XVII SIMPOSIO DE INGENIERÍA ELÉCTRICA (SIE-2017)

Soluciones técnicas para la implementación de IPv6 sobre una red.

Technical solutions for the implementation of IPv6 over a network.

Datos del autor

Nombre y Apellidos: *Ing. Anyell Quintero Infante*
Institución de Procedencia: Etecsa
País: Cuba
E-mail: anyell.quintero@etecsa.cu

Resumen

El presente trabajo desarrolla un estudio para la implementación del protocolo de internet versión 6 (IPv6 por sus siglas), sobre la red de transporte existente en ETECSA como solución a los problemas causados por el agotamiento de las direcciones de la versión anterior (IPv4 por sus siglas)

Se estudian los diferentes métodos que existen para lograr el despliegue de IPv6 en redes de telecomunicaciones llegando a profundizar en el despliegue especifico en redes IP/MPLS (Protocolo de Internet/ Multi-Protocolo de Conmutación mediante Etiquetas). Se evalúa la red desplegada con IPv4 donde se acomete la implementación de IPv6 revisando los posibles métodos que se pueden configurar bajo el requerimiento de no afectar a los clientes IPv4 actuales.

El objetivo principal de la investigación fue diseñar, simular e implementar varias soluciones para la implementación de IPv6 sobre una **red IP/MPLS con IPv4,** que sin impactar a los clientes existentes, permite ampliar las potencialidades de la red instalada soportando nuevos servicios. Se realiza propuesta de diferentes pasos para la implementación de IPv6 sobre una red IP/MPLS, se identifican métodos de migraciones posibles de aplicar en una red IP/MPLS con IPv4 y se logra realizar configuraciones en los elementos de red permitiendo la implementación de IPv6.

El simulador propietario de Huawei eNSP (Plataforma de simulación de red desarrollado por Huawei) se utiliza para el diseño y la simulación de la red, ya que el resultado permite utilizar las configuraciones en

los elementos de una red IP/MPLS con IPv4, logrando la implementación de los diferentes métodos sobre la red. Los métodos que se recomiendan a utilizar para la implementación de IPv6 sobre una red IP/MPLS con IPv4 son las siguientes: VPLS (Servicio de LAN privada virtual): sin modificación en los elementos de la red, 6PE (Mecanismo de transición a IPv6 en conmutadores de borde sobre redes IP/MPLS): generando modificación en los elementos PE (conmutadores de borde) de la red y 6VPE (VPN con IPv6 en los conmutadores de borde): combinando el manejo de IPv6 de 6PE con el manejo de VPN (red privada virtual) de IPv4 sobre MPLS. Todos permiten brindar servicios con soporte de IPv6 sobre una red IP/MPLS con IPv4.

Abstract:

The present work develops a study for the implementation of Internet protocol version 6 (IPv6), on the existing transport network in ETECSA as a solution to the problems caused by the exhaustion of the addresses of the previous version (IPv4 by its acronym)

The different methods that exist to achieve the deployment of IPv6 in telecommunication networks are studied, getting to deepen the specific deployment in IP / MPLS (Internet Protocol / Multi-Protocol of Tag Switching) networks. It evaluates the network deployed with IPv4 where the IPv6 implementation is undertaken reviewing the possible methods that can be configured under the requirement of not affecting the current IPv4 clients.

The main objective of the research was to design, simulate and implement several solutions for the implementation of IPv6 over an IP / MPLS network with IPv4, which without impacting existing clients, allows to extend the potential of the installed network supporting new services. A number of steps are proposed to implement IPv6 over an IP / MPLS network, identify possible migration methods to be applied in an IPv6 network with IPv4, and configure the network elements to allow IPv6 implementation.

The proprietary simulator of Huawei eNSP (Network simulation platform developed by Huawei) is used for the design and simulation of the network, since the result allows to use the configurations in the elements of an IP / MPLS network with IPv4, achieving the Implementation of the different methods on the network. The recommended methods to be used for the implementation of IPv6 over an IPv4 IPv4 network are the following: VPLS (Virtual Private LAN Service): without modification in the elements of the network, 6PE (IPv6 Transition Mechanism in Edge switches over IP / MPLS networks): generating change in the PE (edge switches) elements of the network and 6VPE (VPN with IPv6 in edge switches): combining 6 IPv6 management with VPN management (Virtual private network) over IPv4 over MPLS. All enable IPv6 support over an IP / MPLS network with IPv4.

Palabras Clave: despliegue de IPv6

Keywords: IPv6 deployment

1. Introducción

El crecimiento vertiginoso del número de usuarios y dispositivos que hacen uso de la Internet ha ocasionado un rápido agotamiento de las direcciones IPv4 (Protocolo de Internet versión 4), razón por la cual la implementación del protocolo IPv6 (Protocolo de Internet versión 6) ha generado un gran interés en Cuba y a nivel mundial. Actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

La red IP/MPLS del proveedor de servicios de telecomunicaciones de ETECSA tiene implementado IPv4, si se tiene en cuenta el agotamiento de las direcciones asignadas de IPv4 es imprescindible la preparación para la migración a IPv6[1].

A pesar de que otros países han desarrollado la red IP/MPLS con IPv6, las experiencias foráneas no se pueden aplicar en ningún proveedor de servicio sin evaluar el escenario existente de los servicios y la topología de red IP/MPLS con IPv4, por lo que se hace necesario simular e implementar las diferentes variantes de migración que se adecuan a las características de la red existente. Las características de IPv6 permiten que se adapte eficazmente a las demandas actuales y futuras de las redes. Las mejoras que proporciona IPv6 incluyen la simplificación del encabezado, lo que mejora el manejo de paquetes por parte de los enrutadores intermediarios y también proporciona compatibilidad para extensiones y opciones para aumentar la escalabilidad y la duración, la cantidad de direcciones IPv6 públicas no necesita traducción de direcciones de red y admite capacidades de autenticación y privacidad de forma nativa.

La situación problemática existente corresponde al agotamiento de las direcciones IPv4 que limita el incremento de servicios de transmisión de datos, generado por el programa de informatización de la sociedad, además se debe agregar que en la actualidad los usuarios demandan diversos servicios que requieren de mayor cantidad de direcciones por cada usuario.

Los retos que tiene el operador en la actualidad es la ampliación de los servicios en grandes magnitudes basado en proyectos enfocados a masificar el servicio de internet en los hogares, sitios públicos con tecnología inalámbrica y servicios de datos mediante los equipos terminales móviles, no dejando de visualizar la posibilidad de comenzar con la implementación de IoT (internet de las cosas)[2][3] como demandante de gran cantidad de direcciones IP.

Teniendo en cuenta los diferentes métodos existentes en la implementación de IPv6 sobre una red IP/MPLS y el impacto por la implementación sobre la red que está en servicio, resulta necesaria la simulación de los diferentes escenarios que permiten la migración basado en la topología actual debido al agotamiento de direcciones IPv4 y la posibilidad de brindar nuevos servicios. La necesidad de implementar las soluciones técnicas que se proponen permite la generalización de las mismas según los requerimientos de los usuarios de la red de telecomunicaciones.

2. Metodología

1.1 Características generales del IPv6

El IPv6 [4] es una evolución integral de IPv4, no una revolución. Incluye mejoras y resuelve los problemas existentes en IPv4, ver Anexo 1. Entre las características fundamentales o básicas de IPv6 pueden mencionarse que:

- El direccionamiento que es mucho más amplio, las direcciones pasan de 32 a 128 bits asignadas jerárquicamente. Estas direcciones son identificadores de 128 bits para interfaces y conjuntos de interfaces y son de tres tipos: unicast, anycast y multidifusión.
- En el nuevo proceso de direccionamiento hay un formato nuevo de encabezado en la estructura de las direcciones. Estas pasan de 14 campos alineados a 32 bits en la cabecera a 8 campos alineados a 64 bits para evitar la innecesaria redundancia de la información en IPv4.
- El encaminamiento es jerárquico mediante la agregación de rutas, donde las direcciones dependen estrictamente de la topología de la red. Las agregaciones pueden ser de dos tipos: una en que las direcciones son asignadas del rango de direcciones de cada proveedor y otra en que las direcciones dependen del punto de intercambio al que se conecten.
- La autoconfiguración se incluye en el protocolo base y se sustenta en el intento de la propia pila por auto configurarse y descubrir el camino de conexión a Internet. El proceso incluye la creación de una dirección de enlace local, la verificación de que no está duplicada en dicho enlace y la determinación de la información que ha de ser auto configurado. Existen dos tipos de autoconfiguración, una sin intervención y otra predeterminada.
- La movilidad es una característica obligatoria del IPv6, la cual posibilita que el usuario mantenga la misma dirección IP a pesar de su movilidad, es decir, independientemente del punto de conexión en que se encuentre en cada momento.

Para lograr que las características descritas anteriormente se logren en el despliegue de la red, los nodos IPv6 [5] tienen que almacenar la información de vinculación entre la dirección de partida y la posición

actual a modo de caché y, por lo tanto, serían capaces de enviar los paquetes destinados al nodo móvil directamente a su posición actual. El protocolo define nuevas opciones de destino, una de las cuales debe ser soportada, incluso, en paquetes recibidos por todos los nodos aunque no sean móviles. Otras características de esta nueva versión del protocolo son la versatilidad, que facilita un formato flexible de opciones y la extensión mejorada, la multimedia, que consiste en la identificación de flujos, el multidifusión, que permite el control de ámbitos, y la seguridad, que permite la autenticación y encriptación del protocolo base, además incluye IPsec y beneficia a todas las aplicaciones con ella.

1.1.1 Encabezado de IPv6

El encabezado de IPv4 sufre algunos cambios al dar lugar al encabezado de IPv6[7], algunos campos desaparecen, otros se modifican y aparecen nuevos. Puede observarse en la figura 1 los campos eliminados por el protocolo IPv6.

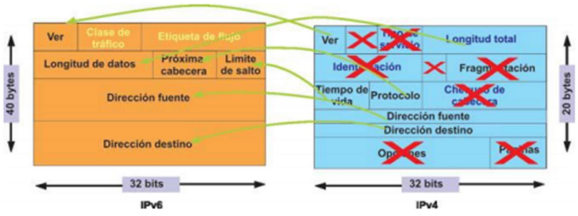

Figura 1 Estructura del paquete IP.
Fuente: http://tunnelingipv6.blogspot.com/2009/11/cabecera-ipv4-ipv6.html

Los campos renombrados son la longitud total por la longitud de datos que tiene un tamaño de 16 bits y puede llegar hasta 65 536 bytes, el protocolo por la próxima cabecera que tiene un tamaño de 8 bits y el tiempo de vida por el límite de salto el cual también tiene un tamaño de 8 bits. Aparecen dos campos nuevos: la clase de tráfico para funciones de prioridad y clase, y la etiqueta de flujo que permite tráficos con requerimientos de tiempo real, tiene longitud de 20 bits; ambos campos facilitan la Calidad de Servicio (QoS) y la Clase de Servicio (CoS). Los campos longitud de cabecera, tipo de servicio, chequeo de cabecera, opciones y relleno fueron eliminados en la nueva versión del protocolo IPv6 para evitar la redundancia innecesaria de la información; y las funciones de los campos identificación, banderas, fragmentación fueron trasladadas al encabezado extendido de fragmentación.

Se muestra en la figura 2, la estructura general que compone el paquete de ambas versiones de protocolos IP, que por mediación de los colores se muestran las diferencias de los campos, para su comprensión guíese en la leyenda.

Figura 2 Estructura del paquete IP y las diferencias entre IPv4 e IPv6
Fuente: http://www.obviomicrobio.com/content/ipv6-vs-ipv4

1.1.2 Diferencias entre IPv4 e IPv6

Las principales diferencias entre ambas versiones del protocolo, se presentan en la tabla 1, según IBM (International Business Machines Corp.) Knowledge Center[8].

Tabla 1 Diferencias entre IPv4 e IPv6.

Versión IP	IPv4	IPv6
Difundido	1981	1999
Tamaño de la dirección	Número de 32 bits	Número de 128 bits
Formato de la dirección	Notación decimal con puntos: 192.0.2.76	Notación Hexadecimal: 2001:0DB8:0234:AB00: 0123:4567:8901:ABCD
Número de Direcciones	2^{32} = 4,294,967,296	2^{128} = 340,282,366,920,938,463, 463,374,607,431,768,211,456
Ejemplos de Notación	192.0.2.0/24 10/8 (un bloque "/8" = 1/256[avo] del total de espacio de direcciones IPv4 = 2^{24}= 16,777,216 direcciones)	2001:0DB8:0234::/48 2600:0000::/12

Fuente: http://blogs.laprensagrafica.com/litoibarra/?p=954

Como elementos esenciales en las diferencias de ambas versiones del protocolo IP tenemos una clasificación que permite comprender con claridad aspectos importantes como son:

- Simplificación de los encabezados

La mejora más importante de IPv6 [9] es la simplificación de los encabezados de los datagramas. El encabezado del datagrama en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas. Aunque las direcciones en IPv6 son cuatro veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

- Seguridad

Todas las implementaciones de IPv6, en un futuro cercano, deben permitir la opción de utilizar IPsec, a diferencia de IPv4 en donde su implementación era opcional (aunque bastante usual), esto nos proporcionará más seguridad [10] para el tráfico de paquetes de datos en la red. [10]

- Conexiones más eficaces

Debido a que se utiliza una cabecera de paquete diferente en IPv6, añadiendo a los datos actuales (origen, tamaño, etc.) otros datos tales como etiquetas de contenido, permite optimizar las transferencias al poder dar prioridad a tipos determinados de archivos (por ejemplo, dar prioridad a los archivos del tipo multimedia o de voz), haciendo a la vez posible que sea el usuario el que decida estas prioridades.

- Multidifusión

La habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

- Autoconfiguración

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red ruteada en IPv6 usando los mensajes de descubrimiento de enrutadores de ICMPv6 (Internet Control Message Protocol versión 6). La primera vez que son conectados a una red, el nodo envía una solicitud usando multidifusión (routers solicitation) pidiendo los parámetros de configuración. Si los enrutadores están configurados para esto, responderán este requerimiento con un "anuncio de enrutador" (router advertisement) que contiene los parámetros de configuración de la capa de red.

- Desaparición de los NAT

Muchas organizaciones que no disponen de suficientes números IP deben utilizar direcciones privadas que apuntan a un único número IP o dirección pública, siendo preciso un NAT que dirija el flujo de datos desde la red interna a la exterior. Uno de los beneficios de IPv6 será la plena disponibilidad de números IP, así se elimina la necesidad del uso de los NAT debido a que hay disponibles direcciones IP de sobra, lo que permite que Internet vuelva a ser una red "entre extremos".

En la tabla 2 se muestra una comparación de las diferentes funciones en ambas versiones del protocolo IP, permitiendo relacionar la forma en que trabaja la nueva versión del protocolo IPv6 con su antecesor. [11]

Tabla 2 Funciones en ambas versiones del protocolo IP

Función	IPv4	IPv6
Asignación de direcciones	DHCPv4	DHCPv6, SLAAC, Reconfiguration
Resolución de direcciones	ARP, RARP	NS, NA (ICMPv6) *Neighbor Solicitation & Advertisement*
Descubrimiento de routers	ICMP Router Discovery	RS, RA (ICMPv6) *Router Solicitation & Advertisement*
Resolución de nombres	DNSv4	DNSv6

Fuente: http://ipv6-equipo5.blogspot.com/p/ipv4-vs-ipv6.html

En el Anexo 2 se plasma en forma de tabla la mayoría de las diferencias entre ambas versiones del protocolo de forma más detalladas. Las diferencias fueron marcadas según IBM de acuerdo a las diferentes clasificaciones identificadas.

1.1.3 RFC's relacionadas con el despliegue del protocolo IPv6

Se considera de gran importancia el estudio profundo del protocolo antes de su implementación para poder realizar configuraciones en los diferentes elementos de la red, para ello mostramos en la tabla 3 algunas RFC's (Requestfor Comments) del protocolo IPv6 que se consideraron las más significativas, según han sido aprobados por el IETF(Internet Engineering TaskForce). En el Anexo 3 se listan la mayoría de las RFC que están relacionados con la nueva versión del protocolo IP.

Tabla 3 Diferentes RFC's del protocolo IPv6

Clasificación	Documento	Título
Especificaciones Básicas	RFC2460 [11]	Especificaciones del Protocolo Internet Versión 6 (IPv6)
Direccionamiento	RFC 2373	Arquitectura de Direccionamiento en IPv6
Enrutador	RFC2080	RIP (*Routing Information Protocol*) para IPv6
DNS (*Domain Name System*)	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ethernet	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
Seguridad[10]	RFC2401	Arquitectura de Seguridad para IP
Multidifusión	RFC2375	Asignación de Direcciones Multidifusión
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
Transición	RFC1933	Mecanismos de Transición para Enrutadores y Hosts IPv6
API (*Application Programming Interface*)	RFC2292/bis	Advanced Sockets API para IPv6
MIB (Base de Información Gestionada)	RFC2452	Base de Información de Gestión para IPv6: TCP(*Transmission Control Protocol*)
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6

Fuente: http://www.consulintel.es/html/ForoIPv6/RFCs.htm

3. Resultados y discusión

1.2 Escenarios de Despliegue de IPv6 sobre redes IP/MPLS

El aspecto más importante dentro de la temática de IPv6 [12] lo constituye el proceso de migración, para lo cual existen algunos mecanismos de migración que permiten la integración o interacción de sistemas IPv4 con IPv6.

Existen varias maneras para entregar servicios IPv6 a los usuarios finales. La más utilizada es el envío de tráfico IPv6 de extremo a extremo[13]. IPv6 sobre IP/MPLS le permite a los dominios IPv6 aislados comunicarse con otros dominios similares empleando una red IP/MPLS con despliegue basado en IPv4. Los mecanismos más importantes para desplegar IPv6 sobre una red IP/MPLS con IPv4 se describen en el próximos epígrafes.[14]

1.2.1 Soporte nativo de IPv6 sobre IP/MPLS con IPv4

Es el método propuesto originalmente para obtener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en toda la red. De esta forma, cuando se establece una conexión hacia un destino sólo IPv4, ver la figura 3, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4 (si bien esto se ha ido modificando para solucionar problemas de time outs, ver —happyeyeballs).

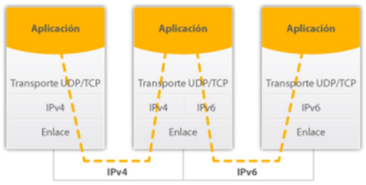

Figura 3 Implementación de IPv6 mediante la implementación de doble pila.
Fuente: https://gestionredes464324.wordpress.com/2013/04/29/osi-teorico-real-tcp-ip-modelo-tcpipel-tcpip-es-la/

Los aspectos fundamentales a tener en cuenta son que:

- La infraestructura de la red requiere actualizar completamente el Plano de Control hacia IPv6.
- Requiere enrutamiento IPv6 en el núcleo de la red.
- Requiere IPv6 LDP (Label Distribution Protocol) en el núcleo de la red.
- Una transición brusca introduce riesgos y costos adicionales para el PS (Proveedor de servicio).

1.2.2 Mecanismos de implementación de IPv6 sobre Túneles IPv4.

Los mecanismos más antiguos para poder atravesar redes que no tienen soporte nativo del protocolo que se está utilizando [15] son los túneles. En general se utilizan túneles encapsulando IPv6 dentro de IPv4, permitiendo de esta forma atravesar redes que no manejan IPv6, pero también podemos encontrar la situación inversa. Los paquetes originales son transportados hasta un punto de la red por medio del protocolo original, luego encapsulados para atravesar la porción de red que no lo soporta y luego des-encapsulados en el otro extremo para ser enviados al destino final en forma nativa. Los túneles manuales se deben configurar explícitamente en algún equipo de la red, mientras que los automáticos se configuran automáticamente en algunos sistemas operativos. En el caso de los primeros, podemos citar los túneles manuales entre dos equipos o mediante —tunnelbrokers‖. Dentro de los mecanismos podemos mencionar la técnica [14] conocida como IPv6 ProviderEdgeRouter (6PE) e IPv6 VPN (red privada virtual) Provider Edge (6VPE: Mecanismo para la implementación de IPv6 en redes IP/MPLS mediante la creación de VPN

con IPv6 en los conmutadores de borde), que se utiliza para encapsular el tráfico IPv6 por parte de los proveedores de servicio que tienen redes IP/MPLS con kkIPv4. Ver la figura 4.

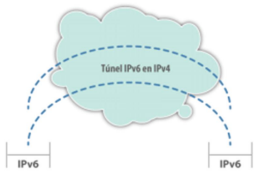

Figura 4 Implementación de IPv6 mediante la implementación de túnel.
Fuente: https://gestionredes464324.wordpress.com/2013/04/29/osi-teorico-real-tcp-ip-modelo-tcpipel-tcpip-es-la/

Esta estrategia no requiere cambios en los enrutadores P, porque se emplean túneles IPv4 para encapsular el tráfico IPv6; de tal manera que aparecería como tráfico IPv4 dentro de la red. [5] Sin embargo este método adolece de los constantes retos de escalabilidad que presentan las técnicas de túnel (la creación y el manejo de túneles, así como el enrutamiento de cada enrutador CE hacia otro enrutador CE).

En el caso particular de los mecanismos 6PE y 6VPE tenemos que soportan el servicio de alcance global con IPv6 y servicios VPN con IPv6 sobre una red IP/MPLS con IPv4. Estas estrategias han resultado muy atractivas para los proveedores que tienen en operación redes configuradas con IPv4, debido a las siguientes razones:

- No se requieren actualizaciones para los enrutadores P, por lo tanto se preserva la estabilidad del núcleo de la red, y se minimizan los costos de la operación.
- Permiten un despliegue gradual, actualizando solamente los enrutadores PE para que ofrezcan servicios IPv6 (y donde se empleen reflectores de rutas (RR) se actualizarán estos, 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 este sitio particular.
- Toman las ventajas de reenvío en el núcleo MPLS y su alto rendimiento.
- Garantizan que el tráfico IPv6 se beneficie automáticamente de las características avanzadas de IP/MPLS que pueden ser desplegadas en el núcleo, tales como FRR (Fast Reroute Techniques in RSVP (Resource Reservation Protocol)-TE), TE (Traffic Engineering), y MPLS QoS.

IPv6 Provider Edge (6PE)

La solución 6PE [16] utiliza el mismo paradigma transparente de enrutamiento y transporte para lograr accesibilidad global con IPv6, sobre el núcleo de una red IP/MPLS con IPv4 que no conoce de IPv6.

La diferencia clave es que la información de accesibilidad (reachability) que se anuncia entre los enrutadores PE vía MP-BGP (Multiprotocol Border Gateway Protocol) ya no emplea prefijos VPN con IPv4; sino que utiliza prefijos IPv6. De manera que los enrutadores PE deben ser actualizados a doble pila, y en lo adelante se denominarán 6PE. Ellos soportarán IPv6 (y típicamente IPv4) en las interfaces de acceso, pero soportarán solamente IPv4, e IPv4 IP/MPLS en las interfaces que apuntan al núcleo.

Los enrutadores P permanecen ajenos a IPv6 y tienen en funcionamiento el enrutamiento IPv4, y distribución de etiquetas IPv4. Esta arquitectura se muestra en la figura 5.

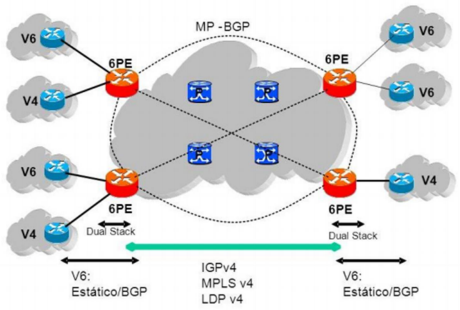

Figura 5 Arquitectura de una red IP/MPLS con implementación de 6PE.
Fuente: https://gestionredes464324.wordpress.com/2013/04/29/osi-teorico-real-tcp-ip-modelo-tcpipel-tcpip-es-la/

Una manera de entender la solución 6PE consiste en considerar que el núcleo IPv4 IP/MPLS transporta eficazmente el tráfico de una VPN adicional, cuyo tráfico y espacio de direcciones en este caso es IPv6. Tal como, en el caso de IPv4 VPNs, los enrutadores del núcleo permanecen ajenos de los enrutadores que pertenecen a esta VPN particular.

Nótese, sin embargo, que esta VPN especial no involucra los mecanismos de la RFC 2547bis[17] (tales como las VRF(*Virtual Routing and Forwarding*), los *route distinguishers*, y *route targets*), porque las tablas de rutas y encaminamientos de IPv6 están naturalmente separadas de las de IPv4.

IPv6 VPN Provider Edge (6VPE)

Al mecanismo mediante el cual se ofrecen los diferentes servicios se le denomina 6VPE, ver figura 6. La estrategia 6VPE combina —el manejo de IPv6 de 6PE con —el manejo de VPN[18] de IPv4 MPLS VPNs; para soportar tales servicios IPv6 VPN sobre un núcleo de la red IPv4 MPLS. Además de los servicios de conectividad global que pueden ser ofertados por la estrategia 6PE, los PS eran cuestionados por sus clientes acerca de la posibilidad de ofrecer servicios IPv6 VPN y con esta solución se resuelve esta situación.

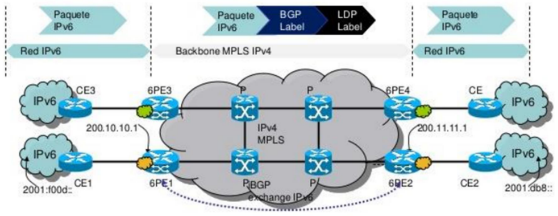

Figura 6 Ejemplo de escenario de una red IP/MPLS con mecanismo 6VPE
Fuente: https://gestionredes464324.wordpress.com/2013/04/29/osi-teorico-real-tcp-ip-modelo-tcpipel-tcpip-es-la/

Las nuevas características de 6VPE respecto a 6PE se expresan a continuación:
- Se emplea una familia de direcciones diferentes para 6VPE en MP-BGP, la cual se denomina: familia de direcciones VPN-IPv6 (*Address Family Identifier* AFI=2 para —IPv6‖, *Sub Address Family Identifier* SAFI=128 para —VPN etiquetadas‖). Una dirección VPN-IPv6 es una entidad de 24 *bytes*, que comienza con el *router distinguisher* (RD) de 8 *bytes*, y termina con la dirección IPv6 de 16 bytes. **El** papel y codificación de las RD es exactamente igual que las VPN con IPv4.

- Se emplea el concepto de VRF de la arquitectura capa 3 MPLS VPN, en la cual cada VPN tiene un conjunto separado de tablas de rutas y encaminamientos, junto con todos los mecanismos asociados al control de la importación y exportación de rutas hacia adentro, y hacia fuera de las VRFs, incluyendo el etiquetado de las rutas con los *route targets*.

- La estrategia 6VPE produce los mismos beneficios que 6PE. Por ejemplo, como en 6PE, solamente los enrutadores PE que realmente conectan servicios IPv6 VPN necesitan ser actualizados para soportar IPv6 y las funcionalidades 6VPE.

De esta manera el PS puede también introducir servicios IPv6 VPN sin la necesidad de ser actualizados, ni de cambios de configuración en los enrutadores de núcleo.

1.2.3 Mecanismos de traducción de protocolos

Esta técnica consiste en utilizar algún dispositivo en la red que convierta los paquetes de IPv4 a IPv6 y viceversa. Ese dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos para permitir la comunicación.

Dentro de esta clasificación podemos mencionar NAT64/DNS64: la red es IPv6 nativa y para alcanzar los sitios que son sólo IPv4 se realiza una traducción al estilo NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96. Es necesario también utilizar una modificación al DNS, ver figura 7, llamada DNS64, que permite generar un registro AAAA (Familia de protocolo que corresponde con autenticación, autorización, contabilización y auditoría) aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A). Una de las propuestas iniciales de mecanismos de traducción fue NAT-PT (Traducción de la Dirección de Red/Traducción de Protocolo) (RFC 2766), que al día de hoy ha sido desaconsejado debido a sus fallas (ver RFC 4966) y ha sido reclasificado como —históricoll por la IETF.

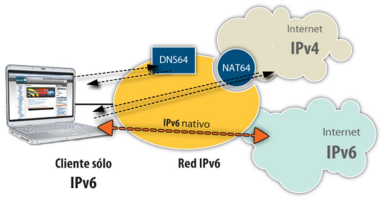

Figura 7 Ejemplo de mecanismo de traducción.
Fuente: https://gestionredes464324.wordpress.com/2013/04/29/osi-teorico-real-tcp-ip-modelo-tcpipel-tcpip-es-la/

A continuación se relacionan los principales mecanismos de traducción que se encuentran bajo análisis por la IETF:

- *Network Address Translation-Protocol Translation (NAT-PT)*
- TCP-UDP(*User Datagram Protocol*) *Relay*
- *Bump-in-the-Stack* (BIS).

- Doble pila *Transition Mechanism* (DSTM)

- *SOCKS(*protocolo de Internet que permite a las aplicaciones Cliente-servidor *--Based Gateway*

Por parte de la comunidad de telecomunicaciones no recomiendan este método por lo complejo que resulta su implementación y las complejas configuraciones en todos los dispositivos, además de tener en

cuenta que aplicaciones se utilizan en la comunicación sin presentar algún tipo de problema en el mecanismo de traducción de ambas cabeceras.

4. Conclusiones

La descripción de los antecedentes, características e implementación del protocolo IPv6 permiten desarrollar un documento auto contenido de consulta para un proveedor de servicio que se plantee migrar una red IP/MPLS con IPv4 a IPv6.

La migración a IPv6 no es trivial, por lo que requiere que el personal técnico encargado del proceso cuente con una preparación técnica en niveles medio y avanzado para enfrentar el proceso de migración.

Se requiere evaluar al personal técnico capacitado en IPv6, lo que permitirá contar con la efectividad de la preparación realizada y pueda enfrentar el proceso de migración sin contratiempos.
Las RFC de mayor relevancia e imprescindible para el dominio del despliegue del protocolo IPv6 son la RFC2740 donde describe en términos de enrutamiento como funciona OSPF para IPv6 y la RFC1886 que establece las extensiones DNS para soportar IPv6.

La importancia que revierte el conocimiento técnico de los diferentes métodos que existen para llevar a cabo la migración, representan el éxito del Proveedor de Servicio en el proceso de implementación, donde se evalúa la factibilidad del despliegue, según las redes desplegadas o en fase de implementación. En estos momentos el método más desplegado en redes en servicio se plantea que es el de túneles, pero el óptimo con vistas al futuro es considerado el método de doble pila, que permite contar con elementos de red que manejan ambas versiones del protocolo IP.

5. Referencias bibliográficas

."Huawei" http://www.huawei.com/en/. Implementaciones de Ipv6 en redes de telecomunicaciones del proveedor Huawei.

2. "Initial Ipv6 Configuration for Cisco IoS ".

3. "Internet Protocol V6 (Ipv6) Feature Overview and Configuration Guide." ALLIET TELESIS.

4. "State management in IPv4 to IPv6 transition." Yong Cui; Yuchi Chen; Jiangchuan Liu; Yiu-leung Lee. (2015).

5. "Ipv6 Addressing and Subnetting Workbook." 1: 61.
6. "Ipv6-Addressing-and-Subnetting-Workbook." 1, 61.
7. "Portal Ipv6 En Cuba" http://www.cu.ipv6tf.org/.
8. "Protocolo De Internet Versión 6." 41.
9. "2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)." S. Aravind; G. Padmavathi (2015).
10. *IP Addressing & Subnetting Inc Ipv6: Including Ipv6*: Elsevier Science, 2000.
11. "Ejemplo De Configuración Del Ipv6 Del Eigrp." (2015): 4.
12. *Ipv6 Best Practices*, 2015.
13. "Ipv6 Routing Protocols " *ISP Workshops*, (2015).
14. "Ibm Knowledge Center" http://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzai2/rzai2compipv4ipv6.htm.
15. "Internet Protocol V6 (Ipv6)." *Allied Telesis* 1 , (2016): 23.
16. "Internet Protocol Version 6: Ipv6 for Consumers." (2016).
17. "Ipv6 Address" https://www.cloudflare.com/ipv6/ (accessed 1/6/2016 2016).
18. "Ipv6, Un Muy Buen Negocio Para Ampliar Clientes." (2016).
19. Portal IPv6 en Cuba. Available from: http://www.cu.ipv6tf.org/.
20. Sergey I. Nikolenko, K.K., G´abor R´etv´ari, Erika R. B´erczi-Kov and Alexander Shalimov How to Represent IPv6 Forwarding Tables on IPv4 or MPLS Dataplanes. 2016. 6.
21. Grossetete, M.T.a.P., IPv6 Integration and Coexistence Strategies for Next-Generation Networks. IEEE Communications Magazine, 2004: p. 9.