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

Soluciones para la implementación de IPv6 en la red de telecomunicaciones de ETECSA

Resumen

El protocolo de Internet IPv6 se está empleando de forma progresiva en las nuevas implementaciones de redes y servicios a nivel mundial. En Cuba, el Ministerio de Comunicaciones ha brindado apoyo para impulsar este desarrollo estableciendo un marco regulatorio mediante varias resoluciones. La presente contribución aborda, a partir de las bondades que ofrece el protocolo IPv6, las posibles soluciones para esta migración tanto en redes metropolitanas como en el núcleo de la red IP/MPLS. Se explican las particularidades de los métodos más empleados en ambos segmentos de la red y se resumen los principales resultados de las recientes pruebas de campo de la tecnología IPv6 ejecutadas sobre el *backbone* IP/MPLS de la red de telecomunicaciones de Cuba.

Palabras clave: IPv6, Red metropolitana, Backbone IP/MPLS, Cuba, Pruebas de campo

Abstract

The Internet protocol IPv6 is being progressively used in new networks and service implementation worldwide. In Cuba, the Communications Ministry of Cuba has supported this approach in order to drive forward this development by establishing a regulatory environment through several resolutions. Based on the facilities provided by the IPv6 protocol, the present contribution approaches the possible solutions for this migration in metropolitan networks as well as in the core of the IP/MPLS network. This paper explains the characteristics of the more used methods in both network segments and sums up the main results of recent field tests regarding IPv6 technology carried out over the Cuban IP/MPLS backbone telecommunications network.

Keywords: *IPv6, Metropolitan Network, Backbone IP/MPLS, Cuba, Field Tests.*

Introducción

El protocolo IPv4 ha servido para direccionar equipos en un mundo interconectado globalmente, que crece cada día y requiere de movilidad con acceso a Internet y a contenidos multimedia. Parece simple, pero la diversidad de redes, equipamiento y sistemas autónomos hacen de esta conectividad mundial un complejo problema, que se acrecienta con el final de la vida útil del rango de direcciones IPv4 públicas disponibles. La IANA —*Internet Authority Number Assignment*— anunció el 3 de febrero del 2011 el fin de los bloques de direcciones IPv4 [1-3].

Para prevenir el agotamiento se adoptaron medidas que hacen menor el impacto de su disminución tales como el establecimiento del método CIDR —*Classless Inter Domain Routing*—, que hace uso eficiente del direccionamiento y limita la máscara de subred (RFC 4632, agosto 2006) [4]; la solicitud de retorno a la IANA de bloques de direcciones no empleados (RFC 1917, febrero 1996) [5]; la declaración de los espacios de direcciones privadas (RFC 1918, febrero 1996); el empleo del protocolo de asignación dinámica de direcciones IP (DHCP —*Dymanic Host Control Protocol*—, RFC 2131, marzo 1997) [6] y la traducción de direcciones privadas a públicas o NAT —*Network Address Translation*—, RFC 3022, enero 2001) [7]. Aunque todas se emplean, no logran resolver definitivamente el problema del agotamiento de IPv4.

Estas circunstancias llevaron al grupo de trabajo del IETF —*Internet Engeering Task Force*— a desarrollar IPv6 como el nuevo protocolo de Internet, con 128 bits para obtener alrededor de 3,4 x 1038 direcciones IP. Este nuevo protocolo es incompatible con las redes y servicios IPv4 existentes, por eso se necesitan mecanismos de transición para cursar tráfico IPv6 a través de redes metropolitanas IPv4 y núcleos de conmutación de paquetes IP/MPLS, basados en técnicas combinadas de túneles, Dual-Stack y NAT.

Ofrecer servicios IPv6 de extremo a extremo sobre redes IPv4, así como lograr una transición paulatina y armónica hacia redes puramente IPv6 es una tarea a largo plazo, que requiere de recursos y de tecnologías para introducir cambios en todos los sectores de la red de telecomunicaciones: acceso, transporte, servicios, contenidos, gestión, facturación y control de la seguridad. Esto debe hacerse de modo que coexistan ambos protocolos. La transición es inevitable, y mientras más se agilice el tránsito, mayor experiencia se alcanzará en el dominio y funcionamiento de las redes involucradas, que a largo plazo redundará en una disminución de los costos totales de implementación.

Teniendo en cuenta el estado actual de la red de telecomunicaciones en Cuba es posible comenzar a dar los primeros pasos para introducir la tecnología y con ello preparar despliegues de nuevos servicios. Hay que valorar los costos asociados al despliegue tecnológico paso a paso, resolviendo los problemas de la coexistencia y considerar el impacto sobre los servicios IPv4 actuales.

Tecnologías de transición más utilizadas

Entre las tecnologías de transición más utilizadas se encuentran Dual-Stack o doble pila de protocolos, los túneles y el NAT. Estas por sí solas no resuelven los problemas que la transición plantea, y requieren combinarse con tecnologías complementarias como Dual-Stack Lite, Dual-Stack + NAT, NAT64, 6RD, L2TP, 6PE/6VPE, entre otras. A continuación se resume el principio de funcionamiento de las más empleadas [8-9].

- 6RD —*Rapid Deployment*—: ofrece transporte IPv6 sobre redes metro IPv4 facilitando un rápido despliegue mediante la combinación de dos elementos: el CPE Dual-S tack —*Customer Premises Equipment*—y un 6RD-GW —*6 RD Gateway*—, que es un enrutador Dual-Stack. Los paquetes IPv6 son encapsulados en IPv4 y enviados a través del túnel hasta el 6RD-GW, entregándolos al *backbone* IPv6 o a la red IP/MPLS. En este último caso, se tendría que emplear otra técnica de transporte, que puede ser 6PE o 6VPE para conducirlos hasta la Internet IPv6. Este método se utiliza en despliegues iniciales y los costos dependen de la cantidad de CPE Dual-Stack, así como de la ubicación de 6RD-GW en los bordes de la red. Tiene como inconveniente que el manejo y gestión de túneles se hace complejo cuando se incrementa el número de usuarios [10].
- DS+NAT444: es una solución madura, aunque costosa, porque todos los dispositivos de red deben soportar Dual-Stack. Se pueden realizar uno o dos NAT para ahorrar direcciones IPv4, pero esto impacta en algunos servicios como los de VoIP. Si se ofrecen servicios de banda ancha conmutada, como PPPoE o BRAS —*Broadband Remote Access Server*—, deben asignarse direcciones IPv4 e IPv6 a los CPE, por lo que la gestión de usuarios se torna más compleja. La funcionalidad

CGN—*Carrier Grade NAT*— se puede ubicar en el propio BRAS, mediante la inserción de una tarjeta, de este modo se hace NAT y se terminan las sesiones de usuario en el mismo equipo. Estos servicios se pueden ofrecer desde la PC o desde el CPE, que funcionaría en modo *bridge* o *routing*, respectivamente [10]. En algunos casos se transita por más de un enrutador antes de obtener los servicios del BRAS, sirviéndose de una VPLS —*Virtual Private LAN Services*—, para establecer un nivel 2 hasta llegar al BRAS [11].

- DS-Lite: es la variante económica de Dual-Stack, ya que solo determinados dispositivos deben serlo. Permite omitir la asignación de una dirección IPv4 al CPE. En su lugar, se asignan únicamente direcciones IPv6 globales. Un entorno Dual-Stack requiere asignación de direcciones públicas IPv4 e IPv6 [12]. DS-Lite crea un túnel automático del tipo 4in6. El *backbone* metro es únicamente IPv6. Esta solución se utiliza en la construcción de nuevas redes metro o en la última etapa de transición. En caso de desplegar servicios PPPoE, el BRAS solo necesita administrar direcciones IPv6, facilitando así la gestión de usuarios ya que se utiliza un solo tipo de protocolo. El CGN puede formar parte del BRAS. Con estos dos elementos se puede transitar IPv4 a través de un *backbone* IPv6 [12].
- NAT64: es una solución futurista utilizada en la última etapa de transición y permite a los hosts IPv6 comunicarse con servidores IPv4. La red metro y los terminales, tanto fijos como móviles, deben soportar solo IPv6. NAT64 está diseñado para usarse en redes metropolitanas cuando las comunicaciones son iniciadas por los hosts IPv6. Se debe mantener un mapeo de direcciones IPv6 a IPv4 que se configura de forma estática por los administradores del sistema o dinámica cuando llega el primer paquete IPv6 al servidor NAT64.
- 6PE (RFC 4798): se utiliza para el tránsito de paquetes IPv6 sobre el *backbone* IP/MPLS empleando enrutadores Dual-Stack en los bordes de la red, en un entorno en que todos los túneles MPLS se establecen dinámicamente [13-14]. Los dominios IPv6 remotos se comunican a través de un núcleo IP/MPLS usando los LSP —*Label Switch Path*—. MP-BGP utiliza dos nuevas extensiones para intercambiar información de ruteo IPv6, que se describen en las RFC 2545 y 2848. Constituyen atributos no transitivos y llevan un conjunto de destinos alcanzables, inalcanzables e información del próximo salto que se transmiten en el paquete de actualización *update*. Los PEs Dual-S tack usan direcciones IPv6 mapeadas a IPv4 para conocer el alcance de los prefijos IPv6. El núcleo conmuta paquetes etiquetados, independientemente del tipo o contenido, basándose solamente en la etiqueta externa y es transparente para el tráfico IPv6. En la red IP/MPLS solo hay que hacer modificaciones en los PE y en los enrutadores reflectores, que deben ser actualizados para soportar Dual-Stack.
- 6VPE: es similar a la anterior en cuanto a principios teóricos, pero con la ventaja de mantener el tráfico segmentado en VPN, de modo que el cliente puede acceder tanto a VPNs IPv4 como IPv6. La diferencia con la solución 6PE radica en que 6VPE soporta diferentes VRF —*Virtual Routing Forwarding*—. Estas VRF son tablas de rutas para cada una de las VPN, que pueden ser VPN L3 Dual-Stack.

De las tecnologías mencionadas, se hizo un análisis de las más factibles a utilizar teniendo en cuenta el escenario cubano. Se llegó a la conclusión de

que Dual-Stack Lite en el entorno metropolitano, conjuntamente con 6PE y 6VPE, son las más factibles porque dependen del equipamiento que las soporte, entre otros factores.

Pruebas de campo de soluciones 6PE y 6VPE sobre la red IP/MPLS en Cuba

El plan de desarrollo de la Empresa de Telecomunicaciones de Cuba, S.A. (ETECSA) contempla un crecimiento de servicios mediante la óptima utilización de la infraestructura de telecomunicaciones existente. La Resolución 156 de 2008 del Ministerio de Comunicaciones dispone, entre otros aspectos, que se transporten señales entre islas IPv6 de extremo a extremo y se ofrezcan los servicios fundamentales relacionados con IPv6, previa conciliación con los órganos rectores correspondientes. Por este motivo, con nuevos enrutadores destinados a servir como BRAS y PE para servicios IPv4, pero con funcionalidades de IPv6, se realizaron las pruebas de este protocolo enfatizando las soluciones 6PE y 6VPE a fin de validar su comportamiento y ofrecer soluciones de transporte de tráfico IPv6 sobre el *backbone* IP/MPLS (Figura 1).

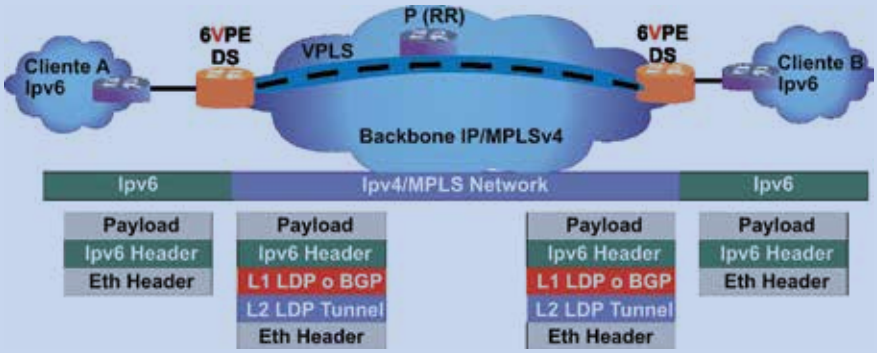

Figura 1. Solución 6VPE. (Fuente: Huawei[10]).

Previo a la realización de las pruebas de campo, se utilizó el simulador eNSP—empresarial *Network Simulation Platform*— para analizar el escenario bajo prueba y tener idea de los resultados a obtener con el equipamiento y el escenario real. Se capturaron paquetes en la interfaz de salida del PE1 hacia P1 (obsérvese el doble etiquetado en MPLS). Los resultados de la simulación fueron coherentes con los obtenidos en el escenario real (Figura 2).

Figura 2. Simulación de la solución 6VPE a través de un backbone IP/MPLS mediante la plataforma eNSP de Huawei. (Fuente: DCDT).

Para las pruebas con equipamiento real se utilizaron dos enrutadores con funcionalidades 6PE/6VPE en los bordes de la red, conectados a dos enrutadores de núcleo existentes. Con la ayuda de un instrumento generador de tráfico STC —*Spirent Test Center*— se transmitieron paquetes IPv6 de un sitio a otro. Como retorno, se dispuso un enlace a 100 Mbps a través de la red SDH —*Synchronous Digital Hierarchy*— (Figura 3). También, se introdujeron elementos adicionales en la red como DHCPv6, servidor AAA —*Authentication, Authorization and Accouunting*— y DNSv6 —*Domain Name Server*— para la prueba de servicios de banda ancha conmutada PPPoEv6. Se simuló Internet mediante una interfaz *loopback* en el extremo opuesto de la red.

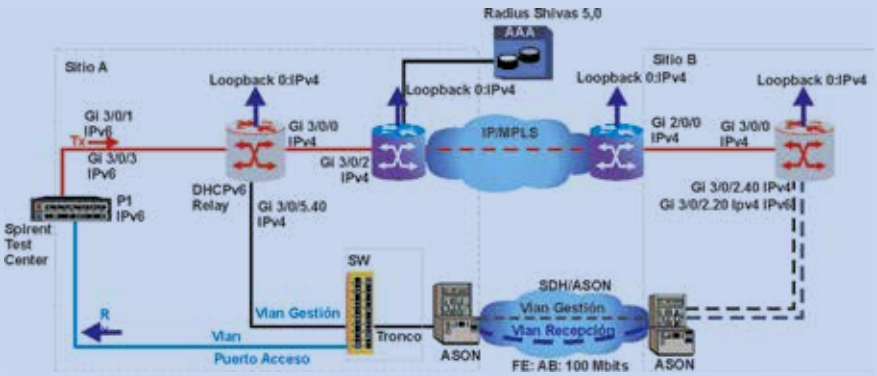

Figura 3. Esquema general de pruebas IPv6. (Fuente: DCDT).

Posteriormente, se comprobaron las funcionalidades básicas de enrutamiento, comenzando por el establecimiento de las rutas estáticas, seguido de la configuración del protocolo ISIS, al tiempo que se comprobaron sus dos nuevos TLV—*Type-Length-Value*—para transportar información de IPv6 —TLV 232 para el direccionamiento de la interfaz IPv6 y TLV 236 para alcanzar la red IPv6— mediante el prefijo de ruteo y la métrica. (Figura 4).

Con la funcionalidad de Dual-Stack para ISIS se anunciaron mediante el instrumento STC más de 1000 rutas IPv4 e IPv6 simultáneamente y se transmitió tráfico de extremo a extremo por estas rutas sin pérdida de paquetes. El propio instrumento colectó estadísticas de las tramas enviadas y dio cuenta de parámetros como demora, *jitter* y pérdida de paquetes.

Asimismo, se comprobó la funcionalidad de GR —*Graceful Restart*— en los protocolos ISIS y BGP4+. Esta funcionalidad permite, en caso de un fallo en el procesador central del enrutador, mantener inalterable la tabla de rutas durante un tiempo, proporcionando a la tarjeta de reserva tiempo suficiente para la conmutación sin afectar el servicio ni la topología lógica de la red, evitando el mecanismo de convergencia y el cálculo del protocolo de enrutamiento interno.

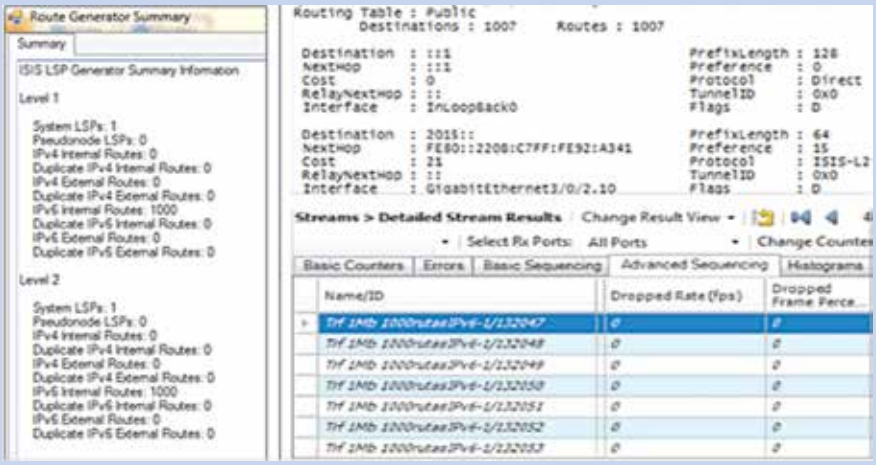

Figura 4. Generación de 1000 rutas IPv4 y 1000 IPv6. Fracción de la tabla de enrutamiento y resultados de pérdidas de paquetes con tráfico IPv6.(Fuente: DCDT).

Se configuró la funcionalidad de multitopología para el protocolo ISIS que permite que se ejecuten dos árboles de análisis del algoritmo SPF —*Short Path First*— de forma independiente, uno para IPv4 y otro para IPv6. Esto es necesario cuando existe más de una ruta para alcanzar un destino.

Con la ayuda del instrumento se probaron los servicios VPLS y VPN Dual-Stack así como PPPoEv4 y PPPoEv6 con doble marca de VLAN (Figura 5).

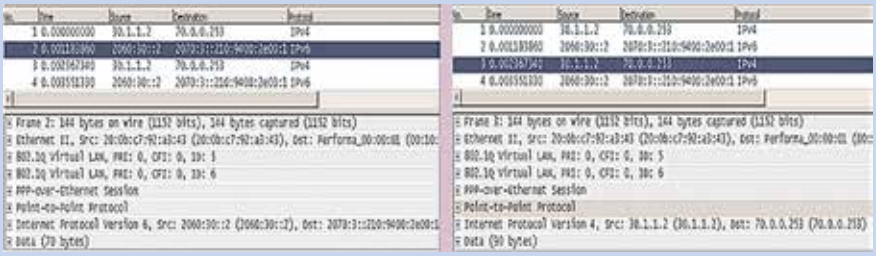

Figura 5. Sesiones simultáneas PPPoEv4 y PPPoEv6 generadas con el instrumento Spirent Test Center. (Fuente: DCDT).

Para que la solución 6PE funcione correctamente, hay que activar la familia IPv6 dentro del protocolo BGP4+ utilizando los pares (peers) IPv4 para establecer las relaciones de vecindad. BGP4+ transportará la información de enrutamiento obtenida por el protocolo de enrutamiento interno, ya sea OSPFv3 —*Open Short Path First*— o ISIS —*Intermediate System Intermediate System*— entre los enrutadores 6PE, utilizando como intermediarios a los enrutadores reflectores sobre los túneles establecidos por el protocolo LDP —*Label Distribution Protocol*— en MPLS. Las rutas IPv6 se almacenan en la tabla global del enrutador. La etiqueta interna la asigna el protocolo BGP4+, mientras que la externa la asigna el protocolo LDP. Con esta solución se

puede brindar transporte transparente entre islas IPv6 de un modo económico [10], [11].

La solución 6VPE tiene gran similitud a 6PE en cuanto a configuración. Debe activarse la familia IPv6 dentro del BGP4+, así como habilitar BGP4+ dentro de la VPN. Esta es la principal diferencia. Esto permite una mayor organización del tráfico y contribuye a reforzar la seguridad manteniendo el aislamiento entre las diferentes VPN. Cada una de ellas hace parecer a los clientes que disponen de una red independiente, cuando en realidad el medio es compartido por usuarios con VPNv4 y VPNv6. En este caso, la etiqueta interna la asignan los protocolos LDP o BGP4+, mientras que la externa, correspondiente al túnel, la asigna el protocolo LDP.

Sobre este tipo de solución pueden ofrecerse servicios de VPN L2 punto a punto, llamados también VLL —*Virtual Leased Line*— o punto-multipunto, como VPLS. La solución 6VPE es un poco más compleja de configurar que 6PE, pero ambas son económicamente factibles.

Mediante el empleo de las soluciones 6PE y 6VPE, se transmitió tráfico extremo a extremo a 100 Mbps con la ayuda del instrumento STC sin reportar pérdida de paquetes. Se probó el servicio FTP —*File Transfer Protocol*— para la descarga de contenidos educativos y se ejecutó una secuencia de más de 30 pruebas. Finalmente, se conectaron dos islas IPv6 pertenecientes a entidades del Ministerio de Educación Superior, durante más de tres meses para evaluar la estabilidad del servicio y su comportamiento (Figuras 6 y 7).

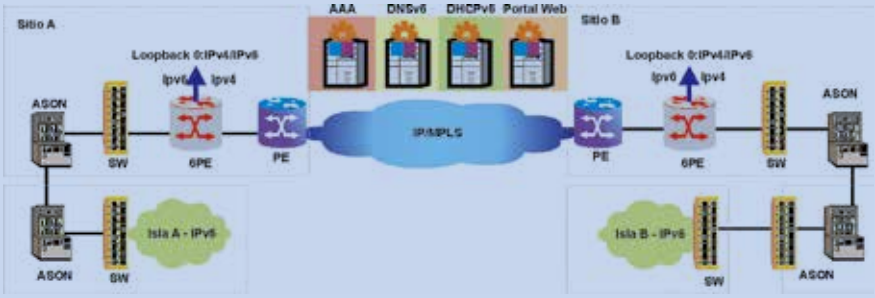

Figura 6. Islas IPv6 conectadas a 100 Mbps a través de la red IP/MPLS. (Fuente: DCDT).

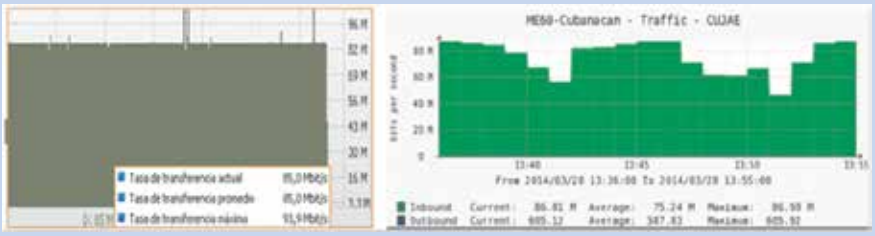

Figura 7. Tasas de transferencia de tráfico entre ambas islas IPv6. (Fuente: DCDT).

Se pudo concluir que en una etapa inicial es posible utilizar los métodos ya probados sobre el *backbone* IP/MPLS, 6PE y 6VPE, para la interconexión de universidades e instituciones de investigación. Para ofrecer servicio PPPoEv6 se emplean servidores DNSv6, DHCPv6 y AAA. Es preciso mantener vigilancia tecnológica sobre el sistema de gestión, provisión y supervisión ya que no estaban funcionando a plena capacidad durante la realización de las pruebas ejecutadas. Para el acceso a Internet se

dispone de bloques asignados por LACNIC —*Latin America & Caribbean Network Information Centre*— para este propósito. La capacitación y el entrenamiento del personal constituyen un punto importante para el mantenimiento de las redes y los servicios involucrados.

Proyección para la implementación

Luego de ejecutar estas pruebas sobre el *backbone* IP/MPLS con el instrumento STC, se planificó una segunda etapa con clientes reales para finales de 2015, con el objetivo de obtener experiencias en la prestación del servicio de extremo a extremo. De resultar satisfactorias estas pruebas, podría desplegarse IPv6 bajo las siguientes modalidades:

1. Servicio de transporte transparente entre islas IPv6 en el entorno nacional, utilizando preferentemente la solución 6VPE. Este servicio favorecería la conexión de universidades y centros de investigación a nivel nacional, por lo que se dispondría de una plataforma de red estable para desarrollar aplicaciones y contenidos sobre el nuevo protocolo, manteniendo este tráfico dentro de la VPN a fin de lograr la uniformidad y conservar el control del mismo.
2. Servicio de Internet IPv6. Este podría hacerse de manera dedicada o conmutada (PPPoE). Para ello deben resolverse a plenitud los problemas asociados a la seguridad, la gestión del equipamiento y la plataforma de provisión de servicios.

La secuencia de acciones para la implementación podría ser la siguiente: Aquellas regiones que dispongan de un 6PE/BRAS se conectarían directamente a través de redes metropolitanas Ethernet o mediante la red de transmisión SDH/ASON. Las que no dispongan de 6PE/BRAS deben utilizar la solución DS-Lite entre sus respectivos equipos de acceso a través de una VPLS —*Virtual Private LAN Services*— hasta la tarjeta CGN que también permite la funcionalidad DS-Lite y termina el túnel. Esta tarjeta pertenece al 6PE/BRAS. Como línea general, todo el equipamiento que se adquiera, ya sea de acceso o de núcleo, debe soportar el protocolo IPv6, con el fin de crear nuevas islas IPv6 y en un futuro acercar a las redes metro la funcionalidad de BRAS/CGN. Deben mejorarse las plataformas de provisión de servicios IPv6, así como la de gestión del equipamiento y la de seguridad, para disponer de los mecanismos adecuados de control. Desde el punto de vista del acceso a Internet deben anunciarse bloques de direcciones fuera del sistema autónomo y configurar las políticas de accesos en los enrutadores de borde. Los enlaces deben ser monitoreados para recolectar estadísticas de tráfico. Esta es una visión preliminar para ir ganando experiencias en el periodo de transición a IPv6.

Conclusiones

Mediante las pruebas realizadas, se demostró la aplicabilidad de los mecanismos de transición 6PE/6VPE sobre el IP/MPLS, lo que permitió el transporte transparente de tráfico entre islas IPv6. También se identificaron los elementos para ofrecer el servicio de banda ancha PPPoEv6, los referidos a la gestión integrada, supervisión y provisión, entre otros.

Se evidenció que es posible comenzar a desplegar IPv6 haciendo un uso racional de los recursos existentes con inversiones progresivas en función de las necesidades de crecimiento del servicio. En consecuencia, se requiere preparar al personal técnico con conocimientos avanzados de IPv6 a fin de optimizar la operación y el mantenimiento de las redes, así como de las aplicaciones y los servicios a implementar.

Referencias

[1] ICANN. Internet Corporation for Assigned Names and Numbers. Global Policy for the Allocation of the Remaining IPv4 Address Space.http://www.icann.org/en/resources/policy/global-addressing/remaining-ipv4. (accesoenero 14, 2014)

[2] ICANN. Internet Corporation for Assigned Names and Numbers. Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied. http://www.icann.org/en/news/press/releases/release-03feb11-en.pdf. (acceso enero 14, 2014).

[3] LACNIC.Fases de Agotamiento de IPv4. http://www.lacnic.net/web/lacnic/agotamiento-ipv4.(accesomayo 15, 2014).

[4] Fuller, V.; Li, T. RFC 4632. Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. 2006. http://www.rfc-editor.org/rfc/rfc4632.txt.(acceso mayo 15, 2014).

[5] Nesser II, P. RFC 1917. An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA. 1996. http://www.rfc-editor.org/rfc/rfc1917.txt. (acceso mayo 15, 2014).

[6] Droms, R. RFC 2131. Dynamic Host Configuration Protocol. http://www.rfc-editor.org/rfc/rfc2131.txt. 1997.(acceso enero 14, 2014).

[7] Srisuresh, P.; Egevang, K. RFC 3022. Traditional IP Network Address Translator (Traditional NAT). http://www.rfc-editor.org/rfc/rfc3022.txt. 2001.(acceso enero 14, 2014).

[8] Asoca, De Saram. Real World IPv6 Migration Solutions. http://www.cu.ipv6tf.org/pdf/Asoka%20De%20Saram%20-%20A10%20Rocky%20Mountatain%20IPv6%20Summit.pdf. 2011.(acceso enero 14, 2014).

[9] Kashimura, Yashuo. IPv6 Transition Technologies. http://www.cu.ipv6tf.org/pdf/Apricot_IPv6_transition_kashimura_rev3.pdf. 2011.(acceso enero 14, 2014).

[10] Huawei Technologies Co., Ltd. IPv6 HSI Service Operation and Maintenance Training. 2010. pp.77- 99.

[11] Huawei Technologies Co., Ltd. IPv6 HSI Service Planning. 2010. pp. 162 - 184.

[12] Huawei Technologies Co., Ltd. IPv6 Technology Principle Training. 2010. pp. 13 - 17.

[13] Leping, W. “Considerations and Practice of NGN”. Huawei Technologies (16), 4-12, 2005.

[14] Huiling, Z. & Bing, D. “Network Evolution -- View from NGN Practice of Global Carriers”. Huawei Technologies, 13-17. 2005.

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