

LAS NGN Y SU EVOLUCION A IMS

Por: MSc. Deborah Reyes Roig, Especialista B en Telemática y MSc. Alberto Javier García García, Especialista Principal, Departamento de Investigación y Desarrollo, Dirección Central de Desarrollo y Tecnología (DCDT), ETECSA.
deborah.reyes@etecsa.cu; alberto.garcia@etecsa.cu

Resumen

El presente trabajo ofrece una síntesis evolutiva desde las redes de conmutación de circuitos hasta las Redes de Próxima Generación (NGN). Se describen las capas, estructura y funcionamiento de las mismas con énfasis en el Subsistema Multimedia basado en IP (IMS), como eslabón fundamental para la unificación del control de las redes fijas y móviles. Se explican las ideas básicas y el orden en que debe realizarse una prueba de campo de la tecnología IMS para evaluar la factibilidad de la incorporación del sistema a la red de telecomunicaciones. De esta manera, se podrían simplificar los procedimientos de operación y mantenimiento, minimizar los costos, facilitar la puesta en marcha de servicios de valor agregado y dar un paso más a favor de la integración de las redes y los servicios.

Palabras clave: 3GPP, IMS, NGN, PSTN, Prueba de campo, Procedimientos.

Abstract

This work offers an evolutionary synthesis from Circuit Switching Networks to Next Generation Networks (NGN) describing layers, structures and functioning; emphasizing in the IP based Multimedia Subsystem (IMS), as main link for the unification of the control regarding fixed and mobile networks. The main ideas and the order for conducting a field test regarding IMS technology for evaluating the viability of incorporating the system to telecom networks are explained. In this way, the operation and maintenance procedures could be simplified, the expenses minimized, the value-added services could be more easily up and running and everything would be another step toward the integration of networks and services.

Keywords: 3GPP, IMS, NGN, PSTN, Field Test, Procedures.

Introducción

La industria de las telecomunicaciones está evolucionando hacia la unificación de las redes y los servicios. Son múltiples las tecnologías alámbricas e inalámbricas disponibles para garantizar el acceso de los usuarios a los servicios. A nivel mundial existe una fuerte tendencia al desarrollo de la banda ancha inalámbrica [1] mediante el empleo de tecnologías de tercera generación 3G / 3,5G como HSPA —*High Speed Packet Access*— y tecnologías como Wimax —*Worldwide Interoperability for Microwave Access*— y LTE —*Long Term Evolution*— debido a que ofrecen facilidades de despliegue rápido y capacidades de transmisión, unido a las ventajas que proporciona la movilidad.

Por su parte, el acceso por fibra óptica en el mundo llega en un alto por ciento hasta las instalaciones de los usuarios o muy cerca de ellas. Las tecnologías de fibra se combinan con xDSL —*Digital Subscriber Line*— que emplea el cobre para proporcionar servicios de banda ancha, reutilizando así la infraestructura existente de los operadores tradicionales de redes de telecomunicaciones y de las empresas de distribución de televisión por cable [2].

Entorno nacional

La Empresa de Telecomunicaciones de Cuba, S.A. (ETECSA) inició un cambio progresivo en todas las capas de la red de telecomunicaciones. La red GSM —*Global System for Mobile Communications*— está diseñada en su mayoría para voz y dispone de pequeñas capacidades para servicios GPRS —*General Packet Radio Service*— y EDGE —*Enhanced Data rates for GSM Evolution*—. Se comenzó a introducir la tecnología 3G en el país y se ha planificado iniciar su despliegue en zonas de interés turístico para garantizar la recuperación de estas inversiones. Por otra

parte, el desarrollo de la fibra ha estado dirigido a la construcción de la red de transporte nacional y las redes provinciales con anillos a fin de garantizar su seguridad; sin embargo, su capilaridad no llega, en la mayoría de los casos, a las cercanías de las instalaciones de los usuarios.

La red fija ha sufrido una migración paulatina, de centrales analógicas a digitales y, de ahí, a nodos de acceso multiservicio MSAN —*Multiservice Access Node*— con tecnología NGN —*Next Generation Network*—, de modo que coexisten la conmutación de circuitos con la de paquetes.

Se trabaja en la expansión de los servicios de correo electrónico, navegación nacional e internacional para el sector residencial y la población en general. Estos servicios se brindaban anteriormente al sector institucional, gubernamental y empresarial. Se utiliza para este propósito la red GPRS del servicio celular, los puntos de acceso a la red Wi-Fi y los enlaces DSL existentes. El desarrollo de las nuevas tecnologías y los servicios forma parte de los programas de informatización de la sociedad cubana para elevar los índices de penetración de voz y datos, que actualmente son bajos.

De redes PSTN a NGN

Las redes de telecomunicaciones hasta hace muy pocos años han sido redes independientes de voz y de datos. Inicialmente surgió la red telefónica pública conmutada —*Public Switched Telephone Network (PSTN)*— para los servicios de voz local y de larga distancia. Las centrales analógicas se sustituyeron por digitales y, utilizando la misma infraestructura, la red digital de servicios integrados permitió extender nuevos servicios al cliente (despertador automático, llamada en espera, conferencia tripartita, entre otros), en sus modalidades de accesos básico a 128 kbps y primario a 2,048 Mbps.

Las redes fijas de banda ancha se desplegaron exitosamente mediante las tecnologías xDSL y las redes ópticas pasivas —*Passive Optical Network (PON)*— con sus variantes: ePON (1 Gbps) y GPON (10 Gbps). Por otro lado, las redes celulares o PLMN —*Public Land Mobile Network*— se extendieron en todo el mundo a partir de la década de 1990 del siglo xx con la 1ra generación de celulares hasta lo que se conoce hoy como evolución a largo plazo o LTE, antesala de la 4ta generación.

El mantenimiento de estas redes fijas y móviles, diferentes en naturaleza, es elevado porque requiere gastos en la capacitación del personal especializado, en el mantenimiento de la propia infraestructura de la red y en las inversiones por obsolescencia tecnológica, multiplicadas por la cantidad de redes diversas para el mismo fin: el transporte y las señales de voz, los datos y el video.

Unificar las redes existentes a través de una infraestructura común de control y servicios basada en la conmutación de paquetes es la meta a alcanzar por las Redes de Próxima Generación (NGN).

Estructura de las redes NGN

Las NGN tienen una estructura formada por capas (Figura 1) y está integrada por los siguientes elementos:

- ♦ **Equipos terminales:** Pueden ser fijos o móviles, PC con *softphone*, *tablets*, celulares o teléfonos IP, capaces de conectarse de forma alámbrica o inalámbrica a los dispositivos de acceso.
- ♦ **Acceso:** Capa formada por *gateways (GW)*, que son traductores de circuitos a paquetes y viceversa, de diferentes capacidades. Existen dispositivos integrados de acceso —*Integrated Access Device (IAD)*— de

pequeña capacidad, entre 2 y 32 abonados, y de gran capacidad que pueden ser de acceso o troncales. Los GW de acceso permiten hasta 1900 abonados por bastidor y los troncales traducen flujos o troncos a paquetes y tienen una capacidad que varía desde un E1 (equivalente a 32 abonados) hasta 192 E1. Esta capa simula las tradicionales tarjetas de línea y de tronco de las centrales telefónicas tradicionales. En el caso de la telefonía móvil, la cadena de acceso es: terminal móvil, radiobase, controlador de radiobase y *gateway*.

♦**Comutación de paquetes:** Es la capa que proporciona conectividad a toda la red. Está constituida por una red de enrutadores basados en el protocolo IP con comutación de etiquetas MPLS —*Multiprotocol Label Switching*— que están dispersos en toda la geografía del país, formando el *backbone* IP/MPLS. Están soportados sobre una red de transmisión y como medio físico utilizan la fibra óptica.

♦**Control:** Está constituido por los llamados *softswitch*. Este órgano de control centralizado para toda la red permite gobernar hasta 2 millones de líneas en un espacio muy reducido, con el consiguiente ahorro de energía en comparación con las centrales tradicionales. Emplea protocolos de señalización H248 para llamadas no multimedia y protocolo de iniciación de sesión SIP —*Session Initiation Protocol*— para llamadas multimedia. El *softswitch* simula el software de control de una central digital de forma centralizada.

♦**Gestión y Servicios:** Contiene un conjunto de servidores para operación, mantenimiento, configuración y provisión de servicios. El objetivo es permitir el monitoreo y la gestión tanto de la red como del servicio para lograr un despliegue ágil de forma homogénea.

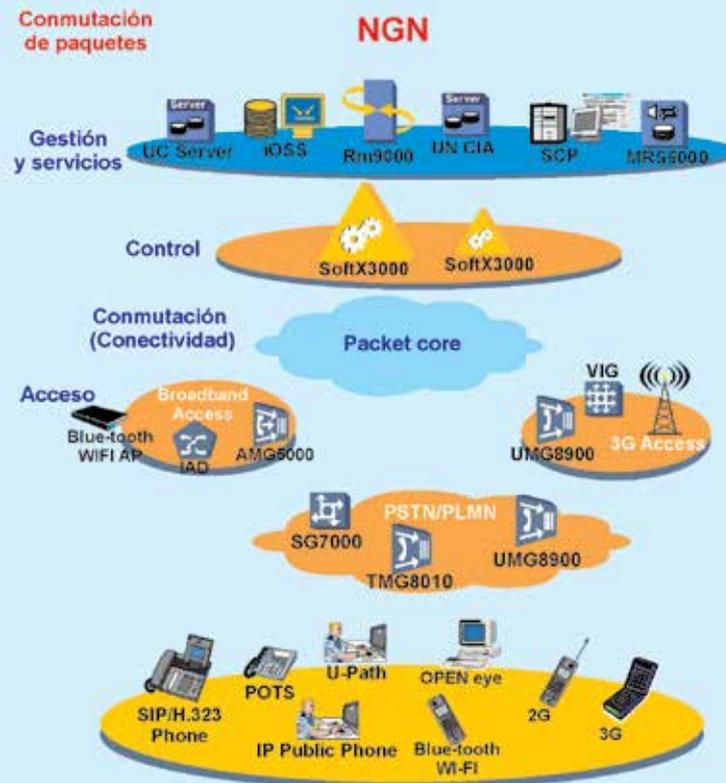


Figura 1. Capas de las NGN. (Fuente: [1]).

Esta es la estructura ideal que se quiere alcanzar con el desarrollo de las NGN a nivel internacional, pero esta etapa evolutiva es muy compleja y la situación real es que existen *softswitch* para la red fija y para la red móvil. Esto se debe a que las interfaces y codificaciones de línea se diferencian en los procedimientos de facturación y lógica del establecimiento de las llamadas. Además, los *softswitch* deben ser redundantes por motivos de seguridad. Aunque las redes fijas y móviles ya tienen puntos de coincidencia, todavía no se alcanza la convergencia total.

El próximo paso dentro del camino evolutivo a las NGN es la unificación del control a través de la filosofía IMS, la cual se describe a continuación.

IP Multimedia Subsystem (IMS)

IMS fue concebido originalmente por el foro 3G.IP, el cual desarrolló su arquitectura que fue llevada al Proyecto 3GPP —*3rd Generation Partnership Project*— como parte de su trabajo de estandarización de sistemas 3G para celulares en el Sistema Universal de Telecomunicaciones Móviles o UMTS, donde apareció por primera vez en la versión 5 [3]. A partir de la versión 5 se integró IMS en el núcleo de la red móvil [4], [5]. Las versiones posteriores fueron poco a poco mejorando el desempeño, por ejemplo:

♦**3GPP Versión 6:** Garantizó la conectividad con las redes inalámbricas —*Wireless Local Area Network (WLAN)*— y la interoperabilidad entre IMS utilizando diferentes redes de conectividad IP. Se estandarizaron los servicios de presencia.

♦**3GPP Versión 7:** Incluyó el soporte de la PSTN de conjunto con TISPN R1.1 mediante la función de *gateway* de control de acceso —*Access Gateway Control Function (AGCF)*— para interconectar redes IMS con redes de otro tipo.

♦**3GPP Versión 8:** Permitió el soporte de LTE e introdujo mejoras en el manejo de las sesiones de emergencia.

♦**3GPP Versión 9:** Incluyó las llamadas de emergencia sobre redes GPRS.

♦**3GPP Versión 10:** Adicionó el soporte para la transferencia entre dispositivos.

♦**3GPP Versión 11:** Proporcionó los servicios de localización a partir de la propia red. Continúan los trabajos de optimización de los procedimientos de llamada y el establecimiento de comunicaciones multimedia.

IMS se define como una arquitectura global de control de servicios y conectividad, basada en el protocolo IP e independiente del acceso, que permite la entrega de varios tipos de servicios multimedia a los usuarios finales. Combina movilidad con conectividad mediante el empleo de una red IP, factores que son cruciales para el éxito de los servicios en el futuro [6]. De este modo, IMS ofrece servicios multimedia sobre una red de conmutación de paquetes a través de diferentes redes de acceso. Fue diseñado para utilizar IPv6, protocolo de Internet que dispone de un espacio de direcciones IP significativamente grande con 128 bits de encabezado (en comparación con el de IPv4 que es de 32 bits), ya que los bloques de direcciones IPv4 se han agotado y se ha previsto una explosión de usuarios por el uso de dispositivos móviles. En la actualidad, los equipos comerciales permiten el uso de IPv4 e IPv6.

De IMS se pueden destacar las siguientes características:

- ♦Permite compartir los recursos de control de sesión, de transporte y los datos de usuario a diferentes aplicaciones.
- ♦Ofrece mecanismos para la gestión de los niveles de calidad de servicio.
- ♦Brinda servicios que combinan diferentes tipos de contenidos multimedia.
- ♦Facilita la creación de entornos en los que las aplicaciones de diferentes proveedores se integran en una única red de forma sencilla.

El concepto NGN tiene una proyección futurista y actualmente se dan pasos para llegar al estado de convergencia. Las diferencias entre la arquitectura NGN y la arquitectura IMS radican en la capa de control, mientras que el resto de la estructura de red permanece constante. Por este motivo, IMS es un paso evolutivo dentro de las NGN para alcanzar la integración total y permite disminuir los costos de operación de las redes de telecomunicaciones.

Las NGN existentes requieren *softswitch* distintos para el control de las redes fijas y móviles. IMS integra el control descomponiendo el *softswitch* actual en bloques funcionales que permiten acceder a los servidores que proveen los servicios para ambas redes. Las demás capas de la arquitectura de red como el acceso, el transporte de señales y las aplicaciones/servicios permanecen inalterables (Figura 2).

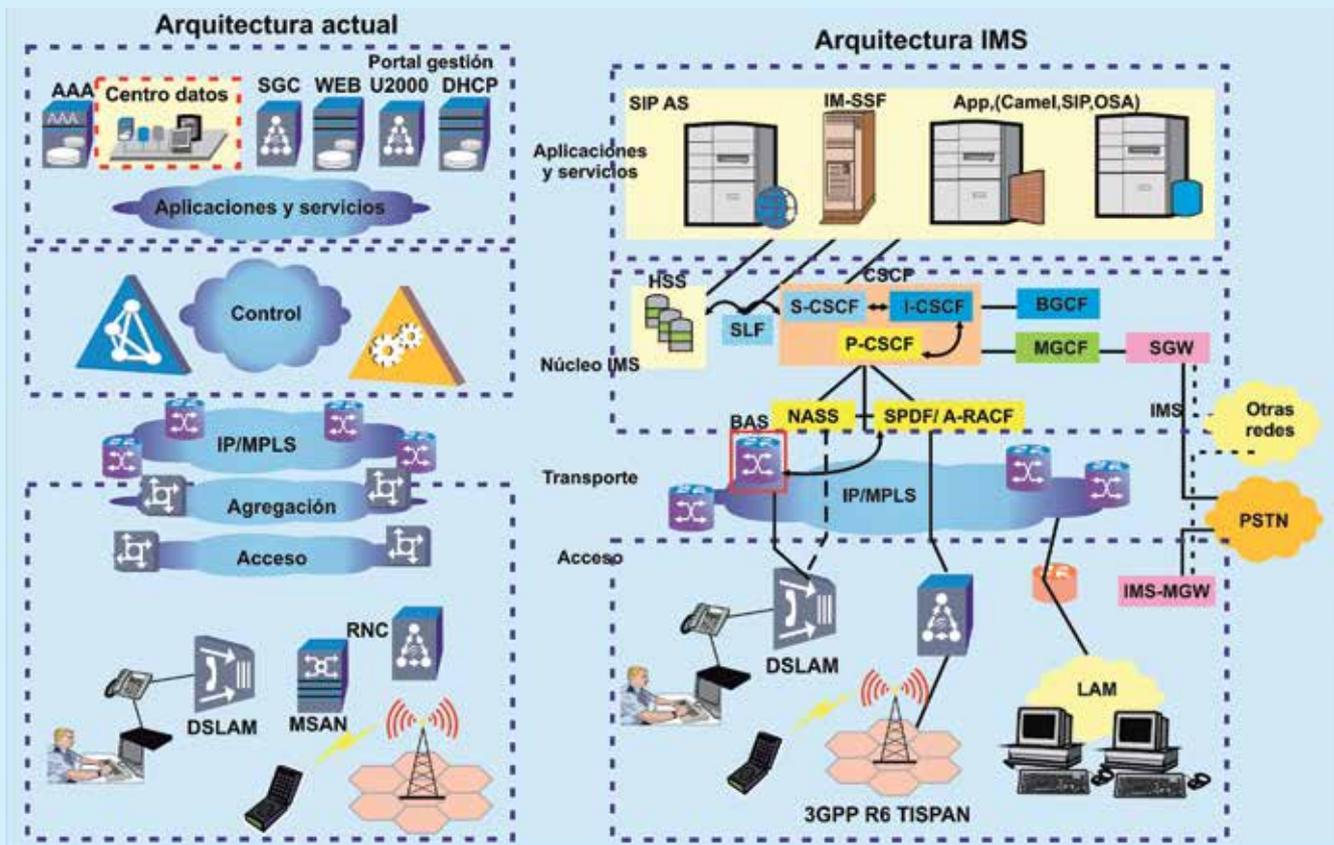


Figura 2. Arquitecturas NGN e IMS. (Fuente: DCDT).

El bloque funcional para el control de IMS se denomina CSCF —*Control Session Control Function*— y se basa en un conjunto de servidores que cooperan entre sí: Proxy (P), Servidor (S), Interrogador (I), Bases de Datos de usuarios: HSS —*Home Subscriber Server*— y SLF —*Subscriber Location Function*—. Existen otros bloques complementarios para la interconexión con la PSTN y otras redes.

Cuando un cliente inicia una sesión multimedia, la señalización SIP llega al Proxy (P) que encripta en IPSec —*IP Security*— para garantizar transacciones seguras. Se redirecciona la señalización hacia el servidor de interrogación (I) que localiza al servidor (S) para atender la solicitud. El servidor (S) pide al HSS una función de autenticación y se la envía al usuario. Este se autentica. Si el proceso es exitoso, (S) lo informa al HSS y obtiene los perfiles para el servicio solicitado. Se conecta finalmente al servidor de aplicación correspondiente y comienza el proceso de facturación del servicio.

Servicios que brinda IMS

IMS brinda un conjunto de servicios multimedia a los cuales se accede a través de una sola dirección IP y con el dispositivo que se disponga [5]. Entre los más importantes se encuentran:

- ♦ **Servicio de presencia:** Permite a los clientes disponer de información sobre los sitios que frecuentan o son importantes como si estuvieran en estos.
- ♦ **Push to talk over cellular (PoC):** Permite la comunicación punto a punto o punto-multipunto entre usuarios al activar un botón del celular.
- ♦ **Servicio de gestión de grupos:** Posibilita que los usuarios guarden sus datos en servidores del proveedor de servicios para acceder

remotamente y modificarlos. Muchos de los servicios de presencia y PoC requieren de estos datos. Admite crear y manejar listas de personas para su uso por cualquier servicio desplegado en la red, por ejemplo, las listas de compañeros, de control de acceso, grupos de chat públicos o privados, etc.

♦**Servicio de mensajería:** Proporciona los medios para que un abonado envíe o reciba mensajes, incluyendo mensajería instantánea, de manera individual o colectiva, como los juegos móviles. Los usuarios se unen a una sala de conversación para recibir el servicio.

♦**Conferencias:** Permite videoconferencias IP entre varios clientes simultáneos. Incluye audio, video, juegos o mensajería instantánea. El servidor de conferencia es el controlador de la misma.

♦**Servicio de localización:** Suministra ubicación sobre la localización física de un usuario de acuerdo a las reglas de seguridad y privacidad impuestas por la red. Los usuarios se benefician con este servicio al determinar la posición de lugares de interés, amigos, familia (cuando están autorizados) o su propia ubicación [7].

Seguridad

IMS aboga por una infraestructura de servicio abierta e interoperable, por lo que una de las principales preocupaciones es la seguridad y esto determinará el futuro del despliegue. Los esquemas de seguridad de IMS son adicionales a los de las redes de acceso IP (GPRS, LTE, WiMAX) ofreciendo un nivel superior de seguridad.

La arquitectura abierta y distribuida garantiza mayor flexibilidad en la implementación y el despliegue, pero también crea una multitud de puntos de interfaces que se deben proteger. Es por ello que el Grupo de Trabajo Técnico de Especificación No. 3 del 3GPP tiene la responsabilidad de realizar el análisis de las posibles amenazas, determinar los requisitos de seguridad y privacidad, especificar las arquitecturas y los protocolos, así como asegurar la disponibilidad de algoritmos criptográficos que necesitan ser parte de las especificaciones de estos sistemas [8].

El despliegue inicial debe satisfacer los requisitos del estándar cumpliendo con la arquitectura de seguridad de la especificación técnica TS 33.203 de la 3GPP que asocia cinco puntos de protección [9]. Este modelo identifica dónde ocurre el intercambio de mensajes SIP y cuáles son los puntos vulnerables. Tiene un enfoque limitado a los componentes IMS de la arquitectura 3G, no especifica los mecanismos de acceso de autorización para los subyacentes dominios de circuito conmutado o de conmutación de paquetes. El objetivo es garantizar la seguridad del acceso y de la señalización SIP entre la red IMS y el usuario final. Cuando un usuario activa su dispositivo o se mueve entre sitios de célula, hay una necesidad mutua en la cual el operador de red debe saber que la suscripción del dispositivo es legítima y el usuario que la red a la que se conecta también lo es. La autenticación de usuario se realiza utilizando funciones *hash* y, si el resultado es exitoso, se procede al registro IMS del terminal con el fin de iniciar una sesión multimedia de forma segura.

De acuerdo con el estándar, el núcleo IMS debe utilizar IPSec para la interacción entre sus bloques funcionales, aunque el hardware se encuentre distribuido en varias localizaciones de red. Asimismo, se debe emplear el mecanismo de autenticación y control de acceso comúnmente llamado AKA —*Authentication and Key Agreement*—. Sin embargo, existen otros mecanismos definidos para

cubrir las necesidades de terminales heredados y permitir un despliegue más rápido, los cuales se describen en la recomendación TR 33.803 que sirve de guía en la selección del método de autenticación más adecuado [10].

Los mecanismos de autenticación mencionados anteriormente se deben extender a nivel de aplicación o servicio mediante lo que se conoce como GAA —*Generic Authentication Architecture*— [11]. Esta arquitectura emplea dos mecanismos de autenticación: uno se basa en la posesión de un secreto compartido entre las entidades comunicantes —*Generic Bootstrapping Architecture* (GBA)— derivada de las claves utilizadas en la autenticación AKA, y la otra basada en criptografía asimétrica (claves pública y privada) o PKI —*Public Key Infrastructure*— y certificados digitales —*Support for Subscriber Certificates* (SSC)—.

Por último, se debe cumplir con las políticas de seguridad entre dominios. Estas políticas se garantizan con *gateways* de seguridad (SEG) que son los responsables de establecer una asociación de seguridad con el SEG par, aplicando las normas de protección de datos, filtrado y capacidades de cortafuegos. La misma es cifrada mediante el protocolo de seguridad IPSec en modo túnel. Se establecen asociaciones de seguridad tanto para la señalización entrante como para la saliente con el objetivo de soportar el tráfico bidireccional.

Numerosos dispositivos, como cortafuegos para SIP, SBC —*Session Border Controller*— y otros *gateways* de aplicaciones específicas, son parte de las soluciones de seguridad propuestas por los proveedores. Se debe evaluar, entre otros elementos, el rendimiento de estos dispositivos, así como la arquitectura fundamental de su despliegue para garantizar el éxito del modelo de seguridad.

Además, se debe tener en cuenta otras áreas implicadas en la gestión de la seguridad como la QoS, la facturación, el cobro y la habilitación de los servicios.

Pruebas a la tecnología IMS en Cuba

Se instaló un núcleo IMS en la capital con el objetivo de lograr la expansión de líneas fijas en el país, al cual se le realizan pruebas de campo para evaluar sus prestaciones y comportamiento. Para ello se configuran los bloques funcionales correspondientes al control CSCF, de servicios, bases de datos y pasarelas de media y de señalización. Se hizo interoperable este núcleo con las redes PSTN, PLMN y NGN existentes a través del MGCF —*Media Gateway Control Function*— y AGCF, permitiendo el acceso al *backbone* IP/MPLS mediante el empleo de conmutadores y cortafuegos del mismo proveedor. Se instalaron nuevos nodos de acceso multiservicio (MSAN) con protocolos de señalización H.248 y SIP lo que permitirá comparar y evaluar la posible inserción de los mismos en la red de telecomunicaciones.

El escenario propuesto para la realización de los protocolos de prueba se muestra en la figura 3.

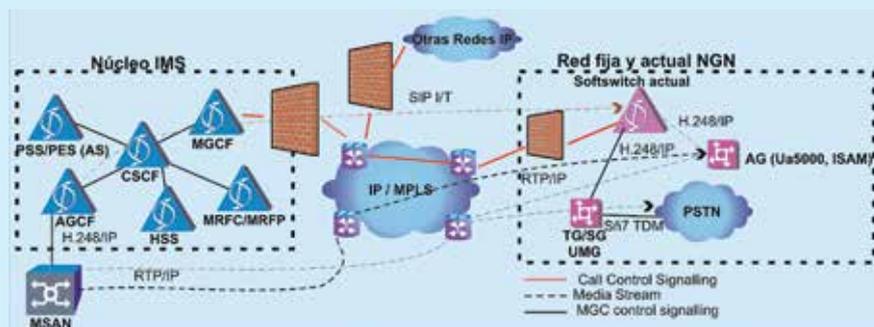


Figura 3. Esquema básico de pruebas. (Fuente: ZTE).

Se comprobó la robustez del hardware, el sistema de energía, los protocolos de señalización y el sincronismo, así como los sistemas de provisión, facturación y gestión. También se crearon nuevos perfiles de usuarios que se almacenan en el HSS y el servidor SSS —*Supplementary Services Server*— para proporcionar y satisfacer la demanda de servicios suplementarios y de emergencia.

Actualmente, se están comprobando los puntos de seguridad para minimizar los riesgos y las vulnerabilidades en la red, mitigando los posibles ataques.

En etapas posteriores se completará la infraestructura de red para garantizar el despliegue de los servicios y recuperar los costos de la inversión.

Conclusiones

La interoperabilidad de IMS con las redes PSTN, PLMN y NGN existentes permitirá extender los servicios nacionalmente a costos inferiores a los que hoy se registran.

Las experiencias prácticas que se obtengan en las pruebas facilitarán la proyección estratégica para la evolución de la red, incluyendo la migración de los nodos de acceso de diferentes fabricantes desde la red NGN existente hacia el nuevo IMS.

La puesta en marcha de la tecnología IMS en el entorno nacional constituye un paso necesario con vistas a la unificación del control de las redes fijo-móvil lo que contribuirá a simplificar los procesos de operación, mantenimiento, provisión y gestión. ▀

Referencias bibliográficas

[1] García, Alberto J. "Redes de Próxima Generación en Cuba: Implementación y experiencias" *Tono Revista Técnica de ETECSA*, vol.6, no.3, 2007, pp.31-38.

[2] Camarillo, Gonzalo; García-Martín, Miguel A. *The 3G IP Multimedia Subsystem (IMS)* L. John Wiley & Sons, Ed. Finlandia, 2004, pp.5-120, 300-350.

[3] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS)* Francia, 2009, pp.1-30, 248-251.

[4] IEEE, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) I*. Transaction, Ed. Sophia Antipolis Cedex - Francia, 2012, pp.1-41.

[5] Poikselka, Miikka; Mayer, Georg. *The IMS. IP Multimedia Concepts and Services*. J. W. S. Ltd, Ed. Finlandia, 2009, pp.3-30, 47-57, 139-218.

[6] Handa, Arun. *System Engineering for IMS Networks*. E. Inc., Ed. Oxford, UK, 2009, pp.3-50.

[7] KEN. Salchow, Jr. *Introduction to the IP Multimedia Subsystem (IMS): IMS Basic Concepts and Terminology*. F. N. inc, Ed. París: White Paper, 2007, p. 4.

[8] 3GPP, 3rd Generation Partnership Project. <http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security> (acceso enero 14, 2014).

[9] 3GPP, 3rd Generation Partnership Project. *Access security for IP-based services*. 2014. http://www.3gpp.org/ftp/specs/archive/33_series/33.203/ (acceso enero 14, 2014).

[10] 3GPP, 3rd Generation Partnership Project. *Coexistence between TISPAN and 3GPP authentication*, 2007. http://www.3gpp.org/ftp/specs/archive/33_series/33.803/ (acceso enero 14, 2014).

[11] 3GPP, 3rd Generation Partnership Project. *Generic Authentication Architecture*. 2013. http://www.3gpp.org/ftp/specs/archive/33_series/33.220/ (acceso enero 14, 2014).

(Artículo recibido en noviembre de 2014 y aprobado en marzo de 2015).