ISSN: 1692-7257 - Volumen 2 – Número 32 - 2018

Revista Colombiana de Tecnologías de Avanzada

Recibido: 16 de marzo de 2018
Aceptado: 18 de abril de 2018

TRANSICIÓN DE IPv4 A IPv6: REVISION

TRANSITION FROM IPV4 TO IPV6: REVIEW

MSc. (c) Yesica Maria Pérez Pérez [*], MSc Andrés Mauricio Puentes Velásquez[**]

[*]**Universidad Francisco de Paula Santander Ocaña,** Facultad de Ingenierías, Grupo de Investigación En Desarrollo Tecnológico en Ingeniería GITYD.
Vía Acolsure, Sede Algodonal, Ocaña, Norte de Santander,
Ocaña, Norte de Santander, Colombia.+575690088.
E-mail: {ymperezp, ampuentesv}@ufpso.edu.co.

Resumen: Es primordial tener claro las incidencias positivas y negativas de implementar un nuevo protocolo base a toda la operación empresarial, y fundamental para la comunicación en red dentro de la compañía. El proceso aún parece complejo y al no verse forzados a realizar el cambio muchas empresas no lo han hecho de forma espontánea por lo que hasta el momento no tienen claro cuándo y cómo harían esta migración, ya que no han visto claramente las ventajas de implementar la nueva versión o porque no existe una forma clara de realizar la implementación sin generar un gran impacto sobre la operación de la red empresarial. La presente revisión se centró en las metodologías, modelos y buenas prácticas seguras aplicadas para la transición de IPV4 a IPV6 y los desafíos claves que surgen de la escasez de direcciones.

Palabras clave: IPV4, IPV6, Transición entre IPV4 a IPV6, Seguridad en IPV6.

Abstract: It is essential to be clear about the positive and negative incidences of implementing a new protocol based on the entire business operation, and fundamental for red communication within the company. The process still seems to be complex and there is no verse to make the change of many companies, it has not been done spontaneously so up to now they are not clear when and how they would do this migration, which was no longer clearly seen. advantages of implementing the new version or because there is no clear way to implement the implementation without generating a great impact on the operation of the business enterprise. In the present review, it focused on the methodologies, models and good practices applied to the transition from IPV4 to IPV6 and the key challenges that arise from the lack of addresses..

Keywords: IPV4, IPV6, Transition from IPV4 to IPV6, IPv6 Security.

1. INTRODUCCIÓN

El Protocolo de Internet (IP) permite la comunicación entre dispositivos pertenecientes a diferentes redes, asignando a cada dispositivo dentro de una red un identificador único. Independiente de las tecnologías usadas, cada dispositivo debe tener una dirección IP para que internet funcione (Levin & Schmidt, 2014); éstas direcciones se han venido asignando utilizando el

protocolo de internet versión cuatro (IPv4), el gran problema es que el número de direcciones que éste permite proveer es limitado. Según lo anunciado por El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) se agotó el stock de direcciones de IPv4 para el sector (Cicileo, 2017), exponiendo su preocupación por la demora de los gobiernos y operadores en el despliegue e implementación del protocolo IPV6 para garantizar la operatividad de los dispositivos actuales y futuros en Internet.

Debido a las escasez de direcciones IPv4, LACNIC comenzó a emitir políticas restrictivas para la entrega de recursos de Internet en el continente, entregando cantidades muy pequeñas de direcciones para solo nuevos contratantes, la opción para los antiguos contratantes es la transferencia por bloques entre ellos (Rojas, 2017).

El 6 de junio del 2012 marcó el comienzo de una implementación coordinada por los principales proveedores de equipamiento de servicios de internet, a pesar de esto, en la actualidad es baja la adopción de IPv6 en internet de forma continua; según las estadísticas arrojadas por Google (Díaz, 2017), a finales del 2017 solo el 21.44% de usuarios acceden a internet por medio del protocolo.

En cada país se crean políticas públicas para incentivar el despliegue de IPv6 a manera de regulaciones gubernamentales, esta situación ha sido detectada por nuevas empresas que ofrecen servicios de internet, las cuales han destacado como una prioridad la implementación de tecnologías asociadas a IPv6 en su modelo de negocio. Según cifras de Google (Google IPv6, 2017), en Colombia en el año 2018, el tráfico para acceso a internet proveniente de equipos con IPv6 fue el 0.42%; este índice de adopción tan bajo podría entenderse por la complejidad de tener que dejar atrás un protocolo que nos ha acompañado desde el año 1981 y que se compenetra con gran cantidad de aplicaciones y servicios.

El proceso de transición aún resulta complejo desde el punto de vista de las empresas por las siguientes razones: al no verse forzadas a realizar el cambio muchas no lo han hecho de forma espontánea; no tienen claridad acerca de cuándo y cómo harían esta migración; desconocen las ventajas de implementar la nueva versión; no hay claridad sobre una forma de realizar la implementación sin generar un gran impacto sobre la operación de la red empresarial.

Uno de los aspectos que despierta más incertidumbre y temores en la comunidad empresarial es la seguridad, sin lugar a dudas debe ser considerado como prioritario dentro de la implementación de IPv6, surgiendo inquietudes acerca de qué ocurrirá con los controles que ya están implementados, si son o no interoperables con esta nueva versión o si la organización está expuesta a mayor número de ataques.

2. METODO

La presente revisión es de tipo narrativo. Partiendo de una descripción general del panorama de la transición de IPv4 a IPv6 resaltando aspectos de tipo técnico, escenarios y aplicabilidad. Para su elaboración se consultaron las bases de datos hemerográficas referenciales o de texto completo como Scopus, Science Direct y la Especializada IEEE, respecto a la estrategia de búsqueda los principales punto de acceso fueron título del artículo, palabras clave y fecha. Se seleccionaron 40 que abordan dentro de sus contenidos temas asociados a metodologías de transición de IPv4 a IPv6 con componentes de seguridad.

3. DESARROLLO DEL TEMA

3.1 Protocolo de Internet versión 4 (IPV4)

El sistema de direccionamiento actual fue desplegado el 1 de enero de 1983 y utiliza 32 bits digitales para representar direcciones (UIT, recuperado 2017) con un límite total de 4.3 billones de direcciones, el espacio total de IPV4 es gestionado por la Autoridad de Asignación de Número de Internet (IANA) a nivel mundial, en los inicios antes de que se regula la asignación se entregaban direcciones de gran espacio por tanto fue necesario crear los 5 registros regionales de internet (RIR) todas los RIR son organizaciones sin fines de lucro (ARIN, recuperado 2017). La política de asignación de IPv4 ha evolucionado significativamente o se ha "reforzado" con el tiempo, con la creación de los cinco RIR desde 1990 y las decisiones de política impuestas por RIR, como el uso del enrutamiento entre dominios sin clase (CIDR), el pago de membresía y el cumplir con los aranceles de los RIR, la evaluación basada en las necesidades y fomentar el uso de la traducción de direcciones de red (NAT), por poner algunos ejemplos (WT/ICT, 2013).

3.2 Protocolo de Internet Versión 6 (IPv6)

IPv6 (Protocolo de Internet, versión 6) fue desarrollado para resolver la crisis del agotamiento de IPv4. Utiliza 128 bits para representar direcciones, lo que genera un espacio equivalente a unos 340 undecillones, o más de 7.9x1028 veces más direcciones que IPv4. Para dar una idea más tangible de la escala, algunos han comparado la cantidad de direcciones IPv6 disponibles con la cantidad de granos de arena en el planeta. Al igual que con IPv4, el espacio de direcciones IPv6 es administrado por IANA y los RIR siguiendo una política similar de "primero en llegar, primero en ser atendido", vinculada al concepto de "necesidad demostrada". Aunque la dirección IPv6 se asigna generosamente en bloques gigantes, a partir de marzo de 2013 solo se utiliza una pequeña fracción (menos de 0,0002%) del espacio total de direcciones IPv6.
En vista del desequilibrio histórico de la distribución de direcciones IPv4 en todo el mundo, el informe de 2005 del Grupo de trabajo de la cumbre mundial sobre la sociedad de la información (CMSI) y el grupo de trabajo sobre Gobernanza de Internet (WGIG) reconoció que "se requiere la gestión de numeración actual para garantizar la distribución equitativa de los recursos y el acceso para todos en el futuro". Algunos han expresado su preocupación de que la política que llevó a la ocupación de una porción sustancial del conjunto finito de direcciones IPv4 ('direcciones IPv4 heredadas') por entidades más adineradas 'expertas en tecnología' pueda volver a funcionar contra los nuevos participantes que buscan asignaciones de direcciones IPv6, especialmente en los países en desarrollo.

Otros creen que dado que el espacio de direcciones IPv6 es virtualmente inagotable, esta "cuasi-inagotabilidad" significa que cualquier problema pasado con respecto a los desequilibrios no surgirá en el futuro y, por lo tanto, las políticas de asignación actuales de los RIR se pueden mantener sin cambios para IPv6. Los que apoyan esta vista también notan que en IPv6 las políticas de asignación de direcciones se aplicaron desde el comienzo de la asignación, mientras que las políticas de IPv4 se desarrollaron retrospectivamente.

3.2.1 Seguridad en IPV6

A medida de que crece la tecnología crecen las amenazas y se abren nuevos campos de estudio, abordar estos desafíos requiere de constancia y proponer nuevas políticas de seguridad, protocolos y modelos. La computación en la nube es un nuevo paradigma de tecnología emergente como lo definen Khalil, Khreishah, Bouktif & Ahmad, (2013) proporcionando un estudio exhaustivo de la seguridad de la computación en la nube el cual clasificó las amenazas de seguridad conocidas y las prácticas existentes para controlarlas.

Según Choudhary & Sekelsky (2010) se debe proteger la infraestructura crítica la cual incluye infraestructura física y de información y comunicaciones; pero antes se deben identificar las amenazas principales como son las vulnerabilidades específicas de IPv6 que debilitan la seguridad de la infraestructura de red y sectores de infraestructura crítica que dependen de IPv6 (Choudhary & Sekelsky, 2010).

En la próxima década se implementarán en varios países de Latinoamérica cambios tecnológicos muy importantes como las elecciones a través del voto electrónico, lo cual tendrá dos características fundamentales de operación: preservar los principios de seguridad de la información tanto en el proceso como en los resultados, y garantizar la disponibilidad y conectividad en la infraestructura de comunicaciones; para este último aspecto se requiere que las nuevas implementaciones tengan en cuenta el despliegue de IPv6.

Según (Isabel & Satizábal) “los usuarios suelen desconfiar de la seguridad de estos sistemas, especialmente cuando el voto se realiza, de manera remota, a través de una red pública como Internet.”

3.2.2 Creación de políticas publicas para incentivar el despliegue IPv6

Incentivar el despliegue de IPv6 ha sido tarea impulsada por los gobiernos, los cuáles planifican y establecen los plazos de entrega para que las distintas entidades gubernamentales adopten IPv6.

En Colombia el Ministerio de las TIC ha emitido dos documentos de lineamientos referentes a IPv6 que pueden ser considerados como buenas practicas para la región, como lo son: La guía de transición de IPv4 a IPv6 y la Guía para el Aseguramiento del protocolo IPv6 los cuales están fundamentados en la seguridad y la privacidad de la información por medio de un marco de referencia que facilita el proceso de transición de IPV4 a IPV6 definiendo el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6,

trazando como objetivo facilitar e incentivar la adopción y el despliegue del protocolo IPv6. Como segunda medida MINTIC presenta una resolución donde define un plazo de adopción para las entidades estatales las cuales deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a mas tardar el 31 de diciembre de 2019 (MINTIC, 2017).

A medida que surgen las necesidades de los operadores de redes respecto a la implementación de IPv6, deben buscar mecanismos de transición viables y posteriormente hacer planes de transición factibles con el objetivo de cubrir la demanda de los clientes

El ministerio de las tecnologías de la información y las comunicaciones de Colombia define los lineamientos para que las entidades públicas comiencen el proceso técnico y metodológico de transición tecnológica, de manera que no se generen traumatismos ni afectación en la continuidad de los servicios.

A nivel general, se establece por el MINTIC un modelo de referencia para la adopción de IPv6 (gráfica 1), donde se sugiere que la infraestructura de TI debe ser la base del proceso de adopción de IPv6, y el camino a la adopción debe tener en cuenta tres componentes importantes: el normativo, la planeación (administrativa y tecnológica) y la implementación tecnológica

Gráfica 1. Modelo de referencia adopción IPv6

Fuente: MinTIC. Guía de transición de IPv4 a IPv6 para Colombia.

Una primera fase del modelo de transición planteado por el MinTIC, establece que se debe contemplar el diagnóstico real del estado tecnológico de la organización, donde se especifiquen aspectos como la topología de red actual y proyección de crecimiento a futuro, inventario de software y hardware, pruebas de validación de aplicativos y de comunicaciones, identificando de manera general esquemas de seguridad de la información y las comunicaciones, es en este punto donde se plantea un nivel de especificidad más alto de los requerimientos de seguridad de acuerdo a la realidad de cada organización.

El Instituto Federal de Telecomunicaciones (IFT), Mexico ha realizado algunas recomendaciones sobre el Internet de las Cosas (IoT) y con las redes IPv6 dentro del IFT como fuera del mismo (Diaz, 2017)

El Ministerio de Comunicaciones de CUBA ha emitido diversas normativas para el despliegue de IPv6 en Cuba, dentro de ellas se encuentra la resolucion Nº. 181 del 2016 por la cual constituye la base para la preparacion progresiva al protocolo IPv6 definiendo etapas y tareas que deben contemplar las personas juridicas en el territorio nacional. (Diaz, 2017).

La Corporación Nacional de Telecomunicaciones E.P. (CNT) de Ecuador adoptó la decisión estratégica temprana de desplegar IPv6, impulsada por dos acuerdos del Ministerio de Telecomunicaciones y Sociedad de la Información de 2011 y 2012 destinados al desarrollo de redes IPv6 en el Ecuador, y por la escasez prevista en el stock de direcciones IPv4 (Diaz, 2017).

EL Instituto Dominicano de Telecomunicaciones INDOTEL ha resuelto exhortar el despliegue del protocolo IPv6 en la República Dominicana por Resolución No. 021/15 de julio de 2015 adoptando un plan de trabajo que tiene como ejes principales: crear el sentido de urgencia, desarrollar acciones de capacitación y concientización, trabajar en conjunto con todas las partes interesadas e impulsar el despliegue de IPv6 en las instituciones del Estado (Diaz, 2017)

Al igual que Colombia y Cuba establecen la adopción por medio de resoluciones en Perú la Secretaria de Gobierno Digital (SEGDI) crea el Decreto Nº 081-2017 – PCM que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública de manera tal que se inicie un proceso de modernización progresiva con un plazo de 4 años. (Diaz, 2017).

Las Organizaciones Intergubernamentales OEA por medio de la Comision Interamericana de Telecomunicaciones (CITEL) invita a los estados miembros a que convoquen a los RIR, comunidades tecnicas locales y a las redes nacionales de educacion e investigación (RNEIs) y la industria a

fortalecer conocimiento y compartir información que incentive el despliegue de IPv6; como segunda medida elaborar maunuales de pautas y estrategias de transicion a IPv6 tomando las mejores practicas de la región de las Americas y otras regiones miembros del CITEL con el apoyo de los registros Regionales de Internet (LACNIC y ARIN) (Cicileo, 2017). Por parte de la Union Internacional de Telecomunicaciones UIT invita a los estados miembros y los miembros de sector a participar en el trabajo actual , aumentar la sensibilizacion a nivel nacional, regional e internacional acordando medios para una mayor colaboracion y coordinanacion entre la UIT y las Organizaciones pertinentes en pro del futuro del internet. (Diaz, 2017)

3.3 Técnicas de transición de IPV4 a IPV6

Debido a que IPv6 se diseñó sin compatibilidad, la transición de IPv4 a IPv6 necesita esencialmente una fase de "doble pila" durante la cual los hosts operen con ambas pilas de protocolos al mismo tiempo, utilizando la pila de protocolos IPv6 para hablar con otros hosts IPv6 y la pila de protocolos IPv4 a otros hosts IPv4. La disponibilidad (o la falta de ella) de direcciones IPv4 es, por lo tanto, un factor que continúa siendo importante durante el período de transición. Por el momento, no hay certeza sobre la duración de esta transición IPv4 / IPv6, expertos de LACNIC temen que el tiempo de esta transición se extienda indefinidamente.

En el momento de crear el protocolo IPv6 uno de los factores importantes fue poder hacer una transición del anterior protocolo IPv4 al nuevo protocolo IPv6, con este objetivo se diseñaron diversos medios para ayudar a su coexistencia mientras se hace una migración completa a IPv6.

Los medios diseñados están clasificados de forma general entre los mecanismos de transición de acuerdo al tipo de técnica utilizada: *Dual Stack*, Túneles y Traducción (LACNIC).

En el caso de *Dual Stack* operan de forma simultánea IPv4 e IPv6, desplegando ambos protocolos completamente, cada protocolo de enrutamiento debe llevar los prefijos correspondientes a cada tecnología de forma transparente para el usuario. Su mayor desventaja es que requiere de equipamiento completo que soporte a ambos protocolos. (Portal IPv6 Cuba)

Los Túneles permiten enviar paquetes IPv6 dentro de paquetes IPv4 y viceversa. En la actualidad, Internet es básicamente una red IPv4 con algunas islas IPv6 por lo general hoy en día el trafico IPv6 viaja encapsulado en paquetes IPv4. Existen diferentes tipos de túneles empleado tecnologías de trafico, entre ellas trafico IPv4 encapsulado en trafico IPv6 (4in6), trafico IPv6 encapsulado en trafico IPv4 (6in4), transmitir paquetes IPv6 entre 2 nodos *Dual Stack* empleando una red IPv4 que permita multidifusión (6over4), tráfico IPv6 sobre una red IPv4 sin la necesidad de configurar túneles de forma explícita (6to4), el caso de 6rd se deriva de 6to4 proponiendo realizar el despliegue de relays 6rd dentro de la infraestructura de un ISP, ISATAP son mecanismos que permiten intercambio de trafico entre nodos dual stack empleando una red IPv4, Teredo ofrece conectividad IPv6 total a nodos IPv4 que no tienen conexión directa con una red IPv6 el cual tiene como característica que funciona eficientemente detrás de NATs y emplea protocolos UDP, Los *Tunnel Setup Protocol* (STP) permiten negociar los parámetros de conexión de un cliente y un servidor, IPv6 *Tunnel Broker* provee conectividad IPv6 a usuarios finales o redes quienes son identificados por medio del identificador 41 en el campo tipo de protocolo de IPv4, final mente *Softwires* que son mecanismos que permiten la coexistencia de protocolos como 6rd o *DL-Lite* para proveer conectividad IPv6 en redes IPv4 puras. (Portal IPv6 CUBA)

Dentro de las técnicas de traducción que mas se usan se encuentra *Stateless IP/ICMP Translation* (SIIT) la cual realiza traducción de encabezados IPv6 a IPv4 y Viceversa, también encontramos DNS64 que es un mecanismo que entrega a los clientes IPv6 un registro AAAA aun si existe un registro A, *Stateless NAT64* es otro mecanismo que permite traslación de direcciones IPv6 a IPv4 pero garantiza una correspondencia uno a uno en lugar de uno a mucho, y finalmente el *Translator* (TRT) funciona como el tradicional NAT-PT pero a su diferencia requiere de traducciones de DNS de registros AAAA a registro A. (Portal IPv6 CUBA)

3.4 Algunos casos de Éxito en la implementación de IPv6.

LACNIC ha concentrado sus fuerzas en incentivar la adopción del protocolo IPv6 encontrando eco en profesionales y organizaciones de América Latina y el Caribe; en el caso del Telecentro Argentina desde septiembre del 2017 todos sus clientes están con *Dual Stack* obteniendo más de 35.000 clientes con *IPv6* y en crecimiento constante de su trafico y un 100% habilitado IPv6 afirmo Alejandro D'egidio,

jefe de Ingeniería de *Backbone* de Telecentro Argentina para LACNIC News (LACNIC, 2017).

Comcast Corporation ofrece servicios televisivos por cable, internet y telefonía, comenzaron su programa de IPv6 aproximadamente hace 10 años donde planificaron un despliegue incremental logrando que hoy en día su red soportara IPv6; como primera fase desplegaron 6to4 el cual permite enviar paquetes IPv6 sobre redes IPv4 omitiendo la necesidad de configurar túneles manualmente, en su segunda fase para facilitar el despliegue rápido de IPv6 utilizaron 6RD el cual se deriva de 6to4 con el cambio de que opera por completo dentro de la red del Proveedor de servicios ISP y luego Dual-Stack. (Diaz, 2017).

Telecom Argentina dentro de su adopcion de IPv6 habilita dual-stack, realizando pruebas con empleados y pruebas con clientes, parametrizando algunos procesos como desactivar tuneles, verificar asignacion de IP y conectividad y finalmente mediciones objetivas de red y subjetivas de percepcion. (Cicileo, 2017)

4. DISCUSIÓN

Se estima que para las grandes organizaciones, puede tomar hasta un par de años realizar una transición completa de IPv4 a IPv6, ya que los protocolos IPv4 e IPv6 no son compatibles (Tadayoni & Henten, 2015), surgiendo la necesidad de utilizar diferentes tecnicas que permitan a los protocolo cohexistir. Dicha cohexistencia aprovecha la experiencia del protocolo IPv4 en el cual se han implementando tecnicas de seguridad innovadoras, pero tiene como desventaja que al implemertar el protocolo IPv6 se queda expuesto a nuevos problemas de seguridad que posiblemente no se tenian en IPv4.

En este apartado se discutirán de forma especial los elementos de seguridad con mayor reincidencia en la coexistencia entre los protocolos de IPv4 e IPv6.

IPV6 surgió para dar solución a la limitante en la cantidad de direcciones disponibles del protocolo IPV4, abriendo enormes posibilidades en materia de soporte de infraestructura de cara a las tecnologías emergentes como internet de las cosas que plantean nuevos desafíos relacionados con la cantidad de dispositivos que estarían interconectados. El crecimiento de la infraestructura siempre ha venido acompañado de un crecimiento en los usuarios y los servicios disponibles, por esta razón, se requieren enormes esfuerzos por preservar la seguridad de las personas y los activos asociados a la información y a su tratamiento. Este aseguramiento se debe dar desde dos perspectivas, la gestión de la seguridad de la información que abarca todas las políticas y labores administrativas que debe implementar una organización para conocer sus capacidades y vulnerabilidades relacionadas con los activos de la información o con las personas, y poder actuar proponiendo un esquema de controles de manera que la organización responda a eventos que la afecten siempre que sea necesario. La otra perspectiva es la tecnológica, en esta se deben emprender un conjunto de metodologías, procedimientos y actividades técnicas, orientadas a entender las posibles brechas desde el punto de vista técnico y tecnológico. En esta última perspectiva, es donde se quiere profundizar en el presente estudio, analizando y formulando soluciones que permitan una adopción segura de IPv6 en las organizaciones.

Siguiendo este precepto, cabe destacar que IPV6 ofrece nuevas características como los es la robustez ya que renovó el protocolo ICMP adicionándole la funcionalidad de *Neighbor Discovery* adoptando las funcionalidades de ARP mejorando el redireccionamiento y descubrimiento de router pero a pesar de sus mejoras también presenta ataques de *DoS*, *Man in the Middle* y seguramente algunos más por descubrir.

Contrarrestando estas vulnerabilidades se diseñaron protocolos como SEND el cual auténtica los mensajes de salida y el protocolo *RA-Guard* que se considera como complemento de SEND y es implementado cuando la infraestructura inhabilita el uso de SEND.

CONCLUSIONES

La estructura de IPv6 la hace más eficiente por sus conceptos de cabecera de extensión y cabecera de fragmentación, pero son propensos a los ataques informáticos, ya que no se ha analizado a profundidad toda la estructura de las cabeceras.

La madurez que ha alcanzado IPv4 por el tiempo y cantidad de redes donde se ha implementado, constituye un aspecto importante que ha dificultado la transición hacia IPv6. Hay múltiples ventajas de implementar IPv6, una de ellas es que por defecto implementa IPsec, lo cual brinda garantías de seguridad, sin embargo, muchas posibles fallas del protocolo se irán descubriendo en el camino, cuando su uso se masifique.

REFERENCIAS

Alvernia Acevedo, S. A., & Rico Bautista, D. W. (2017). Análisis de una red en un entorno IPv6: Una mirada desde las intrusiones de red y el modelo TCP/IP. (U. d. Pamplona, Ed.) Revista Colombiana de Tecnologías de Avanzada, 1(29), 81-91.

Choudhary, A., & Sekelsky, A. (2010). Securing IPv6 network infrastructure: A new security model. *2010 IEEE International Conference on Technologies for Homeland Security, HST 2010.*

Cicileo, G. (2017). Estado de agotamiento de IPV4. LACNIC, Medellin.

Cui, Y., Chen, Y., Liu, J., Lee, Y., Wu, J., & Wang, X. (2015). State management in IPv4 to IPv6 transition. *IEEE Network*.

Cui, Y., Dong, J., Wu, P., Wu, J., Metz, C., Lee, Y., & Durand, A. (2013). Tunnel-based IPv6 transition. *IEEE Internet Computing*.

Czyz, J., Allman, M., Zhang, J., Iekel-Johnson, S., Osterweil, E., & Bailey, M. (2014). Measuring IPv6 adoption. *ACM SIGCOMM Computer Communication Review*.

Diaz, C. (2017). Creación de políticas públicas para incentivar el despliegue IPv6. Ponencia, LACNIC, Medellín.

Google (2018). Estadísticas de IPv6. https://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption. Recuperado el 10 de abril de 2018.

Khalil, I., Khreishah, A., Bouktif, S., & Ahmad, A. (2013). Security concerns in cloud computing. *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013.*

Khan, R., & Shiranzaei, A. (2017). IPv6 security tools - A systematic review. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016.*

LACNIC. (2017). IPv6 portal. Recuperado el 15 de 03 de 2018, de http://portalipv6.lacnic.net/

LACNIC. (s.f.). Portal IPv6. (M. d. transición, Productor) Recuperado el 13 de 03 de 2018, de http://portalipv6.lacnic.net/mecanismos-de-transicion/

Leslie, M. (2016). Whatever happened to *Science*.

Levin, S., & Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons. *Telecommunications Policy*.

Li, X., Bao, C., Chen, M., Zhang, H., & Wu, J. (2011). *The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition.*

Nicolls, V., Le-Khac, N.-A., Chen, L., & Scanlon, M. (s.f.). IPv6 Security and Forensics.

Ministerio de las Tecnologías y las Comunicaciones, MINTIC. (2015.). Guía de Transición de IPv4 a IPV6. Bogotá, D.C, *Colombia*.

Ministerio de las Tecnologías y las Comunicaciones, MINTIC. (3 de Oct de 2017). Resolución Nº 2710 del 3 de Octubre del 2017. Lineamientos para la adopción del protocolo IPv6. Bogotá, D.C, Colombia.

Portal IPv6 Cuba. (s.f.). Recuperado el 13 de 03 de 2018, de http://www.cu.ipv6tf.org/transicionipv6.htm

Portal IPv6 CUBA. (s.f.). Recuperado el 13 de 03 de 2018, de http://www.cu.ipv6tf.org/biblioteca.htm

Putri, M., & Sucahyo, Y. (2017). Factors analysis that affecting the user acceptance towards IPv6 transition. *2016 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2016.*

Rojas, S. (2017). Agotamiento de IPv4 ¿Puedo pedir aún direccionamiento? Lacnic on the Move , 8.

Satizábal, I. (2015). Seguridad de los protocolos de voto electrónico a través de internet: una comparación. (U. d. Pamplona, Ed.) Revista Colombiana de Tecnologías de Avanzada, 2 (26), Pág. 61-67.

Shaharuddin, U., Rahman, R., Kassim, M., & Yusof, M. (2017). Performance comparison of multimedia applicationsover IPv4 and IPv6Dual stack technology. *Proceedings of the 2016 6th International Conference on System Engineering and Technology, ICSET 2016.*

Siddika, F., Hossen, M., & Saha, S. (2017). Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow. *Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017.*

Simulación en tiempo real de enrutamiento de virtualización sobre un banco de pruebas diseñado para las diversas técnicas de transición IPv4-IPv6. (s.f.).

Tadayoni, R., & Henten, A. (2016). From IPv4 to IPv6: Lost in translation? *Telematics and Informatics, 2016* (33), 650-659.

Wing, D. (2010). Network address translation: Extending the Internet address space. *IEEE Internet Computing*.

World Telecommunication/ICT Policy Forum. (2013).

Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey. *IEEE Communications Surveys and Tutorials*.

Zhao, Q., & Ma, Y. (2010). An object-oriented model of IPv4/IPv6 network management. *Journal of China Universities of Posts and Telecommunications*.

Zhao, Q., & Ma, Y. (2013). New IPv4/IPv6 transition solution for data center. *Journal of China Universities of Posts and Telecommunications*.