

**ESTUDIO BÁSICO SOBRE LOS AVANCES DE LA IMPLEMENTACIÓN Y EL
DESPLIEGUE DEL PROTOCOLO IPV6 EN COLOMBIA**

Gustavo Adolfo Guzman Cadavid

Carlos Andrés Rodríguez Segura

2020

Asesor: Mg. Juan Carlos Ramirez

**UNIVERSIDAD SANTO TOMAS
ESPECIALIZACION EN GESTION DE REDES DE DATOS**

TABLA DE CONTENIDO

INTRODUCCIÓN.....	5
1. JUSTIFICACIÓN	7
2. PROBLEMA.....	9
3. GESTIÓN.....	10
3.1. OBJETIVOS	10
3.1.1. Objetivo general	10
3.1.2. Objetivos específicos	10
4. REQUERIMIENTOS	11
4.1. MARCO TEÓRICO.....	11
4.1.1. Antecedentes	11
4.1.2. Terminología.....	27
4.2. MARCO LEGAL.....	45
4.2.1. Ministerio de Tecnologías de la Información y Comunicación.....	46
4.2.2. Ley 1341 de 2009 Artículo 19. Creación, Naturaleza y Objeto de la comisión de regulación de comunicaciones.	46
4.2.3. Resolución 2710 de 2017 lineamientos de implementación del protocolo IPv6 en Colombia.	46
5. PROPUESTA DE SOLUCIÓN.....	47
5.1. Planeación Metodológica.	50

5.2. Desarrollo Tecnológico.....	53
6. CONCLUSIONES Y RECOMENDACIONES.....	58
7. REFERENCIAS	61

TABLA DE FIGURAS

Figura 1. Descripción grafica DS-LITE por ZTE. Fuente: D' Egidio 2012.	32
Figura 2. Mecanismo NAT64/DNS64. Fuente: Ipv6 para operadores de red. 2014.	34
Figura 3. Técnica 6PE y 6VPE. Fuente: Ipv6 para operadores de red. 2014.	36
Figura 4. Mecanismo 464XLAT. Fuente: Ipv6 para operadores de red. 2014.	37
Figura 5. Diagrama Metodología. Fuente: Los autores.	51
Figura 6: Flujo de medición de los requerimientos. Fuente: Colitti 2009.	54
Figura 7: Estadísticas de adopción de IPv6 generadas por Google. Fuente: GOOGLE 2020.	55
Figura 8: Estadísticas sitios web IPv6 suministradas por 6LAB CISCO. Fuente: CISCO 2020. ...	56
Figura 9: Representación de AS PATH del prefijo en la tabla BGP. Fuente: KACZMAREK, 2011.	56
Figura 10: Ambiente de pruebas servicios IPv6 Colombia. Fuente: Los Autores.	58

INTRODUCCIÓN

El tema de esta investigación es el avance de la implementación de IPV6 en las redes de los proveedores de servicios en Colombia, y sobre la relevancia de la implementación de IPV6 Computerworld, una conocida revista impresa y online sobre tecnología de información y comunicaciones, cuyo mercado objetivo son los administradores de tecnología y que se publica en varios países del mundo publicó un artículo que se titulaba “No IoT without IPV6”. En este artículo Charles Sun codirector de tecnología del grupo de trabajo Federal de IPV6 en Estados Unidos se cuestiona si lo próximo grande que viene es el IoT, y llama poderosamente su respuesta que, aunque parece decir si, se condiciona a un factor determinante y es que pase lo otro siguiente “grande” que es IPV6; esto según la respuesta que a si mismo se da Charles Sun en dicho artículo. (Sun, 2016)

Esto es otra evidencia de lo transcendental que es para las economías del mundo lograr una transición rápida y limpia de IPV4 a IPV6, y de que exista este tipo de infraestructura dependerá que tan rápido acceso se tenga a las nuevas tecnologías y por tanto el tener las ventajas competitivas que ofrecen, y así mismo la participación en las nuevas economías que surgirán producto de las tecnologías mismas. Esto se puede ver reflejado hoy en día en la guerra comercial que enfrenta a las economías más grandes del mundo, cuyo trasfondo es el control de aquello que hará posible una de las vertientes más fuertes de IoT y esto es el 5G; valga la pena decir que este mismo también necesita, y se espera sea implementado sobre el protocolo IPV6.

En la Resolución 180 de 2010 la UIT (Unión Internacional de Telecomunicaciones) en la cual hace parte Colombia, se reconoce que la adopción temprana del IPV6 era la mejor forma de evitar las consecuencias que el agotamiento de las direcciones IPV4 puedan implicar para los países miembros; Por su parte el Min Tic (Ministerio de la Información y las telecomunicaciones

en Colombia) consciente de esta problemática en la resolución 2710 de 2017 estableció que máximo el 31 de diciembre del 2019 las entidades de orden nacional deben implementar la tecnología IPv6, en coexistencia con el Ipv4. Para entes territoriales, el plazo máximo es el 31 de diciembre del 2020.

Es por eso por lo que este podría considerarse un momento adecuado y crucial para “medir la temperatura” del país con respecto a este tema, y este proyecto en particular pretende atender dicha necesidad, consultando al mayor número posible de actores involucrados en el tema sobre estos avances y así poder presentar una radiografía de la situación.

1. JUSTIFICACIÓN

En octubre del 2018 los 5 RIR (Regional Internet Registry – Entidades encargadas en el mundo de la administración de los recursos numéricos de Internet) indicaron que ya estaban asignadas las direcciones de su último bloque /8 disponible, y adicionalmente de acuerdo a la reconocida firma de consultoría Gartner se tenía un estimado de 11 mil millones de dispositivos conectados a Internet, también para ese tiempo se estimaba que el número de dispositivos conectados alcanzaría los 20 mil millones para el año 2020. Por otro lado, la ITU (International Telecommunication Unión) estimó en cerca de 3 mil doscientos millones de personas conectadas a Internet de una población global de 7 mil doscientos millones. (Internet Society, 2018)

Todo esto se está materializando y hoy día vemos se ha visto un crecimiento exponencial de dispositivos conectados a Internet y cada uno con la necesidad de tener cada uno su propio direccionamiento único, ocasionando que en regiones como Estados Unidos y Europa ya no tengan direcciones IP disponibles para asignar mientras que en Latinoamérica, el 15 de febrero de 2017 se inició la tercera fase de agotamiento de los segmentos IPV4 Públicos disponibles según lo anuncio LACNIC, quien administra el recurso en la región.

Al inicio de esta fase, en la cual solo se asignarían nuevos bloques de IPV4 a ISP o empresas que no hayan recibido bloques previamente se contaban con un poco más de 5 millones de direcciones disponibles, en este momento ese número se encuentra en 1 millón seiscientas mil, y se espera que el 30 de mayo de 2020 este número sea cero. (LACNIC, 2019)

Los mecanismos planteados para evitar el agotamiento de las direcciones han sido útiles, pero no suficientes ya que cada día (por lo menos en Latinoamérica) nos acercamos al punto de agotamiento. Una de estas estrategias es la recuperación de las direcciones no usadas, el reúso de las asignadas para otros propósitos y otra la tecnología “Network Address Translation” (NAT) la

cual permite que segmentos de red privado como: 192.168.x.x, 172.16.x.x o 10.x.x.x puedan salir a Internet a través de una dirección IP pública (este último con sus limitantes por la cantidad de recursos).

Es reiterativo que la humanidad con la “sed” de estar siempre conectada presiona cada vez más por mayor cantidad de equipos, generando mucha más escasez de direcciones, un claro ejemplo es el IoT (Internet of Things), siendo un tema emergente que no solo muestra una relevancia técnica, sino que tiene fuertes connotaciones sociales y económicas. En esta nueva realidad se integraría a Internet diversos productos: de consumo, bienes duraderos, automóviles y camiones, componentes industriales y de servicios públicos, sensores y otros objetos de uso cotidiano, junto a potentes capacidades de análisis de datos que prometen transformar el modo en que el ser humano trabaja, vive y juega. Se cree que el desarrollo de IoT llevaría el número de dispositivos conectados hasta cien mil millones en 2025 y generaría ingresos cercanos a 11 Billones de dólares. (Internet Society, 2018)

Es por eso por lo que se observan los frecuentes llamados de diversas organizaciones a implementar la siguiente versión del protocolo IP: IPV6. Y no solo a usarlo como un complemento de IPV4, sino que llegue realmente a reemplazarlo por completo. Con esto se activarían 340 trillones de trillones de trillones de direcciones en contraste a las 4.7 Billones de direcciones de IPV4, y permitiría el soporte que se requiere para el presente y futuro desarrollo de Internet, y en consecuencia las tecnologías que las nuevas realidades de la humanidad están requiriendo.

Debido a esta coyuntura y las necesidades enumeradas, se tiene la plena seguridad que conocer el estado de implementación del IPV6 en Colombia, y dar a conocer dicho estudio a la comunidad académica, contribuiría a la creación de una conciencia en sus miembros sobre la necesidad no

sólo conocer este protocolo sino en promover su uso en las nuevas implementaciones; de tal forma que en Colombia pueda aplicarse en el menor tiempo posible y no quede rezagado cuando todos los desarrollos que en estos momentos se están dando lleguen y puedan ser adoptados sin mayor dificultad.

2. PROBLEMA

Todo dispositivo que necesite navegar o quiera ser alcanzado desde Internet requiere el uso de una IP pública, es decir una IP única en todo el mundo; una IP que pueda ser anunciada por la infraestructura de los ISP de tal forma que cualquier usuario desde cualquier lugar de Internet la pueda alcanzar. Ya que la humanidad requiere cada vez más dispositivos conectados a Internet el número de direcciones disponibles empiezan a ser insuficientes y se agotan rápidamente. Como se mencionó anteriormente para Latinoamérica el número de dispositivos ha crecido tanto, que el 15 de febrero de 2017 se inició la tercera fase de agotamiento de estos segmentos IPV4 Públicos según lo anuncio LACNIC, y retomando estas cifras al inicio de esta fase, en la cual solo se asignarían nuevos bloques de IPV4 a ISP o empresas que no hayan recibido bloques previamente, se contaba con un poco más de 5 millones de direcciones disponibles, en este momento ese número se encuentra en 1 millón seiscientas mil, y se espera que el 30 de mayo de 2020 este número sea cero.

Aunque parece una situación novedosa desde hace más de 20 años se detectó que existía la posibilidad de llegar a esta situación, la IETF propuso iniciar el desarrollo del "IP de próxima generación", como resultado de este proceso Steve Deering de Xerox PARC y Craig Mudge diseñaron IPV6 reemplazando IPV4, proceso que quedó plasmado en los primeras RFC como el RFC 2460 en 1998.

Con todos estos antecedentes, muchas pequeñas y medianas empresas en Colombia se pueden cuestionar acerca de: ¿Qué implicaciones les traería implementar sus servicios sobre las redes IPV6 disponibles?, ¿Se podrá hacer de manera transparente obteniendo el mismo desempeño que actualmente obtiene con Ipv4?, o en caso contrario ¿Qué retos o qué dificultades debería sortear?, pero antes de empezar a tratar de responder estos interrogantes, deberemos tratar de responder ¿Qué tan avanzado está el país en la implementación de IPV6?. *

Por último y de acuerdo con la problemática expuesta anteriormente se establece el siguiente interrogante ¿Qué tan avanzada se encuentra la implementación del protocolo IPV6 en la infraestructura de los ISP en Colombia y qué dificultades puede tener una PYME para usar IPV6 en los dispositivos que acceden o deben ser accedidos desde Internet?

3. GESTIÓN

3.1. OBJETIVOS

3.1.1. Objetivo general

Realizar un estudio básico sobre los avances de la implementación y el despliegue del protocolo IPV6 en Colombia.

3.1.2. Objetivos específicos

- Recolectar información sobre el estado del direccionamiento de los principales proveedores por medio del NAP Colombia y LACNIC con el fin de establecer una línea base de estudio.
- Obtener y analizar la información de los proveedores de servicio para evaluar el estado de implementación y despliegue del protocolo IPV6 en sus redes.

- Diseñar pruebas técnicas complementarias que permitan validar el estado IPV6 en Colombia.
- Definir los criterios claves que permitan la implementación de IPV6 en una PYME Colombiana.

4. REQUERIMIENTOS

4.1. MARCO TEÓRICO

4.1.1. Antecedentes

Con el fin de tener una visión más global de lo que se ha investigado en los diferentes países del mundo con respecto al estudio y la implementación de IPV6 se consultaron los siguientes documentos:

1	Despliegue de IPv6 para el Desarrollo Social y Económico en América Latina y el Caribe. Autores: de León Omar, Matinez Carlos, Cicileo Guillermo, Acosta Alejandro, Diaz César, Majó Ernesto, Kaplan Laura. Artículo: 2015 LACNIC (the Internet Addresses Registry for Latin America and the Caribbean) Disponible en: https://www.lacnic.net/innovaportal/file/3035/1/caf-lacnic-despliegue-ipv6-para-desarrollo-socio-economico-en-lac.pdf
	Este trabajo de investigación sobre la transición hacia IPv6 fue realizado por la empresa Teleconsult bajo la coordinación, ejecución y supervisión de LACNIC y de acuerdo a los términos establecidos por la CAF e intenta brindar el más amplio conocimiento sobre todos los aspectos que inciden en la transición hacia

	IPv6 en Latinoamérica. Otros aspectos que aborda son: análisis de los problemas que provoca el agotamiento de las direcciones IPv4, ventajas y metodologías del despliegue de IPv6, el comportamiento de los diferentes agentes, los asuntos económicos y el modelado de las alternativas, las mejores prácticas y casos de éxito. También indicadores primarios y secundarios de la situación actual de la transición, generados en múltiples fuentes, Resultados de la encuesta que provee las razones sobre el porqué de la situación actual y las tendencias. Presenta los resultados de las entrevistas realizadas en 10 países que proveen información consolidada de la situación, tendencias y razones de las partes interesadas en cuanto a sus acciones respecto de la transición hacia IPv6 en dichos países. Adicionalmente se analizan los casos de los operadores que han sido identificados como casos de éxito, junto con otros. Y a partir de todos los análisis realizados se presentan recomendaciones y guías para lograr el despliegue oportuno de IPv6. (de León Omar, Matinez Carlos, Cicileo Guillermo, Acosta Alejandro, Diaz César, Majó Ernesto, Kaplan Laura., 2015)
2	Evaluating IPv6 Adoption in the Internet Autores: Lorenzo Colitti, Steinar H. Gunderson, Erik Kline, Tiziana Refice Artículo: Google Research Publications. Disponible en: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/36240.pdf

	En este artículo los investigadores de Google preocupados por la poca información de calidad existente en ese momento, sobre la conectividad de IPv6 desarrollaron una metodología para medir la adopción de IPv6 desde el punto de vista de los generadores de contenido y adicionalmente evaluar el impacto de implementar IPv6 en estos sitios web para los usuarios. Metodología que fue inicialmente aplicada al mismo sitio web de Google y de la cual se tomaron mediciones durante cerca de un año para presentar las conclusiones del estudio. La metodología esta basada básicamente en solicitar al "browser" del usuario enviar requerimientos en IPv4 e IPv6 a unos servidores instalados especialmente para este propósito de tal forma que una infraestructura adicional pueda analizar y procesar estos requerimientos que llegan a los server mencionados. El análisis de estos datos implica una infraestructura independiente ya que se desarrolla un modelo matemático para el mismo, y requiere procesar millones de requerimientos por día. Algunos de los indicadores generados son: Tasa de conectividad IPv6, Tipo de conectividad, Conectividad por país y Conectividad por Sistema autónomo. (Lorenzo Colitti, 2010)
3	Internet IPv6 Adoption: Methodology, Measurement and Tools. Autores: Hugo Kaczmarek Artículo: 6lab Cisco Disponible en: https://6lab.cisco.com/stats/data/Internet%20IPv6%20Adoption.pdf

	En este artículo los investigadores de Cisco y de L'École polytechnique se esfuerzan inicialmente por mostrar las bondades de IPv6 que impulsarían la adopción de esta tecnología, y posteriormente analizan los ángulos desde los que se debería analizar o medir los niveles de adopción de IPv6, estos puntos de vista serían: Planeación, Core de la Red, Contenido y número de usuarios. Estos puntos de vista a la vez son fases para analizar dentro del proceso. En el artículo se observa que las razones principales de Cisco para medir este despliegue o realizar este proceso de medición para mostrar que los dispositivos Cisco están muy bien preparados para que sus clientes implementen IPv6 sin problema a todos los niveles, adicionalmente poder identificar posibles empresas que requieran su apoyo en el desarrollo de los procesos de migración, e identificar aspectos como que países están presentando un despliegue más rápido de Ipv6. Cisco explica en el documento su metodología que inicial es tomar la información que administran los RIR (Registro Regional de Internet) y procesarla. Otro de los procesos explicados es el cálculo de los AS de Transito. Otros aspectos considerados son el uso de arreglos de datos generados por Geoff Huston de APNIC. (Kaczmarek, 2012)
4	Estudio sobre mecanismos de transición IPv6 soportados por los CPE de la región. Autores: D'Egidio, Alejandro. Artículo: LACINC News IPV6. LACNIC 2020 (the Internet Addresses Registry for Latin America and the Caribbean)

	Disponible en: https://prensa.lacnic.net/news/ipv6/estudio-sobre-mecanismos-de-transicion-ipv6-soportados-por-los-cpe-de-la-region
	Este estudio realizado por personal de LACNIC permite dar una visión muy actual del estado y el uso de los mecanismos de transición utilizados y soportados en los Customer Premises Equipment ‘CPE’ más populares en America Latina y el Caribe; se centran básicamente en tecnologías de acceso a redes fijas como ADSL (Asymmetric Digital Subscriber Line), en DOCSIS (Data Over Cable Service Interface Specification) y en FTTH (Fiber To The Home). Como premisas fundamentales se tenía la importancia de la implementación de IPV6 en todos los ámbitos: ISPs, Proveedores de contenido, Clientes corporativos y Gobierno; y por otro lado los mecanismos de transición, divididos en tres grandes grupos: Doble pila, Soporte IPv6 sobre infraestructura IPv4 y Soporte IPv4 sobre infraestructura IPv6, profundizando en este último por su funcionamiento. En el estudio utilizaron como metodologías encuestas dirigida a los ISP de la región (mayormente ISPs que tuvieran desplegado o en proceso el IPV6) y a los fabricantes de equipos más populares usados por los ISP encuestados. Gracias a la tabulación y análisis de las encuestas y validando equipos y tecnologías utilizadas, llegaron a las siguientes conclusiones: en cuanto al estado del despliegue de IPV6 el 67% de ISPs ofrecen IPV6 a sus clientes; el mecanismo de transición líder es DS-Lite, los fabricantes con mayor presencia en

	los ISPs son Huawei (25%) y ZTE (20%) y el fabricante más innovador es Technicolor al presentar soporte en la mayoría de mecanismos de transición, cabe aclarar que todo se basa para en Equipos locales del cliente ‘CPE’ utilizados por los ISPs. (D’Egidio, 2020)
5	Transición al protocolo IPv6, ¿Dónde estamos? Autores: A. Hamarsheh, Y. AbdAlaziz Artículo: 2019 International Conference on Computer and Information Sciences (ICCIS) Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=8716482
	En este artículo los autores presentan lo que consideran son los principales inconvenientes que están afectando el despliegue de IPV6 en Internet. Presenta gráficos de proyecciones de agotamiento que muestra que estas entidades entre 2020 y 2021 agotaran todas las direcciones disponibles y concluye que el NAT realmente no tuvo mayor efecto como alternativa para prolongar la vida de IPV4. Luego se presentan las alternativas a este tradicional NAT, las cuales son “Large Scale NAT (NAT444)” y “address Plus Port (A+P)” de las que se hace énfasis sobre las desventajas que han tenido. Posteriormente se numeran lo que el autor llama acercamientos a la transición de IpV4 a IPV6 sobre lo cual se menciona que al parecer se va a demorar mucho aún, pero que se requiere sea lo más fluida posible para los usuarios algo que solo puede pasar si los de IPV4 se pueden comunicar con los de IPV6.

	Para que esta comunicación sea posible se plantean al menos tres mecanismos: “Dual Stack”, “Tunelling” y “Translation”. El primero se refiere a la posibilidad que los dos protocolos coexistan sobre la red, el segundo se refiere a emplear la infraestructura existente de IPV4 para cursar el tráfico IPV6 encapsulado; en este caso los túneles pueden ser estáticos o dinámicos. Y el tercero básicamente consiste en hacer una traducción de las direcciones IPV4 a IPV6 y viceversa para comunicar redes, esta traducción se puede hacer desde dos perspectivas: la basada en Host y la basada en la red. La segunda se refiere a la traducción del encabezado del paquete de IPv6 a IPV4 y la primera según se indica se realiza cuando hay incompatibilidad entre el aplicativo y el protocolo. De este segundo tipo hay tres subclases que son: “Bump—In-the-Stack”, “Bump-in-the-host” o “Bump-in-the-API”. Finalizando presentan un interesante protocolo llamado CHANC (Configuring host to Auto-detect Network connectivity), según los autores esto facilitaría que los ISP provean IPV6 a los usuarios así sus redes no tengan IPV6 nativo ya que provee una configuración automática del host de cliente para que puedan usar las funcionalidades que provee la red del ISP. Se termina con una tabla que compara los mecanismos de transición que propuso la IETF con los que proponen los autores. (Ala Hamarsheh, Yazan AbdAlaziz, 2019)
6	Medición de la preparación de IPv6 en el proveedor de contenido basado en la web con mayor acceso en Indonesia. Autores: W. Satriyo Artículo: 2017 The International Conference on ICT for Smart Society (ICISS)

	Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=8288875
	En este artículo se tratan de medir los avances en la implementación de IPV6 para los contenidos más accedidos en la web, en Indonesia. Basándose en datos provistos por los operadores de telecomunicaciones del país. El problema planteado es: ¿No están aun realmente listos los proveedores de contenido para la implementación de IPV6? Los datos analizados se dividieron en 4 categorías de acuerdo con su contenido: Redes sociales, video, música y juegos. Adicionalmente hace un análisis de la necesidad de IPV6 desde las perspectivas de IoT para “Smart City”, Ataques Cibernéticos y el perfil tipo de personas que acceden a Internet en ese país. Finaliza proponiendo una sencilla pero práctica prueba que le permita corroborar los datos generados por los proveedores de Telecomunicaciones, y sobre estas dos bases saca conclusiones y realiza una recomendación pública al gobierno para que requiera a los grandes proveedores de contenido que presten sus servicios en IPv6.. (Wibowo, 2017)
7	Tasa de adopción y desempeño en las redes de Internet inalámbricas 5G Autores: I. Naqvi, A. Siddiqui, A. Farooq Artículo: 2016 IEEE Region 10 Conference (TENCON) — Proceedings of the International Conference Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=7848784
	cuanto la implementación de IPV6 en las redes inalámbricas 5G debido al agotamiento del direccionamiento IPV4. Además de esto realizaron el estudio del

	comportamiento de diferentes servicios sobre este tipo de redes como lo son la transferencia de voz, video streaming a través de los protocolos IPV4 e IPV6. La adopción de IPV6 en las redes inalámbricas impactaría la vida de las personas desde todos los aspectos, debido a que, en la actualidad, muchas de las personas basan su vida en la forma que se comunican los unos con los otros y la forma en que trabajan con este tipo de redes; por lo tanto, es de vital importancia realizar todas las pruebas necesarias para disminuir el tema de la baja calidad en estos servicios con la implementación del nuevo protocolo. Las pruebas fueron realizadas por medio de una configuración básica de la red y un banco de redes inalámbricas simuladas, verificando tiempos de retrasos en la transferencia de paquetes, la mayoría de los casos IPV6 tiene un retraso mayor debido al tamaño del encabezado, pero esto se puede ir reduciendo con políticas definidas en el gobierno, que el gobierno estipule un proceso para su implementación y estimule su ejecución. (Izza Fatima Naqvi, Adeel Khalid Siddiqui, Awais Farooq, 2016)
8	Preparación Empresarial para IPV6 Artículo: Proceedings of the IEEE SoutheastCon 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida Autores: J. Pickard, A. Patrick, A. Robinson Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=7133016
	En un estudio realizado en el año 2015 se buscaba, llamar la atención para asumir el direccionamiento IPV6 en el campo empresarial, en la cual se buscaba por medio de encuestas qué tantas compañías estaban, con desconocimiento total,

	con plena conciencia, interesados, en medio de pruebas, con limitaciones o totalmente bajo la implementación del IPV6. La población objetiva de este estudio fueron diferentes compañías pertenecientes a Carolina del Norte, EEUU, las cuales se obtuvieron de una base de datos de la Universidad de Carolina del Este. Dentro de las organizaciones estudiadas, un dato interesante es que el 38% de estas, eran multinacionales las cuales tenían influencia en sus decisiones alrededor del mundo en los 5 continentes. El 75% de las compañías tienen conciencia de la implementación de IPV6, pero lastimosamente es casi este mismo porcentaje el que no está estudiando activamente la forma de implementarlo en su compañía, solo el 5% tal vez lo vaya a implementar en un corto plazo. Otro aspecto importante de este estudio es que la mayoría de las empresas no tienen conocimiento si su proveedor de servicio ofrece o no conectividad IPV6, y solo el 2% indican que están iniciando una solicitud de espacio IPV6. Por otro lado, algo que deja es el bajo entrenamiento en las diferentes áreas de IPV6 (tecnología, implementación, seguridad, configuración de equipos de red IPV6, configuración de host y sistemas operativos e implementación de aplicativos con IPV6). (Andrew Robinson, John Pickard and Annie Y. Patrick, 2015)
9	Planificación de implementación de IPV6 Autores: J. Pickard - A. Patrick Artículo: Proceedings of the IEEE SoutheastCon 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida

	Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=7133000
	En un taller desarrollado durante un congreso del Instituto de ingenieros eléctricos y electrónicos en Estados Unidos, resumieron la planificación del uso de IPV6 en 5 pasos para desarrollar su implementación a nivel de laboratorio de forma educacional. El primero de los puntos es definir y familiarizarse con la arquitectura de las direcciones IPV6 de acuerdo con lo que se establece en la RFC 4291; es allí donde se definen los tipos y cómo es su representación. En segundo lugar, se debe garantizar que las direcciones tengan un tamaño apropiado; debido a que antes de solicitar la asignación de las direcciones a un ISP es de vital importancia el conocimiento de las políticas y la estructura de la asignación global de acuerdo con la región donde se encuentre. El tercer paso es establecer directrices del direccionamiento, esto quiere decir que lo que se utilizaba para optimizar las direcciones IPV4 es prácticamente obsoleto, pero en este caso se requiere tener mejores prácticas para aumentar el rendimiento operativo y simplificar las políticas de seguridad. Los principios de planificación que plantean son: - Escasa asignación de subredes. – Organización jerárquica de subredes. – Subred uniforme y sumarización. – Mantener subredes de reserva. En el cuarto punto se debe establecer una especie de modelo, el cual no se recomienda obtener desde un direccionamiento IPV4 sino por el contrario debe establecerse desde la estructura de la red u organización. Por último, para el direccionamiento de Host o la asignación de las direcciones tres métodos base, los cuales son asignación manual, asignación por DHCP y por SLAAC, este

	último es de uso exclusivo para IPV6, todos estos tienen su implicación al usarlo y esto depende de lo requerido por la organización. (John L Pickard, Annie Patrick , 2015)
10	Comparativa entre mecanismos de transición IPV6 Autor: J. Palet. Presentación: LACNIC, La Habana mayo 2016 Disponible en: http://slides.lacnic.net/wp-content/themes/slides/docs/lacnic25/miercoles/flip6-transicion_ipv6-v3.pdf
	En la presentación plantean diagramas con los cuales se representan los mecanismos de transición a IPV6 que de hecho sería la recopilación más completa de mecanismos de las referencias consultadas ya que presenta más de 20 de estos. Y de cada uno se presenta un esquema o diagrama explicativo del funcionamiento de cada uno y al final concluye con una tabla donde se comparan todos estos mecanismos vistos desde más de 20 criterios diferentes. (Palet, 2016)
11	Comparación de desempeño entre IPV4 e IPV6 para redes LTE Artículo: Asia-Pacific Network Operations and Management Symposium 2015. APNOMS 2015 Autores: J. Hyun, J. Li, H. Kim, J. Yoo, J. Won-Ki Hong Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=7275417

	Debido al gran crecimiento de usuarios y los usos de estos con el IoT; en Corea del Sur en el año 2015 realizaron una comparación del desempeño para las redes móviles entre IPV4 e IPV6, evaluando principalmente el desempeño, se valida la conexión TCP de acuerdo con las versiones de IP que usan los hosts finales y luego miden el rendimiento con cada protocolo verificando los tiempos de conexión a los sitios establecidos en DUAL STACK. Gracias al agotamiento de las direcciones IPV4 los operadores aceleran cada vez más su migración a IPV6, pero lastimosamente no es posible hacer este cambio de un momento a otro y por su parte debe hacerse de manera progresiva. Los autores nombran tres técnicas que son empleadas por los mobile ISP (Dualstack, Tunneling, Address Translation), en Corea informan que sus operadores utilizan Address Translation la cual consiste en tener traductores del lado del cliente CLAT y del proveedor PLAT, para el caso del cliente traduce las IP de forma algorítmica mientras que del lado del proveedor guardan una base de datos en el núcleo de la red. En conclusión, por medio del estudio del desempeño de las conexiones TCP a diferentes sitios de internet con IPV4 e IPV6 se nota un incremento en el tiempo de respuesta de las paginas por medio de IPV6, de acuerdo a los investigadores por la falta de implementación de IPV6 en las redes centrales de los proveedores, con el crecimiento de la implementación de IPV6 se espera que estas conexiones y tiempos de respuesta sean cada vez menores. (Jonghwan Hyun, Jian Li, Hwankuk Kim, Jae-Hyoung Yoo and James Won-Ki Hong, 2015)
12	Sistema convergente continuo para la transición de IPv4 / IPv6

	Autor: Q. Zhao Artículo: 2017 9th International Conference on Advanced Infocomm Technology Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=8388898
	El artículo inicia planteando la problemática que implica el agotamiento del pool de direcciones IPV4 que tenía disponible la ICANN el 3 de febrero de 2011. Y luego menciona un aspecto histórico interesante y son los RFC producidos por los grupos de trabajo establecidos por IETF para buscar soluciones a esta problemática resaltando que todos estos mecanismos solo permiten a IPv4 e IPV6 coexistir. Luego se centra en explicar su propuesta de un Sistema de Convergencia Fluida para la transición de IPV4 a IPV6 que permita resolver aspectos como el mencionado anteriormente del agotamiento de las direcciones y otros como facilitar la implementación de IPV6 y una transición fluida de IPV4 a IPV6. Según menciona el autor, este sistema estaría principalmente compuesto por módulos “stateful” and “stateless” usados para la traducción de protocolos y que podrían hacer que los hosts con direcciones compartidas IPV4 o IPV6 globales accedan a direcciones IPV4 a través de un Backbone IPV6. El autor también explica que dicho sistema estaría dividido en dos zonas: La zona A o Zona de traslación sin estado y la Zona B o zona de traducción con estado. La Zona A estaría diseñada como una MAN y sería solamente IPV6, aunque tendría varios elementos uno de ellos sería un “Core Router” que

	realizaría la traslación “Stateless”. Luego detalla el funcionamiento de los componentes tildados como claves en el sistema. En el primero llamado Módulo de Traducción de Protocolos se explica de manera detallada como se puede hacer la traducción del encabezado del paquete IPV4 al encabezado del paquete IPV6. El segundo y tercero llamados el Módulos de Mapeo “Stateful” y “stateless” de Direcciones y que es invocado cuando sea necesario por el módulo anterior, se encarga de hacer una asociación una a una de las direcciones IPV4 con las IPV6 sin usar puertos, el primero de IPV6 a IPV4 y el segundo de IPV4 a IPV6. (Qin, 2017)
13	Mecanismo de traducción para la intercomunicación entre IPv4 e IPv6 Habilitado por la ECC. Autores: Akilandeswari, D. Rabara, S. Albert y D.Premila Artículo: International Conference on Communication and Signal Processing, April 3-5, 2018, India Disponible en: https://ieeexplore-ieee-org.crai-ustadigital.usantotomas.edu.co/stamp/stamp.jsp?tp=&arnumber=8524536
	Los autores inician resaltando la tremenda problemática que se ha generado por el explosivo crecimiento de Internet, crecimiento que ha provocado el agotamiento de las direcciones IPV4 disponibles, y luego hace una compilación de las técnicas que se han desarrollado para tratar de solucionar esta problemática; técnicas como: “Dual Stack” donde las dos versiones del protocolo IP conviven de manera separada, “Tunneling” donde los paquetes IPV6 son encapsulados en IPV4 en un extremo de la red y desencapsulados en el otro

	extremo, o de manera similar encapsulando los paquetes IPV4 en IPV6, o “Translation” que consiste en convertir la dirección IPV4 en una dirección IPV6 y viceversa gracias a diferentes mecanismos. Luego se propone un modelo de traducción segura que permitiría prolongar la vida útil de las direcciones IPV4, y después como podría incorporar La Curva Criptográfica Elíptica a este modelo para proveer una alta seguridad. Para finalizar con la descripción de un ambiente experimental de pruebas, el análisis de desempeño del modelo y conclusiones. El modelo usa dos redes heterogéneas, una solamente con host IPV4 y la otra solamente con host IPV6, las cuales se conectan por un routers “Dual Stack” que cumple las funciones de traductor de direcciones IPV4 a IPV6 y viceversa de acuerdo con el esquema de direccionamiento propuesto. Este esquema encapsula direcciones IPV4 en un prefijo de red específico IPV6 para formar una IPV4-convertida dirección IPV6 y una IPV4-traducible dirección IPV6, la primera es usada para representar el nodo IPV4 en la red IPV6 y la segunda es una dirección IPV6 asignada a un nodo IPV6 encargado de la traducción “stateless”. Al final se mide el performance del modelo tomando medidas de parámetros como la latencia, tiempo que toma el “hashing” del paquete y alcanzabilidad del paquete. (D. Akilandeswari, S. Albert Rabara and T. Daisy Premila Bai , 2018)
14	IPV6 para todos. Una guía para el uso y la aplicación de IPV6 en diferentes entornos. Capítulo 1.2, Capítulo 4 Autores: G. Cicileo, R. Gagliano, R. O’Flaherty, M. Rocha, C. Morales, J. Palet, A. Vives.

	Artículo: Internet Society. ISOC-AR Chapter Argentina Disponible en: https://www.internetsociety.org/resources/deploy360/2012/ipv6-for-all-book-isoc-argentina-4/
	En general todos los capítulos del libro pueden servir de base para el proyecto que deseamos desarrollar, Sin embargo, el apartado 1.2 muestra unas estadísticas interesantes sobre la implementación de IPV6 en Latinoamérica, sobre todo algunos parámetros que nos pueden orientar en la investigación. El capítulo 4 representa un aporte práctico que no se ha encontrado fácilmente en el resto de las fuentes y es el hecho que los autores se centran en describir como instalar y configurar muchos servicios básicos en IPV6 sobre los más comunes sistemas operativos, algo muy útil para la fase práctica del proyecto. Básicamente en este capítulo los autores recopilan una serie de comandos paso a paso para la configuración de Telnet, SSH, FTP, Email, Multimedia Streaming, Web y DNS. (Guillermo Cicileo, 2012)

4.1.2. Terminología

En este apartado se pretende profundizar en los principales conceptos que se han considerado relevantes en el estudio que se realizará en el proyecto planteado, y todos estos se relacionan principalmente con IPV6 que es el protocolo de Internet sucesor del protocolo IPv4, el protocolo de direcciones de Internet que se ha utilizado durante muchos años desde los primeros días de la Internet.

Cuando Internet se fundó, esta se estableció como una red de investigación ‘ARPANET’, y su acceso estaba limitado a la comunidad científica y militar. Nunca se pensó que se utilizaría esta red para conectar a todo el mundo, desde un teléfono móvil a un equipo de música y una nevera.

4.1.2.1. Autoridades Reguladoras

- La IANA (Internet Assigned Numbers Authority) es el departamento de la ICANN (Internet Corporation for Assigned Names and Numbers) responsable de coordinar algunos de los elementos importantes que permiten al Internet funcionar sin problemas. Debido a que el Internet es reconocido como una red global libre de coordinación central, existe una necesidad técnica para que los elementos importantes funcionen adecuadamente en conjunto y es la IANA la encargada de realizar este control.
- El RIR (Regional Internet Registry) comprende las 5 distintas entidades (ARIN, LACNIC, RIPE NCC, AFRINIC y APNIC) que se encargan de regular los recursos de internet a nivel mundial, siendo el LACNIC (Registro de Direcciones de Internet para América Latina y Caribe) una organización no gubernamental internacional establecida en Uruguay desde el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa, entre otros recursos para la región de América Latina y el Caribe. El LACNIC es la entidad encargada de asignar para la zona de Latinoamérica y el caribe las direcciones de los protocolos de internet versión 4 y 6 que le han de pertenecer a cada empresa proveedora de servicios de internet o usuario independiente.

4.1.2.2. Dirección IP

Una dirección IP (Internet Protocol) se utiliza en Internet para comunicar un ordenador de una manera similar que un número de teléfono se utiliza para conectar a una línea telefónica.

Cada dirección IP es única y todos los datos que se envían a esa dirección serán enviados a través de la Internet para llegar a su destino.

4.1.2.3. Protocolo IP Versión 4

Las direcciones IPv4 son números binarios de 32 bits que son usados como direcciones en los protocolos IPv4, el cual es utilizado en Internet. Existen tres tipos de direcciones IPv4: Las IPv4 públicas que constituyen el espacio de direcciones de Internet. Estas son distribuidas para ser globalmente únicas. El principal propósito de este espacio de direcciones es permitir la comunicación usando IPv4 sobre Internet y un propósito secundario es permitir la comunicación entre redes privadas interconectadas.

Las direcciones IPv4 privadas corresponden a rangos que han sido reservados para la operación de redes privadas. Cualquier organización puede usar estas direcciones IPv4 en sus redes privadas sin la necesidad de solicitarlo a algún Registro de Internet. La principal condición establecida para el uso de direcciones IPv4 privadas es que los dispositivos que usen estas direcciones IPv4 no necesiten ser alcanzados desde Internet. Y las direcciones IPv4 especiales y reservadas que son rangos reservados para aplicaciones como el multicast. **Invalid source specified.**

4.1.2.4. Protocolo IP Versión 6

IPv6 que es lo que se centra el presente documento como sucesor de IPv4. La creación de IPv6 fue motivada principalmente por el agotamiento de direcciones IPV4 Públicas; es más, muchas predicciones indican que entre el año 2020 y 2021 las direcciones IPv4 Públicas de los cinco RIR (Regional Internet Registry - organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo) se habrán acabado completamente, ya que tendencias tecnológicas como BYOD (Bring Your Own Device - Trae tu

propio dispositivo) en las empresas, IoE o IoT (Internet of Everything o Internet of Things) en el hogar, oficina e industrias, disminución de las brechas tecnológicas en la población, convergencia a redes todo IP en las comunicaciones y aumento demográfico mundial han consumido casi en su totalidad las direcciones IPv4 públicas.

El protocolo IP versión 6 (IPv6) provee una cantidad de direcciones mucho mayor que su predecesor IPv4. En IPV6 el tamaño de las direcciones IP ha crecido de una longitud de 32 bits a 128 bits. Es decir que cantidad de direcciones IP únicas que pueden ser asignadas en IPv6 son aproximadamente 2^{128} o 3.403×10^{38} , que es un número extremadamente grande de direcciones IP posibles. Con este incremento en la longitud de las direcciones IP no habrá problemas de escases por un largo periodo de tiempo además de que garantizará una expansión exponencial de la cantidad de nodos (tabletas, smartphones, vehículos, electrodomésticos, etc.) que se podrán interconectar a través de Internet.

El aumento de la cantidad de direcciones IP para ser asignadas representa prácticamente la característica diferenciadora más conocida entre IPv4 e IPv6. La realidad es que hay otros beneficios tecnológicos que aporta IPv6 que mejoran significativamente al protocolo IP: Auto configuración de las direcciones IP, mejora del enrutamiento en el tráfico multicast, encabezado (header) más simple, mejora en la calidad de servicio (QoS), mejora de la seguridad ya que incluye autenticación y cifrado de la información. También provee mayor número de extensiones y opciones más flexibles y administración más simplificada.

Las direcciones IPv6 se representan en notación hexadecimal agrupando los 128 bits en 8 octetos. Cada octeto tiene un tamaño de 16 bits y están separados por dos puntos (:). Los desarrolladores del protocolo IPv6 eligieron la notación hexadecimal sobre la notación decimal buscando la manera que las direcciones IP no fueran tan largas. **Invalid source specified.**

4.1.2.5. Tecnologías de Transición

Debido a que la implementación del nuevo sistema de direccionamiento no debe interrumpir la navegación en el internet a través de IPv4 para alcanzar aquellos servidores y/o dispositivos que operan aún sobre este protocolo, es necesario para la implementación de IPv6 el uso de una tecnología de transición que permita la coexistencia de ambas versiones del protocolo de Internet.

Actualmente están definidos al menos 3 diferentes tecnologías de transición para la implementación de IPv6, estas se describen a continuación:

4.1.2.5.1. Dual-Stack:

En un sistema Dual-Stack se requiere que ambos protocolos de direccionamiento se encuentren desplegados sobre toda la red simultáneamente. Esta solución permite que las consultas se puedan realizar por ambos sistemas de direccionamiento acorde a la consulta que se realice.

Esta solución es la más viable para la coexistencia de ambos protocolos mientras se da una migración completa. Sin embargo, para las empresas proveedoras de servicio puede representar un reto debido a los recursos de hardware y software que se requieren para sostener dos redes desplegadas por completo sobre la red bajo dos protocolos diferentes.

4.1.2.5.2. Dual-Stack Lite (DS-Lite):

Definido en la RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion.

En la RFC 6908 se definen consideraciones para el despliegue de DS-Lite. Este mecanismo tiene dos componentes principales:

- Basic Bridging BroadBand (B4): Esta funcionalidad embebida en el CPE permite encapsular y enviar el tráfico IPv4 del cliente a través de un túnel IPv6 hasta el AFTR.
- Address Family Transition Router (AFTR): Aquí el tráfico del cliente es desencapsulado del túnel IPv6. El AFTR tiene la funcionalidad de Carrier Grade NAT donde traduce la IPv4 privada del cliente a una IPv4 pública compartida entre varios clientes. (D'Egidio, 2020)

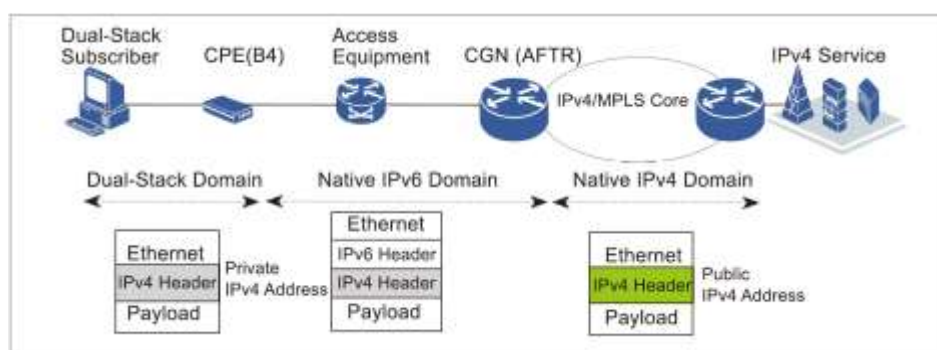


Figura 1. Descripción grafica DS-LITE por ZTE. Fuente: D' Egidio 2012.

4.1.2.5.3. Tunneling:

Para que el Tunneling funcione se requiere de una red superpuesta que cree el túnel entre un protocolo y el otro encapsulando los paquetes IPv6 en paquetes IPv4 y viceversa. La ventaja que presenta este sistema es que los protocolos pueden trabajar sin molestar al uno al otro provisionando la conectividad entre los usuarios del nuevo protocolo. Este sistema de transición presenta dos desventajas que atentan contra la coexistencia de los protocolos: El Tunneling no permitiría que los usuarios de la nueva infraestructura usen los servicios de la otra red sobre IPv4.

No sería posible que los usuarios utilizando distintos sistemas de direccionamiento se comuniquen entre ellos sin la existencia del Dual-Stack dentro de la red local. (Cristian Pérez, 2012)

4.1.2.5.4. Translation:

El Translation permite la comunicación entre redes con un solo tipo de protocolo en uso a través de las cabeceras IP y traducción de direcciones entre los dos tipos de direccionamiento. Esta es una solución que facilita la transición hacia la nueva tecnología conforme los proveedores de servicios de internet y las compañías o clientes finales generan el cambio definitivo sobre las redes.

Este sistema de transición permite una migración gradual hacia el nuevo protocolo otorgando a los usuarios de direccionamiento IPv6 únicamente una experiencia de navegación hacia internet al acceder a servicios sobre IPv4.

Los proveedores y facilitadores de contenido pueden proveer servicios de forma transparente a los usuarios del protocolo IPv6 a través de la tecnología de traducción, con o sin ningún cambio en la red ya existente, lo que permite una continuidad del servicio sobre el protocolo IPv4. (Cristian Pérez, 2012)

4.1.2.5.5. NAT64/DNS64

El mecanismo NAT64 se define en la RFC 6146. Es una técnica stateful para traducción de paquetes y puertos IPv6 a IPv4. Permite, simultáneamente, el uso compartido de direcciones IPv4. El DNS64 se define en la RFC 6147 y es una técnica auxiliar de mapeo para nombres de dominio, que se utiliza en conjunto con NAT64.

Con NAT64 y DNS64 es posible que los usuarios reciban únicamente direcciones IPv6 de parte del proveedor y que incluso así puedan acceder a dispositivos IPv4 en Internet. Para el software de la computadora del usuario, parece que todos los sitios y servicios en Internet fueran IPv6. Para el sitio o servicio en Internet, es como que todas las conexiones se originasen en un usuario IPv4 con una IP compartida. (Alejandro Acosta, 2014)

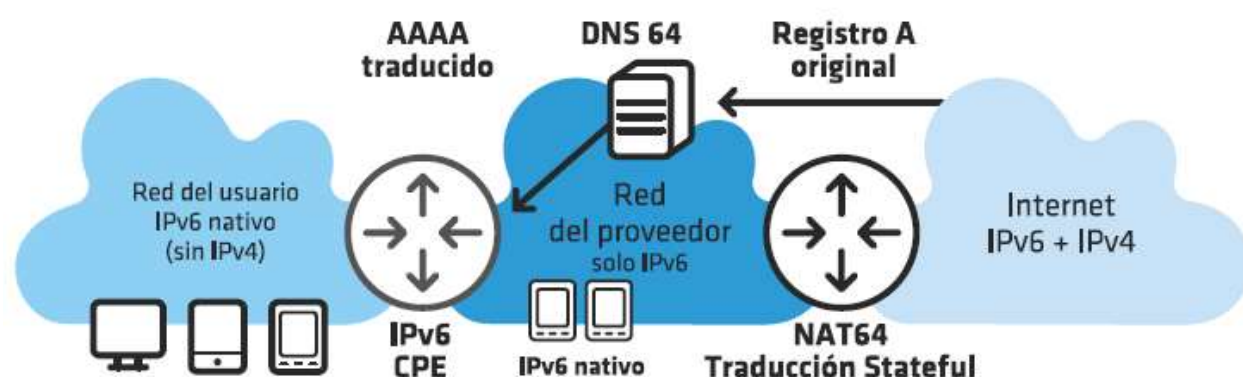


Figura 2. Mecanismo NAT64/DNS64. Fuente: Ipv6 para operadores de red. 2014.

4.1.2.5.6. TEREDO

Teredo es un mecanismo bastante similar a 6to4. Este mecanismo se describe en la RFC 4380 y se incluyó aquí para que los administradores de red sean conscientes de los problemas relacionados con su uso. Actualmente es de poca utilidad práctica.

El prefijo utilizado para los clientes es 2001:0000::/32. Con Teredo se conecta un único cliente, no toda una red. Para el encapsulamiento se utiliza UDP para que los túneles funcionen también en redes con NAT. Además de relays similares a los que se utilizan con 6to4, también existen servidores que ayudan a descubrir el tipo de NAT utilizado por la red del usuario y a iniciar la comunicación.

Los problemas para las redes corporativas son similares a los que se describieron para 6to4. Por ello es conveniente bloquear activamente el uso de esta técnica, lo que se puede lograr deshabilitándola en los sistemas operativos o bien bloqueando en la red el tráfico de salida al puerto UDP 3544. (Alejandro Acosta, 2014)

4.1.2.5.7. 6PE y 6VPE

Actualmente, el uso de MPLS sobre IPv4 está bastante difundido en las redes. 6PE y 6VPE son dos tecnologías que permiten implementar IPv6 sin alterar el núcleo MPLS de la red. Además de la nueva configuración, solo es necesario actualizar el software de los routers de borde, conocidos como PE (Provider Edge), si es que no soportan esta funcionalidad.

Las técnicas 6PE y 6VPE se describen, respectivamente, en las RFC 4798 y 4659. La comunicación se logra utilizando LSP (Label Switch Paths) a través del núcleo MPLS. Ambas técnicas utilizan MP-BGP (Multiprotocol BGP) sobre IPv4 para intercambiar rutas IPv6. Los routers PE deben ser doble pila. Los routers del núcleo MPLS no se dan cuenta que están transportando paquetes IPv6, dado que solo consideran los encabezados MPLS.

En 6PE solamente se mantiene una tabla de enrutamiento, por lo que la técnica es más adecuada para brindar el servicio de Internet. En 6VPE se pueden mantener diferentes tablas de enrutamiento independientes, separadas lógicamente. Por lo tanto, esta técnica es más apropiada para brindar servicios de VPN (Virtual Private Network). (Alejandro Acosta, 2014)

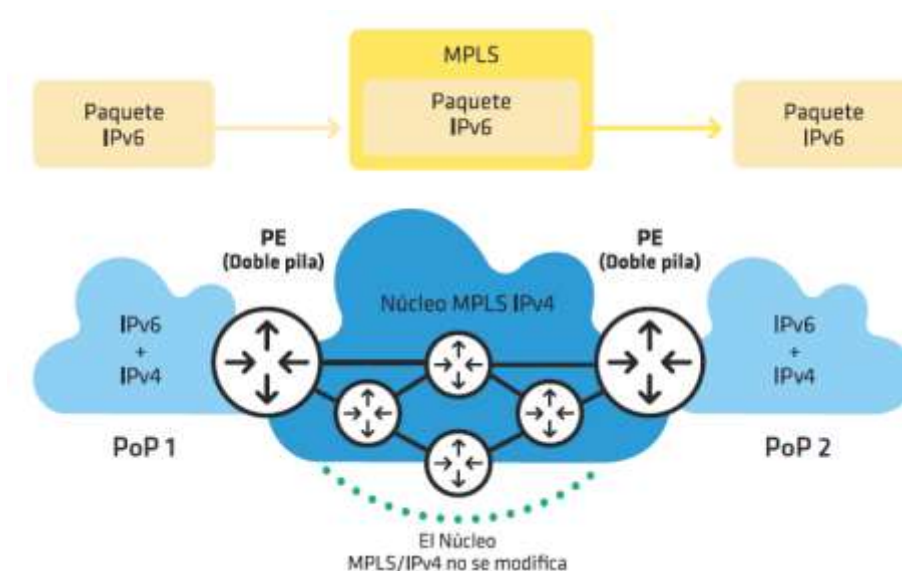


Figura 3. Técnica 6PE y 6VPE. Fuente: Ipv6 para operadores de red. 2014.

4.1.2.5.8. 464XLAT

La técnica 464XLAT está documentada en la RFC 6877 y, a los fines prácticos, se puede considerar como un complemento del mecanismo NAT64 descrito en el punto anterior. Más específicamente, esta técnica consiste en una combinación del uso de traducción stateful entre IPv6 e IPv4 en la red del proveedor, descrita en la RFC 6146 y en la sección anterior, con otro tipo de traducción entre IPv6 e IPv4, stateless, denominada SIIT (Stateless IP/ICMP Translation Algorithm), descrita en la RFC 6145.

Lo que motivó su desarrollo fue justamente la limitación que se presenta con NAT64 y DNS64 en relación con las aplicaciones que no soportan IPv6. Agregando una segunda traducción es posible brindar a los usuarios una dirección IPv4 privada, de forma que funcionen incluso las aplicaciones que no soportan IPv6.

Nótese que para implementar esta tecnología en una red que ya usa NAT64 basta agregar la traducción en la red o en el dispositivo del usuario, sin necesidad de realizar modificaciones en la red del proveedor.

En esta técnica, la traducción stateful en el proveedor recibe el nombre de PLAT (Provider-side Translator). En la red del usuario, la traducción stateless se conoce como CLAT (Customer-side Translator). (Alejandro Acosta, 2014)

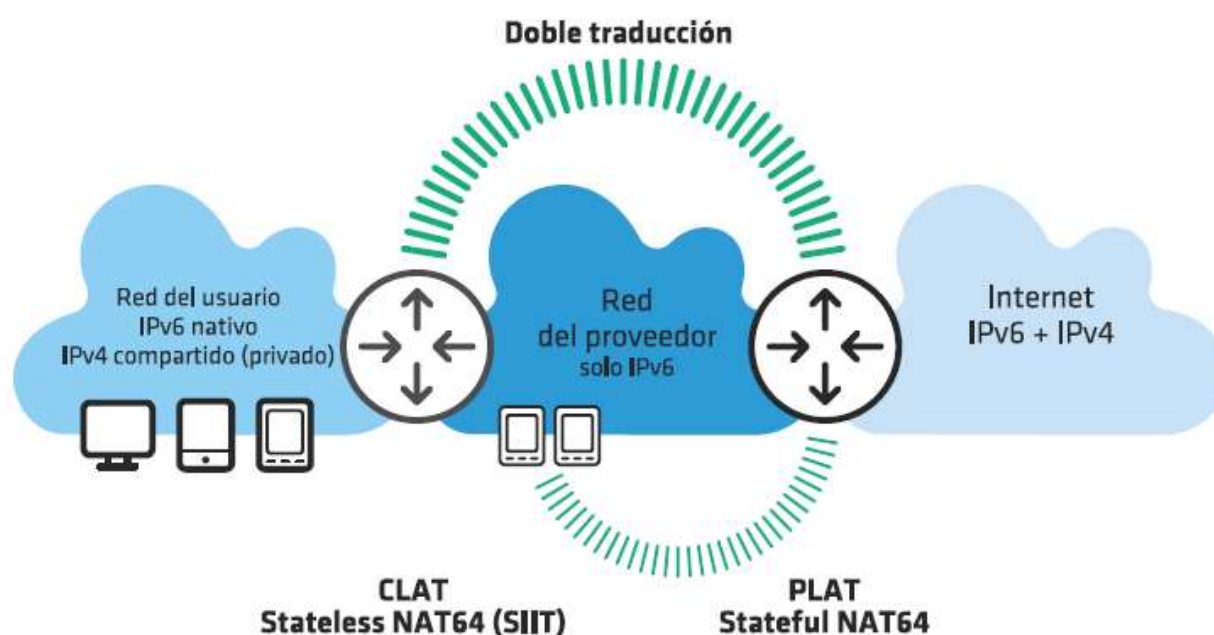


Figura 4. Mecanismo 464XLAT. Fuente: Ipv6 para operadores de red. 2014.

4.1.2.5.9. Carrier Grade NAT (CGN or CGNAT) o Large Scale NAT (LSN).

Es una manera de solucionar el problema de escasez de direcciones IPv4. El NAT tradicional es un mecanismo que se encuentra en la casa de cliente y a diferencia de este, CGNAT utiliza dispositivos en la red Core del proveedor de Servicios para cambiar el direccionamiento privado a público. Al estar ubicado en los dispositivos de la red Core del Proveedor de servicios permite compartir pocas direcciones públicas para una gran cantidad de usuarios incrementando

considerablemente la capacidad para proveer acceso a Internet con las pocas IPv4 disponibles. Este NAT masivo o de gran escala es un cambio en el lugar tradicional donde se hace y se configura la función de NAT desde el equipo de casa del cliente, hacia la red del proveedor de acceso a Internet.

Un escenario de utilización del NAT masivo se puede describir como NAT444,3 porque las conexiones de algunos clientes a los servidores públicos pueden llegar a pasar por tres dominios de direccionamiento IPv4 diferentes: el propio de la red privada del usuario, la red privada del operador e Internet.

Otro escenario de NAT masivo es Dual-Stack Lite, donde la red del operador utiliza IPv6 y por tanto sólo se necesitan dos dominios de direccionamiento IPv4. (Jiang S., Guo D., Carpenter B., 2011)

Utilizar Carrier Grade NAT (CGN) no se considera naturalmente como un mecanismo de transición, ya que lo único que hace es seguir prolongando la vida útil de IPv4.

4.1.2.6. Peticiones de comentarios, RFC (request for comments)

En el mundo de las telecomunicaciones existen las RFC los cuales son documentos que contienen propuestas del uso de las nuevas tecnologías como lo son los protocolos y tecnologías de redes. Muchas de estas son estándares mundiales. Estas pueden ser escritas por cualquier persona, pero deben ser abaladas y revisadas por la Internet Engineering Task Force ‘IETF’.

4.1.2.6.1. Documentos RFC sobre IPV6

RFC 4291: principios básicos del direccionamiento IPv6.

RFC 3306, RFC 3956, RFC 4489: direcciones multicast.

RFC 4038: direccionamientos compatibles IPv4.

RFC 5214 (y 4214 para la antigua versión): direcciones ISATAP.

RFC 4380, RFC 5991 y RFC 6081: direcciones Teredo.

RFC 0791 y 1349: campos de los paquetes IPv6.

RFC 4862: Stateless Autoconfiguration.

RFC 4861: Neighbor Discovery.

RFC 3756: amenazas ligadas a la autoconfiguración.

RFC 3315: DHCPv6.

RFC 4443: ICMPv6.

RFC 4884: extensiones ICMP.

RFC 3596: DNS con IPv6.

RFC 6106: opciones ligadas al DNS y a los avisos de los routers.

RFC 2401 y RFC 4301: protocolo IPsec y descripción de las SA y de las bases de datos asociadas (SAD, SPD, PAD).

RFC 4306, 2407, 2408, 2409: IKE v1 y v2.

RFC 4303 y RFC 2406: ESP.

RFC 4302 y RFC 2402: AH.

RFC 4941: direcciones temporales.

RFC 3756: amenazas ligadas al protocolo de descubrimiento de vecinos.

RFC 3971 y 3972: securización de los vecinos y de los routers.

RFC 2205, 2750, 3936, 4495, 5946, 6437: RSVP.

RFC 6437 Flow Label.

RFC 2474, 2597 y 2598: Diffserv.

RFC 6275: principales funciones y especificaciones de Mobile IPv6.

RFC 4225: securización del modo de enrutamiento optimizado.

RFC 5568: Fast Handover en Mobile IPv6.

RFC 4260: Fast Handover en Mobile IPv6 sobre redes 802.11n.

RFC 3963: protocolo NEMO (Network Mobility).

4.1.2.7. DHCP en IPV6.

El mecanismo de configuración automática de direcciones sigue un modelo de cliente-servidor y se basa en el uso de DHCPv6 (Dynamic Host Configuration Protocol para IPv6) como ocurre con DHCP para IPv4, aunque hay grandes diferencias en el código: DHCP en IPv4 no es más que una extensión del protocolo BOOTP, por lo que tiene una funcionalidad limitada. En cambio, el protocolo DHCPv6 permite establecer los parámetros de configuración de un servidor DHCP para un cliente IPv6.

El cliente IPv6 representa un dispositivo que busca tener conectividad global IPv6 y solicita la información de configuración necesaria para poder establecer esta conectividad. El servidor DHCP constituye un punto central que reagrupa los parámetros de configuración. No necesariamente se ubica en el mismo enlace que el cliente, en cuyo caso, la información DHCP puede intercambiarse a través de un relevo. El servidor puede contener información de configuración para dispositivos ubicados en distintos enlaces. El cliente DHCP debe establecer una conexión directa ya sea con el relevo o con el propio servidor DHCP.

Esta es la gran diferencia entre el DHCP para IPv4 y para IPv6, cuando en IPv4 teníamos un único método de configuración, en IPv6 tenemos dos métodos:

Stateful – Así como en IPv4 el servidor para IPv6 guarda todas las configuraciones que va entregar a los clientes, y guarda un histórico de que equipo recibió cada una de las direcciones.

Stateless – Este es un método completamente nuevo, que nace de la propia concepción del IPv6, acá lo que tenemos de distinto del anterior es que el servidor no va tener un histórico de las direcciones asignadas, y apenas va proveer parámetros adicionales que son comunes a todos los hosts. Esta forma fue pensada para el IPv6 como una manera de obtención rápida de nuevas direcciones, acá el direccionamiento va a utilizar la dirección MAC del equipo para armar una nueva dirección IPv6. Existen dos maneras de trabajar la configuración Stateless: SLAAC (Stateless Address Auto Configuration) Y Stateless. (Cisco, 2012)

4.1.2.8. Agentes de la cadena de valor de Internet

Para que el mundo de Internet funcione, es necesario que en el mundo real existan estructuras físicas de telecomunicaciones y fuerzas capaces de mantenerlas en marcha. Estas personas conforman un ecosistema de agentes con distintos roles, esquemas de contribución y distintos intereses que al fin y al cabo confluyen en el punto donde se da vida a Internet.

Diversos autores se distinguen en la cadena de valor de Internet en varios sujetos, los cuales podrían agruparse de la siguiente forma en Los operadores de redes de telecomunicaciones o ISP (Internet Service Providers), estos sería simplemente la empresa que brinda el servicio de internet al consumidor, la interconexión de estas redes de telecomunicaciones es lo que se conoce como Interred o Internet; Los Proveedores de Contenido o ICP (Internet Content Providers) y los proveedores de aplicaciones o IAP (Internet Application Providers), estos actores también son conocidos como prestadores de servicios Over-The-Top (OTT) como por ejemplo, YouTube, Spotify, Facebook y muchas empresas más, son aquellas empresas que brindan sus servicios y contenido a través del servicio y las redes de Internet construidas por los ISPs. (Salgado, 2015)

4.1.2.9. Internet de las cosas (IoT)

Por lo general, el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana.

La reciente confluencia de diferentes tendencias del mercado tecnológico está permitiendo que la Internet de las Cosas esté cada vez más cerca de ser una realidad generalizada. Estas tendencias incluyen la conectividad omnipresente, la adopción generalizada de redes basadas en el protocolo IP, la economía en la capacidad de cómputo, la miniaturización, los avances en el análisis de datos y el surgimiento de la computación en la nube.

Los cuatro de los modelos de conectividad descritos por la Junta de Arquitectura de Internet incluyen: Device-to-Device (dispositivo a dispositivo), Device-to-Cloud (dispositivo a la nube), Device-to-Gateway (dispositivo a puerta de enlace) y Back-End Data-Sharing (intercambio de datos a través del back-end)

Aunque difieren en cuanto a las cifras exactas, la mayoría de los observadores coincide en que, de aquí al año 2025, se conectarán a Internet miles de millones de nuevos dispositivos —desde sensores industriales hasta electrodomésticos y vehículos—. La Internet de las Cosas continúa creciendo y los dispositivos que requieren conectividad a Internet verdaderamente de extremo a extremo ya no podrán confiar en IPv4, el protocolo que hoy en día utiliza la mayor parte de los servicios de Internet. Estos dispositivos necesitarán una nueva tecnología: IPv6. (Karen Rose, 2015)

4.1.2.10. Smart City

Entendemos por Smart City una ciudad en la que la tecnología proporciona servicios tradicionales y resuelve cuestiones urbanas, por ejemplo, facilitando la movilidad, mejorando los servicios de la ciudad, convirtiéndola en un espacio más sostenible o dando voz a los ciudadanos.

Entre los objetivos de una ciudad inteligente se encuentran: Mejorar la eficiencia y sostenibilidad de la ciudad, Modernizar sus políticas, Fomentar la calidad social y económica, Maximizar la inclusión social, Reducir los residuos y molestias. Para el cumplimiento de todas estas metas, las Smart Cities utilizan la tecnología.

Las redes IPV6 son el componente clave que permite tener una escalabilidad casi ilimitada requerida para el desarrollo de una Smart City a cifras de dispositivos conectados que en algunos casos llegaría hasta el número de 50 Billones en 2025 como estimaban algunos estudiosos del tema. (Gosling, 2016)

4.1.2.11. Indicadores clave de avance del despliegue IPv6 (KPI)

4.1.2.11.1. Indicador Clave de Avance para IPv6 de LACNIC (LACNIC/CAF ICAv6)

Se desarrollo por parte de Teleconsult, LACNIC y CAF este Indicador Clave de Avance hacia IPv6 para poder reflejar de una mejor forma la ponderación de la situación actual en cada país. Esto a pesar del carácter desconcentrado de la Internet que no permite obtener una métrica única altamente correlacionada con el despliegue, este trata de incluir las diferentes métricas que se desarrollaron para cuantifican el despliegue, pero en cada una de las etapas de la cadena de valor. El indicador ICAv6 está definido por la siguiente formula:

$$LACNIC/CAF ICAv6 \% = 0,3 * (0,1 * PACTO + 0,9 * ASTRAN) + 0,7 * \sqrt{CONT * USUARIOS}$$

Estos indicadores parciales le dan peso a la planificación y a las acciones iniciales en el proceso de despliegue de IPv6. (De León, 2015)

4.1.2.11.2. PACTO

Es el porcentaje de prefijos IPv6 que han sido atribuidos o asignados y que se observan con tráfico, con respecto al número total de prefijos atribuidos en la región. Es un indicador de que en el país no solamente se han solicitado y atribuido prefijos IPv6, sino que también algunos de éstos ya tienen tráfico observable. LACNIC le otorga poco a este indicador considerando que es dependiente de la eficiencia con que se haya trabajado la solicitud de prefijos: se puede haber pedido mucho espacio IPv6 y usar poco, pero al mismo tiempo se puede usar lo mismo y haber pedido menos. Si bien en ambos casos el uso es el mismo en cuanto a despliegue, en el primer caso el indicador es menor. (De León, 2015)

4.1.2.11.3. ASTRAN

Sistema Autónomo (AS) con tránsito observado. El sistema autónomo en si mismo no es IPv4 o IPv6, está relacionado y refleja a la entidad como tal. En el indicador se trata de diferencias los AS que proveen tránsito IPv4 y que tienen prefijo IPv6, aparte de los AS que proveen tránsito IPv6, ya que los primeros muestran un camino en la puesta en marcha futura de tránsito IPv6, se usa el promedio siguiente como indicador de tránsito:

$$ASTRAN = 0,5 * (\% AS \text{ Tránsito IPv6} + \% AS \text{ Tránsito IPv4 con prefijo IPv6})$$

Siendo: % AS tránsito IPv6 = porcentaje ponderado de las cantidades de AS que son tránsito en IPv6 respecto de la cantidad de AS que son tránsito en IPv4, y % AS Tránsito IPv4 con prefijo

IPv6 = porcentaje ponderado de AS de tránsito en IPv4 que tiene prefijo IPv6, respecto de la cantidad de AS que son tránsito IPv4 (DE LEON, 2015).

4.1.2.11.4. CONT

Para el indicador de contenido se usa la suma del porcentaje ponderado de sitios accesibles en IPv6 más el porcentaje ponderado de dominios a prueba en IPv6. Es un mecanismo de darle valor a aquellos que LACNIC llama “embriones IPv6”, que están iniciando el camino hacia la prestación de servicios en IPv6, y que son considerados muy útiles en el desarrollo de la región. (De León, 2015)

4.1.2.11.5. USUARIOS

El monitoreo del número de usuarios es complejo y requiere una gran cantidad de datos proveniente de diferentes fuentes que a su vez ya han realizado un análisis previo de sus propios datos.

Para este indicador se usó el promedio del porcentaje de usuarios potencialmente en condiciones de acceder en IPv6, estos valores se toman de entidades generadoras de contenido como Google o de entidades como APNIC. Estas dos fuentes por ejemplo usan metodologías similares, pero sobre universos no coincidentes. (Bournez, 2012)

4.2. MARCO LEGAL

El presente trabajo gira en torno a qué tan desarrollada esta la implementación y el despliegue del protocolo IPV6 en Colombia, a pesar de que en la región no ha sido mucho lo que se ha avanzado, cada gobierno es autónomo de definir cómo y cuándo implementarlo.

Por lo tanto, deben tenerse en cuenta ciertas directrices que el gobierno por medio del ministerio de Tecnologías de la Información y las Comunicaciones de Colombia establece.

4.2.1. Ministerio de Tecnologías de la Información y Comunicación.

Es el ente gubernamental formalizado de esta forma por medio de la ley 1341 del 2009, que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías y las comunicaciones. Dentro de sus funciones principales es velar por el ordenamiento general, la libre competencia, la protección al usuario, la cobertura, la calidad del servicio, la promoción de la inversión en el sector, el desarrollo de nuevas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, la vigilancia y facilitar el libre acceso de los habitantes del país a la información. (MINTIC, 2009)

4.2.2. Ley 1341 de 2009 Artículo 19. Creación, Naturaleza y Objeto de la comisión de regulación de comunicaciones.

En el artículo 19 en la ley 1341 en el gobierno establece a la Comisión de Regulación de Comunicaciones (CRC), Unidad Administrativa Especial, con independencia administrativa, técnica y patrimonial, sin personería jurídica adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones, y será el órgano encargado de promover la competencia, evitar el abuso de posición dominante y regular los mercados de las redes y los servicios de comunicaciones; con el fin que la prestación de los servicios sea económicamente eficiente, y refleje altos niveles de calidad.

4.2.3. Resolución 2710 de 2017 lineamientos de implementación del protocolo IPv6 en Colombia.

El MINTIC referenciados en el anuncio de dado por LACNIC en el 2014 (LACNIC, 2019), tomo la decisión de adoptar dentro de sus políticas para el manejo del direccionamiento el

protocolo IPV6, para evitar un estancamiento en el desarrollo de las redes en el país con respecto a los demás países.

En esta resolución se establecen las medidas para adoptar el protocolo IPV6 para los proveedores de redes y servicios de telecomunicaciones. También establece que estos proveedores deben tener preparadas sus conexiones troncales de acceso a internet, que permitan enrutar los prefijos IPV6 y estén permanentemente operativos.

Por otro lado, en esta norma, se establece un plazo de adopción para las entidades estatales de carácter nacional para el 31 de diciembre del 2019, y las entidades de carácter territorial a más tardar el 31 de diciembre 2020.

La forma en que el MINIC establece esta transición del protocolo IPV4 al IPV6 deberá soportar los servicios de internet en IPV6 nativo en coexistencia con IPV4, esto con el fin de garantizar la operación de la infraestructura de TI de las entidades estatales que aún lo requiera.

5. PROPUESTA DE SOLUCIÓN

Con la conciencia que existe una demanda creciente de direcciones IP por la implementación de tecnologías como IoT o Smart City, y sabiendo que solo con la implementación de redes IPV6 se podría llegar a suplir esta necesidad, se requiere obtener la mayor cantidad de información posible que permita conocer la situación actual de la implementación de IPV6 en las redes de los proveedores de servicios de Colombia.

Al tener que el objetivo de este trabajo es realizar un estudio básico sobre los avances de la implementación y el despliegue del protocolo IPV6 en Colombia, y de acuerdo con la documentación consultada esto abarca al menos 3 aspectos. El primero es determinar qué tan listas están las redes de los proveedores de servicios para funcionar con IPV6, para esto lo más

conveniente es establecer contacto con los principales ISP del país, que podría corresponder a aquellos ISP agrupados en la CCIT (Cámara Colombiana de Informática y Telecomunicaciones) y que podrían coincidir con los que se encuentran interconectados a través del NAP Colombia.

La información que se requiere recopilar de estas empresas consiste básicamente en conocer si los equipos en sus redes de Core, y los equipos con los que prestan los servicios a sus clientes están en capacidad de manejar el protocolo IPv6, o si tienen operando algunas de las tecnologías de transición de IPv4 a IPv6 para proveer conectividad entre servicios IPv4 e IPv6 en las redes de cliente. También en caso de no tener IPv6 operando aún, si tienen algún plan de implementación de este, con algún estimado para esta implementación.

Un aspecto de utilidad para el objetivo del estudio sería conocer las razones por las cuales no se ha requerido la implementación de IPv6 en sus redes, como es el hecho que tengan mecanismos de mitigación al agotamiento de IPv4 como CGNAT u otros que han permitido el crecimiento sin obstáculos, o el hecho que se hayan desplegados tecnologías de última generación en IPv4 sin contemplar su operación en IPv6.

El segundo aspecto para considerar dentro del estudio es la presentación de estadísticas de uso de IPv6 en el país. Y respecto a estas estadísticas el primer paso entonces sería definir los KPI que medirían dichas estadísticas y también la forma más adecuada de presentación de estas. Estos KPI deben definirse de tal forma que puedan dar una idea lo más clara posible del avance del país en el despliegue del protocolo IPv6, y se consideraría la posibilidad de definir algunos KPI primarios y a partir de estos calcular alguno que consolide o concluya el objetivo buscado. También dentro del proceso de investigación se considera adoptar el modelo de KPI usados por otras entidades, y esto estaría relacionado con las fuentes de información ya que el proceso de

medición o toma de estas estadísticas se realizaría en puntos claves donde se refleja el uso del IPv6, puntos que tendrían unas características muy complejas difíciles de reproducir.

Debido a la complejidad de reproducir o acceder a los puntos donde se tomaría la información lo más viable será recaudar esta información de entidades propietarias de la infraestructura donde se encuentran ubicados estos puntos clave, entidades como Google, que siendo un generador de contenido podría indicar que tanto tráfico o requerimientos le llegan de prefijos IPv6 registrados en Colombia; NAP Colombia que podría registrar la cantidad de tráfico IPv6 o prefijos anunciados entre sus miembros o ISP interconectados a través de él. Y LACNIC como administrador de registro de direcciones en Latinoamérica que podría indicar el número de prefijos asignados a entidades dentro del país.

Adicionalmente dentro de este segundo aspecto sería deseable tener algún estado de avance de implementación de IPv6 en las diferentes empresas o entidades, y de acuerdo con lo planteado por MINTIC en la resolución 2710 de 2017 respecto a las políticas de adopción de IPv6 en el país, sería el MINTIC mismo la fuente más confiable para recaudar entonces todo lo relacionado con los KPI que se definan para presentar dicha estadística.

El tercer aspecto que sería deseable medir, es la disponibilidad de servicios sobre IPv6 en Internet como una muestra clara de que tan preparado estaría el país para la transición, es decir conocer que servicios como sitios web, servicios transaccionales, video, herramientas colaborativas, atención de clientes, trámites, compras, etc. Para este análisis que corresponde al punto de vista del usuario final si es factible realizar una implementación propia sobre la cual se realizan las pruebas. La propuesta es conseguir el apoyo de un ISP que provea un canal de acceso a internet IPv6, con su respectivo direccionamiento público; a dicho dispositivo se conectaría un computador de última generación que permita verificar el acceso a los sitios y probar el correcto

funcionamiento de los servicios que previamente se hayan seleccionado. Para la selección de los sitios y los servicios se requiere realizar un estudio previo que permita definir los servicios más utilizados por la población en Colombia.

En el estudio realizado para la elaboración del marco teórico no se encontró un antecedente similar, así que se propone usar otro tipo de estudios para definir los criterios de manera indirecta, por ejemplo buscar estadísticas de los bancos más grandes y del top de los mismos seleccionar algunos para probar el correcto funcionamiento de los servicios en IPv6; así mismo de un listado de las empresas más grandes en Colombia seleccionar 100 basados en el estudio realizado en el 2019 por la revista dinero en dónde se encuentran las 5000 empresas más grandes de Colombia subdivididas en 10 sectores principales y de los cuales se tomara un numero especifico según su area: Agropecuario (5), comercio (10), construcción (10), hidrocarburos y servicios petroleros (10), industria (10), medios (10), minería (5), servicios (10), telecomunicaciones y tecnologías de la información (20) y por ultimo transporte (10). Esta muestra servirá para determinar qué servicios podrían tener disponibilidad a nivel de IPv6. (Dinero, 2019)

Esta implementación requiere un diseño previo de la topología de acuerdo con los recursos que provea el ISP como direccionamiento y DNS. Adicionalmente se requiere definir la metodología con la que se van a presentar los datos obtenidos.

5.1.Planeación Metodológica.

Para el desarrollo apropiado de la investigación se propone llevar a cabo la siguiente metodología dividida en 6 grandes fases, cada una de las cuales está compuesta de actividades y tareas para ser realizadas por el personal que abordará el estudio, esto con el fin de cubrir todos los aspectos que puedan influir en obtener un resultado certero.

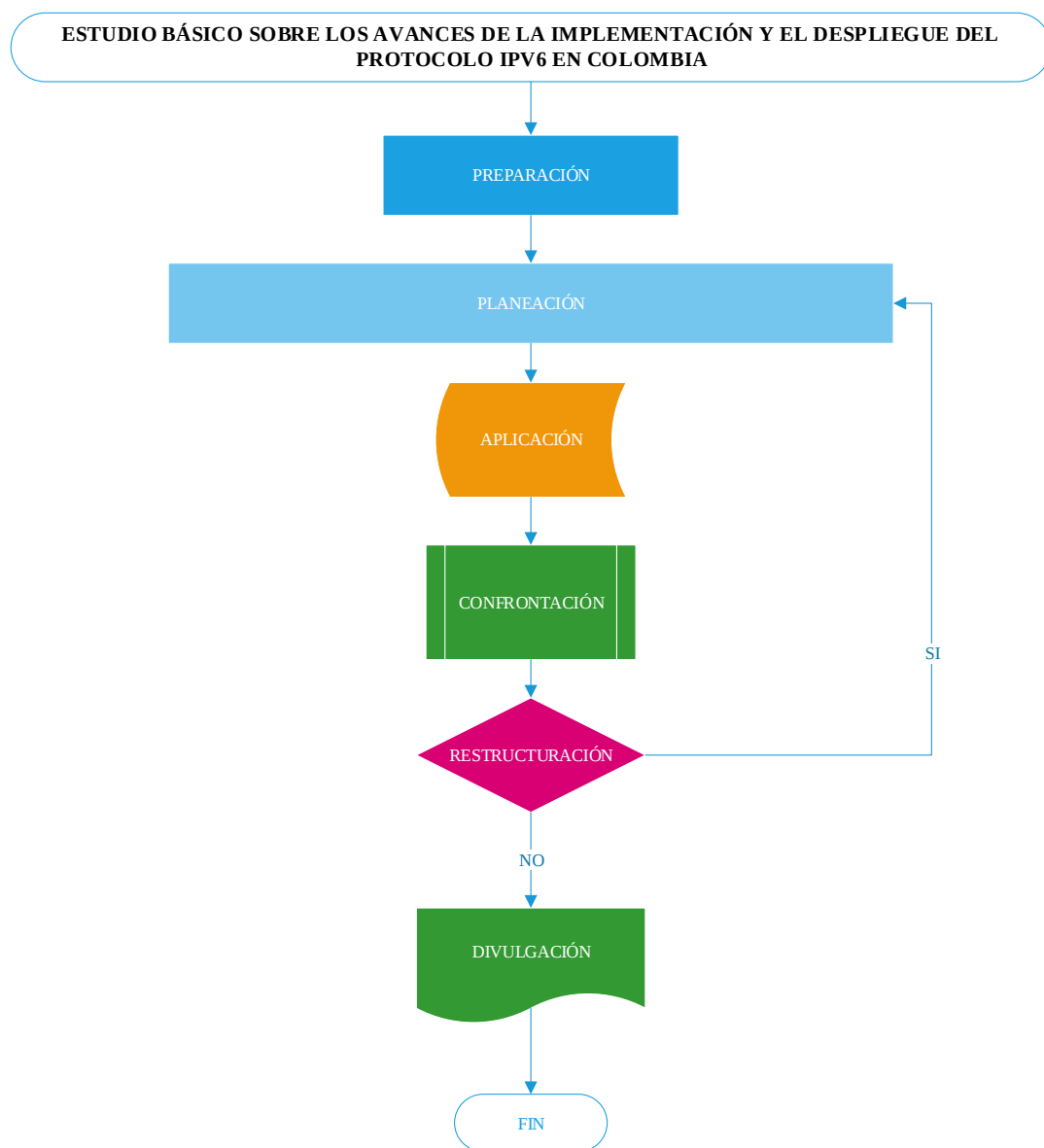


Figura 5. Diagrama Metodología. Fuente: Los autores.

1. Fase de Preparación:

- Revisión documental y de bases de datos especializadas.
- Recopilación de antecedentes nivel LATAM- Resto del Mundo de estudios e implementaciones IPV6.
- Identificación de aspectos legales para la implementación de IPV6 en Colombia.
- Selección y documentación de mecanismos de transición IPV6 usados nivel LATAM.
- Análisis, clasificación y caracterización de la información.

2. Fase de Planeación:

-
- Relación de roles en las etapas de ejecución y recolección de la información del estudio, e inclusión de profesional en estadística y análisis de datos.
 - Definición de los hitos y generación de un cronograma preliminar del estudio.
 - Adquisición y destinación de recursos para actividades de campo y capacitación del personal.
 - De acuerdo con lo nombrado por LACNIC, Google y CISCO definición de los criterios de selección y KPIs.
 - Verificación de las unidades de análisis (100 empresas colombianas más influyentes con presencia en el mundo de las TICs, servicios web preferidos por los internautas, profesionales de TI).
 - Del listado anterior de empresas y empresas NAP COL tomar una premuestra para aplicar estudio.
 - Diseño de las herramientas de recolección de acuerdo los temas relevantes mostrados en los antecedentes.
 - Diseño de topología de laboratorio para la comprobación de datos.
 - Selección de herramientas para el análisis de datos.

3. Fase de Aplicación:

-
- Administración de aspectos legales, protección de la información y uso de datos personales.
 - Uso de instrumentos de recolección de datos.
 - Circulación de los instrumentos de recolección y una promoción para su adecuado diligenciamiento.
 - Aplicación de instrumentos de recolección al público objetivo.
 - Implementación de topología de laboratorio para la comprobación de datos.
 - Tabulación de la información recolectada.
 - Procesamiento y análisis de la información.

4. Fase de confrontación:

-
- Visualización y análisis de resultados.
 - Verificación de elementos no abordados.
 - Observación de instrumentos y herramientas de recolección de datos.
 - Ratificación de herramientas informáticas utilizadas.
 - Revisión de topología de laboratorio para la comprobación de datos.

5. Fase de reestructuración:

-
- Inclusión de elementos no abordados.
 - Uso o implementación de nuevas herramientas informáticas.
 - Rediseño de topología de laboratorio para la comprobación de datos.
 - Revisión final de herramientas y de aspectos generales.

6. Fase de divulgación:

-
- Aplicación de elementos reestructurados.
 - Inclusión y análisis de nuevos datos.
 - Presentación de resultados finales.
 - Análisis final, criterios de implementación y conclusiones del estudio.

5.2.Desarrollo Tecnológico

El Aspecto tecnológico se hace evidente en el desarrollo del proyecto para el segundo y tercer aspecto mencionado en la descripción general de la propuesta. En el segundo punto se ve reflejado en la tecnología usada por proveedores de contenido para medir el número de peticiones que les llegan a sus servidores o las ubicaciones implementadas sobre infraestructura de la Red de Distribución de Contenidos ‘CDN’, e identificar y clasificar el origen de estos, por ejemplo Google (<https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption>) indica que su metodología consiste esta basada en requerimientos que hacen a los clientes web para que envíen requerimientos HTTP a un servidor que trabaja solamente en Ipv4 o uno que es “dual Stack” y luego comparan los resultados. Para esto usan dos “hostnames” llamados “ExpHostNames” que son `dualstack.ipv6-exp.l.google.com` y otro llamado `ipv4.ipv6-exp.l.google.com`. Estos “hostname” funcionan con AAAA y A DNS RRs el primero y ADNS RR solamente el segundo. Para Recibir entonces estas consultas se implementan los servidores en diferentes centros de datos alrededor de mundo, de tal forma que los requerimientos desde los clientes a esos centros de datos sean analizados localmente con ayuda de los DNS de Google. La figura 3 detalla el proceso.

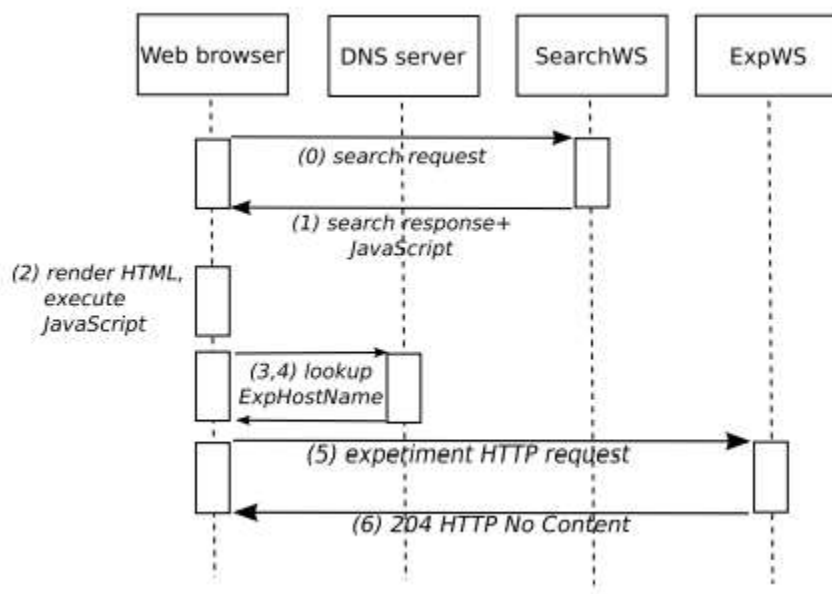


Figura 6: Flujo de medición de los requerimientos. Fuente: Colitti 2009.

Por el análisis de las estadísticas obtenidas de los requerimientos que llega, una vez se realiza una exhaustiva depuración se obtienen estadísticas de clientes web que pueden o no conectarse a los servidores “Dual Stack”, así como la latencia de dichas conexiones. También se mide la Tasa de Conectividad de IPv6 con base en el número de requerimientos exitosos y que muestra el número de clientes que están operando en IPv6. Otro parámetro derivado del análisis anterior es la Conectividad Sobre el Tiempo, que evidencia la disponibilidad en el tiempo de IPv6 para el usuario final. Esta también la Conectividad por Tipo que busca distinguir si la conexión usada es “6to4”, Teredo o ISATAP. Y el que sería el más relevante para el estudio es Conectividad por país, para este se geolocaliza las “ExpClientIP” usando diferentes bases de geolocalización. Otros indicadores adicionales serían Conectividad por Sistema Operativo y Conectividad por Sistema Autónomo obtenido de los diferentes routers de Google.

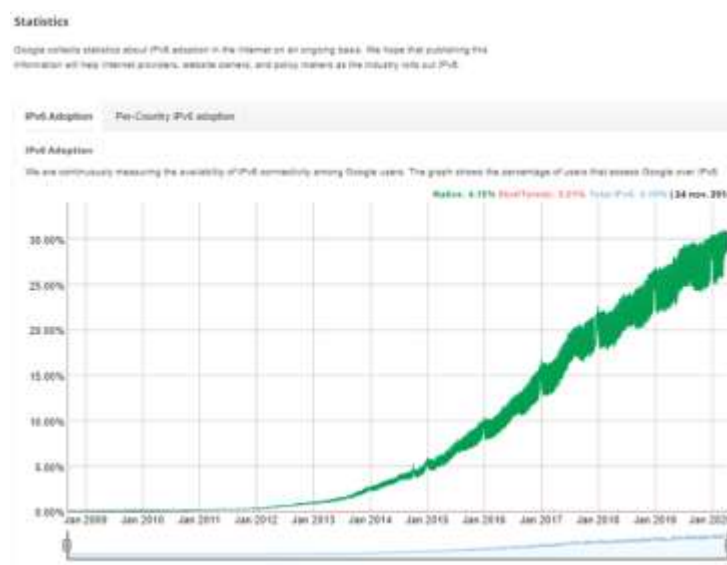


Figura 7: Estadísticas de adopción de IPv6 generadas por Google. Fuente: GOOGLE 2020.

Otra fuente similar son las estadísticas ofrecidas por Cisco (<http://6lab.cisco.com/stats>). Cisco explica que su metodología inicial es tomar la información que administran los RIR (Registro Regional de Internet), a través de la herramienta whois, e identificando así los prefijos asignados; luego estos prefijos son cruzados con las bases de datos de servicios de lookingglass o incluso con tablas de BGP de proveedores de servicios “Tier One con el fin de obtener una gráfica que les muestra finalmente el número de prefijos asignados, enrutables y “vivos”.

Adicionalmente dentro del cálculo de los sitios “vivos”, Cisco usa los arreglos de datos que para APNIC creo Geoff Houston que es uno de los precursores de Internet en Australia. Uno de estos, específicamente arroja datos a nivel de http que permite discernir capacidades “DualStack”, Ipv4 o IPv6 en los orígenes.

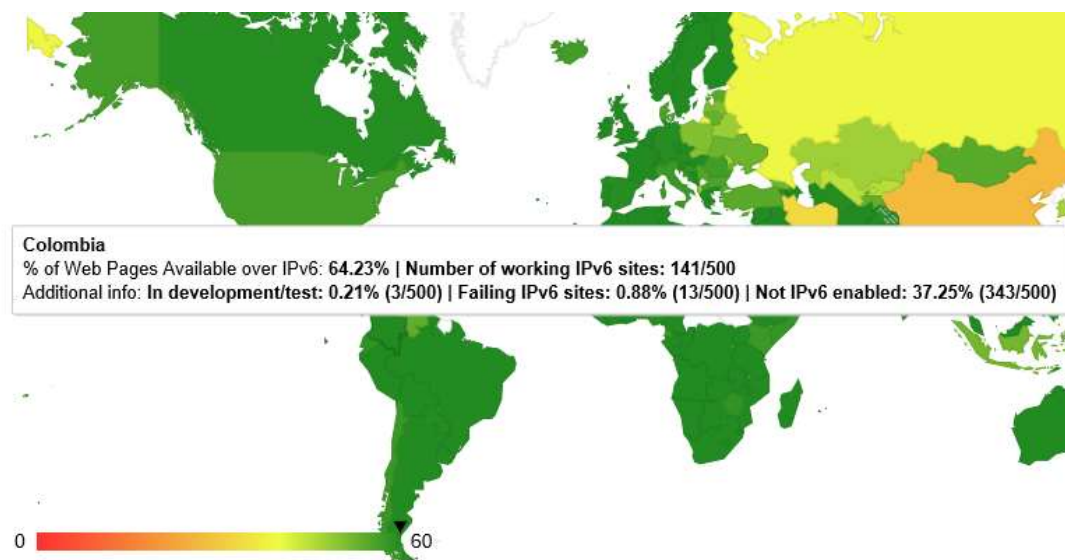


Figura 8: Estadísticas sitios web IPv6 suministradas por 6LAB CISCO. Fuente: CISCO 2020.

Algunos otros de los KPI que nos entrega Cisco son Sistemas Autónomos de Transito (AS), los cuales se sacarían de los patrones reflejados en los prefijos de las tablas de BGP. Para determinarlo el algoritmo asume que todos los AS del “AS Path” en el prefijo son de tránsito, pero luego se elimina el origen y destino de cada ruta, se procesa la tabla y se hayan los más relevantes por el número de veces que aparecen en los prefijos de la tabla. Identificar estos AS de transito es importante para definir el avance de despliegue de IPV6.



Figura 9: Representación de AS PATH del prefijo en la tabla BGP. Fuente: KACZMAREK, 2011.

Otros parámetros importantes proporcionados por Cisco están relacionado con los sitios Web, ya que identifican el número de sitios web que son anunciados a través de los registros en los DNS y mucho más importante el número de estos sitios que son realmente accesibles.

Otras fuentes de información que han desarrollado completos estudios de medición y que proveen KPI similares a los mencionados son: APNIC, Comcastc, Hurricane Electric, IPDN, TNO & GNKS, Max.nl, Tore Anderson (Redpill Linpro), Mark Prior (Juniper Networks), CAIDA y RIPE NCC.

Sería importante poder explorar el uso de los datos que se pueden obtener de la Resolución reversa de los prefijos IPv6 que ha entregado LACNIC. Los servidores DNS de LACNIC son responsables por la resolución reversa de las direcciones IPs asignadas a ISPs y otras organizaciones de la región Latinoamérica y por tanto las de Colombia. Globalmente los servidores para esa función son seis y están ubicados no solo en la región de América Latina y Caribe, sino también en África, América del Norte, Asia y Europa. Estos registros de información para resolución reversa son realizado por las entidades receptoras de los bloques IPV6 a través del sistema de administración de bloques IPs de LACNIC.

Otra herramienta importante que provee LACNIC es el "Registration Data Access Protocol" (RDAP) ha sido pensado para reemplazar el WHOIS tradicional. Con el que se corrigen problemas como la internacionalización, estandarización de las respuestas, inclusión de caracteres especiales, difícil parsing, inclusión nuevos tipos de consultas podrán ser resueltos con el desarrollo de este estándar. Este servicio ha sido desarrollado por técnicos de LACNIC para dar una respuesta unificada a la comunidad de la región cuando necesita buscar la información sobre los recursos numéricos (IPv4, IPv6 y ASNs) asignados por LACNIC así como también de entidades miembros de LACNIC en nuestro WHOIS.

Respecto al tercer aspecto del estudio, la figura 4 muestra la topología de la implementación. Los equipos que se requieren son el servidor de última generación desde donde se probara la lista de sitios que se debe desarrollar con la metodología antes mencionada, adicionalmente

un conversor que entregue un puerto RJ45 al que se conecte el cable de red del servidor. Vale la pena aclarar que este puerto solo puede tener activo el protocolo IPv6, en esta prueba no estaría considerada la opción “Dual Stack” y el todo lo concerniente a IPv4 será evitado al máximo. Este conversor recibirá la fibra que permitirá la conexión al Switch de Acceso a la red del ISP. Este SW es encarga del transporte en Ethernet al puerto del PE Router de la red del proveedor servicio, la interfaz de este equipo habilitada para el ambiente de pruebas será también IPv6 solamente.

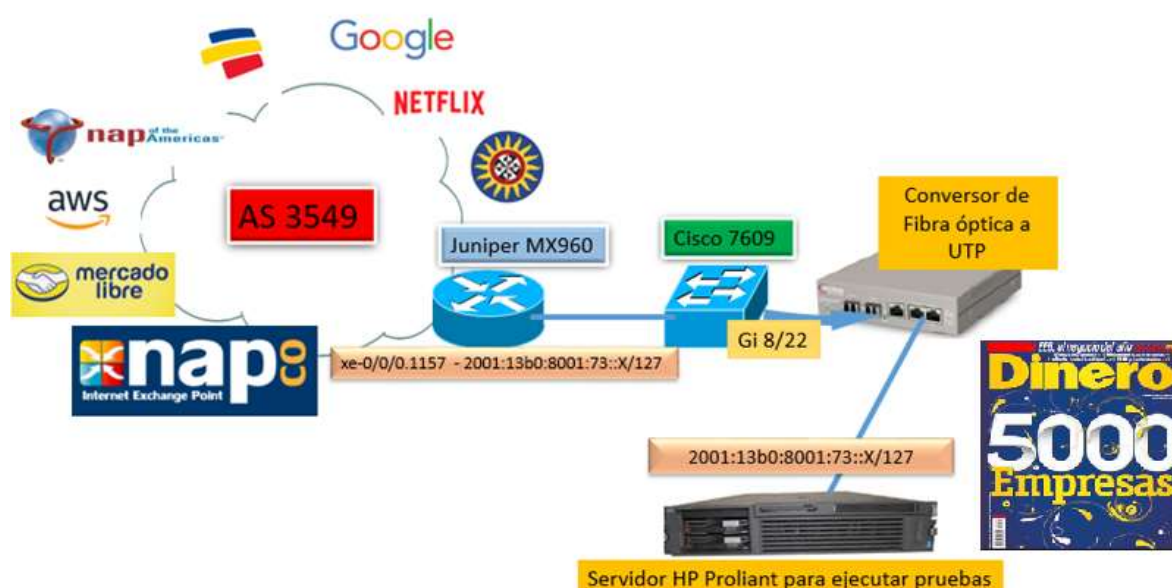


Figura 10: Ambiente de pruebas servicios IPv6 Colombia. Fuente: Los Autores.

6. CONCLUSIONES Y RECOMENDACIONES.

- Se recomienda que para iniciar este estudio se tenga como información de partida la información que se pueda obtener del NAP Colombia, esta debe ser otorgada por personal interno y confiable, debido a que es la fotografía en ese momento del estado de despliegue

IPV6 en servicios, enrutamiento y conectividad de los proveedores que brindan servicios en el país.

- Con base en los antecedentes analizados, se construye un modelo ecléctico integrando las metodologías usadas por CISCO, LACNIC y GOOGLE para la presentación de las estadísticas de IPV6. Por su lado LACNIC en 2015 tuvo en cuenta KPIs como: ICAv6, PACTO, ASTRAN, CONT y USUARIOS, además tomó de CISCO el porcentaje Conglobado de despliegue de IPv6 e Indicador Relativo de un país respecto del mundo; como resultado final generó un indicador único de avance por país. Por otro lado, CISCO se enfoca en medir esto bajo 3 ejes: Planeación, Red de Core y Usuarios; de igual forma los KPI utilizados fueron: Número de Prefijos IP por Región y por país asignados y enrutados, Sistemas Autónomos de tránsito, Contenido Web, Usuarios y Adopción de video IPv6. Adicionalmente hace una correlación de estas métricas para generar datos adicionales y la parte de usuarios al parecer la obtiene de Google y APNIC. En tercer lugar Google utilizó indicadores de tasa de conectividad en IPv6, Conectividad en el tiempo, Conectividad por tipo, Conectividad por sistema operativo, Conectividad por país, Conectividad por sistema Autónomo y Latencia de IPv4 contra Ipv6.
- Observando las tres metodologías hay criterios redundantes los cuales se deben utilizar de forma obligaría en el modelo que se construirá. Adicionalmente se ha identificado que la obtención de la mayoría de estos indicadores o estadísticas, implican implementaciones de hardware complejas y grandes capacidades de computo por lo que de ser posible se tomarán los datos ya procesados por estas fuentes para incorporarlos al estudio.
- Otro aspecto que se observa de los modelos escogidos es la obtención de indicadores concluyentes, es decir, indicadores que reflejen de manera concisa la situación del país,

requieren la construcción de un modelo matemático o estadístico que muestre todas las variables e información recopilada, por lo cual que se debe tener asesoría especializada desde el inicio del proyecto para el diseño y modelado de herramientas de análisis.

- De acuerdo con todo el análisis de KPIs observado en los esquemas escogidos, se ha definido que las fuentes para tener en cuenta serán CISCO, GOOGLE, LACNIC, APNIC, ALEXA, MINTIC y NAP Colombia. La inclusión de nuevas fuentes se podrá tener en cuenta de acuerdo con las necesidades que se vayan observando en el desarrollo del estudio.
- Basados en la información recolectada de las fuentes y los KPIs planteados se debe diseñar una encuesta de forma detallada y dirigida especialmente a los profesionales que administren y proyecten las empresas proveedoras de servicios de internet en el país.
- Inicialmente se planteó dentro del proyecto la opción de realizar un instructivo para que una Pyme pudiera evaluar en su red la compatibilidad de IPv6 o incluso definir un plan para migrarse a IPv6, sin embargo a través del desarrollo del proyecto hemos entendido que esto que en principio parecía ser básico, tiene su complejidad, ya que son varios aspectos los que se deben analizar, y no está solo el tema de transporte o conectividad involucrado, sino que los inventarios y análisis requeridos involucran sistemas operativos y diversas versiones de aplicativos, por lo que sería mejor desarrollar un proyecto independiente para esto.
- Como conclusión y de acuerdo con lo planteado anteriormente es factible realizar un estudio básico sobre los avances de la implementación y el despliegue del protocolo IPV6 en Colombia, llevando a cabo una preparación adecuada, una estricta planeación y la implementación indiscutible de los modelos elegidos y sustentados anteriormente.

7. REFERENCIAS

- D. Akilandeswari, S. Albert Rabara and T. Daisy Premila Bai . (2018). ECC-enabled Translation Mechanism for Intercommunication between IPv4 and IPv6 . *International Conference on Communication and Signal Processing*, 1005-1009.
- Ala Hamarsheh, Yazan AbdAlaziz. (2019). Transition to IPv6 Protocol, Where We Are? 1-6.
- Alejandro Acosta, S. A. (2014). *IPv6 para operadores de Red*. Buenos Aires, Arg: ISOC-Ar Asociación Civil de Argentinos en Internet (Capítulo Argentina de ISOC).
- Andrew Robinson, John Pickard and Annie Y. Patrick. (2015). Analysis of Enterprise IPv6 Readiness. *Proceedings of the IEEE SoutheastCon 2015*, 1-7.
- Bournez, O. (2012, Abril). CISCO. Retrieved from Internet IPv6 Adoption: Methodology, Measurement and Tools.:
<https://6lab.cisco.com/stats/data/Internet%20IPv6%20Adoption.pdf>
- Cisco. (2012). *IPv6 Implementation Guide, Cisco IOS Release 15.2M&T*. Retrieved from
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-dhcp.html>
- Cristian Pérez, M. R. (2012). Implementation and Evaluation of Protocols Translating. *Journal of Computer Science and Technology*, 64-70.
- D'Egidio, A. (2020). Estudio sobre mecanismos de transición IPv6 soportados por los CPE de la región. *LACNIC News*, 37.

de León Omar, Matinez Carlos, Cicileo Guillermo, Acosta Alejandro, Diaz César, Majó Ernesto,

Kaplan Laura. (2015). Despliegue de IPV6 para el desarrollo social y económico en America Latina y el Caribe. *The Internet Addresses Registry for Latin America and the Caribbean*, 116.

De León, O. (2015, Diciembre). *LACNIC*. Retrieved from Despliegue de IPv6 para el desarrollo socio económico en América Latina y el Caribe.:

<https://www.lacnic.net/innovaportal/file/3035/1/caf-lacnic-despliegue-ipv6-para-desarrollo-socio-economico-en-lac.pdf>

Dinero, R. (2019). *Especiales Dinero*. Retrieved from las-5000-empresas-mas-grandes-de-colombia: <https://especiales.dinero.com/las-5000-empresas-mas-grandes-de-colombia/index.html>

Gosling, A. (2016, Enero 27). *APNIC*. Retrieved from Smart cities love IPv6:

<https://blog.apnic.net/2016/01/27/7390/>

Guillermo Cicileo. (2012). IPv6 For All Book (ISOC Argentina). *Internet Society*, 1-145.

Internet Society. (2018). Retrieved from Is the Internet about to run out of IPv4 addresses?:

www.internetsociety.org/deploy360/ipv6/faq/#5

Izza Fatima Naqvi, Adeel Khalid Siddiqui, Awais Farooq. (2016). IPV6 ADOPTION RATE AND PERFORMANCE IN THE 5G WIRELESS INTERNETs. *2016 IEEE Region 10 Conference (TENCON)*, 3850-3858.

Jiang S., Guo D., Carpenter B. (2011, Junio). *An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition*. Retrieved from IETF: <https://tools.ietf.org/html/rfc6264>

- John L Pickard, Annie Patrick . (2015). Workshop: IPv6 Address Planning. *Proceedings of the IEEE SoutheastCon 2015*, 1-2.
- Jonghwan Hyun, Jian Li, Hwankuk Kim, Jae-Hyoung Yoo and James Won-Ki Hong. (2015). IPv4 and IPv6 Performance Comparison. *Asia-Pacific Network Operations and Management Symposium 2015. APNOMS 2015*, 145-150.
- Kaczmarek, H. (2012, Abril). *Internet IPv6 Adoption: Methodology, Measurement and Tools*. Retrieved from 6lab.cisco.com:
<https://6lab.cisco.com/stats/data/Internet%20IPv6%20Adoption.pdf>
- Karen Rose, S. E. (2015, Octubre). *Internet Society*. Retrieved from
<https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf>
- LACNIC. (2019, octubre 03). Retrieved from Fases de Agotamiento de IPv4:
<https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4>
- Lorenzo Colitti, S. H. (2010). Evaluating IPv6 Adoption in the Internet. *Google Inc*, 10.
- MINTIC. (2009). *LEY 1341 DE 2009*. Bogotá: Diario Oficial No. 47.426 de 30 de julio de 2009.
- Palet, J. (2016). *Comparativa entre mecanismos de transición IPV6*. La Habana: LACNIC.
- Qin, Z. (2017). Seamless Converging System for IPv4/IPv6 Transition. *2017 9th International Conference on Advanced Infocomm Technology*, 110-113.
- Salgado, M. J. (2015, Agosto 30). El principio de neutralidad de la red. *Revista De Derecho*, 87-118. Retrieved from <https://www.camjol.info/index.php/DERECHO/article/view/1993>

Sun, C. (2016, Mayo 19). *Computer World Magazine*. Retrieved from No IoT without IPv6:

<https://www.computerworld.com/article/3071625/no-iot-without-ipv6.html>

Wibowo, S. (2017). Measuring IPv6 Readiness on The Most Accessed Web-based Content

Provider in Indonesia . *Artículo: 2017 The International Conference on ICT for Smart Society (ICISS)* , 1-5.