org/es/lte-4g/#:~:text=LTE%20responde%20a%20las%20siglas,Internet%20a%20los%20dispositivos%20m%C3%B3viles. 15 de enero del 2021.
[10] Sitio Web https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic 09 de abril 2021.
[11] MICITT, Informe "ii_informe_de_evaluacion_bienal_del_pndt_2015-2021_final_web_1". Página 96. Junio 2020.
[12] SUTEL, Resolución RCS-019-2018 "RESOLUCIÓN SOBRE METODOLOGÍAS DE MEDICIÓN APLICABLES AL REGLAMENTO DE PRESTACIÓN Y CALIDAD DE LOS SERVICIOS". EXPEDIENTE GCO-NRE-REG-01209-2016. Enero del 2018.
[13] Sitio Web http://slides.lacnic.net/wp-content/themes/slides/docs/lacnic26/lunes/despliegue-IPv6-redesmoviles-lacnog16.pdf 23 de abril 2021.
[14] Sitio Web https://docs.microsoft.com/en-us/previous-versions/aa925828(v=msdn.10)?redirectedfrom=MSDN, 23 de abril 2021.
[15] Sitio Web https://web.archive.org/web/20120626142436/http://www.theipv6experts.net/2011/iphone-ipv6-debugging-simplified-ip6config/ , 23 de abril 2021.
[16] Sitio Web https://issuetracker.google.com/issues/36949094 , 23 de abril 2021.
[17] Sitio Web https://www.xatakandroid.com/sistema-operativo/android-10-esta-1-cada-10-dispositivos-ultimos-datos-distribucion-versiones , 23 de abril 2021
[18] Sitio Web https://www.applesfera.com/ios/adopcion-ios-14-sube-al-81-todos-iphone-presentados-2016 23 de abril 2021
[19] Sitio Web https://developers.google.com/speed/public-dns/docs/dns64 23 de abril 2021
[20] Sitio Web https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption 12 de Agosto 2021
[21] Banco de Desarrollo de América Latina, Libro "Despliegue de IPv6", página 49, 2017.
[22] Ibíd.
[23] Sitio Web https://www.ucr.ac.cr/noticias/2019/05/14/ipv6-mas-direcciones-en-la-ucr-para-conectarnos-con-el-mundo.html 12 Agosto 2021