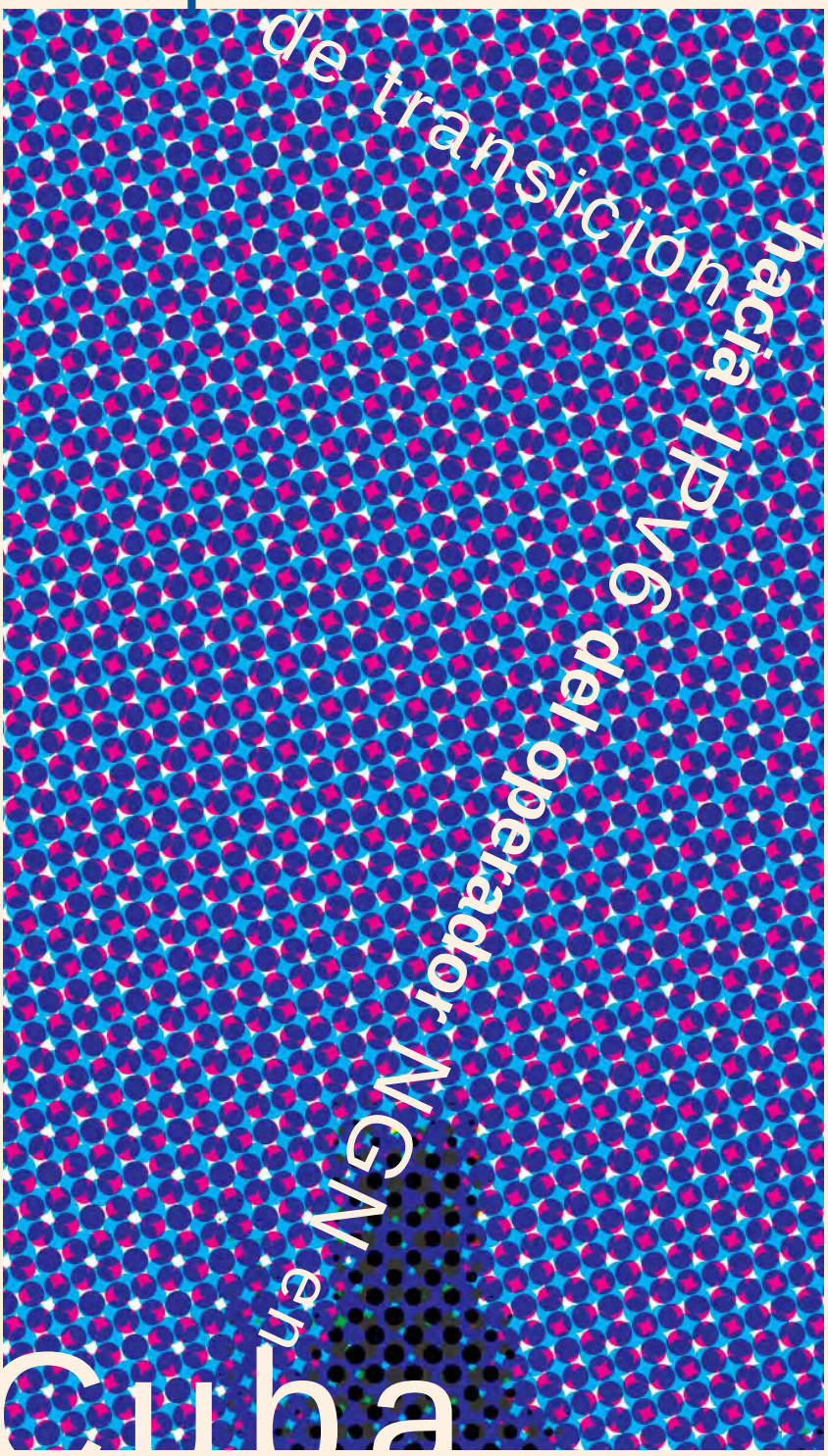
Por MSc. Adolfo Luis Marín Abreu, Jefe de la Unidad Técnica de Control, División Territorial de Sancti Spíritus, ETECSA.
adolfo.marin@etecsa.cu

Propuesta de transición hacia IPV6 del operador NGN en Cuba



Introducción

El Protocolo de Internet (IP) es la base de las comunicaciones en la actualidad a partir de las opciones de la convergencia de servicios de diferentes naturalezas —voz, video y datos— en una misma red, así como la posibilidad de interconectar equipos disímiles a través de redes heterogéneas. Debido al crecimiento de los dispositivos que emplean la arquitectura TCP/IP se ha intensificado el agotamiento de direcciones IPv4; en consecuencia, se ha hecho inaplazable la transición hacia IPv6 [1]. Los operadores de telecomunicaciones tradicionales han ofertado servicios de voz con calidad del servicio —*Quality of Service* (QoS)— garantizada. Sin embargo. al incorporar la VoIP —*Voice over Internet Protocol*— en los actuales escenarios de comunicaciones unificadas, estos han concentrado sus mayores esfuerzos en el tratamiento de la QoS, debido a su impacto sobre las aplicaciones en "tiempo real". El éxito probado del empleo de las comunicaciones basadas en el protocolo IP ha impulsado a los proveedores públicos de telecomunicaciones a implementar dentro de sus esquemas de negocios arquitecturas NGN —*New Generation Networks*— con el objetivo de incorporar los servicios de voz basados en VoIP. IP enfrenta el problema de que no garantiza la calidad de manera intrínseca; sumado a ello la VoIP implementada en el diseño actual de NGN está soportada por IPv4, protocolo que sufre un agotamiento inminente de sus reservas de direcciones. Por tanto, se hace inaplazable para el mundo y para Cuba transitar hacia IPv6 previéndose, además, un período de coexistencia de ambas versiones del protocolo. Este proceso de transición introduce retos considerables, por ejemplo, es necesario avalar la interoperabilidad entre IPv4 e IPv6, el personal técnico debe capacitarse adecuadamente, deben considerarse los nuevos riesgos de seguridad que se introducen, así como el manejo correcto de las plataformas

de negocios actuales. Todos estos retos deben ser enfocados por el Proveedor de Servicios (PS) para disminuir el impacto sobre la QoS y el comportamiento general de la VoIP en los probables escenarios de despliegue de IPv6. Teniendo en cuenta la problemática planteada y los requerimientos necesarios para la operación de NGN en un entorno de operador de servicios públicos de voz; el presente trabajo centra su objetivo en proponer un mecanismo de transición de IPv4 a IPv6 que permita la continuidad de los servicios de voz, sin afectar la QoS, la seguridad y otros parámetros que son imprescindibles para la arquitectura NGN.

Tecnologías de redes de área amplia desplegadas en Cuba

Existe una marcada tendencia mundial al empleo de redes basadas en la arquitectura TCP/IP para dar soporte a todo tipo de servicios y aplicaciones, disminuyendo los costos de operación y mantenimiento, gracias al empleo de una única red de nivel 3. Sin embargo, las redes de nivel 2 que ofrecen el debido soporte a tecnologías de capas superiores están expuestas a cambios relativamente rápidos en lo que concierne a la industria y el mercado.

Diagnóstico de las tecnologías de nivel 2 empleadas en Cuba

Existen varias tecnologías desplegadas en Cuba en el nivel 2 de la Arquitectura TCP/IP. De todas ellas, el backbone IP/MPLS, instalado en Cuba desde 2007, debe asumir el rol principal dentro de las tecnologías de nivel 2 destinadas a trasportar el resto de los protocolos de las capas superiores. Por esta razón, nuestra propuesta se centra en el estudio de los mecanismos de transición hacia IPv6 que han sido diseñados y probados para trabajar en entornos MPLS.

Backbone MPLS para el soporte de la red

Debido a la interrelación existente entre IP/MPLS y el nivel de red tanto para el funcionamiento interno de MPLS como para el funcionamiento de los servicios ofrecidos sobre este tipo de backbone, se analizaran algunas de las características del backbone desplegado en nuestro país.

Cuba cuenta en la actualidad con un backbone MPLS soportado por SDH —*Synchronous Digital Hierarchy*— y la fibra óptica nacional. Este backbone forma parte del desarrollo creciente de las redes de telecomunicaciones y está llamado a ser el principal soporte de datos del país para afrontar los proyectos de conectividad social e informatización de la sociedad. Además, tiene la responsabilidad de ser el soporte para la introducción masiva de las NGN y todos los servicios de valor agregado que incluye esta visión de red.

La arquitectura general del backbone IP/MPLS está formada por varios enrutadores de núcleo a nivel nacional con la redundancia adecuada, tanto física como lógica, enlazados a enrutadores de borde ubicados en cada provincia a los cuales se conectan los equipos de acceso mediante diferentes interfaces. Debe notarse que toda la configuración y explotación de este nuevo backbone se basa en el protocolo IPv4 y todos los servicios que se han comercializado hasta el presente también están soportados con IPv4. Durante la investigación se pudo comprobar que los enrutadores de borde manejan IPv4, pero también son capaces de manejar IPv6, así como MP-BGP, mediante una apropiada configuración y actualización del sistema operativo de los dispositivos, lo cual constituye un elemento de suma importancia a tener en cuenta en la propuesta de las estrategias de transición.

Relación de NGN con el Protocolo de Internet

Las redes NGN están orientadas a las redes basadas en la conmutación por paquetes o datagramas IP son capaces de proveer servicios de telecomunicaciones y de emplear diferentes anchos de banda. Asimismo, utilizan tecnologías de transporte que manejan la calidad de servicio según las necesidades del tráfico y las funciones relacionadas con los servicios son independientes de las tecnologías o niveles que subyacen por debajo del nivel de aplicación de la arquitectura TCP/IP [2].

IPv4 como protocolo de nivel de red empleado en la actualidad

El Protocolo de Internet versión 4 (IPv4) es la cuarta versión en el desarrollo del Protocolo de Internet y la primera versión que fue ampliamente desplegada. IPv4 sigue siendo el protocolo de Internet de capa de red más generalizado [3], cuya descripción aparece en la RFC 791 [4].

IPv4 es un protocolo no orientado a conexión, diseñado para su uso sobre redes de paquetes conmutados de capa de enlace, por ejemplo, Ethernet [5]. Funciona en un modelo de entrega según el "mejor esfuerzo", ya que no garantiza la entrega ni asegura la secuencia adecuada, tampoco evita las entregas duplicadas. Estos aspectos, incluyendo la integridad de los datos, son tratados por un protocolo de capa superior denominado TCP —*Transmission Control Protocol*— [3].

Necesidad de transición hacia IPv6

El principal factor para la inminente transición hacia IPv6 es el agotamiento de las direcciones IPv4, lo que compromete el crecimiento y el desempeño de Internet y, por tanto, el soporte a las nuevas aplicaciones y servicios que exige una sociedad ubicua [6]. Desde el punto de vista de los esquemas de negocios basados en dominios privados, como lo es el operador NGN en Cuba y en muchos de los países que han seguido estas iniciativas, el factor más crítico que condiciona la transición hacia IPv6 está directamente ligado al agotamiento de direcciones públicas. Esto se debe al hecho de que la mayoría de los dispositivos de redes han sido diseñados y deben su evolución y constante desarrollo a las demandas de una red global en crecimiento como Internet. En consecuencia, la transición de Internet hacia IPv6 no obliga a los dominios de redes con direccionamientos privados que emplean IPv4 a realizar la transición de manera inmediata; sin embargo, IPv4 se convertirá muy pronto en un protocolo obsoleto, sin soporte de la industria y sin desarrollo,

expuesto a las vulnerabilidades de interfaces atrasadas, deficiente soporte a la QoS, deficientes mecanismos para manejar los retos de seguridad siempre crecientes en los estándares de redes abiertas, entre otras vulnerabilidades inherentes a la falta de soporte técnico.

La migración afecta tanto a los elementos que componen la NGN desde el punto de vista de la red como a todos los equipos de acceso, la lógica y los softwares de aplicación. La introducción y el despliegue de IPv6 en el entorno NGN mantendrá la vitalidad de la red y el desarrollo de los servicios ofrecidos sobre la arquitectura NGN.

Impactos de la transición hacia IPv6 sobre NGN

La necesidad inminente de transitar hacia IPv6 y coexistir con IPv4 introduce retos de todo tipo, especialmente en los países donde se llevan a cabo varias transiciones sobre capas diferentes de la arquitectura TCP/IP al mismo tiempo. La transición del backbone IP/MPLS puede ocurrir en un momento diferente de la transición de NGN, por lo que deben adoptarse mecanismos de transición:

- Primero, debe transitar IP/MPLS con IPv4 hacia IPv6 debido a que esta arquitectura constituye la columna vertebral de las Redes de Próxima Generación. Esta migración puede ser paulatina, como se verá más adelante, permitiendo en una etapa inicial emplear IPv6 solamente en los extremos de la red. Después, deben transitar los elementos de red que componen la NGN, así como toda la lógica, el control, y la seguridad.
- Continuar con la transición TDM hacia los soportes IP, teniendo en cuenta que la versión 6 del protocolo IP implica novedades en el planeamiento de los nuevos soportes.
- Prestar especial atención al tratamiento de la QoS en IPv4 y planificar adecuadamente el manejo de la QoS con IPv6, de acuerdo a sus nuevas características y capacidades y el mecanismo de transición que se decida aplicar en nuestro escenario.

Aspectos críticos que deben asumirse al prolongar la transición hacia IPv6 en una isla IPv4-NGN

Puede parecer atractivo, e incluso económico, mantener la NGN-IPv4. Sin embargo, se generan impactos y criticidades a corto y mediano plazo que pueden hacer colapsar la continuidad técnica del sistema de telecomunicaciones. A continuación ponemos a consideración algunos de ellos:

- Es conocido que la industria de las telecomunicaciones actual es muy innovadora y responde a esquemas de negocios muy cambiantes [7] que siguen las necesidades de los proveedores de servicios signadas por las demandas de los consumidores, por lo que en un plazo no mayor de 5 años pudieran presentarse problemas impostergables de soporte técnico en varias esferas críticas para el mantenimiento de la disponibilidad y continuidad de los servicios de telecomunicaciones como la discontinuidad de líneas de producción de tecnologías compatibles con IPv4, donde inciden los sistemas operativos, los repuestos, la superación profesional, etc. Estos aspectos impactan directamente sobre las redes de núcleo (IP/MPLS), las redes de agregación (Metro Ethernet), las redes de acceso, los CPE —*Custumer Premise Equipment*— [8] y todo el hardware y software que componen la NGN.
- Otro aspecto crítico es generado cuando los operadores internacionales solamente reciben tráfico IPv6 nativo, tanto para la voz como para todos los servicios multimedia soportados por paquetes de datos. En este caso, deben crearse las condiciones para que los dominios NGN-IPv4 alcancen un punto de acceso internacional compatible con IPv6 o simplemente debe culminarse la migración hacia NGN con IPv6 de manera nativa.

Principales mecanismos para la transición hacia IPV6

Existen diversos mecanismos aplicables a entornos de redes privadas inherentes a dominios propios de los clientes y otros aplicables a redes públicas como Internet. Muchos de los mecanismos existentes en IPv4 han sido extendidos y actualizados para que puedan ser empleados en IPv6. Por ejemplo, se ha desarrollado una versión del protocolo de traslación de direcciones —*Neighbor Acquisition Protocol* (NAT)— denominado NAT64. De igual forma, se desarrolló un método empleado para la asignación dinámica de direcciones IP, DHCPv6, el cual funciona de manera similar a su predecesor DHCP en IPv4, se estandarizó una versión superior del servidor de nombres de dominio, DNSv6, que es capaz de manejar registros de tipo A y AAAA para IPv6 al mismo tiempo; permitiendo que la mayoría de los DNS desplegados por el mundo puedan ser actualizados y respondan a ambas versiones del protocolo IP. Gracias a estos mecanismos generales y a otros destinados a la transición hacia IPv6 como los Tunnel Broker, entre otros tipos de tunelizaciones, se ha hecho posible la transferencia de tráfico entre dominios IPv4 e IPv6. De este modo, existen en la actualidad dos dominios públicos de Internet a los cuáles los clientes pueden acceder empleando muchas veces mecanismos de tunelización automática que son transparentes a los usuarios. No obstante, como ya se analizó, el operador NGN en Cuba soporta su arquitectura sobre un backbone IP/MPLS; por ello, los principales mecanismos del presente estudio son aquellos diseñados para llevar a cabo la transición sobre un backbone MPLS. En este sentido, se recomienda comenzar desde los bordes de la red hacia el núcleo, lo que implica transportar tráfico IPv6 a través de la red IPv4 permitiendo que los dominios aislados que funcionan como IPv6 se comuniquen entre sí, sin tener que efectuar una transición completa hacia IPv6 nativo. En este contexto, es posible emplear IPv4 e IPv6 a

lo largo de toda la red, desde todos los bordes a través del núcleo, o emplear la traducción entre IPv4 e IPv6 para permitirle a los hosts que se comunican con un protocolo que se comuniquen de manera transparente con los hosts que se comunican con el otro. Los cuatro mecanismos básicos son [9]:

- Desplegar IPv6 sobre túneles IPv4.
- Desplegar IPv6 sobre enlaces de datos dedicados.
- Desplegar IPv6 sobre un backbone MPLS.
- Desplegar IPv6 utilizando backbones que soporten el modo *dual stack* (doble pila).

Escenarios de despliegue de IPv6 sobre un backbone MPLS

Existen muchas maneras para entregar servicios IPv6 a los usuarios finales. La más utilizada es el envío de tráfico IPv6 de extremo a extremo. IPv6 sobre MPLS permite a los dominios IPv6 aislados comunicarse con otros dominios similares empleando el backbone IPv4 MPLS. Los mecanismos más importantes para desplegar IPv6 sobre MPLS se describen brevemente a continuación:

Soporte nativo de IPv6 sobre MPLS

La infraestructura del núcleo requiere actualizar completamente el plano de control hacia IPv6 [10]:

- Requiere enrutamiento IPv6 en el núcleo.
- Requiere IPv6 LDP —*Label Distribution Protocol*— en el núcleo.
- Una transición brusca introduce riesgos y costos adicionales para el PS [11].

IPv6 sobre Túneles IPv4: De CE a CE

Esta estrategia no requiere cambios en los enrutadores de núcleo P —*Provider*—, ni en los enrutadores de borde PE —*Provider Edge*—, porque se emplean túneles IPv4 para encapsular el tráfico IPv6 de manera que aparecería como tráfico IPv4 dentro de la red [11]. Sin embargo, este método adolece de los constantes retos de escalabilidad que presentan las técnicas de tunelización, es decir, la creación y el manejo de túneles así como el enrutamiento de cada enrutador CE —*Custumer Edge*— hacia otro enrutador CE [11].

IPv6 empleando circuitos sobre M-PLS

Permiten que sean emulados:

- Circuitos ATM, FR, puerto a puerto sobre Ethernet, VLAN, entre otros.
- Es necesario que los enrutadores PE soporten circuitos sobre MPLS. Soportado por los enrutadores de Internet Cisco 12000 y 7600 [9].
- Esta técnica evita cualquier actualización IPv6 en el núcleo, pero también acarrea retos de escalabilidad.

IPv6 Provider Edge Router (6PE) e IPv6 VPN Provider Edges (6VPE)

Soportan el servicio de alcance global con IPv6 y servicios VPN con IPv6 sobre un backbone IPv4 MPLS. Estas estrategias han probado ser muy atractivas para los proveedores que tienen en operación IPv4 debido a las siguientes razones [11]:

- No requieren actualizaciones para los enrutadores P, por tanto, se preserva la estabilidad del backbone y se minimizan los costos de la operación.
- Permiten un despliegue gradual, actualizando solamente los enrutadores PE para que ofrezcan servicios IPv6, donde se empleen RR —Reflectores de Rutas— se actualizarán o, en su lugar, se desplegará una malla separada de RR para IPv6.
- Son muy escalables porque se apoyan en un solo lado del modelo de provisión como en la arquitectura MPLS VPN, por lo cual la adición de un nuevo sitio involucra solamente la configuración del puerto en cuestión para ese sitio particular.
- Toman las ventajas de reenvío en el núcleo de MPLS y su alto rendimiento.
- Garantizan que el tráfico IPv6 se beneficie automáticamente de las características avanzadas de MPLS, que pueden ser desplegadas en el núcleo como FRR —*Fast Reroute*— en RSVP-TE, TE y MPLS QoS.

IPv6 Provider Edge (6PE)

La solución 6PE utiliza el mismo paradigma transparente de enrutamiento y transporte para lograr alcanzabilidad global con IPv6 sobre un backbone IPv4 MPLS que no conoce IPv6. La diferencia clave es que la información de alcanzabilidad que se anuncia entre los enrutadores PE vía MP-BGP ya no emplea prefijos VPN con IPv4, sino que utiliza prefijos IPv6. De manera que los enrutadores PE deben ser actualizados a *dual-stack* y se denominarán 6PE. Ellos soportarán IPv6 (y típicamente IPv4) en las interfaces de acceso, pero soportarán solamente IPv4 e IPv4 MPLS en las interfaces que apuntan al núcleo. Los enrutadores P permanecen ajenos a IPv6 y tienen en funcionamiento el enrutamiento y la distribución de etiquetas IPv4 [11]. Una forma de entender la solución 6PE consiste en considerar que el núcleo IPv4 MPLS transporta eficazmente el tráfico de una VPN adicional cuyo tráfico y espacio de direcciones en este caso es IPv6. Al igual que en IPv4 VPNs, los enrutadores del núcleo permanecen ajenos a los enrutadores que pertenecen a esta VPN particular. Nótese, sin embargo, que esta VPN especial no involucra los mecanismos de la RFC 2547bis [12], tales como VRF —*Virtual Route Forwarding*—, los RD —*Route Distinguishers*— y RT —*Route Targets*— porque las tablas de rutas y encaminamientos de IPv6 están naturalmente separadas de las de IPv4 [11].

Topología de la NGN en Cuba con IPV4

Las NGN son redes de alcance global y se pueden dividir en cuatro capas o niveles: Capa de Acceso, Capa de Transporte, Capa de Control y Capa de Aplicación/Servicios (Figura 1). Estas capas están separadas entre sí e interactúan por medio de interfaces y protocolos abiertos. El control de llamadas y servicios radica en el *softswitch*, que

es el cerebro de esta estructura y está separado lógica y físicamente de los dispositivos de conmutación y de acceso. Este tipo de redes soporta diferentes QoS para diferentes servicios pues, además de transportar voz, datos y multimedia en tiempo real, también transporta datos en tiempo no real y brinda servicios a una amplia variedad de dispositivos cableados e inalámbricos [13].

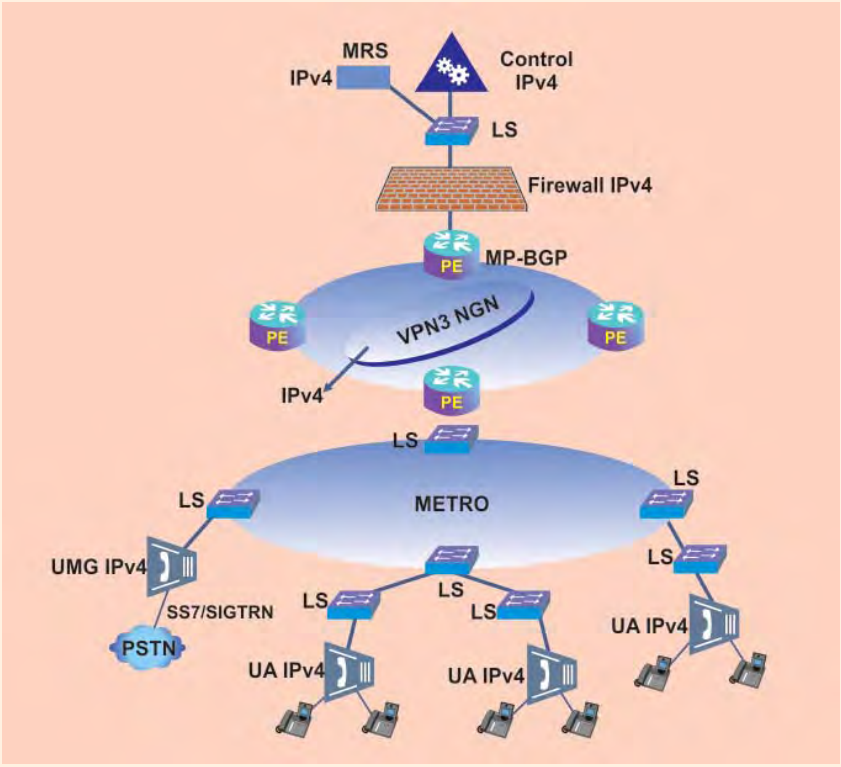


Figura 1 Arquitectura NGN con IPv4 (Fuente: [14]).

La capa de Servicios/Aplicación

Es la capa de mayor diferencia entre los distintos operadores. Proporciona los servicios y las aplicaciones disponibles en la red. Estos servicios serán ofrecidos por la red sin importar dónde esté ubicado el usuario y serán tan independientes como sea posible de la tecnología de acceso. Se brinda a los abonados todos los tipos de servicios como redes inteligentes, video en demanda, correo electrónico, correo de voz, servicio Web, entre otros. La capa la componen los servidores de aplicaciones y de medios, los que se encargan de proveer las funciones y características de la red, por ejemplo, el establecimiento de las conexiones, el encaminamiento, la facturación, los servicios avanzados que son posibles de implementar por medio de la señalización y la información que se deduce de esta [15]. En nuestra propuesta, todos los servicios y aplicaciones tienen que ser actualizados para que manejen IPv6.

La capa de Control

La capa de control es la más importante dentro de la arquitectura de la NGN. En esta capa se encuentran los dispositivos que controlan el transporte de los datos en la red y el acceso a la misma. Estos dispositivos son llamados softswitch, controlador de pasarela de medios o agente de llamada —*Call Agent*—. El *softswitch* utiliza estándares abiertos para crear redes integradas de última generación en las que la inteligencia asociada a los servicios está desligada de la infraestructura de red. Se considera la pieza central en las primeras implementaciones de las NGN. Este dispositivo es la combinación de hardware y software que provee control de llamada y servicios inteligentes para redes de conmutación de paquetes y puede conmutar el tráfico de voz, datos y video eficientemente. Los componentes principales del *softswitch* se denominan: MG —*Media Gateway*—, MGC —*Media Gateway Controller*— y SG —*Signalling Gateway*—. Aunque muchas veces estos componentes se encuentran integrados pueden estar separados, lo que requiere el uso de protocolos de comunicación entre los mismos para llevar a cabo las diferentes funciones de control que en la mayoría de los casos se ejercen sobre los recursos de la red que deben ser direccionados con el Protocolo de Internet. En este caso, nuestra sugerencia es actualizar el sistema operativo de los diferentes elementos involucrados en el control para que manejen IPv6. El *softswitch* debe soportar las siguientes funciones [15]:

- Control de llamada
- Protocolos de establecimiento de llamadas: H.323, SIP
- Protocolos de control de medios: MGCP, MEGACO H.248.
- Control sobre la clase y calidad del servicio.
- Protocolo de Control SS7: SIGTRAN (SS7 sobre IP).
- Procesamiento SS7 cuando usa SIGTRAN.
- Detalle de las llamadas para la facturación.
- Control de manejo del ancho de banda.
- Control de pasarela de medios.
- Control de pasarela de señalización.
- Registro de *gatekeeper* (controlador de acceso).

La capa de Transporte

Esta capa no es más que el backbone de alta velocidad, el cual soporta el tráfico de paquetes para todos los servicios, es decir, voz, datos, video y otros. Es uno de los principales responsables de la QoS de extremo a extremo, mantiene la conectividad entre todos los componentes y la separación física entre

las funciones dentro de la NGN. Esta compuesto por enrutadores y conmutadores que permiten la conmutación de las señales por la red asegurando alta capacidad y confiabilidad. Este nivel adopta la tecnología de conmutación de paquetes IP y se reconoce como la más prometedora para NGN [13]. En Cuba se emplea MPLS y el servicio más difundido es VPN capa 3. En esta estructura, los paquetes IPv4 entran por el enrutador de borde PE. El PE de entrada analiza el campo dirección destino y coloca una etiqueta. Así, dicho paquete viaja a través de una VPN denominada NGN. En el PE de salida se extrae la etiqueta al paquete y se entrega al destino IP en el dominio del cliente en cuestión. La información de cómo alcanzar el destino a través de las trayectorias óptimas es descubierta y distribuida mediante el protocolo MP-BGP, el cual lee la información de destino y actualiza a todos los enrutadores, lo que contribuye a la QoS. Esta información la intercambia con un protocolo interior de MPLS, que es el protocolo de distribución de etiquetas —*Label Distribution Protocol*—, quién se encarga de actualizar las tablas de conmutación de etiquetas.

La capa de Acceso

Esta capa incluye una diversidad de tecnologías usadas para llegar al cliente. Está compuesta por una variedad de dispositivos que permiten a los usuarios finales tener conectividad con la NGN, estos pueden ser MG, AMG, TMG o SMG, IAD y puntos de acceso inalámbrico. Además, existen los dispositivos que realizan las funciones de los tres primeros mencionados; estos son conocidos como UMG —*Universal Media Gateways*— [15].

En la topología cubana los equipamientos que se utilizan son teléfonos analógicos tradicionales, que no poseen ningún tipo de inteligencia. El último punto IP es el elemento de acceso, —Universal Access (UA). En los UA se establecen sesiones como mecanismos para identificar cada dispositivo telefónico como una entidad única dentro del sistema NGN; la sesión se establece con un par de números, la dirección IP y la identificación del terminal —*Terminal Identification* (TID) —. Según nuestra propuesta, los dispositivos susceptibles al protocolo IP deben ser actualizados para que manejen el protocolo IPv6.

Propuesta de arquitectura de NGN en Cuba con IPV6

El propósito primario de las soluciones de transición hacia IPv6 consiste en permitir a los operadores que ofrecen servicios sobre la arquitectura NGN proveer servicios a clientes que han desplegado IPv6 en sus redes [16]. Teniendo en cuenta las mejores garantías de QoS, se propone la migración de los principales actores de NGN hacia IPv6, donde se mantiene el núcleo de MPLS con IPv4, y todas las configuraciones son elaboradas en base a IPv4 como la ingeniería de tráfico, el manejo de la QoS, la fiabilidad de la red, etc. En este sentido, se recomienda actualizar los PE para que manejen la dualidad de protocolos (IPv4/IPv6) e implementar el mecanismo 6VPE [17], como se muestra en la figura 2.

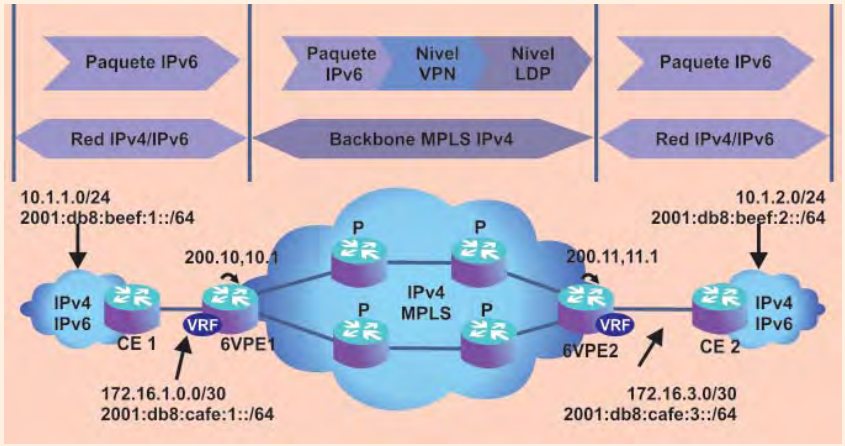


Figura 2 Redes Privadas Virtuales, 6VPE (Fuente: [18]).

El mecanismo 6VPE emplea la infraestructura MPLS con IPv4 en el núcleo para proveer VPN/IPv6, utilizando el plano de control con IPv4 (LDPv4, TEv4, IGPv4). Además, posee características arquitecturales similares a las VPNv4 como RT, VRF —Virtual Routing and Fowarding— y pueden contener rutas VPNv4 y VPNv6 asociadas a IPv6 para formar las direcciones VPNv6 [18]. En la figura 3 aparece la propuesta de arquitectura NGN durante la transición hacia IPv6 en la que se implementa una VPNv6 para gestionar el tráfico de señalización y el de voz a través del mecanismo 6VPE [17]. El MP-BGP tiene que ser actualizado para que distribuya las familias de direcciones IPv4 e IPv6. La red Metro y demás dispositivos de nivel 2 (Lanswitch) no sufren cambios esenciales en cuanto al manejo de IPv6, solo en las IP empleadas en la gestión propia del dispositivo. Los elementos que participan en el control, así como cualquier otro enrutador que exista en la arquitectura NGN, deben ser actualizados para lidear con el nuevo protocolo de red, IPv6. Lo mismo ocurre con los equipos de acceso, mientras que los dispositivos finales no sufren ninguna modificación debido a que no poseen inteligencia embebida. Los paquetes IPv6 atraviesan la red Metro para interconectarse a través de la VPN de NGN, mediante el mecanismo 6VPE, con el resto de los elementos que forman la arquitectura NGN. En consecuencia, se obtiene una propuesta donde los principales actores de la arquitectura NGN de Cuba (MGW y MGC) y todos los actores de NGN involucrados en la capa de red deben ser actualizados para que

manejen IPv6 de manera nativa, manteniendo la capa de transporte IP/MPLS con IPv4 en el núcleo a fin de no alterar el comportamiento del resto de los clientes que se apoyan en este backbone para extender sus redes privadas por todo el país. Esta propuesta se aproxima al escenario D descrito por la ITU-T [16].

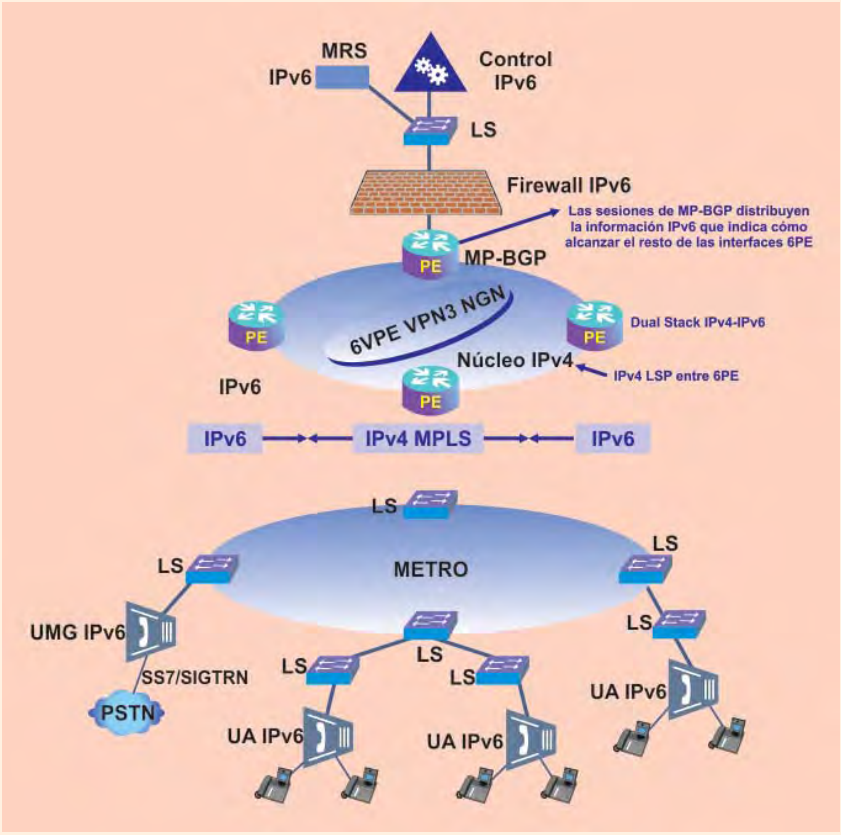


Figura 3 Arquitectura NGN con IPv6 con 6VPE en el núcleo MPLS (Fuente: [14]).

Consideraciones de seguridad

Para el proveedor de servicios, la seguridad en la arquitectura resulta de vital importancia para la continuidad del servicio y el éxito de la facturación de las llamadas. En la propuesta de transición hacia IPv6 de la arquitectura NGN en Cuba, los elementos de seguridad deben ser actualizados para que manejen IPv6, tanto a nivel de red como a nivel de aplicación. Además, la seguridad en sí constituye un aspecto significativo dentro de la QoS. Por ejemplo, si una red aplica diferentes QoS a diferentes paquetes, los clientes tratarán de aplicar la mejor QoS a sus paquetes sin autorización. En una red con el modelo del "mejor esfuerzo", los clientes no se interesan por diferenciar sus paquetes en cuanto a QoS debido a que todos los paquetes son tratados de manera similar. No existen mecanismos de seguridad para validar el campo "Tipo de Servicio" del datagrama IP o el campo "Precedente bits" de la trama Ethernet; incluso si existieran estos mecanismos, no resultaría práctico su implementación por el encarecimiento del hardware ya que se necesitaría, por ejemplo, autenticar cada trama que se encuentra atravesando un enlace de 10 GB Ethernet [19]. La mejor solución para la seguridad de nuestro modelo reside en proveer puntos de seguridad en los extremos de la red mediante cortafuegos actualizados a IPv6. Entre el control (*softswitch*) y el resto de la arquitectura se puede colocar un Eudimon y en los diferentes puntos de acceso se pueden emplear SBC —*Session Border Control*—.

Por otra parte, en el nivel de red se debe efectuar el control de QoS a través de las listas de acceso —*Access Control List* (ACL)—. Mediante las ACL, los paquetes que no están debidamente marcados así como los que se encuentran marcados erróneamente pueden descartarse de acuerdo a las políticas establecidas por el PS [19]. Además, las ACL pueden configurarse teniendo en cuenta los siguientes parámetros:

- DSCP—*Differentiated Services Code Point*— que viaja en el campo Clase de tráfico —*Traffic Class*— de la cabecera de IPv6
- La dirección IPv6 de origen y destino
- Permitir o no la fragmentación del paquete IPv6
- Permitir o no las fragmentaciones iteradas
- Determinar las cabeceras de Extensión —*Next Headers*— que serán permitidas

Esta técnica tiene la ventaja de que la complejidad de la seguridad de la QoS no se distribuye por toda la red, simplificando la configuración de los nuevos actores dentro de la NGN, incluso en el entorno de transición hacia IPv6. No obstante, debe prestarse especial atención a los puntos donde se aplican las reglas de seguridad, en los cuales pueden existir fallos o colas por diversos motivos que pudieran atentar contra la QoS extremo a extremo.

Conclusiones

A lo largo del artículo se ha realizado una caracterización de la tecnología NGN empleada en Cuba y se ha expuesto una propuesta concreta al proveedor de servicios para la transición de la NGN hacia IPv6. Como base de la propuesta se sugiere migrar todos los actores de la NGN, excepto el nivel de transporte. Para ello se identificó IP/MPLS como la tecnología implementada en Cuba con mejores perspectivas de soportar el tránsito hacia IPv6. Este no altera el núcleo de MPLS, mantiene todas las configuraciones funcionales

de IPv4 en cuanto a QoS, ingeniería de tráfico, enrutamiento y, al mismo tiempo, está en correspondencia directa con el principal servicio que se configura, y se comercializa en Cuba con el objetivo de construir redes de conectividad de nivel 3 (VPN-3).

Referencias bibliográficas

[1] López, T.A. Lanzamiento Mundial de IPv6. 6 de Junio de 2012. http://www.redclara.net/index.php?option=com_content&view=article&id=1037%3A6-de-junio-de-2012-lanzamiento-mundial-de-ipv6&catid=6%3Anoticias&Itemid=352&lang=es. (Consulta septiembre 19, 2012).

[2]Marín Abreu, A.L. Impactos sobre las Redes de Próxima Generación de la Migración hacia IPv6. (Consulta enero 11, 2012).

[3] Mashable, I. IPv4. 2012 http://mashable.com/follow/topics/ipv4. (Consulta abril 10, 2012).

[4] Postel, J. RFC: 791 Internet Protocol. 1981 http://www.rfc-es.org/rfc/rfc0791-es.txt. (Consulta abril 3, 2012).

[5] Law., D. IEEE 802.3 Ethernet Working Group. http://www.ieee802.org/3/. (Consulta mayo 24, 2012).

[6] Marín, A. and J. Gómez. Retos de seguridad con IPV6 en un entorno ubicuo. (Consulta abril 1, 2011).

[7] Fransman, M. Evolution of the Telecommunications Industry into the Internet Age E1. http://www.telecomvisions.com/articles/pdf/FransmanTelecomsHistory.pdf. (Consulta enero 13, 2012).

[8] Singh, H. and W. Beebee. IPv6 CPE Router Recommendations draft-wbeebee-ipv6-cpe-router-04. http://tools.ietf.org/html/draft-wbeebee-ipv6-cpe-router-04. (Consulta enero 13, 2012).

[9] CISCO, S.y. "IPv6 Deployment Strategies". http://www.cisco.com/en/US/tech/tk872/technologies_white_paper09186a00800c9907.shtml. (Consulta abril 13, 2012).

[10] CISCO. IPV6 Over Multiprotocol Label Switching: IPV6 Provider Edge Router and IPV6 VPN Provider Edge Router". http://www.cisco.com. (Consulta abril 6, 2012).

[11] Guichard, J.F., François Le y Vasseur, Jean-Philippe. Definitive MPLS Network Designs. IPv6 Over MPLS Networks. http://www.fengnet.com/book/Definitive%20MPLS%20Network%20Designs/toc.html. (Consulta abril 4, 2012).

[12] Semeria, C. RFC 2547bis: BGP/MPLS VPN Fundamentals. http://www.juniper.net/solutions/literature/white_papers/200012.pdf. (Consulta marzo 30, 2012).

[13]Olivera Moreno, R. Propuesta de Implementación de NGN en Granma. (Consulta mayo 24, 2012).

[14] Gómez Mutis, A. "Voz sobre el Protocolo de Internet en entornos de transición hacia IPv6". *Telecomunicaciones y Electrónica*. 2012, UCLV: Santa Clara.

[15] Camacho Aguilera, R.L. Propuesta de situación de las Centrales Tandem con tecnología de Redes de Próxima Generación. (Consulta mayo 24, 2012).

[16] ITU. Roadmap for IPv6 Migration from NGN Operators' Perspectives, ITU-T draft Recommendation Y.ipv6migration. https://datatracker.ietf.org/documents/LIAISON/file961.pdf. (Consulta enero 13, 2012).

[17] Clercq, J.D.C., M. y Faucheur, F. Le. RFC 4659 - BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN. http://tools.ietf.org/html/rfc4659. (Consulta abril 3, 2012).

[18] Contreras, G. IPv6 over MPLS 6PE and 6VPE. http://lacnic.net/documentos/seminarios/6PE_6VPE_LACNIC.pdf. (Consulta junio 5, 2012).

[19] Networks, E. Quality of Service for Voice-over-IP Networks. http://www.extremenetworks.com/libraries/whitepapers/WPQoSVoIPNetworks_1314.pdf. (Consulta junio 8, 2012).